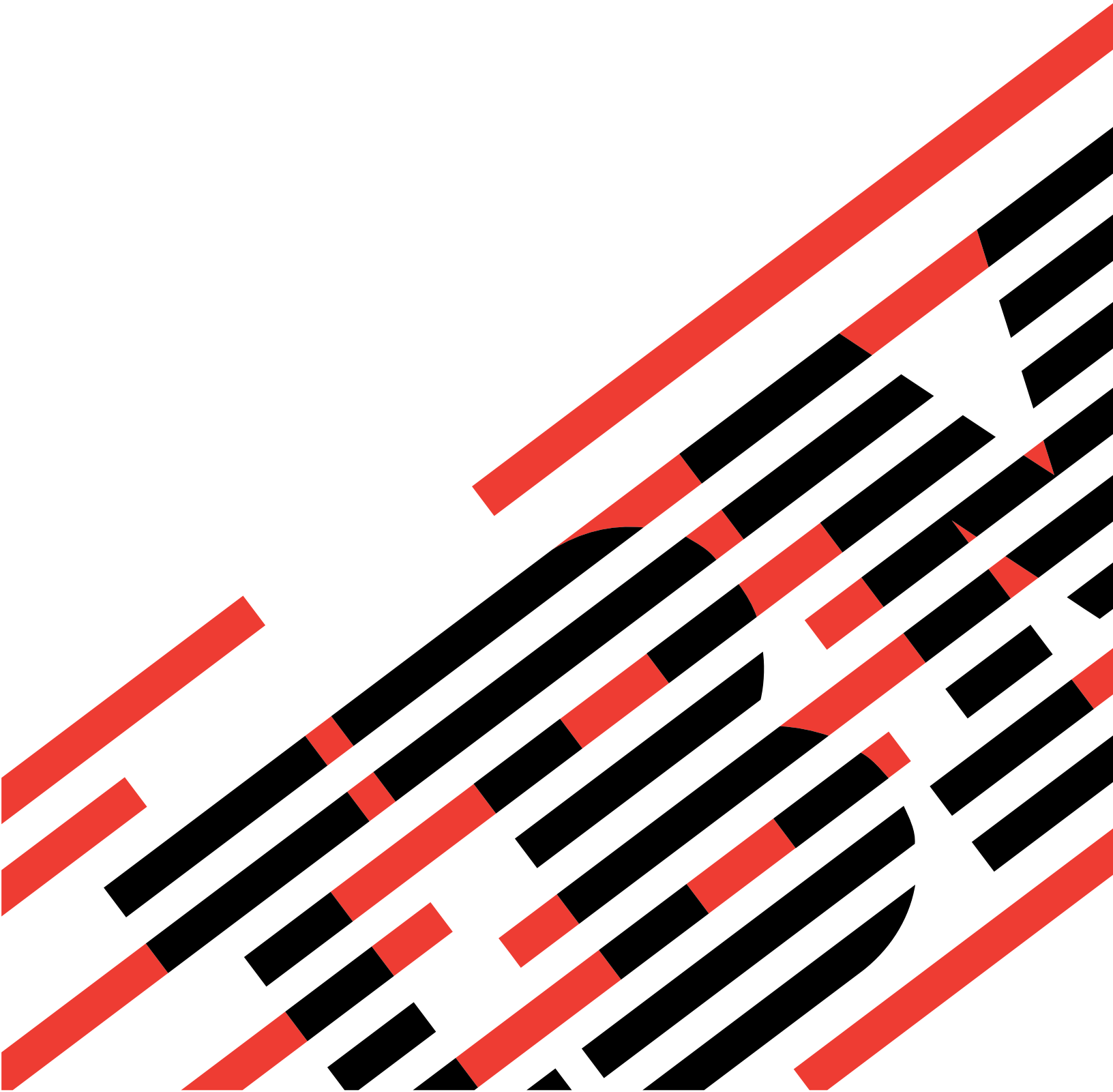
IBM

eserver

iSeries

Servicii directoare reţea (LDAP)



IBM

@server

iSeries

Servicii directoare reţea (LDAP)

Cuprins

Componentă 1. Directory Services (LDAP)

Servicii director 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.

Dacă sunteţi familiar cu Servicii director, veţi vrea să porniţi prin a citi despre ce e nou pentru această ediţie. Dacă vreţi, puteţitipări sau afişa o versiune PDF a Servicii director informaţiei.

Următoarele subiecte vă introduc Servicii director şi vă funizează informaţii pentru a vă ajuta să vă administraţi serverul LDAP pe serverul iSeries al domneavoastră:

Pentru informaţii suplimentare despre Servicii director, visitaţi Servicii director pagina web Legătură în afara Centrului de informare.

Serverul LDAP care Servicii director furnizează este un director IBM SecureWay .

Capitol 1. Ce e nou pentru V5R2

Serviciile de directoare are următoarele îmbunătăţiri şi noi caracteristici.

- Serviciile de directoare este parte a sistemelor de operare de bază începând în V5R1. Opţiunea 32 nu mai este disponibilă începând cu V5R2.
- Noi îmbunătăţiri de securitate au fost făcute pentru protejarea viitoare oricăror date memorate pe serverul de directoare.
- Serverul de directoare LDAP poate acum fi folosit ca un controler de domeniu pentru un domeniu Enterprise Identity Mapping (EIM).
- O nouă opţiune este disponibilă pentru administratori ce pot fi folosite pentru a acorda acces administratorilor la serverul de directoare pentru utilizatori căror le-a fost dat acces la identificatorul funcţiei Directory Services Administrator (QIBM_DIRSRV_ADMIN) (ID) al sistemului de operare prin iSeries Navigator suportul de aplicaţii.
- Puteţi selecta ca serverul de directoare să folosească adrese IP specifice sau puteţi selecta să folosiţi toate adresele IP configurate pe server. Consultaţi “Schimbarea portului sau a adresei IP” pe pagina 21 pentru mai multe informaţii.
- API-ul **ldap_set_option** are o nouă caracteristică de urmărire pentru V5R2. Opţiunea LDAP_OPT_DEBUG poate fi folosită pentru a ajuta diagnosticarea problemelor cu clienţii care foloseşte LDAP C API. Pentru mai multe informaţii, consultaţi “Folosirea opţiunii LDAP_OPT_DEBUG pentru a urmări erori” pe pagina 63sau consultaţi Directory Services API din iSeries Information Center .

Cum să vedeţi ce e nou sau modificat:

Pentru a vă ajuta să vedeţi unde modificări tecnice au fost făcute, această informaţie foloseşte:

- marchează unde informaţiile noi sau modificate încep.
- Imaginea marchează unde informaţiile noi sau modificate se sfârşeşte.

Capitol 2. Tipăriţi acest subiect

Pentru a vedea sau descărca versiunea PDF, selectaţi Servicii director (LDAP) (cam 323 KB sau 66 pagini).

Alte informaţii

Puteţi vedea sau tipări şi oricare din următoarele PDF:

- *Implementarea LDAP Cookbook* .
- *Înţelegerea LDAP* .
- *Folsind LDAP pentru Directory Integration: O prvire la Directorul IBM SecureWay, Active Directory, şi Domino* .
- *Implementarea şi Folosirea practică a LDAP pe iSeries Server* .

Pentru a salva un PDF pe staţia de lucru în scopul vizualizării sau tipăririi:
1. Deschideţi PDF-ul în browser (apăsaţi pe legătura de mai sus).
2. În meniul browser-ului, selectaţi **File**.
3. Selectaţi **Save As...**
4. Navigaţi în directorul în care doriţi să salvaţi fişierul PDF.
5. Selectaţi **Save**.

Descărcarea Adobe Acrobat Reader

Dacă aveţi nevoie de Acrobat Reader pentru a vedea sau tipări aceste PDF-uri, puteţi descărca o copie de la site-ul Adobe Web (www.adobe.com/products/acrobat/readstep.html) .

Capitol 3. Începutul cu Servicii director

Servicii director furnizează un server Lightweight Directory Access Protocol (LDAP) pe serverul iSeries. LDAP rulează peste Transmission Control Protocol/Internet Protocol (TCP/IP) şi obţien popularitate ca un serviciu de diectore pentru aplicaţiile Internet şi non-Internet. Realizaţi majoritatea operaţiilor de setare şi administrare ale serverul de directoare OS/400-based LDAP prin interfaţa grafică utilizator (GUI) a iSeries Navigator. Pentru a administra Servicii director, trebuie să aveţi instalat iSeries Navigator pe un PC care este conectat la serverul domneavoastră iSeries. Puteţi folosi Servicii director cu aplicaţiile activate-LDAP cum ar fi aplicaţii mail care caută adrese e-mail la serverele LDAP.

Pe lângă serverul LDAP, Servicii director include de asemenea:

- Un client OS/400-bazat LDAP. Acest client include un set de interfeţe utilizator program (API) pe care le puteţi folosi în programele OS/400 pentr a vă crea propriile aplicaţii client. Pentru informaţii despre aceste API-uri, consultaţi subiectul Directory Services sub Programarea în Centru de informare iSeries.
- Versiunea 3.2 a IBM SecureWay Directory Client Software Development Kit (SDK). SDK include un client Windows LDAP şi următoarele unelte:
  - Unealta de gestionare director IBM SecureWay (DMT) vă furnizaeză o interfaţă grafică utilizator pentru gestionarea conţinutului directorului.
  - utilitare ale liniei de comandă (ldapsearch, ldapadd, etc.)
  - C LDAP APIs (fişiere biblitecă, fişiere antet şi sursă de cod eşantion)
  - Furnizor de servicii IBM JNDI LDAP (ibmjndi.jar)
  - documentaţie online pentru toate articolele de mai sus. Consultaţi fişierul readme pentru locaţia şi numeel acestor fişiere HTML.

Dacă aţi folosit Servicii director cu o ediţie anterioară a OS/400, consultaţi “Migrarea la V5R2 de la o ediţie anterioară a Servicii director” pe pagina 11.

Pentru o introducee la LDAP, consultaţi “LDAP elementar” pe pagina 8. Dacă aţi folosit serverele LDAP pe alte platforme ar trebui să citiţi acest subiect căci conţien unele informaţii specifice OS/400.

Când v-aţi familiarizat cu informaţiile elementare, continuaţi cu “Planificarea serverului domneavoastră de directoare LDAP” pe pagina 11.

Pentru informaţii despre instalarea şi configurarea serverului domneavoastră de directoare, consultaţi “Instalarea şi configurarea Servicii director” pe pagina 14.

Documentaţie

Subiectul Servicii director Centru de informare furnizează o privire generală asupra LDAP şi se concentrează specific pe gestionarea serverului de directoare LDAP pe OS/400. Această documentaţie furnizează de asemenea documentaţie completă pentru SecureWay Directory Client SDK. Pentru informaţii suplimentare LDAP, consultaţi referinţele LDAP după cum urmează:

- *LDAP Implementation Cookbook* .
- *Înţelegerea LDAP* .
- *Folsind LDAP pentru Directory Integration: O prvire la Directorul IBM SecureWay, Active Directory, şi Domino* .
- *Implementarea şi Folosirea Practică a LDAP pe serverul iSeries* .
- *LDAP: Programarea Aplicaţiilor activate-director cu Lightweight Directory Access Protocol* de Tim Howes şi Mark Smith.

- *Înţelegerea şi Lansarea Serviciilor de directoare LDAP* de Mark C. Smith, Gordon S. Good şi Tim Howes.

Informaţii suplimentare despre Servicii director pe serverul iSeries sunt disponibile la pagina hoem iSeries Directory Services .

Notă: Unele din materialeel conţinute în acest document este o derivare de la documentaţi LDAP furnizată de Universitatea din Michigan. Copyright © 1992-1996, Regents of the University of Michigan, All Rights Reserved.

LDAP elementar

Lightweight Directory Access Protocol (LDAP) este un protocol de serviciu de directoare care rulează peste Transmission Control Protocol/Internet Protocol (TCP/IP). LDAP versiunea 2 este definit formal în Internet Engineering Task Force (IETF) Request pentru Comments (RFC) 1777, *Lightweight Directory Access Protocol*. LDAP versiunea 3 este definit formal în IETF RFC 2251, *Lightweight Directory Access Protocol (v3)*. Puteţi vedea aceste RFC-uri pe Internet al următorul URL:

http://www.ietf.org

Serviciile de directoare LDAP urmează un model client/server. Unul sau mai multe servere LDAP conţin datele directorului. Un client LDAP se conectează la un server LDAP şi face o cerere. Serverul răspunde cu o replică sau cu un indicator (o referinţă) la alt server LDAP.

Folosirea LDAP:

Deoarece LDAP este mai mult un director de servicii decât o bază de date, informaţiile din directorul LDAP sunt de obicei descriptive, informaţii bazate pe atribute. Utilizatorii LDAP citesc în general informaţiile din director mult mai des decât le modifică. Actualizările sunt de obicei simple mofificări totul-sau-nimic. Folosirile comune ale directoarelor LDAP includ directoarele telefoanelor online şi directoarele e-mail.

Structura de directoare LDAP:

Modelul Directorului de servicii LDAP este bazat pe **intriări** (care mai sunt referite ca şi **obiecte**). Ficare intrare consistă din unul sau mai multe **atribute**, cum ar fi numele sau adresa, şi un **tip**. Tipurile consistă din şiruri mnemonice, ca şi cn pentru numele comun sau mail pentru adrese e-mail.

Directorul exemplu din Figura 1 pe pagina 10 arată o intrare pentru Tim Jones care include atributele *mail* şi *telephoneNumber*. Alte atribute posibile includ *fax*, *titlu*, *sn* (pentru surname), şi *jpegPhoto*.

Fiecare director are o **schemă**, cae este un set de reguli care determină structura şi conţinutul directorului. Ar trebui să folosiţi unealta IBM SecureWay Directory Management (DMT) pentru a edita fişierele schemă pentru serverul LDAP al domneavoastră. După ce instalaţi Servicii director, fişierele sunt localizate pe sistemul domneavoastră la /QIBM/UserData/OS400/DirSrv.

Notă: Copiile originale ale fişierelor schemă implicite sunt localizate la /QIBM/ProdData/OS400/DirSrv. Dacă vreţi să înlocuiţi fişierele din directorul UserData, puteţi copia aceste fişiere în directorul /QIBM/ProdData/OS400/DirSrv.

Fiecare intrare 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.

Fiecare intrare director are şi următoarele **atribute operaţionale**, pe care serverul LDAP le menţine automat:

- CreatorsName, care conţine DN asociat folosit când se crea intrarea.
- CreateTimestamp, care conţine timpul la care a fost creată intrarea.
- modifiersName, care conţine DN-ul asociat folosit când intrarea a fost modificată ultima dată (iniţial aceasta este ca şi CreatorsName).
- modifyTimestamp, care conţine timpul la care intrarea a fost modificată ultima dată (iniţial aceasta este la fel ca şi CreateTimestamp).

Tradiţional, intrările director LDAP sunt aranjate într-o structură ierarhică care reflectă graniţa politicală, geografică sau organizaţională (consultaţi Figura 1 pe pagina 10). Intrările care reprezintă ţări apare 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.

Nu sunteţi limitat la ierarhia tradiţională când vă structuraţi directorul. Structura componentei domeniului, de exemplu, atrage popularitate. Cu această structură, intrările sunt compuse din părţi ale numelor domeniilor TCP/IP. De exemplu, dc=ibm,dc=com may be preferable to o=ibm,c=us.

LDAP referă la intrări cu **Nume distinctiv** (DN). Numele distinctive consistă din numele intrării înseşi la fel şi numele, în ordinea de jos în sus, a obiectelor de peste el din director. De exemplu, DN-ul complet pentru intrare din colţul stânga jos a Figura 1 pe pagina 10 is cn=Tim Jones, o=IBM, c=US. Fiecare intrare are cel puţin un atribut care este folosit pentru a numi intrare. Acest atribut numind este apelat de **Numele distinctiv relativ (RDN)** al intrării. Intrarea de mai sus de un RDN dat este numit **Nume distinctiv părinte** . În exemplul de mai sus, cn=Tim Jones numeşte intrarea, aşa încât este RDN. o=IBM, c=US este DN-ul părinte pentru cn=Tim Jones.

Pentru a da unui server LDAP capabilitatea de a gestiona o parte a unui director LDAP, specificaţi numele distinctive parinte de cel mai înalt nivel în configuraţia serverului. Aceste nume distinctiv sunt numite **sufixe**. Serverul poate accesa toate obiectele din director care sunt sub sufixul specificat în ierarhia directorului. De exemplu, dacă un server LDAP conţine directorul afişat în Figura 1 pe pagina 10, ar trebui să aibă sufixul o=ibm, c=us specificat în configuraţie pentru a fi în stare să răspundă la cererile clientului privind Tim Jones.

