System i

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

Versiunea 6 Ediţia 1

System i

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

Versiunea 6 Ediţia 1

Notă

Înainte de a folosi aceste informaţii şi produsul la care se referă, citiţi informaţiile din “Observaţii”, la pagina 307.

Această ediţie este valabilă pentru IBM i5/OS (număr produs 5761-SS1) versiunea 6, ediţia 1, modificarea 0 şi pentru toate ediţiile şi modificările ulterioare, până se specifică altceva în noile ediţii. Această versiune nu rulează pe toate modelele RISC şi nici pe modelele CISC.

© Copyright International Business Machines Corporation 1998, 2008. Toate drepturile rezervate.

Cuprins

© Copyright IBM Corp. 1998, 2008

IBM Tivoli Directory Server pentru i5/OS (LDAP)

IBM Tivoli Directory Server pentru i5/OS (numit în cele ce urmează Directory Server) este o funcţie din i5/OS ce furnizează un server LDAP (Lightweight Directory Access Protocol). LDAP rulează peste TCP/IP (Transmission Control Protocol/Internet Protocol), fiind un serviciu de director foarte răspândit pentru aplicaţiile Internet şi non-Internet.

Următoarele subiecte vă oferă informaţii pentru a vă ajuta să înţelegeţi şi să uilizaţi Directory Server.

Ce este nou în V6R1

Citiţi despre informaţiile noi sau modificate semnificativ în colecţia de subiecte IBM Tivoli Directory Server pentru i5/OS (LDAP).

Rezolvarea conflictelor de replicare

Într-o reţea cu mai multe servere master, IBM Tivoli® Directory Server poate detecta şi rezolva automat modificările conflictuale, astfel încât directoarele de pe toate serverele să rămână consistente. Când sunt detectate conflicte de replicare, modificarea conflictuală este raportată în istoricul serverului şi înregistrată, de asemenea, într-un fişier istoric ″pierdute şi găsite″, astfel încât un administrator să poată recupera datele pierdute.

- Privire generală asupra replicării
- Modificarea setărilor istoricului de pierdute şi găsite
- Vizualizarea fişierului istoric de pierdute şi găsite

Comanda ldapmodify

În comanda ldapmodify a fost adăugată opţiunea -e errorfile, pentru a specifica fişierul în care sunt scrise intrările refuzate. A fost adăugată opţiunea -n pentru ca modificările ce urmează să fie făcute să fie precedate de un semn de exclamare şi tipărite în ieşirea standard.

- ldapmodify şi ldapadd
- LDIF (LDAP Data Interchange Format)

Replicarea cu mai multe fire de execuţie

Puteţi replica folosind mai multe fire de execuţie, îmbunătăţind debitul general al replicării.

- Replicarea cu mai multe fire de execuţie
- Acordurile de replicare

Criptarea parolei

IBM Tivoli Directory Server oferă o opţiune de configurare ce permite criptatea datelor parolei de utilizator înainte de stocarea lor în director. Această opţiune de criptare poate fi utilizată pentru a împiedica datele de parolă cu text în clar să fie accesate de utilizatorii de director obişnuiţi sau de un utilizator de director administrativ.

- Criptarea parolei
- Setarea proprietăţilor pentru politica de parolă

Atributul IBMAttributeTypes

IBM Tivoli Directory Server 6.0 permite folosirea primelor 128 de caractere ale unui atribut pentru a crea numele de tabelă.

© Copyright IBM Corp. 1998, 2008

- Atributul IBMAttributeTypes

Modificări de schemă nepermise

Puteţi mări dimensiunea coloanei prin modificarea schemei. Aceasta vă permite să măriţi lungimea maximă a atributelor modificând schema cu Administrarea web sau utilitarul ldapmodify.

- Modificări de schemă nepermise

Director distribuit

IBM Tivoli Directory Server a fost conceput pentru a fi un director distribuit. Cuplat cu un server proxy, caracteristica de director distribuit permite ca un grup de directoare să apară ca şi cum ar fi un singur director. Folosind caracteristica de director distribuit şi caracteristica de server proxy, pot fi implementate directoare care conţin milioane de intrări.

- Directoarele distribuite

ldapmodrdn

IBM Tivoli Directory Server suportă modifyDN cu atributul newsuperior pentru un nod frunză.

- ldapmodrdn

Folosirea TRCTCPAPP pentru a ajuta la găsirea problemelor

Puteţi folosi comanda TRCTCPAPP pentru a urmări o instanţă activă de server.

- Folosirea TRCTCPAPP pentru a ajuta la găsirea problemelor

Accesul la citire pentru utilizatorii proiectaţi

Puteţi interzice toate operaţiile de căutare direcţionate către back-end-ul de utilizator proiectat.

- Operaţiile LDAP
- Accesul la citire pentru utilizatorii proiectaţi

Mai multe interfeţe de server

Puteţi avea mai multe servere de director pe sistemul dumneavoastră i5/OS®. Fiecare server este cunoscut ca o instanţă. Dacă folosiţi serverul de director pe o ediţie anterioară de i5/OS, va fi migrat la o instanţă cu numele QUSRDIR. Puteţi crea mai multe instanţe ale serverului de director pentru a vă întreţine aplicaţiile.

- Gestionarea instanţelor
- Configurarea Directory Server

Considerente privind migrarea

IBM Tivoli Directory Server este actualizat la o versiune nouă prima dată când este pornit serverul.

- Migrarea la V6R1 de la V5R4 sau V5R3

Politică de parolă

Conturile administrative pot fi blocate ca urmare a unui număr prea mare de autentificări eşuate. Această caracteristică se aplică doar conexiunilor client la distanţă. Contul este resetat la pornirea serverului. Este definit un atribut nou, care permite blocarea administrativă a unui cont.

- Setarea parolei administrative şi a politicii de blocare
- Setarea proprietăţilor pentru politica de parolă

Poate fi folosită operaţia extinsă de cerere stare cont, pentru a extrage starea unui cont particular: deschis (activat), blocat sau expirat.

- ldapexop

Altele

Echivalenţa IBM® Tivoli® Directory Server: Directory Server V6R1 este echivalent cu IBM Tivoli Directory Server Versiunea 6.0.

- Centrul de informare Tivoli software

Cum puteţi vedea ce este nou sau modificat

Pentru a vă ajuta să vedeţi care sunt modificările tehnice, în aceste informaţii sunt folosite:

- Imaginea  , pentru a marca locul în care încep informaţiile noi sau modificate.
- Imaginea  , pentru a marca locul în care se termină informaţiile noi sau modificate.

În fişierele PDF, puteţi vedea bare de revizuire (|) în marginea din stânga a informaţiilor noi sau modificate.