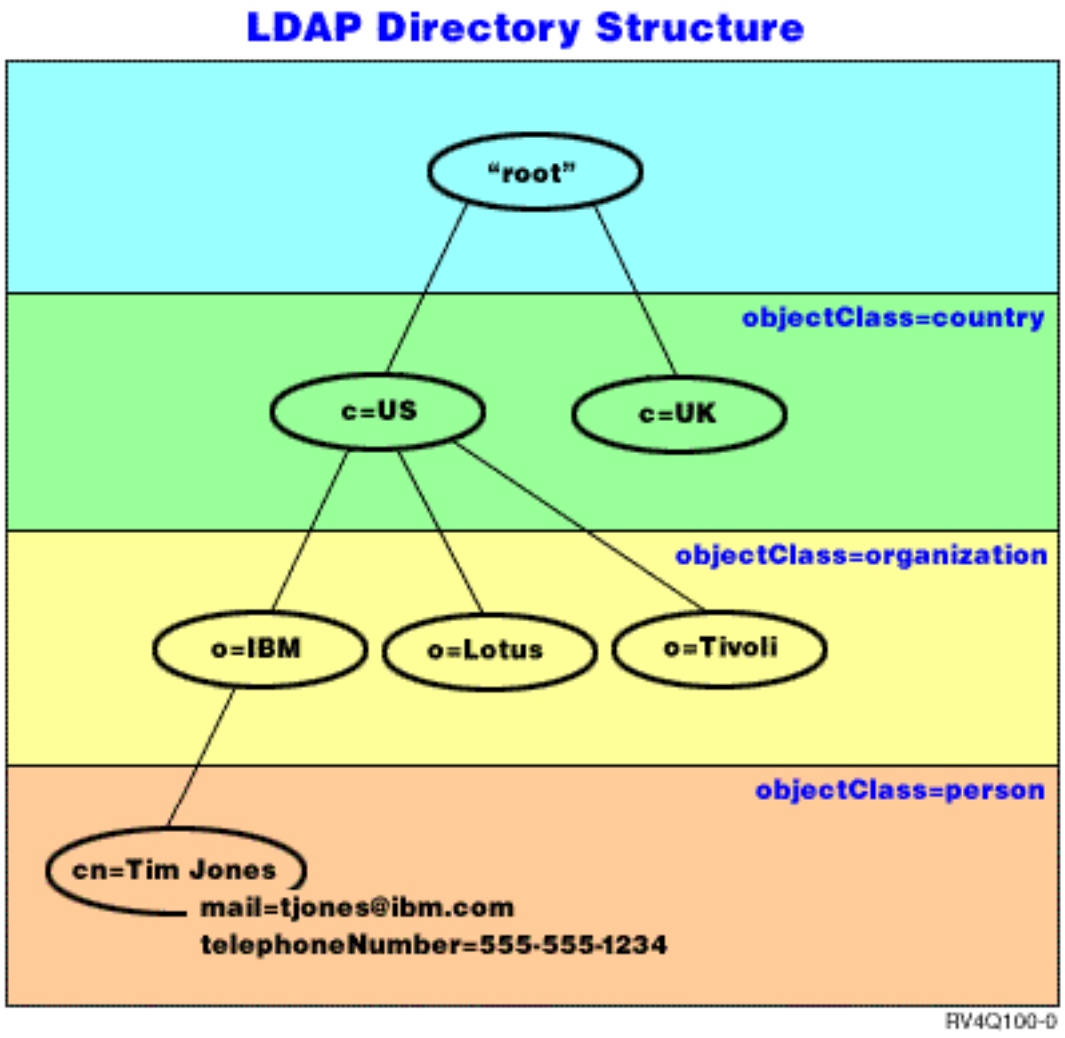


Figura 1. Structura elementară a directoarelor LDAP

Note despre LDAP şi Servicii director:

- Începând cu V4R5, şi serverul LDAP OS/400 şi clientul LDAP OS/400 sunt bazaţi pe LDAP versiunea 3. Puteţi folosi un client V2 cu un V3 server. Totuşi, nu puteţi folosi un client V3 cu un server V2 până când nu asociaţi ca şi client V2 şi folosiţi doar API-uri V2. Consultaţi consideraţiile LDAP V2/V3 pentru mai multe detalii.
- Clientul Windows LDAP este de asemenea bazat pe LDAP versiunea 3.
- Deoarece LDAP este un standard, toate serverele LDAP partajează multe caracteristici elementare. Totuşi, datorită diferenţelor de implementare, nu sunt toate complet compatibile cu cealalt. Serverul LDAP furnizat de Servicii director este aproape compatibil cu alte servere de directoare LDAP din directorul IBM SecureWay şi grupul produs Director IBM Totuşi, el ar putea să nu fie la fel de compatibil cu alte servere LDAP.
- Datele pentru serverul LDAP care furnizează Servicii director se află într-o bază de date OS/400.

Mai multe informaţii:

Pentru exemple despre folosirea directoarelor LDAP, consultaţi următoarele:

- Secţiunea 1.6 Start rapid: Un exemplu LDAP public, în redbook *Understanding LDAP*.
- Secţiunea 3.3 Scenarii exemple, în carte roşie Understanding LDAP.

Pentru a învăţa mai multe despre conceptele LDAP, consultaţi Capitol 5, “Concepte şi informaţii de referinţă Servicii director” pe pagina 33.

Consideraţii pentru folosirea LDAP V2 cu LDAP V3

Începând cu V4R5, şi serverul LDAP OS/400 şi clientul LDAP OS/400 sunt bazaţi pe LDAP versiunea 3. Nu puteţi folosi un client V3 cu un V2 server. Totuşi, puteţi folosi ldap_set_option() API pentru a modifica versiunea unui client V3 la V2. Apoi puteţi trimite cu succes cereri în client la un server V2.

Puteţi folosi un client V2 cu un server V3. Fiţi conştient că o cerere de căutare, totuşi, serverul V3 poate trimite datele înapoi în intervalul determinat al formatului UTF-8, în timp ce un client V2 poate fi în stare doar să manipuleze date în setul de caractere IA5.

Notă: LDAP versiunea 2 este definit formal în Internet Engineering Task Force (IETF) Request pentru Comments (RFC) 1777, *Lightweight Directory Access Protocol*. LDAP versiunea 3 eset definită formal în IETF RFC 2251, *Lightweight Directory Access Protocol (v3)*. Puteţi vedea aceste RFC-uri pe Internet al următorul URL:

http://www.ietf.org

Planificarea serverului domneavoastră de directoare LDAP

Înainte de a instala Servicii director 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 domneavoastră şi să determinaţi ce sufixe şi atribute va necesita serverul domneavoastră.
- **Decideţi cât de mare va fi directorul domneavoastră 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 Servicii director 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 căsuri de securitate veţi lua**. Servicii director suportă folosirea Secure Sockets Layer (SSL) şi Digital Certificates la fel şi Translation Layer Security (TLS) pentru comunicaţiile de securitate. Începând cu V5R1, autentificarea Kerberos este suportată.
- Servicii director vă permite să controlaţi accesul la obiectele director cu listele de control acces (ACL). Puteţi de asemenea folosi auditarea securităţii OS/400 pentru a proteja directorul.

Migrarea la V5R2 de la o ediţie anterioară a Servicii director

V5R2 a OS/400 introduce noi caracteristici şi capabilităţi la Servicii director. Aceste modificări afectează şi serverul de directoare LDAP şi interfaţa grafică utilizator (GUI) a iSeries Navigator. Pentru a beneficia de avantajele noilor caracteristici GUI, trebuie să instalaţi iSeries Navigator pe un PC care poate comunica peste TCP/IP la serverul iSeries. iSeries Navigator este o componentă a iSeries Access pentru Windows. Dacă aveţi instalată o versiune anterioară iSeries Navigator, ar trebui să modernizaţi la V5R2.

V5R2 a OS/400 suportă modernizări de la V4R5 şi V5R1. Când modernizaţi la V5R2 a OS/400, şi datele directorului LDAP şi fişierele schemă a directorului sunt migrate automat pentru a conforma formatelor V5R2. Dacă aveţi un server Servicii director LDAP rulând sub V4R3 sau V4R4 a OS/400 şi vreţi să migraţi serverul la V5R2, trebuie să realizaţi nişte operaţii suplimentare de migrare .

Când modernizaţi la V5R2 a OS/400, trebuie să ştiţi unele probleme de migrare:

- Cand modernizaţi la V5R2, Servicii director migrează automat fişierele schemă la V5R2 şi şterge fişierele schemă vechi. Totuşi, dacă aţi şters sau redenumit fişierele schemă, Servicii director nu le poate migra. Puteţi primi o eroare sau Servicii director poate asuma că fişierele au fost deja migrate.
- Servicii director migrează datele directorelor la formatul V5R2 prima dată când porniţi serverul sau importaţi un fişier LDIF. Planificaţi să alocaţi ceva timp pentru ca această migrare să fie completă. Dacă modernizaţi la V5R2 de la V4R4 sau anterior, fiţi conştient că datele directorului va necesita approximativ de două ori mai mult spaţiu de memorare în V5R2 decât necesita anterior. Aceasta este deoarece în V4R4 sau versiuni anterioare, Servicii director suporta doar setul de caractere IA5 şi salva date în ccsid 37 (format octet singur). Servicii director suportă setul complet de caractere ISO 10646.

  După ce modernizaţi la V5R2, ar trebui să vă porniţi serverul o dată pentru a migra datele existente înainte de a importa noi date. Dacă încercaţi să importaţi date înainte de a porni serverul o dată şi nu aveţi suficientă autoritate, importul poate eşua.
- V4R4 şi ediţiile anterioare ale Servicii director nu iau zonele temporale în cont când crează intrări amprentă de timp. Începând cu V4R5, zona temporală este folosită în toate adăugirile şi modificările la director. Prin urmare, dacă modernizaţi la V5R2 de la V4R4 sau anterior, Servicii director ajustaţi atributele existente createtimestamp şi modifytimestamp să reflecte zona temporală corectă. Face asta prin subextragerea zonei temporale care este definită curent pe sistemul iSeries de la amprentele de timp care sunt memorate în director. Notaţi că dacă zona temporală curentă nu este aceeaşi zonă temporală care a fost activă când intrările au fost create sau modificate original, noile valori amprentă de timp nu vor reflecta zona temporală originală.
- Urmând migrarea, serverul de directoare LDAP va porni automat când porneşte TCP/IP. Dacă nu vreţi ca serverul de directoare să pornească automat, folosiţi iSeries Navigator pentru a schimba setarea.

Migrarea de la V4R3 sau V4R4 Servicii director la V5R2

V5R2 a OS/400 nu suportă modernizare directă de la V4R3. Dacă vreţi să migraţi un server LDAP V4R3 sau V4R4 Servicii director la V5R2, puteţi urma una din următoarele proceduri:

- Porniţi instalarea OS/400 de la V4R3 sau V4R4 la ediţia interimară
- Salvarea bibliotecii bazei de date şi pornirea instalării OS/400 de la V4R3 sau V4R4 la V5R2

Porniţi instalarea OS/400 de la V4R3 sau V4R4 la o ediţie interimară

Deşi modernizarea de la V4R3 şi V4R4 a OS/400 la V5R2 nu e suportată, următoarele modernizări sunt suportate:

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

O cale de a vă migra Servicii director serverul este de a modeerniza la o ediţie interimară (V4R5 sau V5R1), apoi la V5R2. Pentru informaţii detailate despre OS/400 procedurile de instalare, consultaţi *Instalarea software-ului* . 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 sunt migrate automat.
2. Penrtu V4R4 sau V4R3, faceţi instalarea V4R5 sau V5R1 a OS/400.
3. Faceţi instalarea V5R2 a OS/400.
4. Porniţi serverul Directory Services dacă nu e deja pornit.
5. Folosiţi Directory Management Tool pentru a modifica fişierele schemă pentru orice schimbare utilizator pe care aţi notat-o în pasul 1.
6. Reporniţi serverul Directory Services.

Salvarea bibliotecii bazei de date şi pornirea instalării OS/400 de la V4R3 sau V4R4 la V5R2

Altă cale de a vă migra Servicii director serverul este de a salva biblioteca bazei de date care Servicii director foloseşte V4R3 sau V4R4, apoi restauraţi-o după instalarea V5R2. Această vă scuteşte de pasul de instalare a unei ediţii interimare. Totuşi, setările serverelor nu sunt migrate, aşa încât trebuie să reconfiguraţi setările serverului. Pentru informaţii detailate despre OS/400 procedurile de instalare, consultaţi *Instalare 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 diverse setări de configurare în Servicii director proprietăţile serverului, incluzând numele bibliotecii bază de date.
3. Salvaţi biblioteca bazei de date care este specificat în Servicii director configuraţia serverului.
4. Notaţi configuraţia publicării.
5. Instalarea stratch a sistemului la V5R2 a OS/400.
6. Folosiţi EZ-Setare pentru a configura serverului Directory Services.
7. Restauraţi biblioteca bazei de date pe care aţi salvat-o în pasul 3.
8. Folosiţi Directory Management Tool pentru a modifica fişierele schemă pentru orice schimbare utilizator pe care aţi notat-o în pasul 1.
9. Folosiţi iSeries Navigator penrtu a reconfigura Directory Services. Specificaţi biblioteca bazei de date care aţi salvat-o si restaurat-o.
10. Folosiţi iSeries Navigator penrtu a reconfigura publicarea.
11. Reporniţi serverul Directory Services.

Probleme de modernizare

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:**

  V3R2 Client Access foloseşte fişierele inel de chei pentru a stabili conexiunile Secure Sockets Layer (SSL) la serverul de directoare LDAP. iSeries Access pentru Windows foloseşte memorări de certificate, care sunt câteodată numite baze de date de chei, pentru a stabili conexiuni SSL. Dacă aţi folosit un fişier inel de chei cu serverul de directoare LDAP, fişierul inel de chei trebuie convertit la o bază de date chei pentru a continua să folosiţi SSL. Prima dată când încercaţi să porniţi o conexiune SSL la serverul de directoare LDAP, iSeries Navigator vă va alerta de această modificare. Dacă alegeţi să convertiţi cheia sunteţi promptat să specificaţi unele informaţii pentru baza de date de chei înainte ca conversia să fie făcută.

  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 domneavoastră 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 Servicii director 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 domneavoastră.

De asemeenea fiţi conştient că pot fi probleme suplimentare asociate cu modernizarea ediţiei curente de la alte ediţii .

Instalarea şi configurarea Servicii director

Servicii director (LDAP) este instalat automat când instalaţi OS/400. Serverul de directoare include o configuraţie implicită care porneşte automat serverul de directoare când TCP/IP este pornit. Serverul de directoare mai porneşte şi publicarea informaţiilor computer de la OS/400 la serverul de directoare. Pentru a personaliza setările serverului de directoare LDAP, rulaţi Servicii director Vrăjitorul de configurare . Trebuie să aveţi autorizările speciale *ALLOBJ şi *IOSYSCFG pentru a folosi vrăjitorul.

Directory Services este integrat în sistemul de bază de operare începând cu V5R1 şi opţiunea 32 nu mai e disponibilă începând cu V5R2.

Configurarea serverului de directoare LDAP

Dacă sistemul domneavoastră nu a fost configurat pentru a publica informaţii pe un alt server LDAP şi nici un server LDAP nu e cunoscut de serverul TCP/IP DNS, atunci Servicii director este instalat automat cu o configuraţie implicită limitată. Servicii director furnizează un vrăjitor pentru a vă asista în configurarea serverului de directoare LDAP penru nevoile domneavoastră. Puteţi rula acest vrăjitor ca parte a EZ-Setup sau să rulaţi vrăjitorul mai târziu din iSeries Navigator. 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 directoarelor nu sunt şterse, dar în locul rămân memorate în biblioteca pe care aţi selectat-o în timpul instalării (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, apăsaţi clic-dreapta pe **Director** şi selectaţi **Propretăţi**. 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.

Pentru a porni Servicii director Vrăjitorul de configurare, urmaţi aceşti paşi:

1. În iSeries Navigator, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Apăsaţi **TCP/IP**.
4. Faceţi clic-dreapta pe **Director** şi selectaţi **Configurare**.

Notă: Dacă aţi configurat deja serverul de directoare, apăsaţi **Reconfigurare** mai degrabă decât **Configurare**.

Urmaţi instrucţiunile din vrăitorul Configurare Server de directoare pentru a vă configura serverul de directoare LDAP.

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.

Când vrăjitorul este terminat, serverul domneavoastră de directoare LDAP are o confuguraţie de bază. Dacă rulaţi Lotus Domino pe sistemul domneavoastră, portul 389 (portul implicit pentru serverul LDAP) poate fi deja utilizat de funcţia Dominos LDAP . Trebuie să faceţi una din următoarele:

- Modificaţi portul care îl foloseşte Lotus Domino
- Modificaţi portul pe care îl foloseşte Servicii director
- Folosiţi adrese IP specifice

Acum puteţi porni serverul. Totuşi, înainte de a-l porni, puteţi dori să faceţi una din următoarele:
- Să importaţi date pe server
- Să activaţi securitatea Nivel socketi siguri (SSL)
- Să activaţi autentificarea Kerberos
- Să setaţi o referinţă

Activare SSL pe serverul de directoare LDAP

Dacă aveţi instalat Digital Certificate Manager pe sistemul domneavoastră, puteţi folosi securitatea Secure Sockets Layer (SSL) pentru a proteja accesul la serverul domneavoastră de directoare LDAP. Înainte de activarea SSL pe serverul de directoare, puteţi găsi de folos să citiţi o privire generală despre folosirea SSL cu Servicii director.

Pentru a folosi o conexiune SSL când vă administraţi serverul de directoare LDAP de la iSeries Navigator sau să folosiţi SSL cu clientul Windows LDAP, trebuie să aveţi unul din produsele Client Encryptions (5722CE2 sau 5722CE3) instalate pe PC-ul domneavoastră.

Pentru a activa SSL pe serverul domneavoastră LDAP, folosiţi interfaţa Digital Certificate Manager. Puteţi lansa Digital Certificate Manger din directorul **Internet** în iSeries Navigator sau de la pagina **Network** a serverelor de directoare în dialogul **Properties**.

Pentru a lansa Digital Certificate Interface de la pagina **Network** urmaţi paşii:
1. În iSeries Navigator, expandaţi **Network**.
2. Expandare **Servere**.
3. Apăsaţi **TCP/IP**.
4. Faceţi clic-dreapta pe **Directory** şi selectaţi **Proprietăţi**.
5. Apăsaţi pe tabela **Network**.
6. Apăsaţi **Digital Certificate Manager**.

   Digital Certificate Manager va lansa browserul implicit de Internet.

Consultaţi Securizarea serverului de directoare LDAP pentru paşii specifici pe care trebuie să-i urmaţi pentru a assigna un certificat digital la serverul de directoare.

După ce SSL este activat, puteţi modifica portul pe care serverul de directoare LDAP îl foloseşte pentru conexiuni sigure.

Activarea autentificării Kerberos pe serverul de directoare LDAP

Dacă aveţi configurat Serviciul de autentificare reţea configurat pe sistemul domneavoastră, puteţi seta serverul de directoare LDAP să folosească autentificarea Kerberos. Înainte de activarea Kerberos pe serverul de directoare, puteţi găsi de folos să citiţi o privire generală despre folosirea Kerberos cu Servicii director.

Pentru a activa autentificarea Kerberos, urmaţi aceşti paşi:
1. În iSeries Navigator, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Apăsaţi **TCP/IP**.
4. Faceţi clic-dreapta pe **Director** şi selectaţi **Proprietăţi**.
5. Apăsaţi fişa **Kerberos**.
6. Bifaţi **Activare autentificare Kerberos** .
7. Specificaţi alte setări din pagina **Kerberos** corespunzător cu situaţia domneavoastră. Consultaţi paginile de ajutor online pentru informaţii despre câmpurile individuale.

Configuraţie implicită pentru Servicii director

Serverul de directoare LDAP 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 Servicii director Vrăjitorul de configurare sau au modificat setăriel directoarelor cu paginile de proprietăţi.
- Publicarea Servicii director nu este configurată.
- Serverul de directoare LDAP nu poate găsi informaţiile LDAP DNS.