Pentru a găsi alte informaţii despre ce este nou sau modificat în această ediţie, vedeţi Memo către utilizatori.

Fişierul PDF pentru IBM Tivoli Directory Server pentru i5/OS (LDAP)

Puteţi vizualiza şi tipări fişierul PDF pentru IBM Tivoli Directory Server pentru i5/OS (LDAP).

Pentru a vizualiza sau descărca versiunea PDF acestui document, selectaţi IBM Tivoli Directory Server pentru i5/OS (LDAP) (aproximativ 2700 KB).

Alte informaţii

Pentru a vizualiza sau tipări PDF-uri ale manualelor şi publicaţiilor IBM Redbooks înrudite, vedeţi “Informaţii înrudite” la pagina 305.

Salvarea fişierelor PDF

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

1. Faceţi clic dreapta pe legătura PDF-ului din browser-ul dumneavoastră.
2. Faceţi clic pe opţiunea de salvare locală a PDF-ului.
3. Navigaţi la directorul unde doriţi să salvaţi fişierul PDF.
4. Faceţi clic pe **Save**.

Descărcarea programului Adobe Reader

Trebuie să aveţi instalat pe sistem Adobe Reader pentru a vizualiza sau tipări aceste PDF-uri. Puteţi descărca o copie gratuită de pe situl Web Adobe (www.adobe.com/products/acrobat/readstep.html)  .

Concepte privind Directory Server

Informaţii privind conceptele Directory Server.

Directory Server implementează specificaţiile Internet Engineering Task Force (IETF) LDAP V3. Include, de semenea, îmbunătăţiri adăugate de IBM în zone funcţionale şi performante. Această versiune utilizează IBM DB2 Universal Database pentru iSeries pentru memoria de rezervă ce este furnizată per integritatea tranzacţiilor de operaţii LDAP, operaţii de înaltă performanţă şi copie de rezervă on-line şi capabilitate de restaurare. Interoperează cu clienţii bazaţi pe IETF LDAP V3.

Directoare

Serverul de director permite accesul la un tip de bază de date care memorează informaţii intr-o structură ierarhică similară modului în care i5/OS sistemul de fişiere integrat este organizat.

Dacă este cunoscut numele unui obiect, pot fi extrase caracteristicele sale. Dacă este cunoscut numele unui anumit obiect individual, se poate căuta în director pentru o listă de obiecte care îndeplinesc o anumită cerinţă. De obicei căutările în directoare pot fi realizate după criterii specifice, nu numai după un set predefinit de categorii.

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

Un director poate fi centralizat sau distribuit. Dacă un director este centralizat, într-o anumită locaţie există un server de director (sau un cluster de servere) care furnizează acces la directorul respectiv. Dacă directorul este distribuit, există mai multe servere, de obicei dispersate geografic, care furnizează acces la director.

Când un director este distribuit, informaţiile stocate în director pot fi partiţionate sau replicate. Când informaţiile sunt partiţionate, fiecare server de director memorează un subset unic de informaţii, care nu se suprapune cu celelalte. Cu alte cuvinte, fiecare intrare de director este memorată de un singur server. Tehnica de partiţionare a directorului este de a folosi referral-i LDAP. Referral-ii LDAP permit utilizatorului să trimită cererile LDAP (Lightweight Directory Access Protocol) la spaţii de nume diferite sau similare de pe un server diferit. Când sunt replicate informaţiile, aceeaşi intrare de director este stocată pe mai multe servere. Într-un director distribuit, unele informaţii pot fi partiţionate, iar altele pot fi copiate.

Modelul serverului de director LDAP se bazează pe intrări (care mai sunt numite şi obiecte). Fiecare intrare conţine unul sau mai multe atribute, cum ar fi un nume sau o adresă şi un tip. De obicei tipurile conţin şiruri mnemonice, cum ar fi cn pentru nume comun sau mail pentru adresa de poştă electronică (e-mail).

Exemplul de director din Figura 1 la pagina 5 arată o intrare pentru Tim Jones, care include atributele mail şi telephoneNumber. Printre celelalte atribute posibile se numără fax, title şi jpegPhoto.

Fiecare director are o schemă, aceasta fiind un set de reguli care determină structura şi conţinutul directorului. Puteţi vizualiza schema folosind unealta de administrare prin Web.

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

În plus faţă de atributele definite de schemă, intrările au de asemenea un set de atribute care sunt întreţinute de server. Aceste atribute, numite atribute operaţionale, specifică informaţii cum ar fi momentul în care a fost creată intrarea şi controlul accesului.

În mod tradiţional, intrările directorului LDAP sunt aranjate într-o structură ierarhică care reflectă graniţa politică, geografică sau organizaţională (consultaţi Figura 1 la pagina 5). Intrările care reprezintă ţări sau regiuni apar la începutul ierarhiei. Intrările ce reprezintă stări sau organizaţii naţionale ocupă al doilea nivel în jos din ierarhie. Intrările de sub acestea pot reprezenta persoane, unităţi organizaţionale, imprimante, documente sau alte elemente.

LDAP face referire la intrări folosind nume distinctive (DN-uri). Numele distinctive sunt alcătuite din numele intrării propriu-zise şi din numele obiectelor aflate deasupra lui în director, în ordinea de jos în sus. De exemplu, DN-ul complet pentru intrarea din colţul din stânga-jos, Figura 1, este cn=Tim Jones, o=IBM, c=US. Fiecare intrare are cel puţin un atribut care este utilizat pentru a denumi intrarea. Acest atribut de numire este cunoscut ca nume distinctiv relativ (RDN - Relative Distinguished Name) al intrării. Intrarea de deasupra unui RDN dat se numeşte nume distinctiv părinte. În exemplul de mai sus, cn=Tim Jones numeşte intrarea, deci este RDN-ul. 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 părinte de cel mai înalt nivel în configuraţia serverului. Aceste nume distinctive se numesc sufixe. Serverul poate accesa toate obiectele din director care sunt sub sufixul specificat în ierarhia directorului. De exemplu, dacă un server LDAP conţinea directorul arătat în Figura 1, ar fi trebuit să aibă specificat în configuraţia sa sufixul o=ibm, c=us pentru a putea răspunde interogărilor clientului cu privire la Tim Jones.

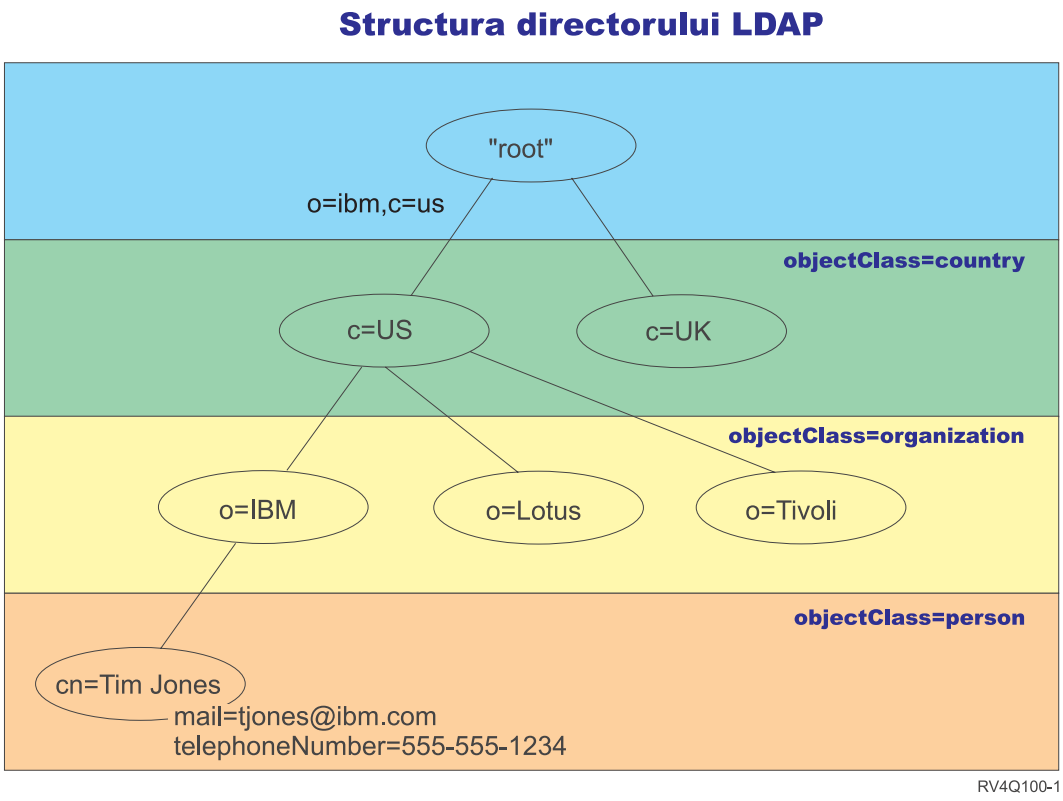


Figura 1. Structura directorului LDAP

Când vă structuraţi directorul, nu sunteţi limitat la ierarhia tradiţională. De exemplu, câştigă teren structura componentei de domeniu. În această structură, intrările sunt compuse din părţi ale numelor de domeniu TCP/IP. De exemplu, se poate opta pentru dc=ibm,dc=com în loc de o=ibm,c=us.

Să presupunem că doriţi să creaţi un director folosind structura de componentă a domeniului, care va conţine date despre angajaţi cum ar fi numele, numerele de telefon şi adresele de e-mail. Folosiţi sufixul sau contextul de numire bazat pe domeniul TCP/IP. Acest director poate fi vizualizat într-o formă similară cu următoarea:

```
/
|
+- ibm.com
   |
   +- employees
      |
      +- Tim Jones
```

```
|  555-555-1234
|  tjones@ibm.com
|
+- John Smith
   555-555-1235
   jsmith@ibm.com
```

Când sunt introduse datele în Directory Server, acestea pot arăta similar cu următoarele:

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

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

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

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

Observaţi că fiecare intrare conţine valori de atribut numite objectclass. Valorile objectclass definesc ce atribute sunt permise în intrare, cum ar fi telephonenumber sau givenname. Clasele de obiect permise sunt definite în schemă. Schema este un set de reguli care definesc tipurile de intrări permise în baza de date.

Clienţii şi serverele de director

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

Un API defineşte o interfaţă de programare pe care un anumit limbaj de programare o foloseşte pentru a accesa un serviciu. Formatul şi conţinutul mesajelor schimbate între client şi server trebuie să respecte un protocol convenit. LDAP defineşte un protocol de mesaje care este folosit de clienţii şi serverele de director. Există de asemenea un API LDAP asociat pentru limbajul C şi moduri de accesare a directorului dintr-o aplicaţie Java folosind JNDI (Java Naming and Directory Interface).

Securitatea directorului

Un director trebuie să suporte capabilităţile de bază necesare pentru a implementa o politică de securitate. Este posibil ca directorul să nu furnizeze direct capabilităţile de securitate necesare, ci să aibă integrat un serviciu de securitate de reţea de încredere, care să furnizeze serviciile de securitate de bază. În primul rând, este necesară o metodă pentru a autentifica utilizatorii. Prin autentificare se verifică dacă utilizatorii sunt cine pretind a fi. O schemă de autentificare elementară constă dintr-un nume de utilizator şi o parolă. După ce sunt autentificaţi utilizatorii, trebuie determinat dacă au autorizarea sau permisiunea de a realiza operaţia cerută pentru obiectul respectiv.

Autorizarea se bazează deseori pe liste de control al accesului (ACL-uri). Un ACL este o listă de autorizări care poate fi ataşată obiectelor şi atributelor din director. Un ACL listează ce tip de acces este permis sau refuzat fiecărui utilizator sau grup de utilizatori. Pentru a face ACL-urile mai scurte şi mai uşor de gestionat, utilizatorii cu aceleaşi drepturi de acces sunt deseori puşi în grupuri.

Concepte înrudite

“Schema” la pagina 14
O schemă este un set de reguli care controlează modalitatea prin care datele pot fi stocate în director. Schema defineşte tipul de intrări permise, structura atributelor lor şi sintaxa atributelor.

“Atributele operaţionale” la pagina 89
Există mai multe atribute care au o semnificaţie specială pentru Directory Server cunoscute ca atribute operaţionale. Acestea sunt atribute care sunt menţinute de către server şi ori reflectă informaţiile pe care serverul le administrează legate de o intrare, ori afectează operarea serverului.

“Nume distinctive (DN-uri)” la pagina 9
Fiecare intrare din director are un nume distinctiv (DN). DN-ul este numele care identifică în mod unic o intrare din director. Prima componentă a DN-ului se numeşte nume distinctiv relativ (RDN - Relative Distinguished Name).

API-urile LDAP (Lightweight Directory Access Protocol)
Vedeţi API-urile LDAP (Lightweight Directory Access Protocol) pentru informaţii suplimentare despre API Directory Server

“Securitatea Directory Server” la pagina 50
Vedeţi cum puteţi să folosiţi o varietate de funcţii pentru a securiza Directory Server.

Informaţii înrudite

Situl web The Java Naming and Directory Interface (JNDI) Tutorial

Directoarele distribuite

Un director distribuit este un mediu de lucru în care datele sunt partiţionate pe mai multe servere de director. Pentru a face ca directorul distribuit să apară ca un director unic în aplicaţiile client, se foloseşte un server proxy (sau mai multe) care conţine informaţii despre toate serverele şi datele pe care le păstrează.