Dacă serverul de directoare LDAP foloseşte configuraţia implicită, atunci se întâmplă următoarele:
- Serverul de directoare LDAP porneşte automat când porneşte TCP/IP.
- Sistemul crează 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 Servicii director pagina de proprietăţi.
- Un sufix impicit este creat care este bazat pe numele IP ale sistemelor. Un sufix de obiecte ssitem este de asemenea creat bazat pe numele sistemului. De exemplu, dacă numele sistemelor IP este mary.acme.com, sufixul este dc=mary,dc=acme,dc=com.
- Serverul de directoare LDAP foloseşte datele implicite ale librăriei QUSRDIRDB. Sistemul le crează în ASP-ul sistem.
- Serverul foloseşte portul 389 pentru comunicaţii nesigure. Dacă un certificat digital a fost configurat pentru LDAP, nivelul socket securizat (SSL) este activat şi portul 636 este folosit pentru comunicaţii sigure.

Următoarele impicite apoi există pentru Servicii director publicare:
- Sistemul publică informaţii la serverul de directoare LDAP
- Publicarea nu foloseşte SSL
- Publicarea foloseşte containere sun sufixul implicit
- Pentru autentificarea la serverul de directoare, OS/400 foloseşte ID-ul cn=Administrator şi parola generată de sistem.
- Sistemul publică doar informaţiile de sistem

Unealta de gestionare directoare IBM SecureWay

Unealta de gestionare director IBM SecureWay (DMT) vă furnizaează o interfaţă grafică utilizator pentru gestionarea conţinutului directorului LDAP. Operaţiile pe care le puteţi realiza cu DMT le includ pe următoarele:
- Răsfoirea schemei de directoare
- Adăugarea, editarea şi ştergerea claselor de obiecte
- Adăugarea, editarea şi ştergerea atributelor
- Răsfoirea şi căutarea arborilor de directoare
- Adăugarea, editarea, vizualizarea şi ştergerea intrărilor
- Editarea intrări RDN
- Gestionare ACL

DMT este parte a clientului Windows LDAP care este inclus cu Servicii director. Clientul este livrat într-un director cu sistem de fişiere integrate.

Pentru a instala clientul Windows LDAP, incluzând DMT, pe un PC, urmaţi aceşti paşi:
1. În iSeries Navigator, expandaţi **Sisteme de fişiere**.
2. Expandaţi **Partajări de fişiere**.
3. Faceţi dublu-clic pe **Qdirsrv**.
4. Faceţi dublu-clic pe **UserTools**.
5. Faceţi dublu-clic pe **Windows**.
6. Faceţi dublu-clic pe **setup.exe** pentru a porni instalarea lui DMT. Urmaţi instrucţiunile de pe ecran pentru a completa instalarea.

Documentaţia pentru Unealta de gestionare directoare IBM SecureWay (DMT) eset localizată în fişierul dparent.htm. Acest fişier este copiat în directorul IBM SecureWay Directory pe PC-ul domneavoastră când instalaţi clientul.

Capitol 4. Administrarea serverului de directoare LDAP

Pentru a administra serverul de directoare LDAP, 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 se utilizează integrarea autorizărilor, un administrator poate fi de asemenea un utilizator proiectat care are ID de autorizare pentru funcţia Administrator Servicii de director.

Administrarea serverului de directoare include următoarele sarcini:

Pornirea serverului de directoare LDAP

Penrtu a porni serverul de directoare LDAP urmaţi aceşti paşi:

1. În iSeries Navigator, expandaţi **Network**.
2. Expandare **Servere**.
3. Apăsaţi **TCP/IP**.
4. Apăsaţi clic-dreapta pe **Director** şi selectaţi **Start**.

   Serverul de directoare poate avea nevoie de mai multe minute pentru a porni depinde de viteza serverului domneavoastră 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 modernizarea de la o versiune anterioară a Servicii director, poate dura cu câteva minute mai mult decât de obicei deoarece serverul trebui să migreze fişierele. Puteţi verifica starea serverului periodic să vedeţi dacă a pornit.

Notă: Serverul de directoare poate fi pornit de asemenea de la o sesiune 5250 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.

Oprirea serverul de directoare LDAP

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.

Penrtu a opri serverul de directoare LDAP urmaţi aceşti paşi:
1. În iSeries Navigator, expandaţi **Network**.
2. Expandare **Servere**.
3. Apăsaţi **TCP/IP**.
4. Apăsaţi clic-dreapta pe **Director** şi selectaţi **Stop**.

   Serverul de directoare poate avea nevoie de mai multe minute pentru a se opri depinde de viteza serverului domneavoastră, de cantitatea de activitate a serverului şi de cantitatea de memorie disponibilă. Puteţi verifica starea serverului periodic să vedeţi dacă s-a oprit.

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 domneavoastră. ENDTCP va opri de asemenea TCP/IP.

Verificarea stării serverului de directoare

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

Pentru a verifica starea serverului de directoare, urmaţi aceşti paşi:
1. În iSeries Navigator, expandaţi **Network**.
2. Expandare **Servere**.
3. Apăsaţi **TCP/IP**. iSeries Navigator 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, apăsaţi 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 timp suplimentar caree cerut pentru a verifica starea celorlalte servere TCP/IP.

Verificarea job-urilor serverului de directoare LDAP

La un moment veţi vrea să monitorizaţi job-uri specifice pe serverul de directoare LDAP. Pentru a verifica job-urile server, urmaţi aceşti paşi:
1. În iSeries Navigator, expandaţi **Network**.
2. Expandare **Servere**.
3. Apăsaţi **TCP/IP**.
4. Apăsaţi clic-dreapta pe **Director** şi selectaţi **Server jobs**.

Activarea notificării de evenimente

Servicii director 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 iSeries Navigator, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Apăsaţi **TCP/IP**.
4. Faceţi clic-dreapta pe **Director** 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 notificările de evenimente, consultaţi Appendix C: Event Notification din manualul IBM SecureWay Directory Version 3.2: Client SDK Programming Reference .

Specificarea setărilor de tranzacţie

Servicii director suportă tranzacţii, ceea ce permite ca un grup de operaţii director LDAP să fie tratat ca o singură unitate. Pentru informaţii suplimentare consultaţi “Tranzacţii” pe pagina 37.

Pentru a configura setările de tranzacţii ale serverului dumneavoastră, urmaţi aceşti paşi:
1. În iSeries Navigator, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Apăsaţi **TCP/IP**.
4. Faceţi clic-dreapta pe **Director** şi selectaţi **Proprietăţi**.
5. Apăsaţi **Tranzacţii**.
6. Specificaţi setările de tranzacţie.

Notă: Setările de tranzacţie pot avea impact asupra performanţei serverului domneavoastră LDAP, prin urmare, puteţi dori să experimentaţi diferite setări.

Schimbarea portului sau a adresei IP

Serverul de directoare LDAP activat de Servicii director foloseşte următoarele porturi implicite:
- 389 pentru conexiuni nesecurizate.
- 636 pentru conexiuni securizate (dacă aţi folosit Managerul de certificate digitale pentru a activa Servicii director ca o aplicaţie care poate folosi un port sigur).

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 Servicii director, sau puteţi folosi adrese IP diferite pentru cele două servere, dacă aplicaţiile suportă legarea la o anumită adresă IP.

Pentru un exemplu al serverului LDAP Domino care intră în conflic cu serverul Servicii de director iSeries, consultaţi Găzduirea LDAP Domino şi Servicii de director pe acelaşi iSeries

Pentru a modifica porturile pe care le utilizează serevrul LDAP, urmaţi aceşti paşi:
1. În iSeries Navigator, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Apăsaţi **TCP/IP**.

4. Faceţi clic-dreapta pe **Director** 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 iSeries Navigator, 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.

Mutarea datelor directorului LDAP între sisteme

Serverul Servicii director LDAP al domneavoastră poate rula independent de alte servere. Totuşi, puteţi găsi folositor să-l aveţi rulând cu alte servere. Aceasta poate include:

- “Importarea unui fişier LDIF”
- “Exportarea unui fişier LDIF”
- “Setarea replica serverului de directoare” pe pagina 23
- “Publicarea informaţiilor pe serverul de directoare” pe pagina 26

Importarea unui fişier LDIF

Puteţi transfera informaţii între diferite servere de directoare LDAP folosind fişierele LDAP Data Interchange Format (LDIF). Înainte de a începe această procedură, transferaţi fişierul LDIF la serrverul dumneavoastră iSeries ca un fişier şir.

Pentru a importa un fişier LDIF la serverul de directoare LDAP, urmaţi aceşti paşi:

1. Dacă serverul de directoare este pornit, opriţi-l. Consultaţi “Oprirea serverul de directoare LDAP” pe pagina 20 pentru informaţii despre oprirea serverului de directoare.
2. În iSeries Navigator, expandaţi **Network**.
3. Expandare **Servere**.
4. Apăsaţi **TCP/IP**.
5. Apăsaţi clic-dreapta pe **Directory** şi selectaţi **Tools**, apoi **Import File**.

Notă: Puteţi de asemenea folosi utilitarul ldapadd pentru a importa fişierele LDIF.

Exportarea unui fişier LDIF

Puteţi transfera informaţii între diferite servere de directoare LDAP folosind fişierele LDAP Data Interchange Format (LDIF), consultaţi “Formatul de interschibare a datelor LDAP” pe pagina 34. 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 iSeries Navigator, expandaţi **Network**.
2. Expandare **Servere**.
3. Apăsaţi **TCP/IP**.
4. Apăsaţi clic-dreapta pe **Directory** şi selectaţi **Tools**, apoi **Export File**.

Notă: Dacă nu specificaţi o locaţie pentru fişierul LDIF în care să fie exportat, va fi salvat la directorul implicit specificat în OS/400 profilul domneavoastră de utilizator. Dacă nu v-aţi schimbat directorul implicit, directorul implicit este directorul rădăcină.

Note:

1. Asiguraţi-vă că setaţi authoritatea fişierului LDIF pentru a preveni accesul neautorizat la datele directorului. Pentru a face asta, apăsaţi clic-dreapta pe fişierul din iSeries Navigator, apoi selectaţi **Permissions**.
2. Puteţi crea un fişier plin sau parţial LDIF cu utilitarul ldapsearch, consultaţi “Utilitarul ldapsearch” pe pagina 52. Folosiţi opţiunea -L şi redirectaţi ieşirea într-un fişier.

Setarea replica serverului de directoare

Puteţi seta replica serverului de directoare LDAP serverele de directoare pe alte iSeries servere. Servicii director foloseşte LDAP standard protocolul versiunea 3 protocol pentru a replica.

Note:

1. Nu puteţi replica între serverele LDAP versiunea 3 şi LDAP versiunea 2. Prin urmare, sistemul în care-l replicaţi trebuie să folosească aceeaşi versiune LDAP ca şi sistemul din care replicaţi. V4R3 şi V4R4 a OS/400 suportă LDAP versiunea 2. V4R5 şi ediţii posterioare suportă LDAP versiunea 3
2. Puteţi replica Servicii director directorul la IBM SecureWay V3.2 sau servere posterioare pe alte platforme. Pentru a face asta, serverul domneavoastră de directoare OS/400 trebuie configurat să folosească mecanismul 3.2 ACI. Dacă serverul întâlneşte o problemă când încearcă să replicheze, va opri replicarea. Dacă se întâmplă asta, replica domneavoastră va fi incompletă.

Urmaţi aceşti paşi pentru a seta o nouă replică pe serverul de directoare.

1. Dacă nu aţi făcut-o deja, configuraţi şi master server şi replica server.

   Notă: Asiguraţi-vă că schema şi sufixele se potrivesc pe ambele servere.
2. Opriţi master server-ul.
3. (opţional) Setarea datelor LDAP pentru replicare iniţială. Puteţi sări acest pas dacă nu aveţi date iniţiale pe care vreţi să le transferaţi la serverul replica de la master server.
4. (opţional) Mutarea datelor LDAP la master server. Săriţi acest pas dacă una din următoarele se aplică la replica server al domneavoastră:
   - Este un nou server de directoare LDAP.
   - Nu conţine date pe care vreţi să continuaţi să le menţineţi.
5. Setarea noului replica server.
6. Setarea master server să aibă o nouă replica.
7. Asiguraţi-vă că serverul master permite actualizările:
   a. În iSeries Navigator, expandaţi sistemul pe care rulează serverul de directoare master.
   b. Expandaţi **Reţea**.
   c. Expandare **Servere**.
   d. Apăsaţi **TCP/IP**.
   e. Faceţi clic-dreapta pe **Directory** şi selectaţi **Proprietăţi**.
   f. Dacă este deja bifat, bifaţi **Permisiune actualizare directoare**.

Notă: Aceste instrucţiuni presupun că şi master server şi replica server sunt pe sisteme pe care le gestionaţi de la iSeries Navigator pe acelaşi PC. Dacă vă gestionaţi sistemele de PC-uri separate, puteţi muta între două PC-uri pentru a realiza această operaţie. Dacă master sau replica server rulează pe un sistem de operare IBM altul de OS/400, consultaţi documentaţia pentru acea platformă pentru a seta acel server.

Setarea datelor LDAP pentru replicare iniţială

Puteţi avea date existente pe serverul de directoare master LDAP pe care vreţi să-l adăugaţi la un nou replica server. Pentru a face asta, trebuie să exportaţi directorul către un fişier LDIF. Cât timp se exportă fişierul LDIF, trebuie să preveniţi master server să nu fie actualizat. Puteţi face aceasta în unul din modurile:

- Opriţi serverul de directoare LDAP. Depinzând de cantitatea de date din directorul domneavoastră, aceasta poate necesita ca serverul domneavoastră să stea oprit pentru o perioadă extinsă de timp.

- Modificaţi proprităţile serverului aşa încât să nu fie permise actualizările. Aceasta permite serverului să continue să răspundă la cererile de căutare ân timp ce fişierul LDIF este exportat. Pentru a lua această opţiune, urmaţi următorii paşi:
  1. În iSeries Navigator, expandaţi sistemul pe care rulează serverul de directoare master.
  2. Expandaţi **Reţea**.
  3. Expandare **Servere**.
  4. Apăsaţi **TCP/IP**.
  5. Faceţi clic-dreapta pe **Directory** şi selectaţi **Proprietăţi**.
  6. Dacă **Permitere actualizări de director** este bifată, debifaţi-o. Aceasta va preveni actualizările în director până când replicarea este setată complet.
  7. Selectaţi **OK**.
  8. Opriţi, şi apoi reporniţi, serverul de directoare LDAP.

După ce aţi oprit serverul sau aţi modificat proprietăţile serverului pentru a nu permite actualizări de directoare, realizaţi aceste sarcini:

1. Exportaţi directorul într-un fişier LDIF.
2. Transferaţi fişierul LDIF la sistemul pe care va rula serverul replica.

După ce fişierul LDIF este transferat la sistemul pe care replica server va rula, trebuie să importaţi datele pe replica server:

1. În iSeries Navigator, expandaţi sistemul pe care rulează serverul de directoare replica.
2. Dacă replica server nu e deja oprit, opriţi-l acum. Reîmprospătaţi starea serverelor până când starea este **Oprit**.
3. Expandaţi **Reţea**.
4. Expandare **Servere**.
5. Apăsaţi **TCP/IP**.
6. Faceţi clic-dreapta pe **Directory** şi selectaţi **Proprietăţi**.
7. Dacă **Permitere actualizări director** este nebifată, bifaţi-o.Aceasta va permite datelor să fie importate.
8. Selectaţi **OK**.
9. Importaţi fişierul LDIF care l-aţi transferat în pasul 2.
10. Faceţi clic-dreapta pe **Directory** şi selectaţi **Proprietăţi**.
11. Debifaţi **Permitere actualizare directoare**.

Mutarea datelor LDAP la serverul master

Odată ce faceţi un server de directoare LDAP într-un server replică, nu mai puteţi actualiza datele în el. Dacă aveţi date existente pe serverul pe care-l configuraţi să fie server de directoare LDAP replică, veţi vrea probabil să le mutaţi pe serverul aşa încât să mai poată fi menţinut. Pentru aceasta, urmaţi aceşti paşi:

1. În iSeries Navigator, expandaţi sistemul pe care rulează serverul de directoare replica.
2. Expandaţi **Reţea**.
3. Expandare **Servere**.
4. Apăsaţi **TCP/IP**.
5. Faceţi clic-dreapta pe **Directory** şi selectaţi **Proprietăţi**.
6. Dacă **Permitere actualizări de director** este bifată, debifaţi-o. Aceasta va preveni actualizările în director până când replicarea este setată complet.
7. Selectaţi **OK**.
8. Opriţi serverul de directoare LDAP.
9. Exportaţi directorul într-un fişier LDIF.
10. Transferaţi fişierul LDIF la sistemul pe care va rula serverul master.

După ce fişierul LDIF este transferat la sistemul pe care master server va rula, trebuie să importaţi datele pe master server:

1. În iSeries Navigator, expandaţi sistemul pe care rulează serverul de directoare master.
2. Dacă master server nu e deja oprit, opriţi-l acum. Reîmprospătaţi starea serverelor până când starea este **Oprit**.
3. Expandaţi **Reţea**.
4. Expandare **Servere**.

5. Apăsaţi **TCP/IP**.
6. Faceţi clic-dreapta pe **Directory** şi selectaţi **Proprietăţi**.
7. Dacă **Permitere actualizări director** este nebifată, bifaţi-o.Aceasta va permite datelor să fie importate.
8. Selectaţi **OK**.
9. Importaţi fişierul LDIF care l-aţi transferat în pasul 10 pe pagina 24 al procedurii anterioare.
10. Faceţi clic-dreapta pe **Directory** şi selectaţi **Proprietăţi**.
11. Debifaţi **Permitere actualizare directoare**.

Setarea noii replicări

Urmaţi aceşti paşi pentru a seta noul server de replicare.

Notă: Serverul de replicare trebuie configurat şi oprit înainte să realizaţi această procedură.

1. În iSeries Navigator, expandaţi sistemul pe care rulează serverul de directoare de replicare.
2. Expandaţi **Reţea**.
3. Expandaţi **Servere**.
4. Apăsaţi **TCP/IP**.
5. Dacă serverul nu este deja oprit, opriţi serverul acum. Reîmprospătaţi starea serverelor până când starea este **Oprit**.
6. Faceţi clic-dreapta pe **Director** şi selectaţi **Proprietăţi**.
7. Apăsaţi pe fişa **Replicare**.
8. Selectaţi **Utilizarea unui server de replicare**.
9. În câmpul **Nume folosit de serverul principal pentru actualizări**, selectaţi un nume pentru serverul master care să fie utilizat când se loghează pe serverul de replicare atunci când efectuează actualizări. Acesta poate fi un nume distinctiv (DN) sau un utilizator Kerberos.