Serverele proxy distribuie cereri de intrare la serverele corespunzătoare şi adună rezultatele să returneze un răspuns unit către client. Un set de servere back-end îşi reţin porţiunile directorului distribuit. Aceste servere back-end sunt de fapt servere LDAP standard cu suport adiţional pentru serverul proxy pentru emitere de cereri în numele utilizatorului ce s-ar putea sa fie definit într-un server diferit sau să aparţină unor grupuri ce sunt definite pe servere diferite.

Serverul de director v6.0 IBM Tivoli şi mai târziu (platforme distribuite) furnizează un asemenea director distribuit cu servere proxy, servere back-end şi unelte pentru configurarea unui asemenea director. Un asemenea director este capabil să scaleze până la câteva milioane de intrări.

Suportul IBM Directory Server pentru i5/OS pentru directoare distribuite

IBM Directory Server pentru i5/OS este capabil să acţioneze ca back-end într-un director distribuit IBM Tivoli Directory Server. i5/OS Directory Server nu poate să acţioneze ca server proxy şi nici nu conţine uneltele necesare pentru setarea unui director distribuit. Un server proxy poate să ruleze pe o altă platformă, iar datele să se afle pe unul sau mai multe servere de director i5/OS sau o combinaţie de servere de director i5/OS şi Tivoli.

Pentru a partiţiona datele de director existente de pe un server de director i5/OS pentru a fi folosite în topologia de director distribuit, trebuie să fie exportate datele într-un fişier LDIF din directorul i5/OS, trebuie rulată unealta de setare a directorului distribuit furnizată de Tivoli pe platformele Tivoli folosind fişierul LDIF şi apoi datele trebuie să fie reîncărcate pe serverele de director i5/OS şi Tivoli care participă ca servere backend pentru directorul distribuit. Procesarea nu este diferită pentru serverele i5/OS sau serverele platformei Tivoli şi utilizatorii au deja unealta de setare a directorului distribuit, deoarece deţin serverul proxy pe o platformă Tivoli.

Controalele şi operaţiile extinse pentru a suporta directoare distribuite

Din moment ce utilizatorii şi grupurile de care aparţin pot fi distribuite pe mai multe servere, IBM Tivoli Directory Server are definit un set de elemente de control şi de operaţii extinse pentru a suporta apartenenţa la grup şi controlul accesului într-un director distribuit. De asemenea, este furnizat un mecanism pentru crearea unei ″cozi de auditare″ înapoi, până la clientul iniţial.

Notă: O intrare de director este păstrată pe un server şi pe replicile sale. Dar într-un director distribuit este posibil ca un utilizator să aparţină unuia sau mai multor grupuri de pe un server şi să aparţină altor grupuri, definite pe alt server. Tot aşa, este posibil ca utilizatorul propriu-zis să nu fie definit pe serverul back-end ce procesează o cerere particulară.

Controlul de auditare

Controlul de auditare este mecanismul pe care serverul proxy îl utilizează ca să trimită identificatorul unic al cererii de client iniţiate de serverul proxy către serverele back-end. Pe lângă un identificator unic, împreună cu Controlul de auditare este trinis de asemenea IP-ul clientului. Acest identificator unic este utilizat pentru a potrivi intrările de pe serverul proxy cu intrările de auditare de pe serverul back-end. Dacă o cerere este transmisă prin mai multe servere, informaţia IP pentru fiecare server este adăugată la sfârşit, furnizând o coadă prin fiecare server, înapoi la clientul original.

Operaţia extinsă de evaluare a apartenenţei la grup

Această operaţie extinsă permite unui client autorizat (serverul proxy) să trimită informaţii despre un utilizator către un server back-end şi să ceară o listă a grupurilor (static, imbricat sau dinamic) în care utilizatorul este un membru al serverului back-end.

Controlul de apartenenţă la grup

Acest control permite unui client autorizat (serverul proxy) să trimită o listă de grupuri ce urmează să fie utilizate pentru controlul de acces. Controlul accesului este evaluat utilizând această listă de grupuri, în locul listei de grupuri pe care serverul ar determina-o în mod normal, ce se bazează pe informaţiile de grup stocate local, pe server. În utilizarea tipică, această listă de grupuri este lista cu grupurile pe care serverul proxy la strânge de la fiecare server back-end utilizând operaţia extinsă Evaluare apartenenţă la grup.

Suportul de auditare pentru directoarele distribuite

Auditarea securităţii i5/OS a fost îmbunătăţită, fiind adăugat suportul pentru directoare distribuite.

- **Control de auditare**: Urmărirea unei cereri înapoi la clientul original este utilă. I5/OS auditează ″controlul de auditare″ adăugând un câmp “de rutare” la intrările de jurnal de auditare a securităţii DI existente. Conţinutul nu este verificabil, dar vine de la un client autorizat să folosească autorizarea proxy, ceea ce înseamnă că ar trebui să fie un client de încredere.

- **Control de apartenenţă la grup**: Prezenţa controlului de grupu este auditată în două părţi: un câmp caracter singular “aserţiune apartenenţă la grup” a fost adăugat la intrarea de jurnal de auditare securitate DI. Serverul poate, de asemenea, să fie configurat să auditeze opţional lista de grupuri furnizată de client. Când această opţiune este configurată, serverul auditează, de asemenea, un câmp ″referinţă încrucişată XD″ în jurnalul de intrări DI şi creează unul sau mai multe intrări de jurnal de auditare securitate XD cu un câmp ″referinţă încrucişată XC″ ce se potriveşte cu lista de grupuri (până la 5 grupuri per intrare de jurnal)

Vedeţi subiectul Referinţă de securitate în legăturile înrudite de mai jos pentru mai multe detalii despre auditarea securităţii i5/OS. Puteţi de asemenea să vizitaţi situl Web Internet Engineering Task Force şi să căutaţi *rfc4648* pentru a afla mai multe despre configurarea auditării pentru serverul de director.

Pentru informaţii suplimentare despre directoarele distribuite şi setarea directoarelor distribuite, vedeţi subiectul Directoarele distribuite în Centrul de informare Tivoli Software.

Concepte înrudite

“Auditarea” la pagina 51
Auditarea vă permite să depistaţi detaliile anumitor tranzacţii Directory Server.

Informaţii înrudite

Auditările securităţii
Pentru informaţii suplimentare despre auditare, vedeţi subiectul Auditarea securităţii.

Identificatorii de obiecte (OID) pentru controale şi operaţii extinse

Nume distinctive (DN-uri)

Fiecare intrare din director are un nume distinctiv (DN). DN-ul este numele care identifică în mod unic o intrare din director. Prima componentă a DN-ului se numeşte nume distinctiv relativ (RDN - Relative Distinguished Name).

Un DN este alcătuit din perechi atribut=valoare separate de virgule, ca de exemplu:

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

Pentru a alcătui un DN poate fi folosit oricare dintre atributele definite în schema directorului. Este importantă ordinea perechilor de valori ale atributului de componentă. DN conţine o componentă pentru fiecare nivel al ierarhiei directorului, de la rădăcină la nivelul unde se află intrarea. DN-urile LDAP încep cu cel mai specific atribut (de obicei un nume) şi continuă progresiv cu atributele apropiate, terminând de obicei cu atributul de ţară. Prima componentă a DN-ului se numeşte nume distinctiv relativ (RDN - Relative Distinguished Name). Aceasta identifică o intrare faţă de orice altă intrare care are acelaşi părinte. În exemplul de mai sus, RDN-ul ″cn=Ben Gray″ separă prima intrare de a doua (care are RDN-ul ″cn=Lucille White″). Aceste două exemple de DN sunt în rest echivalente. Perechea atribut=valoare care alcătuieşte RDN-ul pentru o intrare trebuie să fie de asemenea prezentă în intrare. (Această condiţie nu este valabilă şi pentru celelalte componente ale DN-ului.)

Urmăriţi acest exemplu de creare a intrării pentru o persoană:

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

Regulile escape pentru DN

Unele caractere au un înţeles special într-un DN. De exemplu = (egal) separă numele şi valoarea unui atribut, iar , (virgulă) separă perechile atribut=valoare. Caracterele speciale sunt **,** (virgula), **=** (egal), **+** (plus), **<** (mai mic decât), **>** (mai mare decât), **#** (semn număr), **;** (punct şi virgulă), \ (slash înapoi) şi ″ (ghilimele, ASCII 34).

În valoarea unui atribut un caracter special poate fi marcat ca escape, pentru a înlătura înţelesul special. Pentru a marca drept escape aceste caractere speciale sau alte caractere într-o valoare de atribut dintr-un şir DN, folosiţi următoarele metode:

1. Când caracterul este unul dintre caracterele speciale, precedaţi-l cu un backslash (’\’ ASCII 92). Acest exemplu arată o metodă de marcare ca escape a unei virgule într-un nume de organizaţie:

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

   Aceasta este metoda de preferat.
2. Sau înlocuiţi caracterul cu un backslash şi două cifre hexazecimale, care formează un octet în codul caracterului. Codul caracterului **trebuie** să existe în setul de coduri UTF-8.

   ```
   CN=L. Eagle,O=Sue\2C Grabbit and Runn,C=GB
   ```
3. Înconjuraţi întreaga valoare atribut cu ″″ (ghilimele) (ASCII 34), care nu fac parte din valoare. Între perechea de ghilimele, toate caracterele sunt luate ca atare, exceptând \ (backslash). Caracterul \ (backslash) poate fi folosit pentru a marca drept escape un backslash (ASCII 92) sau ghilimele (ASCII 34), oricare dintre caracterele menţionate anterior sau perechi de cifre hexazecimale, ca în metoda 2. De exemplu, pentru a marca drept escape ghilimelele din cn=xyz"qrs"abc, se foloseşte forma cn=xyz\"qrs\"abc sau pentru a marca drept escape un \:

   ```
   "trebuie să marcaţi un singur backslash, astfel \\"
   ```

   Alt exemplu, "\Zoo" este ilegal, deoarece ’Z’ nu poate fi marcat ca escape în acest context.

Pseudo DN-uri

Pseudonumele distinctive sunt folosite în definiţii şi evaluări ale controlului de acces. Directorul LDAP suportă mai multe pseudonume distinctive (de exemplu, ″group:CN=THIS″ şi ″access-id:CN=ANYBODY″), care sunt folosite pentru a referi numere mari de DN-uri care partajează o caracteristică comună, în relaţie fie cu operaţia ce este realizată, fie cu obiectul asupra căruia este realizată operaţia.

Trei pseudonume distinctive sunt suportate de Directory Server:

- access-id: CN=THIS

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

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

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

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

Unele exemple de pseudonume distinctive:

Exemplu 1

Să considerăm următorul ACL pentru obiectul: cn=personA, c=US

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

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

În acest exemplu, persoana A primeşte permisiunile acordate ID-ului ″CN=THIS″ şi permisiunile acordate ambelor grupuri de pseudonume distinctive, ″CN=ANYBODY″ şi ″CN=AUTHENTICATED″.

Exemplu 2

Să considerăm următorul ACL ca obiect: cn=personA, c=US AclEntry: access-id:cn=personA, c=US: object:ad

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

Pentru o operaţie realizată asupra cn=personA, c=US:

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

În acest exemplu, persoana A primeşte permisiunile acordate ID-ului ″CN=THIS″ şi cele acordate DN-ului ″cn=personA, c=US″. Reţineţi că permisiunile de grup nu sunt acordate, deoarece există o intrare ACL mai specifică (″access-id:cn=personA, c=US″) pentru legarea DN (″cn=personA, c=US″).

Procesare îmbunătăţită DN

Un RDN compus al unui DN poate fi alcătuit din mai multe componente, conectate prin operatorii ‘+’. Serverul îmbunătăţeşte suportul pentru căutările intrărilor ce au un astfel de DN. Un RDN compus poate fi specificat în orice ordine ca bază pentru operaţia de căutare.

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

Serverul suportă o operaţie extinsă de nominalizare DN. Operaţiile extinse de nominalizare DN normalizează DN-urile folosind schema serverului. Această operaţie extinsă poate fi de folos aplicaţiilor care folosesc DN-uri.