   Dacă selectaţi un DN:

   - Apăsaşi butonul **Parolă** de lângă câmpul **Nume folosit de serverul master pentru actualizări**. Introduceţi o parolă pentru serverul master care să fie utilizată când se loghează pe serverul de replicare pentru a realiza actualizări.

     Notă: Ar trebui să notaţi această parolă şi numele care l-aţi introdus în pasul 9. Veţi avea nevoie de ele când setaţi serverul master pentru replicare.

   Dacă selectaţi **Adăugare utilizator Kerberos** :

   - Veţi fi întrebat pentru a introduce numele Kerberos (în format LDAP/*numegazdă*, unde *numegazdă* este numele de gazdă complet determinat al serverului master) şi domeniul implicit (cum ar fi ACME.COM) al serverului master.

     Notă: Pentru a folosi Kerberos, trebuie să aveţi activat Kerberos pe ambele servere master şi de replicare.
10. În câmpul **URL server master**, introduceţi numele serverului master în format URL. Dacă serverul domneavoastră master foloseşte un port altul decât cel implicit, introduceţi acest număr de port ca parte a URL.
11. Apăsaţi fişa **Bază de date/Sufixe**. Dacă sufixul pe care doriţi să îl replicaţi nu este în listă, adăugaţi-l.
12. (opţional) Dacă vreţi să folosiţi SSL (Secure Sockets Layer) la replicare, folosiţi Managerul de certificate digitale pentru a activa SSL pentru server. Puteţi porni Managerul de cerificate digitale din fişa **Reţea**. Pentru informaţii suplimentare despre activarea SSL pe un server de directoare, consultaţi “Activare SSL pe serverul de directoare LDAP” pe pagina 15.
13. Selectaţi **OK**.

Setarea master server pentru a avea o nouă replica

Urmaţi aceşti paşi pentru a seta noul server să aibă o nouă replică.

Notă: Trebuie să aveţi configurat şi pornit master server-ul domneavoastră înainte de a realiza această procedură.

1. În iSeries Navigator, expandaţi sistemul pe care rulează serverul de directoare master.
2. Expandaţi **Reţea**.

3. Expandare **Servere**.
4. Apăsaţi **TCP/IP**.
5. Faceţi clic-dreapta pe **Directory** şi selectaţi **Proprietăţi**.
6. Dacă este deja bifat, bifaţi **Permisiune actualizare directoare**.
7. Selectaţi **OK**.
8. Opriţi, şi apoi porniţi serverul de directoare LDAP. Reîmprospătaţi starea serverelor până când starea este **Pornit**.
9. Din ou, faceţi clic-dreapta pe **Director** şi selectaţi **Proprietăţi**.
10. Apăsaţi pe tabela **Replication**.iSeries Navigator vă poate prompta să introduceţi informaţiile de conectare. Introduceţi aceste informaţii, apoi apăsaţi **OK**.
11. Apăsaţi **Add.**
12. În câmpul **Server** , introduceţi numele replica server în format URL.
13. Selectaţi metoda domneavoastră de autentificare.

    Pentru a folosi un nume distinctiv (DN) şi parola:

    a. Selectaţi **Folosire DN şi parolă**.
    b. În câmpul **Conectare ca**, introduceţi numele care l-aţi specificat în pasul 9 pe pagina 25 când setaţi replica server.
    c. Apăsaţi **Parolă** şi introduceţi parolă care aţi specificat-o în pasul 9 pe pagina 25 când setaţi replica server.

    Pentru a folosi Kerberos:

    - Selectaţi **Folosire cont master servers Kerberos** . Master server îşi va folosi numele director Kerberos pentru a se autentifica.

      Notă: Pentru a folosi Kerberos, trebuie să aveţi Kerberos activat pe ambele servere master şi replica.
14. Dacă vreţi să folosiţi Secure Sockets Layer (SSL) când replicaţi, folosiţi Digital Certificate Manager pentru a activa SSL pentru server. Puteţi porni Digital Certificate Manger din tabela **Reţea**. Pentru informaţii suplimentare despre activare SSL pe un server de directoare, consultaţi “Activare SSL pe serverul de directoare LDAP” pe pagina 15.
15. Dacă replica server nu foloseşte portul implicit, specificaţi numele portului în câmpul **Port**.
16. Dacă nuu vreţi să actualizaţi replica server de fiecare dată când o intrare pe master server se modifocă, selectaţo **Time**. Apoi specificaţi cât de des vreţi ca master server să aactualizeze replica.
17. Selectaţi **OK**.
18. Apăsaţi tabela **Database/Suffixes**. Dacă sufixul care vreţi s-o replicaţi nu este în listă, adăugaţi-l.
19. Activaţi actualizarea directoarelor pe fiecare replica server:
    a. În iSeries Navigator, expandaţi sistemul pe care rulează serverul de directoare replica.
    b. Expandaţi **Reţea**.
    c. Expandare **Servere**.
    d. Apăsaţi **TCP/IP**.
    e. Faceţi clic-dreapta pe **Directory** şi selectaţi **Proprietăţi**.
    f. Dacă **Permitere actualizări director** este nebifată, bifaţi-o.
    g. Selectaţi **OK**.
20. Dacă fiecare replica server nu e deja pornit, porniţi-l acum.

Notă: Un server nu poate fi şi master server şi replica server.

Publicarea informaţiilor pe serverul de directoare

Vă puteţi configura sistemul pentru a publica anumite informaţii în serverul de directoare LDAP pe aceleşi sistem sau pe diferite sisteme. OS/400 automat publică această informaţie la serverul de directoare LDAP când folosiţi iSeries Navigator pentru a modifica această informaţie pe OS/400. Informaţia pe care o puteţi publica include sistem (sisteme şi imprimante), partajări de tipărire, informaţii utilizator şi Poliţe de calitate şi de servicii TCP/IP. Pentru mai multe informaţii despre Calitatea serviciilor, consultaţi Configuraţia LDAP şi QoS .

Dacă DN-ul părinte căruia datele îi sunt publicate nu există, Servicii director le crează automat. S-ar putea să aveţi instalat alte aplicaţii OS/400 care publică informaţii într-un director LDAP. În plus, puteţi apela interfeţe program aplicaţii (API-uri) de la propriile programe pentru a publica alte tipuri de informaţii la directorul LDAP.

Note:

1. Când configuraţi OS/400 să publice informaţii despre tipul utilizatorilor serverului de directoare LDAP, automat exportă intrări de la directorul de distribuţie sistem la serverul LDAP. Foloseşte interfaţa program aplicaţie QGLDSSDD (API) pentru a face asta. Aceasta păstrează de asemenea directorul LDAP sincronizat cu modificările care sunt făcute în directorul de distribuţie sistem. Pentru informaţii despre QGLDSSDD API, consultaţi OS/400 subiectul Director de servicii sub Programarea în Centru de informare iSeries. Imformaţiile disponibile le includ pe următoarele:
   - Cum să apelaţi manual acest API.
   - Cum să preveniţi anumiţi utilizatori de a fi exportaţi la serverul LDAP.
   - Cum exportă câmpurile directorului de distribuţie sistem.
2. Când configuraţi OS/400 să publice tipul de informaţii Sistem la serverul de directoare LDAP şi selectaţi una sau mi multe imprimante de publicat, sistem va păstra automat directorul LDAP sincronizat cu modificările care sunt făcute la aceel imprimante din sistem. Informaţiile de imprimantă care pot fi publicate includ locaţia imprintei, viteza în pagini pe minut, dacă suportă duplex şi color, tipul şi modelul şi descrierea sa. 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.
3. Puteţi de asemnea publica OS/400 informaţii la un server de directoare LDAP care nu este pe un OS/400 dacă configuraţi serverul să folosească schema IBM.

Pentru a vă configura sistemul să publice OS/400 informaţii într-un server de directoare LDAP urmaţi aceşti paşi:

1. În iSeries Navigator, apăsaşi clic-dreapta pe sistemul domneavoastră şi selectaţi **Proprietăţi**.
2. Apăsaţi tabela **Director de servicii**.
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 **Details**.
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**(Activ) Directory server**. În dialogul care apare, introduceşi numele serverului de directoare LDAP unde vreţi să publicaţi OS/400 informaţia, apoi apăsaţi**OK**.
8. În câmpul **Sub DN**, introduceţi numele distinctiv părinte (DN) unde vreţi să adăugaţi informaţiile pe 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. Consultaţi “Folosirea autentificării Kerberos cu serverul de directoare LDAP” pe pagina 39 pentru mai multe 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 publica informaţia OS/400 la serverul de directoare LDAP care este pe altă platformă. Trebuie să publicaţi informaţiile utilizator şi sistem la un server de directoare care foloseşte o schemă compatibilă cu Servicii director schema. Definiţiile schemei IBM SecureWay director care include iSeries Directory Services, poate fi găsită la pagina web Directory Services .

Trebuie să publicaţi partajările de tipărire la un serverul de directoare care suportă schema Microsofts Active Directory. Publicarea partajărilor de imprimantă la Active Directory permite utilizatorilor să configureze iSeries imprimantele direct de la Windows 2000 desktop cu vrăjitorul Windows 2000 Add Printer. Pentru a face asta în vrăjitorul Add Printer, specificaţi că vreţi să găsiţi o imprimantă în Windows 2000 Active Directory.

API-uri pentru publicarea OS/400 informaţiilor la serverul de directoare

Servicii director furnizează suport built-in pentru publicarea informaţiilor de utilizator şi sistem. Aceste elemente sunt listate pe pagina **Director de servicii** a dialogului sistem **Proprietăţi**. 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 pe pagina **Director de servicii** la fel. Ca utilizatori şi sistem, sunt dezactivate iniţial şi le configuraţi folosind aceeaşi procedură. Programul care adaugă datele la directorul LDAP este numit agentul de publicare. Tipul de informaţii care e publicat, cum apare pe pagina **Director de servicii**, este numit nume agent.

Următoarele API-uri vă vor permite să încorporaţi pulicarea în propriile domneavoastră programe:

QgldChgDirSvrA
O aplicaţie foloseşte formatul CSVR0500 pentru a adăuga iniţial un nume de agent care este marcat ca o intrare dezactivată. Instrucţiunile pentru utilizatorii aplicaţiei ar trebui să-i instruiască să folosească iSeries Navigator pentru a merge la pagina de proprietăţi a Directorului de servicii pentru a configura agentul de publicare. Exemple ale numelor agenţilor sunt numele agent ale sistemelor şi utilizatorilor automat disponibile la pagina **Director de servicii**.

QgldLstDirSvrA
Folosiţi acest format API LSVR0500 pentru a lista care agenţi sunt disponibili curent pe sistemul domneavoastră.

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.

Specificarea unui server pentru referinţe director

Pentru a asigna referinţe server pentru serverul de directoare, urmaţi aceşti paşi:
1. În iSeries Navigator, expandaţi **Network**.
2. Expandare **Servere**.
3. Apăsaţi **TCP/IP**.
4. Apăsaţi clic-dreapta pe **Director**, şi selectaţi **Proprietăţi**.
5. Selectaţi **Add**.
6. La prompt, specificaţi numele serverului referinţă 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 referinţă nu foloseşte portul implicit, specificaţi nuumărul corect al portului ca parte a URL-ului, ca portul 400 este specificat în al doile exemplu de mai sus.
7. Selectaţi **OK**.

Adăugarea sufixelor la serverul de directoare LDAP

Adăugarea unui sufix la serverul de directoare LDAP permite serverului să gestioneze acea parte a arborelui de directoare.

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 domneavoastră, nu puteţi adăuga ou=rochester, o=ibm, c=us.

Pentru a adăuga un sufix la serverul de directoare, urmaţi aceşti paşi:
1. În iSeries Navigator, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Apăsaţi **TCP/IP**.
4. Faceţi clic-dreapta pe **Director** şi selectaţi **Proprietăţi**.
5. Apăsaţi tabela **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.

Înlăturarea sufixelor de la serverul de directoare

Pentru a înlătura un sufix de la serverul de directoare LDAP faceţi aceşti paşi:
1. În iSeries Navigator, expandaţi **Network**.
2. Expandare **Servere**.
3. Apăsaţi **TCP/IP**.
4. Faceţi clic-dreapta pe **Directory** şi selectaţi **Proprietăţi**.
5. Apăsaţi tabela **Database/Suffixes**.
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 Servicii director

Servicii director 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.

Consultaţi Backup and Recovery, SC41-5304 pentru informaţii despre salvarea şi restaurarea datelor OS/400.

Gestionare dreptului de proprietate şi a accesului la datele directorului

Gestionare dreptului de proprietate şi a accesului la datele directorului include următoarele operaţii:
- “Lucrul cu proprietăţile dreptului de proprietate a obiectelor de directoare”
- “Lucrul cu listele de acces control (ACL)”
- “Lucrul cu grupuri ACL”

Lucrul cu proprietăţile dreptului de proprietate a obiectelor de directoare

Pentru a seta proprietăţile dreptului de proprietate a directoarelor de obiecte, urmaţi aceşti paşi:
1. În iSeries Navigator, expandaţi **Network**.
2. Expandare **Servere**.
3. Apăsaţi **TCP/IP**.
4. Apăsaţi clic-dreapta pe **Director** şi selectaţi **Autoritate**.

   Dacă nu sunteţi deja conectat la serverul de directoare, apare dialogul **Conectare la serverul de directoare** . Conectaţi-vă ca administratorul serverului sau ca proprietarul obiectului ale cărui proprietăţi vreţi să le lucraţi.
5. Din arborele directorului, selectaţi obiectul ale cărui proprietăţi vreţi să le lucraţi apoi apăsaţi **OK**.

Lucrul cu listele de acces control (ACL)

Lucrul cu listele de acces control (ACL) includ asignarea explicită şi implicită a ACL-urilor la obiectelor directorelor, adăugând utilizatori la ACL-uri, înlăturând utilizatori la ACL şi răsfoirea obiectelor director. Notaţi că începând cu V5R1 Servicii director suportă un nou model ACL, aşa încât dacă aţi folosit ACL-uri înainte veţi vrea să vă refamiliarizaţi cu ele.

Pentru a lucra cu ACL-uri, urmaţi aceşti paşi:
1. În iSeries Navigator, expandaţi **Network**.
2. Expandare **Servere**.
3. Apăsaţi **TCP/IP**.
4. Apăsaţi clic-dreapta pe **Director** şi selectaţi **Autoritate**.

   Dacă nu sunteţi deja conectat la serverul de directoare, apare dialogul **Conectare la serverul de directoare** . Conectaţi-vă ca administrator de server sau ca deţinătorul obiectului cu a cărui ACL vreţi să lucraţi.
5. Din arborele directorului, selectaţi obiectul ale cărui ACL vreţi să le lucraţi apoi apăsaţi **OK**.
6. Apăsaţi tabela **ACL**.

Lucrul cu grupuri ACL

Pentru a lucra cu Grupuri ACL , urmaţi aceşti paşi:
1. În iSeries Navigator, selectaţi **Reţea**.
2. Selectaţi **Servere**.
3. Apăsaţi **TCP/IP**.
4. Faceţi clic-dreapta pe **Director** şi selectaţi **Grupuri ACL** .

Lucrul cu accesul administrativ pentru utilizatori autorizaţi

| Începând cu in V5R2, puteţi acorda acces de administrator profilelor utilizator cărora le-a fost dat acces la
| identificatorul funcţiei Directory Services Administrator (QIBM_DIRSRV_ADMIN) (ID).

| De exemplu, dacă profilul utilizator JOHNSMITH are acordat acces la ID-ul funcţiei Directory Services
| Administrator şi acces Grant administrator la opţiunea utilizatori autorizaţi este selectat de la dialogul

Directory property profilul JOHNSMITH are autoritate de administrare LDAP. Când acest profil este folosit pentru a asocia la serverul de directoare folosnd 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 mai multe informaţii despre utilizatori proiectaţi consultaţi “Backend proiectat pe sistemului de operare” pe pagina 40.

Pentru a selecta această opţiune, urmaţi aceşti paşi:

1. În iSeries Navigator, expandaţi **Network**.
2. Expandaţi **Servere**.
3. Faceţi clic-dreapta pe **Directory** şi selectaţi **Proprietăţi**.
4. La tabela **General** sub **informaţia Administrator** , selectaţi opţiunea **Grant administrator access to authorized users**.

Pentru a seta funcţia de autoritate Directory Services Administrator ID într-un profil utilizator, urmaţi aceşti paşi:

1. În iSeries Navigator, faceţi clic-dreapta pe numele sistemului şi selectaţi **Application Administration**.
2. Apăsaţi tabela **Host Applications**.
3. Expandaţi **Operating System/400**.
4. Apăsaţi **Directory Services Administrator** pentru a evidenţia opţiunea.
5. Apsaţi butonul **Customize**.
6. Expandaţi **Users**, **Groups**, sau **Uses not in a group**, care este corespunzător pentru utilizatorul care-l vreţi.
7. Selectaţi un utilizator sau grup să fie adăugat la lista **Access allowed**.
8. Apăsaţi butonul **Adăugare**.
9. Apăsaţi **OK** pentru a salva.
10. Apsaţi **OK** pe dialogul **Application Administration**.

Urmărirea accesului şi a modificărilor la directorul LDAP

Vreţi să urmăriţi accesul şi modificările la directorul dumneavoastră LDAP. Puteţi folosi istoricul de modificări ale directoarelor LDAP pentru a ţine evidenţa modificărilor directorului. Jurnalul de modificări este localizat sub sufixul special cn=changelog. Este memorat în biblioteca QUSRDIRCL.

Pentru a activa jurnalul de modificări, urmaţi aceşti paşi:

1. În iSeries Navigator, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Apăsaţi **TCP/IP**.
4. Faceţi clic-dreapta pe **Director** şi selectaţi **Proprietăţi**.
5. Apăsaţi tabela **Bază de date/Sufixe**.
6. Selectaţi **Înregistrare modificări directoare**.
7. (opţional) În **Maxim intrări** specificaţi numărul maxim de intrări pe care le păstrază jurnalul.

   Notă: Deşi acest parametru este opţional, ar trebui să specificaţi un număr maxim de intrări. Dacă nu specificaţi un număr maxim de intrări, jurnalul de modificare 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 jurnalului de modficări sunt numai pentru citire.

Orice utilizator care este în Lista de control acces pentru sufixul cn=changelog poate căuta intrări în jurnalul 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 serverul de directoare

Servicii director suportă OS/400 auditarea securităţii. Dacă variabila de sistem QAUDCTL are specificat *OBJAUD, puteţi activa auditarea obiectului prin iSeries Navigator.

Pentru a activa auditarea obiecului pentru Servicii director, urmaţi aceşti paşi:
1. În iSeries Navigator, 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 domneavoastră.

Modificările în setările de auditare vor avea efect de îndată ce apăsaţi **OK**. Nu trebuie să reporniţi serverul de directoare LDAP. Pentru informaţii suplimentare consultaţi “Securitatea Servicii director” pe pagina 38

Ajustarea performanţei serverului de directoare LDAP

Puteţi ajusta performanţa serverului domneavoastră de directoare LDAP prin schimbarea unei din următoarele:
- Mărimea căutărilor
- Timpul maxim permis pentru căutări
- Setările de tranzacţii ale serverului
- Numărul de conexiuni bază de date şi fire de execuţie server

Pentru a ajusta valorile performanţei a serverului de directoare, urmaţi aceşti paşi:
1. În iSeries Navigator, expandaţi **Network**.
2. Expandare **Servere**.
3. Apăsaţi **TCP/IP**.
4. Faceţi clic-dreapta pe **Directory** şi selectaţi **Proprietăţi**.
5. Apăsaţi tabelul **Performanţă**.

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 iSeries Navigator, expandaţi **Network**.
2. Expandare **Servere**.
3. Apăsaţi **TCP/IP**.
4. Faceţi clic-dreapta pe **Directory** şi selectaţi **Proprietăţi**.
5. Apăsaţi tabela **Database/Suffixes**.

Capitol 5. Concepte şi informaţii de referinţă Servicii director

Următoarele informaţii conceptuale şi de referinţă vă vor ajuta să învăţaţi şi să rulaţi serverul domneavoastră LDAP Servicii director:

Pentru informaţii despre bazele LDAP şi planificarea serverul domneavoastră LDAP, consultaţi şi Capitol 3, “Începutul cu Servicii director” pe pagina 7.

Listele de control acces LDAP (ACL)

În multe cazuri, nu doriţi să restricţionaţi accesul la date pe serverul de directoare LDAP. De exemplu, un server LDAP din reţeaua Intranet a companiei dumneavoastră poate conţine un director de telefoane ale angajaţilor companiei. Probabil, doriţi ca toţi angajaţii să fie capabili să vadă datele din acest director.

Totuşi, preşedintele companiei nu vrea ca toţi angajaţii să-i aibă acces la numărul său de telefon. În acest caz, puteţi crea o **listă de control acces (ACL)**. Cu această ACL, puteţi restrânge accesul la intrarea sa de pe server doar pentru acei angajaţi de la care preşedintele doreşte să primească telefoane.

Cu ACL, puteţi controla cine are autorizarea de a adăuga şi şterge obiecte director. Puteţi de asemenea specifica dacă utilizatorii au abilitatea să citească, scrie, căuta şi compara atributele directoarelor. ACL pot fi ori moştenite sau explicite. De aceea, puteţi folosi ACL în unul din următoarele moduri:

- Să setaţi explicit o ACL pentru un anumit obiect.
- Să specificaţi că obiectele moştenesc ACL de la obiecte mai sus în ierarhia de directoare LDAP.

Poate preşedintele din exemplul anterior nu dorea ca toţi angajaţii să poată avea acces la numărul său de telefon. Dorea, totuşi, ca toţi managerii să poate avea acces la acesta. Într-un asemenea caz, puteţi utiliza un **Grup ACL** pentru a simplifica acordarea autorizării pentru manageri. Grupurile ACL vă permit să acordaţi acces unor anumite grupuri de utilizatori, mai degrabă, decât să acordaţi autorizări pe baze individuale. Acest lucru este, în mod special, util dacă acelaşi grup de persoane are nevoie de acces la mai mult de un set obiecte. Dacă aceiaşi manageri care aveau acces la numărul de telefon al preşedintelui, de exemplu, mai târziu au nevoie de acces la intrările de salarizare, puteţi refolosi grupul ACL.

Modele ACL

Toate vrsiunile de Servicii director suportă un model de permisiuni la nivel de clase de acces. În acest model, fiecare tip de atribut LDAP are o clasificare de Normal, Sensibil sau Critic. Fişierele schemă de atribute controlează aceste clasificări. Când adăugaţi un utilizator la o ACL de obiecte, specificaţi ce clasificări poate poate citi, scrie, căuta şi compara utilizatorul. În majoritatea schemelor, numărul de telefon va fi clasificat ca un atribut Normal. De aceea, pentru a da managerilor din exemplul de mai sus acces la numărul de telefon al preşedintelui, le veţi da acces de citire pentru atributele Normal din obiectul director al preşedintelui. În continuare aceştia nu vor putea accesa informaţiile Sensibile şi Critice. Toate versiunile de Servicii director suportă setarea permisiunilor la nivel de clasă de acces.

Servicii director suportă de asemenea un model de permisiuni la nivel de atribut. În acest model, puteţi specifica autorizările de citire, scriere, căutare şi comparare pentru anumite atribute, în ciuda clasei lor de acces. Consideraţi din nou exemplul de mai sus. În modelul permisiunilor la nivel de atribut, puteţi da managerilor acces la citire la atributul telephoneNumber, chiar dacă nu aveau acces la atributele Normal în general.

Modelul de permisiuni la nivel de atribut este compatibil doar cu SecureWay Servicii director versiunea 3.2 şi serverele de mai sus. Implicit aceasta nu este activată. Aveţi opţiunea de activare a sa atunci când lucraţi cu ACL-uri. După ce este activat, modelul poate fi dezactivat doar prin reconfigurarea serverului şi restaurarea bazei de date de directoare. Înainte de a vă hotărî să activaţi acest model, trebuie să cunoaşteţi că nu veţi putea să îl administraţi de la orice client LDAP V2 (inclusiv versiunile pre-V5R1 ale iSeries Navigator) şi că această încercare poate corupe intrările ACL.

Valori ACL speciale

Iniţial, toate obiectele din serverul de directoare Servicii director au un ACL care conţine un grup ACL special, CN=Anybody, care include toţi utilizatorii de directoare. Implicit acest grup are acces de citire, căutare şi comparare la atributele din clasa normal pentru toate obiectele.

Puteţi dori ca unele obiecte să aibă aceleaşi permisiuni de acces pentru toţi utilizatorii care se leagă la serverul de directoare cu o conexiune care nu este anonimă. Pentru a realiza aceasta, folosiţi grupul listă de control acces (ACL) special cn=Authenticated.

Pentru a specifica ce permisiuni de acces are un obiect pentru el, puteţi folosi DN-ul special cn=this. Aceasta dă posibilitatea intrărilor fiu care-şi moştenesc ACL-urile să fie automat autorizate pentru a realiza operaţii asupra propriilor obiecte.

Informaţii suplimentare

Pentru a administra ACL prin iSeries Navigator, nu trebuie să cunoaşteţi detaliile despre cum implementează Servicii director ACL-urile. Totuşi, dacă vreţi să specificaţi atribute legate de ACL atunci când folosiţi fişiere LDIF sau doriţi să folosiţi ACL-uri cu utilitarele în linie de comandă LDAP , va trebui să vă familiarizaţi cu attributele pe care le utilizează ACL. Pentru informaţii despre atributele ACL, consultaţi ducumentul referinţă Access Control Lists al documentaţiei IBM SecureWay Directory Management Tool .

Pentru informaţii despre setarea şi modificarea ACL-urilor şi a grupurilor ACL, urmaţi aceste legături:

“Lucrul cu listele de acces control (ACL)” pe pagina 30
“Lucrul cu grupuri ACL” pe pagina 30

Formatul de interschibare a datelor LDAP

Formatul de interschibare a datelor LDAP (LDIF) vă furnizează cu o metodă simplă de a transfera informaţiile directoarelor între serverele de directoare LDAP. Fişierele LDIF ţin intrările directorului LDAP într-un format text simplu. Formatul fişierelor LDIF pe care serverul de directoare îl foloseşte s-a schimbat începând cu V4R5 a Servicii director. Fişierele LDIF consistă dintr-o secvenţă de linii care descriu o intrare director sau un set de schimbări la o intrare director. Ele nu le pot descrie pe ambele.

Formatul general a unei intrări LDIF este:

```
version: 1
dn: distinguished name
attrtype1: attrvalue1
...
```

unde:

- *version* afişează versiunea formatului de fişiere LDIF. Numărul versiunii trebuie să fie 1. Dacă numărul de versiune este absent, fişierul LDIF este considerat a fi într-un format de fişier LDIF mai vechi. Când fişierul LDIF este versiunea 1, conţinutul TREBUIE să fie encodat UTF-8.
- *distinguished name* este nume distinctiv al intrării director
- *attrtype1* este un atribut de tip LDAP (cum ar fi cn sau ou)
- *attrvalue1* este valoarea atributului

Fiecare intrare poate avea mai multe atribute. Fiecare atribut apare într-o linie separată. Dacă o valoare atribut este mai lungă decât o singură linie, poate fi continuat pe linia următoare şi est eprecedat de un spaţiu sau caracterul tab.

Linii goale separă intrări multiple cu acelaşi fişier LDIF. Orice linie care începe cu un semnul de liră sterlină (#) este o linie de comentarii şi trebuie ignorată când se analizează un fişier LDIF.

Orice nume distinctiv sau valoare atribut care întâlneşte una din următoarele condiţii ar trebui encodată in baza 64:
- Conţine început de linie sau linie nouă.
- Poneşte cu două puncte (:), SPAŢIU sau mai-puţin-de (<).
- Se terină cu spaţiu.

Atributele encodate baza-64 sunt desemnate prin folosirea a două semne de două puncte între numele atributului şi valoare.

Referinţe externe sunt în fişierul:// format URL. Acolo ar trebui să fie caracterele două puncte şi semnul mai-puţin-de (:<) între tipul atributului şi valoarea referinţă externă.

Aici sunt câteva exemple de fişiere LDIF:

Examplul 1: Un fişier simplu LDAP cu două intrări

```
version: 1
   dn: cn=Barbara Jensen, ou=Rochester, o=Big Company, c=US
   objectclass: top
   objectclass: person
   objectclass: organizationalPerson
   cn: Barbara Jensen
   cn: Barbara J Jensen
   cn: Babs Jensen
   sn: Jensen
   uid: bjensen
   telephonenumber: +1 408 555 1212
   description: A big sailing fan.

   dn: cn=Bjorn Jensen, ou=Rochester, o=Big Company, c=US
   objectclass: top
   objectclass: person
   objectclass: organizationalPerson
   cn: Bjorn Jensen
   sn: Jensen
   telephonenumber: +1 408 555 1212
   description:Babs is a big sailing fan, and travels extensively in
   search of perfect sailing conditions.
   title:Product Manager, Rod and Reel Division
```

Exemplul 2: Un fişier conţinând o valoare encodată bază-64

```
version: 1
   dn: cn=Gern Jensen, ou=Rochester, o=Big Company, c=US
   objectclass: top
   objectclass: person
   objectclass: organizationalPerson
   cn: Gern Jensen
   cn: Gern O Jensen
```

```
   sn: Jensen
   uid: gernj
   telephonenumber: +1 408 555 1212
   description:: V2hhdCBhIGNhcmVmdWwgcmVhZGVyIHlvdSBhcmUhICBUaGlzIHZhbHVlIGlzIGJ
    hc2UtNjQtZW5jb2RlZCBiZWNhdXNlIGl0IGhhcyBhIGNvbnRyb2wgY2hhcmFjdGVyIGluIGl0ICh
    hIENSKS4NICBCeSB0aGUgd2F5LCB5b3Ugc2hvdWxkIHJlYWxseSBnZXQgb3V0IG1vcmUu
```

Examplul 3: Un fişier ce conţien o serie de înregistrări e modificare şi comentarii

Notă: Fişierele LDIF cu înregistrări de modificare nu pot fi importate direct în server. Totuţi, ele sunt suportate de utilitarele LDAP .

```
version: 1
   # Add a new entry
   dn: cn=Fiona Jensen, ou=Rochester, o=Big Company, c=US
   changetype: add
   objectclass: top
   objectclass: person
   objectclass: organizationalPerson
   cn: Fiona Jensen
   sn: Jensen
   uid: fiona
   telephonenumber: +1 408 555 1212
   jpegphoto:< file:///usr/local/directory/photos/fiona.jpg

   # Şterge o intrare existentă
   dn: cn=Robert Jensen, ou=Rochester, o=Big Company, c=US
   changetype: delete

   # Modifică o intrare relativ la numele distinctiv
   dn: cn=Paul Jensen, ou=Rochester, o=Big Company, c=US
   changetype: modrdn
   newrdn: cn=Paula Jensen
   deleteoldrdn: 1
```

Ordinea de intrări din fişierul LDIF este importantă. Pentru a adăuag cu succes o intrare care este specificată în fişierul LDIF la un director LDAP, intrarea sa părinte trebuie să fie prima existentă în directorul namespace. În exemplul de mai sus, a doua şi a treia intrare nu pot fi adăugate dacă prima intrare nu există.

Similar, pentru a importa un fişier LDIF într-un server care suportă anumite sufixe, fişierul LDIF trebue să aibă intrări pentru acele sufixe. De exemplu, dacă serverul domneavoastră a avut sufixul ou=Rochester, o=Big Company, c=US, fişierul LDIF afişat mai sus poate fi importat. Dar dacă serverul domneavoastră în locul sufixului o=Big Company, c=US, trebuie să aveţi o intrare pentru acel sufix specificat mai întâi în fişierul LDIF, aşa cum este afişat aici:

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

Formatul specific şi conţinutul fişierelor LDIF sunt determinate de schema serverului de la care sunt exportate. Puteţi importa un fişir LDIF la orice server LDAP care foloseşte o schemă identică ca şi serverul de la care fişierul a fost exportat. Vânzători diferiţi de servere LDAP folosesc scheme diferite (cu diferite clase de obiecte şi atribute). Prin urmare, s-ar putea să nu fiţi apt să importaţi un fişier LDIF care este de un server la alt server.

O Cerere pentru comentarii (RFC) pe specificaţiile fişierului LDIF este disponibilă la următorul URL:

Lhttp://www.ietf.org/rfc/rfc2849.txt

Proceduri înrudite:

“Importarea unui fişier LDIF” pe pagina 22
“Exportarea unui fişier LDIF” pe pagina 22

Consideraţii suport limbă naţională (NLS)

Începând cu V4R5, şi serverul OS/400 Serviciile de directoare LDAP şi clientul OS/400 LDAP sunt bazate pe LDAP versiunea 3. Fiţi conştient de următoarele consideraţii NLS:

- Datele sunt transferate între serverele LDAP şi clienţii în format UTF-8. Toate caracterele ISO 10646 sunt permise.
- Serverul Serviciillor de directoare LDAP foloseşte metoda de mapare UTF-16 pentru a memora date în baza de date.
- Serverul şi clientul fac comparaţii cu şiruri în cazul senzitiv. Algoritmii majuscule nu vor fi corecţi pentru toate limbile (locurile).

Pentru mai multe informaţii despre UCS-2, consultaţi subiectul Globalizare sub Planificare din Centru de informare iSeries.

Drept de proprietate a obiectelor directorului LDAP

Fiecare obiect din directorul domneavoastră 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 proprităţile dreptului de proprietate şi lista de control acces (ACL) atributele unui obiect. Dreptul de proprietate a obiectelor poate fi moştenit sau explicit. Pentru a to 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.

Servicii director 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 obiecet. 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.

Proceduri înrudite:

"Lucrul cu proprietăţile dreptului de proprietate a obiectelor de directoare" pe pagina 30

referinţe director LDAP

Referinţele permit serverelor de directoare LDAP 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 serverr LDAP.

Servicii director vă permite să folosiţi două tipuri diferite de referinţe. Puteţi specifica serverele implicite de referinţă , unde serverul LDAP va referi clienţi oricând orice DN nu este în director. Vă puteţi de asemena folosi clientul LDAP pentru a adăuga intrări le serverul de directoare care are referinţe objectClass. Aceasta vă permite să specificaţi referinţe care sunt bazate pe ce DN specific un client cere.

Notă: Cu Servicii director, referinţele obiectelor trebuie să conţină doar un nume distinctiv (dn), o objectClass (objectClass), şi o referinţă (ref). Consultaţi "Utilitarul ldapsearch" pe pagina 52 pentru un exemplu care ilustrează această restricţie.

Serverele de referinţă sunt înrudite cu serverele replică. Deoarece datele pe servere replică nu pot fi modificate de clienţi, replica referă orice cereri de a schimba datele director la master server.

Tranzacţii

Vă puteţi configura serverul de directoare LDAP al sistemului dumneavoastră pentru a permite clienţilor să folosească trranzacţii. 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.

Pentru informaţii suplimentare despre tranzacţii, consultaţi anexa Limited Transaction Support a IBM SecureWay Directory Client SDK Programming Reference Legătură în afara Centrului de informare.

Serverul de directoare replică LDAP

Informaţia memorată pe serverele de directoare replică LDAP este identică cu informaţia pe serverul de directoare LDAP principal sau master. Aici sunt două beneficii principale în a avea unul sau mai multe replici ale directorului LDAP:

- Replicile fac directoarele să caute mai rapid. În loc de a avea toţi clienţii să caute direct cereri la un singur master server, puteţi împărţi cererile între master server şi replica server.
- Replicele furnizează o copie de siguranţă la master server. Dacă master server nu este disponibil, o replică poate susţine cererile de căutare şi să furnizeze acces la datele directoarelor.

Serverele replică sunt numai citire. Când un utilizator ceautorizat încearcă să modifice o intrare la un server replică, referă cererea la servdrul de directoare master.

Proceduri înrudite:

“Setarea replica serverului de directoare” pe pagina 23

Securitatea Servicii director

Auditarea securităţii

Începând cu V5R1, Servicii director suportă auditarea securităţii 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 OS/400 înainte ca auditarea intrărilor de directoare să funcţioneze. Dacă variabila sistem QAUDCTL are specificat *OBJAUD, puteţi activa auditarea

obiectelor prin iSeries Navigator. Pentru mai multe informaţii despre auditare, consultaţi *Security - Reference*

 sau subiectul Security auditing din Centru de informare iSeries.

Autentificarea şi securitatea conexiunii

Servicii director furnizează următorul mecanism pe care-l puteţi folosi pentru a îmbunătăţi securitatea comunicaţiilor dintre cliecţii LDAP şi serverul de directoare LDAP:

- Conexiuni SSL (Secure Sockets Layer)
- Autentificare Kerberos
- Criptarea CRAM-MD5 a parolei

Folosirea Secure Sockets Layer (SSL) şi Translation Layer Security cu serverul de directoare LDAP

Pentru a face comunicaţiile serverului domneavoastră de directoare LDAP mai sigure, Servicii director poate folosi securitatea Secure Sockets Layer (SSL).