Sintaxă nume distinctiv

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

```
<nume> ::= <nume-componentă> (<separator-spaţiu> )
          | <nume-componentă> <separator-spaţiat> <nume>

   <separator-spaţiat> ::= <spaţiu-opţional>
                  <separator>
                  <spaţiu-opţional>

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

   <spaţiu-opţional> ::= ( <CR> ) *( " " )

   <nume-componentă> ::= <atribut>
           | <atribut> <spaţiu-opţional> "+"
             <spaţiu-opţional> <nume-componentă>

   <atribut> ::= <şir>
```

```
        | <cheie> <spaţiu-opţional> "=" <spaţiu-opţional> <şir>

<cheie> ::= 1*( <cheiechar> ) | "OID." <oid> | "oid." <oid>
<keychar> ::= litere, numere şi spaţiu

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

<şir> ::= *( <şirchar> | <şir> )
          | '"' *( <şirchar> | <special> | <pereche> ) '"'
          | "#" <hex>


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

<pereche> ::= "\" ( <special> | "\" | '"')
<şirchar> ::= orice caracter exceptând <special> sau "\" or '"'


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

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

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

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

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

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

Concepte înrudite

"Directoare" la pagina 4
Serverul de director permite accesul la un tip de bază de date care memorează informaţii intr-o structură ierarhică similară modului în care i5/OS sistemul de fişiere integrat este organizat.

"Securitatea Directory Server" la pagina 50
Vedeţi cum puteţi să folosiţi o varietate de funcţii pentru a securiza Directory Server.

"Controalele şi operaţiile extinse" la pagina 91
Controalele şi operaţiile extinse permit extinderea protocolului LDAP fără a-l modifica.

Sufixul (contextul de numire)

Un sufix (numit şi context de numire) este un DN care identifică cea mai de sus intrare dintr-o ierarhie de director păstrată local.

Datorită schemei de numire relativă folosită în LDAP, acest DN este de asemenea sufixul oricărei alte intrări din acea ierarhie a directorului. Un server de director poate avea sufixe multiple, fiecare identificând o ierarhie de director păstrată local, de exemplu, o=ibm,c=us.

Intrarea specifică care se potriveşte sufixului trebuie adăugată directorului. Intrarea pe care o creaţi trebuie să folosească o clasă obiect care conţine atributul de numire folosit. Puteţi folosi unealta de administrare Web sau utilitarul Qshell ldapadd pentru a crea intrarea corespunzătoare acestui sufix.

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

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

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

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

- cn=schema conţine reprezentarea accesibilă LDAP a schemei
- cn=changelog păstrează istoricul de modificare al serverului, dacă este activat
- cn=localhost conţine informaţii nereplicate care controlează câteva aspecte ale operaţiei serverului, de exemplu, obiecte de configurare ale replicării
- cn=IBMpolicies conţine informaţii despre operaţii server care *sunt* copiate
- cn=pwdpolicy conţine politica de parolă a serverului
- sufixul ″os400-sys=system-name.mydomain.com″ furnizează accesabilitate LDAP la obiectei5/OS, limitate curent la grupuri şi profile utilizator

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

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

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

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

Clasa obiect domain are de asemenea câteva atribute opţionale pe care le-aţi putea folosi. Vizualizaţi schema sau editaţi intrarea pe care aţi creat-o folosind unealta de administrare Web pentru a vedea atributele suplimentare pe care le puteţi folosi.

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

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

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

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

Aplicaţiile pe care le folosiţi ar putea avea nevoie de definirea unor anumite sufixe sau de utilizarea unei anumite convenţii de numire. De exemplu, dacă directorul dumneavoastră este folosit pentru a gestiona certificate digitale, aţi putea fi nevoit să structuraţi o parte a directorului pentru ca numele de intrare să se potrivească cu subiectul DN al certificatelor pe care le deţine.

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

Concepte înrudite

"Taskuri de intrări de director" la pagina 185
Folosiţi aceste informaţii pentru a gestiona intrările directorului.

"Taskuri de schemă" la pagina 176
Folosiţi aceste informaţii pentru a gestiona schema.

Operaţii înrudite

"Adăugarea şi înlăturarea sufixelor serverului de director" la pagina 119
Folosiţi aceste informaţii pentru a adăuga sau a înlătura sufixul unui server de director.

Referinţe înrudite

"ldapmodify şi ldapadd" la pagina 207
Utilitarele de linie de comandă modificare-intrare LDAP şi adăugare-intrare LDAP.

Schema

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

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

Pentru informaţii suplimentare înrudite cu schema, vedeţi următoarele:

Concepte înrudite

"Directoare" la pagina 4
Serverul de director permite accesul la un tip de bază de date care memorează informaţii intr-o structură ierarhică similară modului în care i5/OS sistemul de fişiere integrat este organizat.

"Taskuri de intrări de director" la pagina 185
Folosiţi aceste informaţii pentru a gestiona intrările directorului.

"Taskuri de schemă" la pagina 176
Folosiţi aceste informaţii pentru a gestiona schema.

Schema serverului de director

Schema pentru Directory Server este predefinită, totuşi, puteţi modifica schema, dacă aveţi cerinţe suplimentare.

Directory Server include suport dinamic de schemă. Schema este publicată ca parte a informaţiilor directorului şi este disponibilă în intrarea subschemă (DN=″cn=schema″). Puteţi interoga schema folosind API-ul ldap_search() şi puteţi s-o modificaţi folosind ldap_modify().

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

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

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

Schema furnizează valori pentru următoarele tipuri de atribute:

- objectClasses
- attributeTypes
- IBMAttributeTypes
- reguli de potrivire
- sintaxe ldap

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

Un exemplu de intrare de schemă poate conţine:

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

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

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

ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.5 DESC 'Binary' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.7 DESC 'Boolean' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.12 DESC 'DN' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.15 DESC 'Directory String' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.24 DESC 'Generalized Time' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.26 DESC 'IA5 String' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.27 DESC 'INTEGER' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.50 DESC 'Telephone Number' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.53 DESC 'UTC Time' )
```

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

Informaţiile schemei pot fi modificate prin API-ul ldap_modify. Cu DN ″cn=schema″ puteţi adăuga, şterge sau înlocui un tip de atribut sau o clasă obiect. Puteţi furniza de asemenea o descriere completă. Puteţi adăuga sau înlocui o intrare schemă cu definiţia versiunii 3 LDAP sau cu definiţiaextensiei atributului IBM sau cu ambele definiţii.

Concepte înrudite

“Taskuri de schemă” la pagina 176
Folosiţi aceste informaţii pentru a gestiona schema.

API-urile LDAP (Lightweight Directory Access Protocol)
Vedeţi API-urile LDAP (Lightweight Directory Access Protocol) pentru informaţii suplimentare despre API Directory Server

“Clasele de obiecte” la pagina 17
O clasă de obiecte specifică un set de atribute folosite pentru a descrie un obiect.

“Atributele” la pagina 18
Fiecare intrare din director are un set de atribute asociate cu aceasta prin clasa sa de obiecte.

Referinţe înrudite

“Atributul IBMAttributeTypes” la pagina 20
Atributul IBMAttributeTypes poate fi folosit pentru a defini informaţii de schemă care nu sunt acoperite de standardul LDAP Versiunea 3 pentru atribute.

“Reguli de potrivire” la pagina 21
O regulă de potrivire furnizează indicaţii pentru compararea şirului în timpul unei operaţii de căutare.

“Sintaxă atribut” la pagina 23
O sintaxă de atribut defineşte valorile permise pentru un atribut.

“Schemă dinamică” la pagina 27
Este posibil să modificaţi dinamic schema.