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

- Să configuraţi şi să administraţi Servicii director de la staţia domneavoastră de lucru folosind o conexiune SSL. Aceasta include operaţiile care le realizaţi de la iSeries Navigator.
- Pentru a folosi o conexiune SSL cu aplicaţii pe care le creaţi cu interfeţele program aplicaţie client (API-uri) Windows.

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 domneavoastră 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), 34 a OS/400, instalată pe sistemul domneavoastră. DCM furnizează o interfaţă pentru ca să creaţi şi să gestionaţi certificatele digitale şi memorările de certificate. Consultaţi documentaţia pentru Digital Certificate Manager pentru informaţii despre certificatele digitale şi despre folosirea DCM. Pentru informaţii despre pe iSeries, consultaţi Securizarea aplicaţiilor cu SSL. Pentru informaţii despre TLS pe serverul iSeries, consultaţi protocoalele Supported SSL şi Transport Layer Security (TLS) .

Folosirea autentificării Kerberos cu serverul de directoare LDAP

Servicii director vă permite să setaţi serverul de directoare LDAP să folosească 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 domneavoastră. Trebuie să mai aveţi configurat şi serviciul de autentificare în reţea.

Suportul Kerberos al Servicii director furnizează suport pentru mecanismul GSSAPI SASL. Aceasta dă posibilitatea clienţilor LDAP SecureWay şi Windows 2000 să folosească autentificarea Kerberos cu serverul de directoare LDAP.

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

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

nume-serviciu este LDAP, nume-gazdă este numele complet determinat TCP/IP al sistemului şi realm este domeniul implicit specificat în configuraţia sistemelor Kerberos.

De exemplu, pentru un sistem numit my-as400 din domeniul TCP/IP acme.com, cu un domeniu implicit Kerberos ACME.COM, numele de principal Kerberoes al serverului LDAP va 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). Prin convenţie, numele domeniilor Kerberos sunt scrise cu majuscule şi numele de gazdă sunt scrise cu litere mici.z LDAP/ trebuie să fie cu majuscule. Serverul de directoare nu poate fi configurat să folosească autentificarea Kerberos dacă nu a fost configurat nici un domeniu implicit.

Când eset folosită autentificarea Kerberos, serverul de directoare LDAP asociază un nume distinctiv (DN) cu conexiunea care determină acesul 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 directorul pentru o intrare care specifică această identitate Kerberos după cum urmează:
  - Serverul caută directorul pentru un obiect krbRealm-V2 care are un atribut krbRealmName-V2 care se potriveşte cu domeniul Kerberos. Dacă găseşte o asemenea intrare, apoi caută DN-urile care sunt specificate în atributul princSubtree pentru o intrare cu un atribut krbPrincipalName care se potriveşte cu numele principalului şi numele domeniului. Dacă DN-ul configurat în krbAliasedObjectName conţine DN-ul întrării găsite anterior, este foflosit DN-ul configurat în krbAliasedObjectName. Altfel, este utilizat DN-ul intrării. Acestă metodă este folosită tipic atunci când un KDC Kerberos memorează informaţiile principalului Kerberos în directorul LDAP.
  - Dacă eşuează căutarea descrisă anterior, serverul caută pentru o intrare director care foloseşte clasa auxiliară ibm-securityIdentities şi are o valoare a atributului altSecurityIdentities de KERBEROS:principal@realm. Această metodă poate fi folosită pentru a asocia identităţi Kerberos cu intrări director când KDC nu memoarează principalii în director.

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. Secţia Servicul de configurare autentiifcare reţea conţine informaţii despre adăugarea informaţiilor în fişiere tabelă de chei.

Backend proiectat pe sistemului de operare

Backend-ul proiectat pe sistem are abilitatea de a mapa obiecte OS/400 ca intrări în arborele de directoare accesibil LDAP. Obiectele proiectate sunt reprezentări LDAP ale obiectelor OS/400 în locul intrărilor memorate actual în baza de date a serverului LDAP. Cu V5R2, profilele utilizator OS/400 sunt singurele obiecte care sunt mapate sau proiectate ca intrări în arborele de directoare. Maparea obiectelor profile de utilizator este referită ca backend-ul prioectat al utilizatorului OS/400.

Operaţiile LDAP sunt mapate în obiectele de bază OS/400 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.

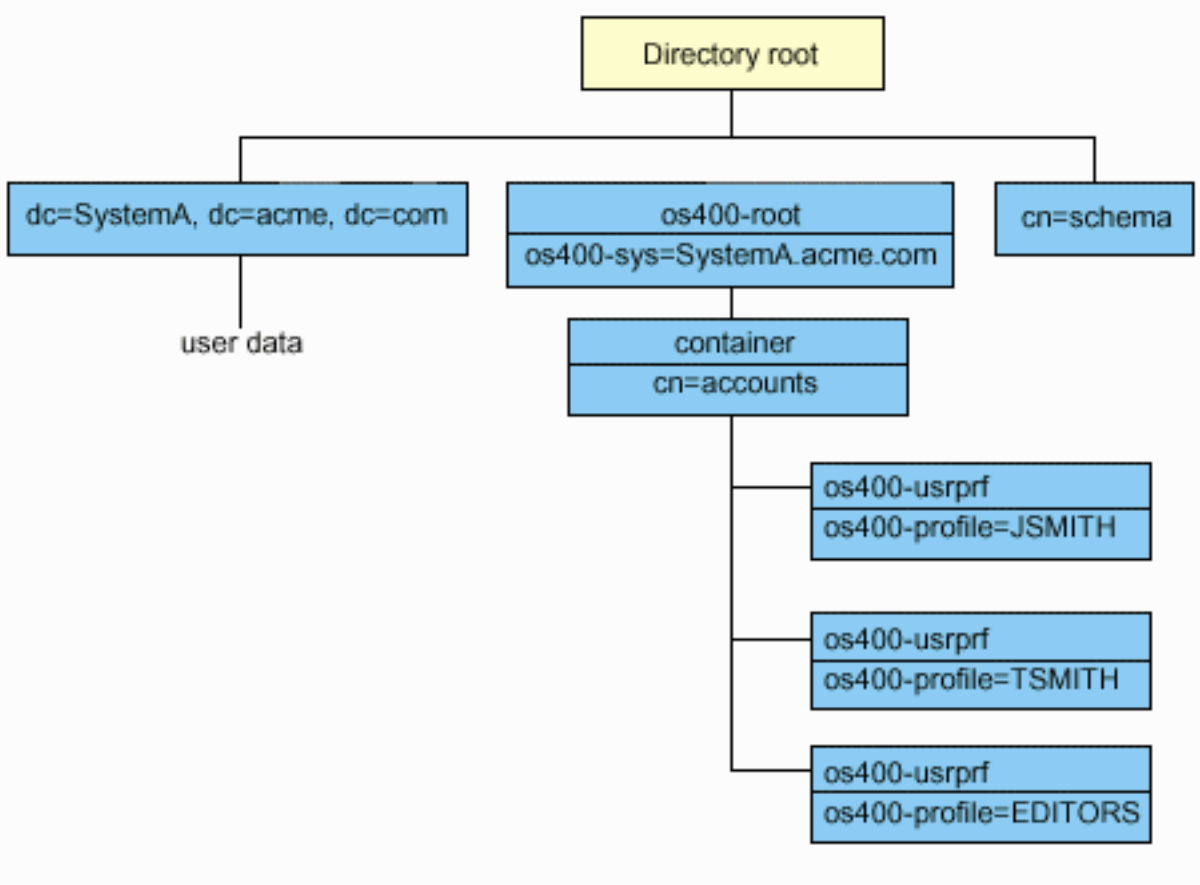
Pentru informaţii detailate despre backend-ul proiectat în sistemul de operare, consultaţi următoarele:

- “Arborele de informaţii director proiectat utilizator OS/400” pe pagina 41
- “Operaţii LDAP” pe pagina 41
- “DN-uri legate administrator şi replică” pe pagina 45
- “Schema proiectată-utilizator OS/400” pe pagina 45

Arborele de informaţii director proiectat utilizator OS/400

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 domneavoastră. Objectclass este os400-root. Deşi DIT nu poate fi modificat sau şters, puteţi reconfigura sufixul obiectelor sistem. Totuşi, trebuie să vă asiguraţi că sufixul curent nu este folosit în ACL-uri sau în altă parte în sistem unde wntries va trebui modificat.

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 îndeplinită specificând numele distinctiv al profilului de utilizator proiectat (DN) pentru DN-ul asociat şi parola OS/400 a profilului de utilizator 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. 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 1. Comporrtamentul sistemului proiectat backend 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.
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.

Tabela 1. Comporrtamentul sistemului proiectat backend pentru operaţii de căutare (continuat)

Cerere de căutare	Baza de căutare	Scopul de căutare	Filtrul de căutare	Comentarii
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 valori nume distinctive (DN), objectclass şi profil-os400 sunt returnate pentru profilele 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 1. Comporrtamentul sistemului proiectat backend pentru operaţii de căutare (continuat)

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. Consultaţi comanda Delete User Profile (DLTUSRPRF) 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

  Următoarea este o valoare de control:
  - 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 de valoarilor de control sunt următoarele:

- *NODLT: specifică faptul că profilul nu poate fi şters dacă deţine vreun obiect
- *CHGOWN SMITH: specifică să 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 după cum urmează:

```
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 ale 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 Administrare server de directoare (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” pe pagina 30.

Schema proiectată-utilizator OS/400

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 tipic cuvântul cheie al atributului (cum

ar fi CRTUSRPRF sau CHGUSRPRF) pe comenzile profilului utilizator. Consultaţi “Arborele de informaţii director proiectat utilizator OS/400” pe pagina 41 pentru informaţii suplimentare.

Servicii director şi al OS/400

Servicii director şi al OS/400

Servicii director foloseşte suportul bază de date OS/400 pentru a memora informaţii director. Servicii director foloseşte controlul commitment pentru a memora intrările director în baza de date. Acesta necesită suportul de jurnalizare OS/400.

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 domneavoastră, 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 comanda de la o linie de comandă OS/400:

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

Dacă jurnalul de modificări este configurat, îi puteţi şterge receptorii de jurnal cu următoarea comandă:

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

Penru informaţii despre comenzile de jurnalizare, consultaţi subiectul Comenzile OS/400 sun Programarea în Centru de informare iSeries.

Capitol 6. Utilitarele liniei de comandă LDAP

Servicii director include cinci utilitare care vă permit să realizaţi acţiuni pe serverul de directoare LDAP din mediul de comandă Qshell pe OS/400. Aceste utilitare folosesc API-urile LDAP Puteţi folosi aceste utilitare de la linia de comandă qsh sau să le apelaţi din programele domneavoastră. Le puteţi găsi folositoare ca exemple de programare. Când instalaţi clientul Windows LDAP care este inclus cu Servicii director, instalaţi codul care este foarte similar ca şi codul sursă pentru utilitarele shell.

Utilitarele sunt după cum urmează:
- "Utilitarele ldapmodify şi ldapadd", care adaugă şi modifică intrările directorului LDAP.
- "Utilitarul ldapdelete" pe pagina 50, care înlătură intrări din directorul LDAP.
- "Utilitarul ldapsearch" pe pagina 52, care caută directorul LDAP de intrări.
- "Utilitarul ldapmodrdn" pe pagina 56, care modifică Numele distinctiv relativ (RDN) a intrărilor de directoare LDAP.

Consultaţi "Note despre folosrea SSL cu utilitarele liniei de comandă LDAP" pe pagina 58 pentru informaţii despre folosirea SSL cu utilitarele liniei de comandă.

Utilitarele ldapmodify şi ldapadd

Utilitarul ldapmodify vă permite să modificaţi sau să adăugaţi intrări la serverul de directoare LDAP din shell-ul de comandă QSH de pe sistemul domneavoastră. Foloseşte interfeţele de programare aplicaţii (API)ldap_modify, ldap_add şi ldap_delete. Utilitarul ldapadd funcţionează aproape identic cu utilitarul ldapmodify, cu excepţia că indicatorul -a este activat automat.

Format:

ldapmodify [-a] [-V] [-b] [-c] [-r] [-M] [-n] [-v] [-F] [-R] [-C *charset***] [-d** *debuglevel***] [-D** *binddn***] [-w** *passwd* **] [-m** *mechanism***] [-O***hopcount***] [-h** *ldaphost***] [-p** *ldapport***] [-f** *file***] [-Z] [-K** *keyfile***] [-P** *keyfilepw***] [-N** *certificatename***]**

ldapadd [-V] [-b] [-c] [-r] [-M] [-n] [-v] [-F] [-R] [-C *charset***] [-d** *debuglevel***] [-D** *binddn* **] [-w** *passwd***] [-m** *mechanism***] [-O***hopcount***] [-h** *ldaphost***] [-p** *ldapport***] [-f** *file***] [-Z] [-K** *keyfile***] [-P** *keyfilepw***] [-N** *certificatename***]**

Notă: Dacă nu furnizaţi informaţii de intrare din *fişier* prin folosirea opţiunii **-f**, utilitarul va aştepta să citească intrări de la intrarea standard. Pentru a termina aşteptarea, apăsaţi tasta SysReq, apoi alegeţi 2. Terminaţi cererea anterioară.

Diagnoze:

Starea de ieşire este 0 dacă nu s-a produs nici o eroare. Erorile au ca rezultat o stare de ieşire non-zero şi un mesaj de diagnoză la ieşirea standard de eroare.

Apăsaţi aici pentru a vedea exemple de utilizare a acestor utilitare.

Parametri:

-V	Specifică versiunea LDAP pe care o foloseşte utilitarul pentru a se lega la serverul LDAP. Implicit, foloseşte o conexiune LDAP V3. Pentru a selecta explicit LDAP V3, specificaţi -V 3. Specificaţi -V 2 pentru a rula ca o aplicaţie LDAP V2.
-a	Doar ldapmodify foloseşte acest parametru. Indică faptul că utilitarul va adăuga intrări implicit mai degrabă decât să le modifice. Urilizarea acestui parametru are acelaşi efect cu folosirea ldapadd.

-b	Prosupune că orice valori care încep cu `/ sunt valori binare şi că valoarea actuală este într-un fişier a cărui cale este specificată în locul în care apar normal valorile.
-c	Modul de operare continuu. Erorile sunt raportate, dar ldapmodify sau ldapadd continuă cu modificările sau adăugirile. Implicit este să iasă după ce raportează o eroare.
-r	Înlocuieşte valorile existente cu cele implicite.
-M	Gestionează obiecte referinţă ca intrări obişnuite.
-n	Afişează ce va fi făcut, dar nu modifică intrările. Este util pentru depanarea împreună cu -v.
-v	Foloseşte modul comunicativ, cu multe diagnostice scrise la ieşirea standard.
-F	Forţează aplicarea tuturor modificărilor, în ciuda conţinutului liniilor de intrare care încep cu replica: (implicit, liniile replica: sunt comparate împotriva gazdei şi potului serverului LDAP folosite, pentru a decide dacă o înregistrare a istoricului de replicare ar trebui efectiv aplicată).
-R	Specifică faptul că referinţele nu trebuie urmate automat.
-C *charset*	Specifică faptul că şirurile furnizate ca intrare pentru utilitar sunt repreztentate într-un set local de caractere (*charset*) şi trebuie convertite la UTF-8. Folosiţi opţiunea pentru setul de caractere **-C** dacă pagina de cod a şirului de intrare este diferit de la valoarea paginii de cod a jobului. Consultaţi documentaţia pentru API-ul ldap_set_iconv_local_charset() pentru a vedea valorile suportate pentru *charset*.
-d *debuglevel*	Setează nivelul de depanare la *debuglevel*.
-D *binddn*	Folosiţi *binddn* pentru a vă lega la directorul LDAP. *binddn* ar trebui fi un DN cu reprezentre şir.
-w *passwd*	Folosiţi *passwd* ca parolă pentru autentificare.
-m *mechanism*	Folosiţi *mechanism* pentru a specifica mecanismul SASL pe care îl utilizează clientul pentru a se lega la server. Clientul foloseşte API-ul ldap_sasl_bind_s(). Mecanismele includ CRAM-MD5 (parole criptate), EXTERNAL (foloside cu SSL) şi GSSAPI (Kerberos). Comanda ignoră parametrul **-m** dacă **-V 2** este setat. Dacă nu specificaţi **-m**, este utilizată autentificarea simplă.
-O*hopcount*	Specificaţi *hopcount* pentru a seta numărul maxim de hop-uri pe care biblioteca client le va lua când urmează referinţe. Numărul de hop-uri implicit este 10.
-h *ldaphost*	Specifică o gazdă alternativă pe care rulează serverul LDAP.
-p *ldapport*	Specifică un port TCP (Transmission Control Protocol) alternativ pe care îl ascultă serverul LDAP. Portul LDAP implicit este 389. Dacă nu e specificat şi este specificat **-Z**, portul implicit este LDAP SSL 636.
-f *file*	Citeşte 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.
-Z	Foloseşte o conexiune SSL pentru a comunica cu serverul LDAP. Opţiunea **-Z** este suportată doar de versiunile cu suport SSL ale acestei unelte.
-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 determinat al fişierului bază de date de chei. Dacă utilitarul nu poate localiza baza de date de chei, va folosi un set codat hardware de rădăcini de autorităţi de certificare de încredere implicite. Fişierul bază de date chei conţine tipic unul au mai multe certificate de la 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**.
-P *keyfilepw*	Specifică parola bazei de date de chei. Acestă parolă este necesară pentru a accesa informaţiile criptate din baza de date de chei (incluzând chiea privată). Dacă este asociat un fişier de parole ascunse cu fişierul bază de date de chei, parola este obţinută din acest fişier şi acest parametru nu este necesar. Acest parametru est ignorat dacă nu este specificat nici unul dintre parametrii **-Z** sau **-K**.

-N *certificatename*	Specifică eticheta asociată cu certificatul client din fişierul bază de date chei. Notaţi că dacă serverul LDAP este configurat pentru a realiza doar autentificare server, nu mai este necesar un certificat de client. Dacă serverul LDAP este configurat pentru a realiza autentificare client şi server, este necesar un certificat client. *certificatename* nu este necesar dacă a fost asociată implicit o pereche de chei certificată/privată implicită. Similar, *certificatename* nu este necesar dacă este o singură pereche de chei certificată/privată în fişierul bază de date chei. Acest parametru est ignorat dacă nu este specificat nici unul dintre parametrii **-Z** sau **-K**.

Format de intrare alternativ:

Utilitarul ldapmodify suportă un format de intrare alternativ pentru a menţine compatibilitatea cu versiunile mai vechi ale utilitarului. Acest format constă din una sau mai multe intrări care sunt separate de linii goale. Fiecare intrare are următorul format:

```
Nume distinctiv (DN)
attr=value
[attr=value...]
```

unde *attr* este numele atributului şi *value* este valoarea. Implicit, valorile sunt adăugate. Dacă daţi indicatorul de linie de comandă **-r**, implicit este să se înlocuiască valorile existente cu cea nouă. Notaţi că este permis pentru un attribut dat să apară de mai multe ori (de exemplu, puteţi adăuga mai mult de o valoare pentru un atribut). Notaţi de asemnea că puteţi folosi un backslash (\) pentru a continua valori de-a lungul liniilor şi pentru a păstra linii noi în valoarea însăşi. Pentru a înlătura o valoare, precedaţi valoarea *attr* cu o liniuţă (-). Semmnul de egal (=) şi valoarea trebuie omise pentru a înlătura un întreg atribut. *attr* trebuie precedat de un semn plus (+) pentru a adăuga o valoare în prezenţa indicatorului **-r**.

Exemple: ldapmodify şi ldapadd

Exemplul 1:

Dacă 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:< file:///tmp/modme.jpeg
-
delete: description
-
```

comanda ldapmodify -b -r -f /tmp/entrymods va face următoarele:

- Înlocuieşte conţinutul intrărilor atribut mail Modify Me cu valoarea modme@student.of.life.edu.
- Adaugă un titlu de Grand Poobah.
- Adaugă conţinutul fişierului /**tmp**/**modme.jpeg** ca jpegPhoto.
- Înlătură complet atributul description.

Puteţi reliza acelesşi modificări ca mai sus cu fostul format de intrare al 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
```

Comanda pentru utilizarea fostului format ar fi:

```
ldapmodify -b -r -f /tmp/entrymods
```

Exemplul 2:

Se presupune că fişierul /**tmp**/**newentry** există şi are următorul conţinut:

```
dn: cn=John Doe, o=University of Higher Learning, c=US
objectClass: person
cn: John Doe
cn: Johnny
sn: Doe
title: Manager
mail: johndoe@student.of.life.edu
uid: jdoe
```

Comanda ldapadd -f /tmp/entrymods va adăuga o nouă intrare pentru John Doe, folosind valorile din fişierul /tmp/newentry.

Exemplul 3:

Dacă fişierul /**tmp**/**newentry** există şi are conţinutul:

```
dn: cn=John Doe, o=University of Higher Learning, c=US
changetype: delete
```

Comanda ldapmodify -f /tmp/entrymods va înlătura intrarea pentru John Doe.

Utilitarul ldapdelete

Utilitarul ldapdelete vă permite să ştergeţi una sau mai multe intrări de la un server de directoare LDAP. Rulează prin shell-ul de comandă QSH pe OS/400. Foloseşte interfaţa de program a aplicaţiei ldap_delete (API).

Format:

ldapdelete [-V] [-M] [-n] [-v] [-c] [-R] [-C charset] [-d *debuglevel***] [-f** *file***] [-D** *binddn***] [-w** *passwd***] [-m** *mechanism***] [-O** *hopcount***] [-h** *ldaphost***] [-p** *ldapport***] [-Z] [-K** *keyfile***] [-P** *keyfilepw***] [-N** *certificatename***] [***dn***]...**

Notă: Dacă nu furnizaţi argumente *dn*, comanda ldapdelete va aştepta să citească o listă de DN-uri de la intrarea standard. Pentru a termina aşteptarea, apăsaţi tasta SysReq, apoi alegeţi 2. Terminaţi cererea anterioară.

Diagnostic:

Starea de ieşire este 0 dacă nu a apărut nici o eroare. Rezultatele de eroare dintr-o stare de ieşire non-zero şi un mesaj diagnostic au fost scrise la eroarea standard.

Apăsaţi here pentru a vedea exemple cu folosirea utilitarului ldapdelete.

Parametri:

-V	Specifică versiunea LDAP pe care utilitarul o foloseşte pentru a se asocia la serverul LDAP. Implicit, foloseşte o conexiune LDAP V3. Pentru a selecta explicit LDAP V3, specificaţi -V 3. Specificaţi -V 2 pentru a rula ca o aplicaţie LDAP V2.
-M	Gestionează obiecte referinţă ca intrări obişnuite.

-n	Afişează ce va fi făcut dar nu şterge intrări. Folositoare pentru depanarea în conjuncţie cu **-v**.
-v	Foloseşte modul comunicativ, cu multe diagnostice scrise la ieşirea standard.
-c	Modul de operare continuu. Erorile sunt reportate, dar ldapdelete va continua cu ştergerile. Implicit este să iasă după ce raportează o eroare.
-R	Specifică faptul că referinţele nu trebuiesc automat urmate.
-C *charset*	Specifică nuumele distinctive (DNs) livrate ca intrare pentru utilitarul ldapdelete sun reprezentate în setul de caractere local (*charset*). Folosiţi **-C** *charset* pentru a înlocui implicitul, unde şirurile trebuiesc livrate în UTF-8. Folosiţi opţiunea **-C** dacă şirul de intrare pagină de cod este diferit de la valoarea pagină de cod job. Consultaţi documentaţia pentru ldap_set_iconv_local_charset() API pentru a vedea valorile suportate *charset*.
-d *debuglevel*	Setează nivelul de depanare la *debuglevel*.
-f *file*	Citeşte o serie de linii din *fişier*, realizând o ştergere LDAP pentru fiecare linie din fişier. Fiecare linie din fişier ar trebui să conţină un singur nume distinctiv (DN).
-D *binddn*	Folosiţi *binddn* pentru a asocia la directorul LDAP. *binddn* ar trebui fi un DN reprezentat-şir.
-w *passwd*	Folosiţi *passwd* ca parolă pentru autentificare.
-m *mechanism*	Folosiţi *mechanism* pentru a specifica mecanismul SASL de folosit pentru a asocia la server.Va fi folosit ldap_sasl_bind_s() API used. Mecanismele includ CRAM-MD5 (parole criptate), EXTERNAL (foloside cu SSL) şi GSSAPI (Kerberos). Parametrul -m este ignorat dacă -V 2 este setat. Dacă **-m** nu este specificat, este folosită autentificarea simplă.
-O *hopcount*	Specificaţi *hopcount* pentru a seta numărul maxim de hop-uri pe care biblioteca client le va lua când se urmează referinţe.Numărul de hop-uri implicit este 10.
-h *ldaphost*	Specifică o gazdă alternativă pe care rulează serverul LDAP.
-p *ldapport*	Specifică un port Transmission Control Protocol (TCP) alternativ pe care serverul LDAP îl ascultă. Portul LDAP implicit este 389. Dacă nu e specificat şi **-Z** este specificat, portul implicit este LDAP SSL 636.
-Z	Foloseşte o conexiune SSL pentru a comunica cu serverul LDAP. Opţiunea **-Z** este suportată doar de versiunile SSL-activate ale acestui instrument.
-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 determinat. 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**.
-P *keyfilepw*	Specifică parola bazei de date chei. Acestă parolă este necesară pentru a accesa informaţiile criptate din bază de date chei (incluzând chiea privată). Dacă un fişier ascunzător de parole este asociat cu fişierul bază de date chei, parola este obţinută din fişierul ascunzătoare şi acest parametru nu este necesar. Acest parametru est ignorat dacă nici unul din **-Z** sau **-K** nu sunt specificaţi.
-N *certificatename*	Specifică eticheta asociată cu certificatul client din fişierul bază de date chei. Notaţi că dacă serverul LDAP este configurat pentru a realiza doar Server Authentication, nu mai este necesar un certificat client. Dacă serverul LDAP este configurat pentru a realiza Client şi Server Authentication, este necesar un certificat client. *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 est ignorat dacă nici unul din **-Z** sau **-K** nu sunt specificaţi.
dn	Specifică unul sau mai multe argumente *dn*. Fiecare *dn* ar trebui să fie DN reprezentat-şir.

Exemplu: ldapdelete

Următoarea comandă va încerca să şteargă intrarea numită cu commonName Delete Me direct de mai jos de intrarea organizaţională University of Life:

```
ldapdelete cn=Delete Me, o=University of Life, c=US
```

Poate fi necesar să furnizaţi o *binddn* şi *passwd* (consultaţi opţiunile **-D** şi **-w**).

Utilitarul ldapsearch

Utilitarul ldapsearch vă permite să căutaţi o intrare pe serverul domneavoastră de directoare LDAP de la interfaţa de comandă QSH pe OS/400. Acesta foloseşte interfaţa de programare aplicaţii ldap_search (API).

Căutarea foloseşte un filtru care se conformează cu reprezentarea şir pentru filtrele LDAP. Pentru mai multe informaţii despre filtrele de căutare LDAP, conultaţi informaţiile ldap_search API din subiectul Directorul de servicii OS/400 sub Programarea în Centru de informare iSeries.

Dacă utilitarul ldapsearch găseşte una sau mai multe intrări, extrage atributele care sunt specificate de *attrs* şi tipăreşte intrările şi valorle la ieşirea standard. Dacă nu listaţi vreun atribut, acesta întoarec toate atributele.

Format:

ldapsearch [-V] [-n] [-v] [-t] [-A] [-B] [-L] [-M] [-R] [-C *charset***] [-d** *debuglevel***] [-F** *sep***] [-f** *file***] [-D** *binddn***] [-w** *bindpasswd***] [-m** *mechanism***] [-O** *hopcount***] [-h** *ldaphost***] [-p** *ldapport***] [-Z] [-K** *keyfile***] [-P** *keyfilepw***] [-N** *certificatename***] [-b** *searchbase***] [-s** *scope* **] [-a** *deref***] [-l** *time limit***] [-z** *size limit***]** *filter* **[***attrs...***]**

Diagnostic:

Starea de ieşire este 0 dacă nu a apărut nici o eroare. Rezultatele de eroare dintr-o stare de ieşire non-zero şi un mesaj diagnostic au fost scrise la eroarea standard.

Format de ieşire:

Dacă ldapsearch găseşte una sau mai multe intrări, acesta scrie fiecare intrare la ieşirea standard în forma:

```
Nume distinctiv (DN)
attributename=value
attributename=value
attributename=value
...
```

Intrările multiple sunt separate cu o singură linie goală. Dacă folosiţi opţiunea **-F** pentru a specifica un caracter separat, ieşirea afişează acel caracter în locul caracterului egal (=). Dacă folosiţi opţiunea **-t**, numele fişierului temporar înlocuieşte valoarea actuală. Dacă specificaţi opţiunea **-A**, doar partea attributename este scrisă.

Apăsaţi aici pentru a cedea exemple despre folosirea utilitarului ldapsearch.

Parametri:

-V	Specifică versiunea LDAP pe care utilitarul o foloseşte pentru a se asocia la serverul LDAP. Implicit, foloseşte o conexiune LDAP V3. Pentru a selecta explicit LDAP V3, specificaţi -V 3. Specificaţi -V 2 pentru a rula ca o aplicaţie LDAP V2.
-n	Afişează ce va fi făcut dar nu realizază căutarea. Folositoare pentru depanarea în conjuncţie cu **-v**.
-v	Foloseşte modul comunicativ, cu multe diagnostice scrise la ieşirea standard.

-t	Scire valorile extrase într-un set de fişiee temporare. Aceasta este folositoare pentru manipularea valorilor binare cum ar fi jpegPhoto sau audio.
-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	A nu se suprima afişarea valorilor binare. Aceasta este folositoare când se manipulează valori care apar în seturi alternative de caractere cum ar fi ISO-8859.1. Această opţiune este implicată de **-L**
-L	Afişează rezultatele căutării în format LDIF. Această opţiune activează de asemenea opţiunea **-B**, şi cauzează opţiunea **-F** să fie ignorată.
-M	Gestionează obiecte referinţă ca intrări obişnuite.
-R	Specifică faptul că referinţele nu trebuiesc automat urmate.
-C *charset*	Specifică care şiruri furnizate ca intrare la utilitarul ldapsearch sunt reprezentate în setul local de caractere (*charset*). Intrările şir include filtrul, asocierea DN şi DN-ul bază. Similar, când se afizează date, ldapsearch va converti datele primite de la serverul LDAP la caracterele specificate. Folosiţi opţiunea **-C** dacă şirul de intrare pagină de cod este diferit de la valoarea pagină de cod job. Consultaţi documentaţia pentru ldap_set_iconv_local_charset() API pentru a vedea valorile suportate *charset*.De asemenea, dacă opţiunea -C şi -L sunt specificate, intrarea este asumată să fie în setul specificat de caractere dar ieşirea de la ldapsearch este întotdeauna păstrat în reprezentarea sa UTF-8, sau o reprezentare encodată-64 a datelor când sunt detectate caractere ne-tipăribile. Acesta este cazul de când fişierele standard LDIF conţin doar UTF-8 (sau encodate-64 UTF-8) reprezentări a datelor şir.
-d *debuglevel*	Setează nivelul de depanare la *debuglevel*.
-F *sep*	Folosiţi *sep* ca separator de câmp între numele şi valorile atributului. Separatorul implicit este `=, doar dacă flagul **-L** a fost specificat caz în care această opţiune este ignorată.
-f *file*	Citeşte o serie de linii din realizând o căutare LDAP pentru fiecare linie din fişier. Fiecare linie din fişier ar trebui să conţină un singur nume distinctiv (DN).
-D *binddn*	Folosiţi *binddn* pentru a asocia la directorul LDAP.*binddn* ar trebui fi un DN reprezentat-şir.
-w *passwd*	Folosiţi *passwd* ca parolă pentru autentificare.
-m *mechanism*	Folosiţi *mechanism* pentru a specifica mecanismul SASL de folosit pentru a asocia la server.Va fi folosit ldap_sasl_bind_s() API used. Mecanismele includ CRAM-MD5 (parole criptate), EXTERNAL (foloside cu SSL) şi GSSAPI (Kerberos). Parametrul **-m** este ignorat dacă **-V** 2 este setat. Dacă **-m** nu este specificat, este folosită autentificarea simplă.
-O *hopcount*	Specificaţi *hopcount* pentru a seta numărul maxim de hop-uri pe care biblioteca client le va lua când se urmează referinţe.Numărul de hop-uri implicit este 10.
-h *ldaphost*	Specifică o gazdă alternativă pe care rulează serverul LDAP.
-p *ldapport*	Specifică un port Transmission Control Protocol (TCP) alternativ pe care serverul LDAP îl ascultă. Portul LDAP implicit este 389. Dacă nu este specificat şi **-Z** este specificat, portul implicit LDAP Secure Sockets Layer (SSL) 636 este folosit.
-Z	Foloseşte o conexiune SSL pentru a comunica cu serverul LDAP. Opţiunea **-Z** este suportată doar de versiunile SSL-activate ale acestui instrument.
-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 determinat. Dacă utilitarul nu poate localiza baza de date de chei, va folosi un set hard-codced 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**.

-P *keyfilepw*	Specifică parola bazei de date chei. Acestă parolă este necesară pentru a accesa informaţiile criptate din bază de date chei (incluzând chiea privată). Dacă un fişier ascunzător de parole este asociat cu fişierul bază de date chei, parola este obţinută din fişierul ascunzătoare şi acest parametru nu este necesar. Acest parametru est ignorat dacă nici unul din **-Z** sau **-K** nu sunt specificaţi.
-N *certificatename*	Specifică eticheta asociată cu certificatul client din fişierul bază de date chei. Notaţi că dacă serverul LDAP este configurat pentru a realiza doar Server Authentication, nu mai este necesar un certificat client. Dacă serverul LDAP este configurat pentru a realiza Client şi Server Authentication, este necesar un certificat client. *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 est ignorat dacă nici unul din **-Z** sau **-K** nu sunt specificaţi.
-b *searchbase*	Folosiţi *searchbase* ca punct de plecare pentru căutare în locul implicitului. Dacă **-b** nu este specificat, acest utilitar va examina mediul variabilei LDAP_BASEDN pentru o definiţie *searchbase*.
-s *scope*	Specifică scopul căutării. *scope* ar trebui să fie una din base, one sau sub pentru a specifica un obiect bază, un-nivel sau o căutare subarbore. Implicit este sub.
-a *deref*	Specifică cum diferenţierea alias-urilor. *deref* ar trebui să fie una din niciodată, întotdeauna, căutare sau căutaţi să specificaţi dacă alias-urile nu sunt niciodată diferenţiate, totdeauna diferenţiate, diferenţiate când se caută sau diferenţiate doar când se localizează obiectul bază pentru căutare. Implicit este ca niciodată să nu se diferenţieze alias-urile.
-l *timelimit*	Aşteaptă cel mult *timelimit* secunde pentru ca o căutare să se facă.
-z *sizelimit*	Limitează rezultatele căutării la cel mult *sizelimit* intrări. Aceasta îl face posibil de plasat legat sus de numărul de intrări care sunt întoarse pentru o operaţie de căutare.
filter	Specifică numele filtrului pe care le foloseşte căutarea.
attrs...	Specifică atributele pe care utilitarul le extrage dacă căutarea găseşte una sau mai multe intrări. Dacă nu listaţi vreo valoare pentru *attrs*, utilitarul întoarce toate atributele.

Exemple: ldapsearch

Exemplul 1:

Comanda ldapsearch cn=john parte a cn telephoneNumber realizează o căutare subarbore (folosind baza implicită de căutare) pentru intrări cu un commonName al părţii john . Căutarea extrage valorile commonName şi valorile telephoneNumber şi le tipăreşte la ieşirea standard. Dacă căutarea găseşte două intrări, ieşirea arată similar cu aceasta:

```
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
```

Exemplul 2:

Comanda ldapsearch -t uid=jed jpegPhoto audio realizează căuatare subarbore folosind baza implicită de căutare pentru intrări cu ID-ul utilizator al jed. Căutarea extrage jpegPhoto şi valorile audio şi le scrie în fişierele temporare. Dacă căutarea găseşte o intrare cu o valoare pentru fiecare din atributele cerute, ieşirea arată similar cu aceasta:

```
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
```

Example 3:

Comanda ldapsearch -L -s one -b c=US o=university* o description realizează o căutare un-nivel la vivelul c=US. Această căutare caută toate organizaţiile ale căror organizationName începe cu university. Căutarea îşi afişează rezultatele în format LDIF. Aceasta extrage valoarea atributului organizationName şi valoarea descripţiei atributului şi le tipăreşte la ieşirea standard care arată similar 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
...
```

Exemplul 4:

Aşa cum s-a discustat în “referinţe director LDAP” pe pagina 37, Servicii director directoarele LDAP pot conţine obiecte referinţă, furnizând din ce conţin doar următoarele:

- Un nume distinctiv (dn).
- O objectClass (objectClass).
- Un atribut referinţă (ref).