Suportul pentru schema obişnuită

IBM Directory suportă schema de director standard.

IBM Directory suportă schema de director standard, după cum este definită în următoarele:

- RFC-urile IETF (Internet Engineering Task Force) LDAP Versiunea 3, cum ar fi RFC 2252 şi 2256.
- CIM (Common Information Model) de la DMTF (Desktop Management Task Force).
- LIPS (Lightweight Internet Person Schema) da la Network Application Consortium.

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

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

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

Informaţii înrudite

IETF (Internet Engineering Task Force)

DMTF (Desktop Management Task Force)

Network Application Consortium

Clasele de obiecte

O clasă de obiecte specifică un set de atribute folosite pentru a descrie un obiect.

De exemplu, dacă aţi creat clasa de obiecte **tempEmployee** , aceasta ar putea conţine atribute asociate unui angajat temporar, precum **idNumber**, **dateOfHire** sau **assignmentLength**. Puteţi adăuga clase de obiecte personalizate pentru a servi necesităţile organizaţiei dumneavoastră. Schema IBM Directory Server furnizează unele tipuri de bază de clase de obiecte, printre care se numără:

- Grupuri
- Locaţii
- Organizaţii
- Persoane

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

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

Tipul clasei de obiecte

O clasă de obiecte poate fi de trei tipuri:

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

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

Auxiliară:
Acest tip indică atribute suplimentare care pot fi asociate cu o intrare aparţinând unei anumite clase obiect structurală. Deşi o intrare poate aparţine unei singure clase obiect structurale, aceasta ar putea aparţine mai multor clase obiect auxiliare.

Moştenirea clasei de obiecte

Această versiune Directory Server suportă moştenirea obiectelor pentru clasa de obiecte şi pentru definiţiile atributului. Poate fi definită o nouă clasă de obiecte, cu clase părinte şi cu atribute suplimentare sau modificate.

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

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

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

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

Atributele

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

Atributele

Fiecare intrare din director are un set de atribute asociate cu aceasta prin clasa sa de obiecte.

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

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

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

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

Pentru informaţii suplimentare, vedeţi următoarele:

Elemente subschemă obişnuită:

Elementele sunt utilizate pentru a defini gramatica valorilor atributelor subschemei.

Următoarele elemente sunt folosite pentru a defini gramatica valorilor atributelor subschemei:

- alpha = ’a’ - ’z’, ’A’ - ’Z’
- număr = ’0’ - ’9
- anh = alpha / number / ’-’ / ’;’
- anhstring = 1 * anh
- keystring = alpha [anhstring]
- numericstring = 1 * number
- oid = descr / numericoid
- descr = keystring
- numericoid = numericstring *(″.″ numericstring)
- woid = whsp oid whsp ; set de oid-uri de orice formă (OID-uri numerice sau nume)
- oids = woid / (″(″ oidlist ″)″)
- oidlist = woid *(″$″ woid) ; descriptori de obiecte folosiţi ca nume de elemente ale schemei

- qdescrs = qdescr / (whsp ″(″ qdescrlist ″)″ whsp)
- qdescrlist = [qdescr *(qdescr)]
- whsp ″'″ descr ″'″ whsp

Atributul objectclass:

Atributul objectclass listează clasele obiect suportate de către server.

Fiecare valoare a acestui atribut reprezintă o definiţie separată de clasă obiect. Definiţiile clasei obiect pot fi adăugate, şterse sau modificate prin modificări corespunzătoare ale atributului objectclass al intrării cn=schema. Valorile atributului objectclass au următoarea gramatică, definită de RFC 2252:

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

De exemplu, definiţia clasei obiect person este:

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

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

Concepte înrudite

"Taskuri de schemă" la pagina 176
Folosiţi aceste informaţii pentru a gestiona schema.

Atributul attributetypes:

Atributul attributetypes tipăreşte atributul suportat de server.

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

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

```
         whsp ")"

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

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

- “Reguli de potrivire” la pagina 21
- “Sintaxă atribut” la pagina 23

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

De exemplu, atributul ″description″ are următoare definiţie:

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

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

Concepte înrudite

“Taskuri de schemă” la pagina 176
Folosiţi aceste informaţii pentru a gestiona schema.

Atributul IBMAttributeTypes:

Atributul IBMAttributeTypes poate fi folosit pentru a defini informaţii de schemă care nu sunt acoperite de standardul LDAP Versiunea 3 pentru atribute.

Valorile IBMAttributeTypes trebuie să respecte următoarea gramatică:

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

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

   IBMwlen = whsp len
```

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

DBNAME
Puteţi furniza cel mult 2 nume, dacă sunt într-adevăr 2 nume date. Primul este numele de tabelă folosit pentru

acest atribut. Al doilea este numele coloanei folosit pentru valoarea normalizată total a atributului din tabelă. Dacă furnizaţi un singur nume, este folosit şi pentru numele de tabelă, şi pentru numele de coloană. Dacă nu furnizaţi nici un DBNAME, atu nci un nume bazat pe primele 128 de caractere ale numelui atributului (care trebuie să fie unic) este utilizat. Numele tabelelor baze de date sunt trunchiate la 128 de caractere. Numele coloană sunt trunchiate la 30 de caractere.

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

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

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

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

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

Reguli de potrivire:

O regulă de potrivire furnizează indicaţii pentru compararea şirului în timpul unei operaţii de căutare.

Regulile de potrivire sunt împărţite în trei categorii:
- Egalitate
- Ordonare
- Subşir

Serverul de director suportă potriviri de egalitate pentru toate sintaxele, cu excepţia celei binare. Pentru atributele definite folosind o sintaxă binară, serverul suportă doar căutările de existenţă, ca de exemplu ″(jpegphoto=*)″. Pentru sintaxele IA5 String şi Directory String, o definiţie a atributului poate fi extinsă mai departe sub forma case exact (diferenţiere majuscule) sau case ignore (nediferenţiere majuscule). De exemplu, atributul cn foloseşte regula de potrivire caseIgnoreMatch, care face valorile ″John Doe″ şi ″john doe″ echivalente. Pentru regulile de potrivire case ignore (nediferenţiere majuscule), compararea se efectuează după convertirea valorilor la majuscule. Algoritmul uppercase nu este sensibil la locale şi nu poate fi corect pentru toate locale-urile.

Serverul de director suportă potriviri de subşiruri pentru atributele sintaxelor Directory String, IA5 String şi Distinguished Name. Filtrele de căutare pentru potrivirile de subşiruri folosesc caracterul ″*″ pentru a se potrivi cu zero sau mai multe caractere dintr-un şir. De exemplu, filtrul de căutare ″(cn=*smith)″ se potriveşte cu toate valorile cn care se termină cu şirul ″smith″.