Acest exemplu demonstrează căutările unde un obiect referinţă este implicat.

Presupunem că System_A conţine intrarea referinţă:

```
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 se afle 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 şi nu trimite controlul manageDsaIT atunci serverul întoarce o referinţă. De exemplu, prin folosirea -M pe ldapsearch serverul LDAP pe System_A răspunde la client cu următorul URL:

```
ldap://System_B:389/cn=Barb Jensen,
 ou=Rochester, o=Big Company, c=US
```

Clientul foloseşte această informaţie pentru a emite o cerere la System_B. Dacă intrarea pe System_A conţine atribute în plus faţă de dn, objectclass, şi ref, serverul ignoră acele atribute.

Când clientul primeşte un răspuns referinţă de la un server, acesta emite cererea din nou, de această dată server-ului la care se referă URL-urile returnate. Dacă căutarea a fost realizată cu domeniul onelevel, ererea referinţă necesită domeniul bază. Rezultatele acestei căutări variază depinzând de valoarea pe care o specificaţi pentru domeniul căutării (**-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 se află în sau sub ou=Rochester, o=Big Company, c=US pe ambele System_A şi System_B. Clientul primeşte o referinţă de la System_A şi caută System_B, întorcând cn=Barb Jense,ou=Rochester,o=Big Company,c=US.

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 loc, serverul întoarce URL-ul referinţă la client:

```
ldap://System_B:389/cn=Barb Jensen,
  ou=Rochester, o=Big Company, c=US??base
```

Clientul în schimb lansează o cerere:

```
 ldapsearch -h System_B -b cn=Barb Jensen, ou=Rochester, o=Big Company, c=US
     -s base sn=Jensen
```

Aceasta întoarce intrarea cn=Barb Jensen,ou=Rochester,o=Big Company,c=US.

Utilitarul ldapmodrdn

Utilitarul ldapmodrdn vă permite să modificaţi Numele distinctiv relativ (RDN) a intrărilor serverului de directoare LDAP. Îl felosiţi de la shell-ul de comandă QSH pe OS/400. Se foloseşte interfaţa program aplicaţi ldap_modrdn (API).

Format:

ldapmodrdn [-V] [-r] [-M] [-n] [-v] [-c] [-R] [-C *charset***] [-d** *debuglevel***] [-D** *binddn***] [-w** *passwd***] [-m** *mechanism***] [-O** *hopcount***] [-h** *ldaphost***] [-p** *ldapport***] [-Z] [-K** *keyfile***] [-P** *keyfilepw***] [-N** *certificatename***] [-f** *file* **] [***dn rdn***]**

Note:

1. Dacă daţi argumentele liniei de comandă *dn* şi *rdn*, *rdn* va înlocui RDN-ul intrării care este specificat de DN, *dn*. Altfel, conţinutul fişierului (sau intrarea standard dacă nu daţi flagul **-f**) ar trebui să consiste din una sau mai multe intrări.

   ```
   Nume distinctiv (DN)

   Nume distinctiv relativ (RDN)
   ```

   Una sau mai multe linii goale separă fiecare pereche DN/RDN.
2. Dacă nu furnizaţi informaţiile intrării de la *fişier* prin folosirea opţiunii **-f** (sau de la perechea liniei de comandă *dn* şi *rdn*), comanda ldapmodrdn va aşteăta să citească intrtări de la intrarea standard. Pentru a termina aşteptarea, apăsaţi tasta SysReq, apoi alegeţi 2. Terminaţi cererea anterioară.

Diagnostic:

Starea de ieşire este 0 dacă nu a apărut nici o eroare. Rezultatele de eroare dintr-o stare de ieşire non-zero şi un mesaj diagnostic au fost scrise la eroarea standard.

Apăsaţi aici pentru a vedea un exemplu de folosirea utilitarului ldapmodrdn.

Parametri:

-V	Specifică versiunea LDAP pe care utilitarul o foloseşte pentru a se asocia la serverul LDAP. Implicit, foloseşte o conexiune LDAP V3. Pentru a selecta explicit LDAP V3, specificaţi -V 3. Specificaţi -V 2 pentru a rula ca o aplicaţie LDAP V2.
-r	Înlătură valorule vechiului nume distinctiv relativ (RDN) de la intrare. Implicit este de a păstra vechile valori.
-M	Gestionează obiecte referinţă ca intrări obişnuite.
-n	Afişează ce va fi făcut dar nu modifică intrări. Folositoare pentru depanarea în conjuncţie cu **-v**.
-v	Foloseşte modul comunicativ, cu multe diagnostice scrise la ieşirea standard.
-c	Modul de operare continuu. Erorile sunt reportate, dar ldapmodrdn va continua cu modificarea. Implicit este să iasă după ce raporteză o eroare.
-R	Specifică faptul că referinţele nu trebuiesc automat urmate.
-C *charset*	Specifică faptul că şirurile furnizate ca intrare la utilitar sunt repreztentate într-un set local de caractere (*charset*) şi trebuie convertit la UTF-8. Folosiţi opţiunea **-C** dacă şirul de intrare pagină de cod este diferit de la valoarea pagină de cod job. Consultaţi documentaţia pentru ldap_set_iconv_local_charset() API pentru a vedea valorile suportate *charset*.
-d *debuglevel*	Setează nivelul de depanare la *debuglevel*.
-D *binddn*	Folosiţi *binddn* pentru a asocia la directorul LDAP. *binddn* ar trebui fi un DN reprezentat-şir.
-w *passwd*	Folosiţi *passwd* ca parolă pentru autentificare.
-m *mechanism*	Folosiţi *mechanism* pentru a specifica mecanismul SASL de folosit pentru a asocia la server.Va fi folosit ldap_sasl_bind_s() API used. Mecanismele includ CRAM-MD5 (parole criptate), EXTERNAL (foloside cu SSL) şi GSSAPI (Kerberos). Parametrul -m este ignorat dacă -V 2 este setat. Dacă **-m** nu este specificat, este folosită autentificarea simplă.
-O *hopcount*	Specificaţi *hopcount* pentru a seta numărul maxim de hop-uri pe care biblioteca client le va lua când se urmează referinţe.Numărul de hop-uri implicit este 10.
-h *ldaphost*	Specifică o gazdă alternativă pe care rulează serverul LDAP.

-p *ldapport*	Specifică un port Transmission Control Protocol (TCP) alternativ pe care serverul LDAP îl ascultă. Portul LDAP implicit este 389. Dacă nu e specificat şi **-Z** este specificat, portul implicit este LDAP SSL 636.
-Z	Foloseşte o conexiune SSL pentru a comunica cu serverul LDAP. Opţiunea **-Z** este suportată doar de versiunile SSL-activate ale acestui instrument.
-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 determinat. 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**.
-P *keyfilepw*	Specifică parola bazei de date chei. Acestă parolă este necesară pentru a accesa informaţiile criptate din bază de date chei (incluzând chiea privată). Dacă un fişier ascunzător de parole este asociat cu fişierul bază de date chei, parola este obţinută din fişierul ascunzătoare şi acest parametru nu este necesar. Acest parametru est ignorat dacă nici unul din **-Z** sau **-K** nu sunt specificaţi.
-N *certificatename*	Specifică eticheta asociată cu certificatul client din fişierul bază de date chei. Notaţi că dacă serverul LDAP este configurat pentru a realiza doar Server Authentication, nu mai este necesar un certificat client. Dacă serverul LDAP este configurat pentru a realiza Client şi Server Authentication, este necesar un certificat client. *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 est ignorat dacă nici unul din **-Z** sau **-K** nu sunt specificaţi.
-f *file*	Citeşte informaţiile intrare modificate de la un LDIF file în locul intrării standard sau linia de comandă (prin specificarea *dn* şi a noului *rdn*). Intrarea standard poate fi furnizată de asemenea de la un fişier (< file).
dn rdn	Specifică numele distinctiv al unei intrări pentru a redenumi şi noul nume distinctiv relativ pentru o intrare.

Exemplu: ldapmodrdn

Asumaţi că aţi creat deja următorul fişier /**tmp**/**entrymods** şi are următorul conţinut:

```
cn=Modify Me, o=University of Life, c=US
cn=The New Me
```

Următoarea comandă:

```
ldapmodrdn -r -f /tmp/entrymods
```

va modifica RDN-ul al intrării Modify Me de la Modify Me la The New Me. Vechiul cn, Modify Me va fi înlăturat.

Note despre folosrea SSL cu utilitarele liniei de comandă LDAP

Pentru a folosi caracteristicele Secure Sockets Layer (SSL) ale utilitarelor liniei de comandă, trebuie să aveţi instalat una din Cryptographic Access Provider Products (5722-ACx).

“Folosirea Secure Sockets Layer (SSL) şi Translation Layer Security cu serverul de directoare LDAP” pe pagina 39 discuţii folosind SSL cu Servicii director serverul LDAP. Această informaţie include estionarea şi crearea Autorităţilor certificate 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 certificate de încredere (CAs). 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 asocia la serverul de directoare. De exemplu, dacă serverul LDAP foloseşte un certificat high-assurance 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-ul 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 asocia 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.

Capitol 7. Depanare Servicii director

Din păcate, chiar serverele de încredere cum ar fi Servicii director serverul LDAP au câteodată probleme. Când serverul de directoare LDAP are probleme, următoarele informaţii vă pot ajuta să aflaţi ce e greşit şi cum să reparaţi problema.

- “Procedura elementară de depanare pentru Servicii director”
- “Erori comune client LDAP” pe pagina 63

Pentru informaţii suplimentare despre Servicii director problemele comune, consultaţi Servicii director pagina home  la următorul URL:

`http://www.iseries.ibm.com/ldap`

Procedura elementară de depanare pentru Servicii director

Puteţi găsi codurile de întoarcere pentru erorile LDAP în fişierul ldap.h, care este localizat pe sistemul domneavoastră în QSYSINC/H.LDAP.

Când aveţi o eroare pe serverul domneavoastră de directoare LDAP şi vreţi mai multe detalii altă acţiune de luat este de a vedea jurnalul job QDIRSRV . Pentru erorile reproducibile, puteţi folosi comanda Trace TCP/IP Application (TRCTCPAPP APP(*DIRSRV)) pentru a rula o urmă a erorilor. Consultaţi “Folosirea TRCTCPAPP pentru a ajuta la găsirea problemelor” pe pagina 62 pentru mai multe informaţii.

Servicii director foloseşte mai multe servere Structured Query Language (SQL). Când apare o eroare SQL jurnalul job QDIRSRV va conţine uzual următorul mesaj:

```
SQL error -1 occurred
```

În aceste situaţii jurnalul job QDIRSRV vă va reeri la jurnalul job server SQL. Totuşi, în unele cazuri QDIRSRV poate să nu conţină acest mesaj şi această referinţă, chiar dacă un server SQL este cauza problemei. În aceste instanţe, vă va ajuta să ştiţi care servere SQL at trebui pornite, şi la ce le foloseşte Servicii director.

Când serverul de directoare LDAP porneşte normal, generează mesaje similare cu următoarele:

Notă: Mesajele şi numărul joburilor server SQL pornite poate diferi în oricare din următoarele cazuri:

- Porniţi serverul penru prima dată.
- Trebuie să apară migrarea.
- Serverul domneavoastră foloseşte jurnal de modificări.
- Serverul domneavoastră este setat pentru a permite un număr mai mare de conexiuni bază de date.

```
                                                        Sistem:   WARMERS
 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.
     Serverul Directorul de servicii pornit cu succes.
```

Servicii director foloseşte primul server SQL, 057448/QUSER/QSQSRVR, în timpul pornirii serverului LDAP. Servicii director poate porni servere SQL suplimentare în timpul pornirii serverului LDAP necesar dacă vă porniţi serverul pentru prima dată dacă trebuie să apară migrarea sau dacă serverul domneavoastră foloseşte jurnalul de modificare. După pornire, aceste servere SQL sunt abandonate.

În acest exemplu, nu au fost folosite severe SQL suplimentare pentru migrarea sau pornirea serverului şi jurnalul de modificări nu este configurat. Servicii director foloseşte următorul server SQL (057340/QUSER/QSQSRVR) pentru replicare.

Ultima conexiune din acest exemplu (057288/QUSER/QSQSRVR) este folosită pentru adăugare, modificare, modrdn şi ştergere. Cealalte conexiuni sunt folosite penru căutare, asociere şi comparare.

Pe serverele de directoare **Database**/**Suffixes** în pagina Proprietăţi iSeries Navigator specificaţi numărul total de servere SQL decât Servicii director foloseşte pentru operaţii cu directoare după pornirea serverului. În plus, un server SQL este întotdeauna configurat pentru replicare.

Monitorizarea erorilor şi accesul cu Servicii director jurnalul job

Vizualizarea jurnalului job pentru serverul domneavoastră LDAP vă poate alerta la erori şi să vă ajute să monitorizaţi accesul la server.

Dacă serverul domneavoastră este pornit, urmaţi aceşti paşi pentru a vizualiza juranul job QDIRSRV:
1. În iSeries Navigator, expandaţi **Network**.
2. Expandare **Servere**.
3. Apăsaţi **TCP/IP**.
4. Apăsaţi clic-dreapta pe **Director** şi selectaţi **Server jobs**.
5. Din meniul **Fişier**, alegeţi **Jurnalul Job** .

Dacă serverul domneavoastră este oprit, urmaţi aceşti paşi pentru a vizualiza juranul job QDIRSRV:
1. În iSeries Navigator, expandaţi **Operaţii elementare** .
2. Apăsaţi **Ieşire imprimantă** .
3. QDIRSRV apare în coloana **Utilizator** a panoului dreapta al iSeries Navigator. Pentru a vizualiza juranlul job, faceţi dublu-clic pe **Qpjoblog** în stânga QDIRSRV în aceeaşi linie.

   Notă: iSeries Navigator 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: Servicii director foloseşte alte resurse sistem pentru a realiza unele operaţii. Dacă apare vreo eroare cu una din aceste resurse, jurnalul job va indica unde să se meargă pentru informaţii. În unele cazuri Servicii director 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 domneavoastră 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 Trace TCP/IP Application (TRCTCPAPP) cu opţiunea *DIRSRV poate fi folosită pe serverul de directoare LDAP pentru a ajuta în găsirea problemelor cu clienţii sau aplicaţiile.

Pentru mai multe informaţii detailate despre folosirea comenzii TRCTCPAPP cu LDAP la fel şi restricţiile pe authorităţile cerute, consultaţi descripţiile comenzii TRCTCPAPP (Trace TCP/IP Application) .

Pentru informaţii generale despre folosirea urmăririi de comunicaţii, consultaţi Communications trace.

Folosirea opţiunii LDAP_OPT_DEBUG pentru a urmări erori

| Începând cu V5R2, puteţi folosi opţiunea LDAP_OPT_DEBUG a **ldap_set_option()** API pentu a aurmări
| probleme cu clienţi care folosesc LDAP C API. 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 **ldap_set_option()** API est efolosită.

| Un exemple 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 job-ului client.

| Pentru a afişa informaţiile interactiv, tastaţi următoarele la promptul iSeries:

```
| DSPPFM  QAPOZDMP  QPOZnnnnnn
```

| unde nnnnnn este numărul job-ului.

| 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(QAPOZDMP  LIB(QTEMP)  DEV(*SAVF)  SAVF(xxx)
```

| unde *xxx* iste numele 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 a condiţiilor erorilor clientului LDAP consultaţi subiectul OS/400 Directory Services sub Programarea în Centru de informare iSeries.

Mesajel de eroare client au următorul format:

```
[Eşuare operaţie LDAP ]:[Condiţiile erorii clientului API LDAP ]
```

Notă: Expliocarea acestor erori asumă că clientul comunică cu un server LDAP pe OS/400. Un client ce comunică cu un server pe o platformă diferită poate avea erori similare dar cauzele şi rezoluţiile vor fi diferite.

Mesajele comune le includ pe următoarele:

- “ldap_search: Depăşirea limitei de timp” pe pagina 64
- “[Eşuarea operaţiei LDAP]: Eroare de operaţii” pe pagina 64

- “ldap_bind: Nu există un asemenea obiect”
- “ldap_bind: Autentificare necorespunzătoare”
- “[Operaţia LDAP eşuată]: Insuficient acces”
- “[Operaţie LDAP eşuată]: Nu se poate contacta serverul LDAP”
- “[operaţie LDAP eşuată]: Eşec la conectarea la serverul ssl” pe pagina 65

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:

- Măriţi limita timpului de căutare pentru serverul de directoare LDAP. Consultaţi “Ajustarea performanţei serverului de directoare LDAP” pe pagina 32pentru informaţii despre cum să faceţi aceasta.
- Reduceţi activitatea pe sistemul domneavoastră. Puteţi de asemenea reduce numărul de joburi client LDAP active care rulează.

[Eşuarea operaţiei LDAP]: Eroare de operaţii

Mai multe lucruri pot genera această eroare. Pentru a obţine informaţii despre cauza acestei erori pentru o anumită instanţă, consultaţi istoricele de job ale serverului, QDIRSRV şi Structured Query Language (SQL), cum este descris în “Procedura elementară de depanare pentru Servicii director” pe pagina 61.

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 “Procedura elementară de depanare pentru Servicii director” pe pagina 61.

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 OS/400, care are un atribut UID şi nu un atribut userpassword. Aceasta cauzează o comparare să fie făcută între parola specificată şi parola utilizator OS/400, care nu se potrivesc.
- O intrare reprezintă un utilizator proiectat şi o metodă de asociere 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 “Procedura elementară de depanare pentru Servicii director” pe pagina 61.

[Operaţia 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 “Procedura elementară de depanare pentru Servicii director” pe pagina 61.

[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 de joburi QDIRSRV, cum este descris în “Procedura elementară de depanare pentru Servicii director” pe pagina 61.Dacă serverul de Servicii de director a pornit cu succes, în istoricul de joburi QDIRSRV va fi mesajul Serverul de Servicii de director a pornit cu succes.

[operaţie LDAP eşuată]: Eşec la 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 pentruz a vă asigura că certificatele dumneavoastră sunt setate corespunzător, apoi reporniţi serverul şi încercaţi să vă conectaţi din nou.
- 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 OS/400, sunt disponibile informaţii de eroare SSL suplimentare. Consultaţi documentaţia pentru API-urile individuale Servicii director pentru detalii.

Tipărit în S.U.A.