Sortarea potrivirilor este suportată pentru sintaxele Integer, Directory String, IA5 String şi Distinguished Name. Pentru sintaxele şirurilor, sortarea este bazată pe o sortare de octeţi simplă a valorilor de şir UTF-8. Dacă atributul este definit cu o regulă de potrivire case ignore, sortarea se efectuează folosind valorile şirurilor cu majuscule. După cum am observat mai înainte, algoritmul uppercase ar putea să nu fie corect pentru toate obiectele locale.

În IBM Directory Server, comportamentul subşirurilor şi de potrivire sortare este implicat de către regula de potrivire: toate sintaxele care suportă potrivire de subşir au o regulă implicită de potrivire subşir, iar toate sintaxele noi care suportă sortarea au o regulă implicită de sortare. Pentru atributele definite folosind regula de potrivire case ignore, regulile implicite de subşir şi sortare sunt de asemenea case ignore (ignorare majuscule).

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

Reguli de potrivire ale sortării		
Regulă de potrivire	**OID**	**Sintaxa**
caseExactOrderingMatch	2.5.13.6	Sintaxă şir director
caseIgnoreOrderingMatch	2.5.13.3	Sintaxă şir director
distinguishedNameOrderingMatch	1.3.18.0.2.4.405	DN - nume distinctiv
generalizedTimeOrderingMatch	2.5.13.28	Sintaxă Generalized Time

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

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

Referinţe înrudite

“Timpul generalizat şi UTC” la pagina 33
Directory Server suportă sintaxele cu timp generalizat şi timp universal (UTC).

Reguli de indexare:

Regulile de indexare ataşate atributelor fac posibilă extragerea mai rapidă a informaţiilor.

Dacă este dat doar atributul, nu se menţine nici un index. Directory Server furnizează următoarele reguli de indexare:

- Egalitate
- Ordonare
- Aproximare
- Subşir
- Reverse

Specificaţiile regulilor de indexare pentru atribute:

Specificând o regulă de indexare pentru un atribut se controlează crearea şi menţinerea unor indecşi speciali ai valorilor atributului. Aceasta îmbunătăţeşte timpul de răspundere pentru căutările cu filtru care includ acele atribute.

Cele cinci tipuri posibile de reguli de indexare sunt înrudite cu operaţiile aplicate în filtru de căutare.

Egalitate
Se aplică următoarelor operaţii de căutare:
- equalityMatch '='

De exemplu:
```
"cn = John Doe"
```

Ordonare
Se aplică următoarelor operaţii de căutare:
- greaterOrEqual '>='
- lessOrEqual '<='

De exemplu:
```
"sn >= Doe"
```

Aproximare
Se aplică următoarelor operaţii de căutare:
- approxMatch '~='

De exemplu:
```
"sn ~= doe"
```

Subşir Se aplică următoarelor operaţii de căutare:
- substring '*'

De exemplu:
```
"sn = McC*"
"cn = J*Doe"
```

Reverse
Se aplică următoarelor operaţii de căutare:
- '*' substring

De exemplu:
```
"sn = *baugh"
```

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

Sintaxă atribut:

O sintaxă de atribut defineşte valorile permise pentru un atribut.

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

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

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

Sau încercaţi să includeţi informaţii despre ordine în valoare:

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

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

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

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

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

Atributele booleene conţin şirurile TRUE sau FALSE.

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

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

Atributele Generalized Time conţin o reprezentare sigură pentru anul 2000 sub formă de şir a datei şi orei folosind timpi GMT cu un offset de fus orar GMT opţional.

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

Atributele întregi conţin reprezentarea şirului text a valorii. De exemplu, 0 sau 1000. Valorile atributelor sintaxei Întreg trebuie să se găsească în intervalul de la -2147483648 la 2147483647.

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

Atributele timp UTC folosesc un format de şir mai vechi, fără an 2000 sigur, pentru a reprezenta data şi timpul.

În schema director, sintaxa unui atribut este specificată folosind OID-uri (Object Identifiers- Identificatori de obiect) alocaţi fiecărei sintaxe. Următoarea tabelă prezintă sintaxele suportate de serverul director şi OID-urile corespunzătoare.

Sintaxa	OID
Sintaxă Attribute Type Description	1.3.6.1.4.1.1466.115.121.1.3
Binary - şir de octeţi	1.3.6.1.4.1.1466.115.121.1.5

Sintaxa	OID
Boolean - TRUE/FALSE	1.3.6.1.4.1.1466.115.121.1.7
Sintaxă şir director	1.3.6.1.4.1.1466.115.121.1.15
Sintaxă DIT Content Rule Description	1.3.6.1.4.1.1466.115.121.1.16
Sintaxă DITStructure Rule Description	1.3.6.1.4.1.1466.115.121.1.17
DN - nume distinctiv	1.3.6.1.4.1.1466.115.121.1.12
Sintaxă Generalized Time	1.3.6.1.4.1.1466.115.121.1.24
Sintaxă şir IA5	1.3.6.1.4.1.1466.115.121.1.26
Descriere tip atribut IBM	1.3.18.0.2.8.1
Sintaxă Integer - număr intreg	1.3.6.1.4.1.1466.115.121.1.27
Sintaxă LDAP Syntax Description	1.3.6.1.4.1.1466.115.121.1.54
Matching Rule Description	1.3.6.1.4.1.1466.115.121.1.30
Matching Rule Use Description	1.3.6.1.4.1.1466.115.121.1.31
Name Form Description	1.3.6.1.4.1.1466.115.121.1.35
Sintaxă Object Class Description	1.3.6.1.4.1.1466.115.121.1.37
Şir care conţine OID-uri. OID este un şir care conţine digiţi (0-9) şi puncte zecimale (.).	1.3.6.1.4.1.1466.115.121.1.38
Sintaxă număr telefon	1.3.6.1.4.1.1466.115.121.1.50
Sintaxă UTC Time. UTC-Time este formatul şirului timp definit de standardele ASN.1. Vedeţi ISO 8601 şi X680. Folosiţi această sintaxă pentru a stoca valorile timp în format UTC-Time.	1.3.6.1.4.1.1466.115.121.1.53

Concepte înrudite

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

Referinţe înrudite

"Timpul generalizat şi UTC" la pagina 33
Directory Server suportă sintaxele cu timp generalizat şi timp universal (UTC).

Identificatorul de obiect (OID)

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

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

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

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

American National Standards Institute (ANSI) este autoritatea de înregistrare pentru numele de organizaţii din Statele Unite sub procesul global de înregistrare stabilit de International Standards Organization (ISO) şi International Telecommunication Union (ITU). Informaţii suplimentare despre organizarea înregistrării numelui pot fi găsite pe

site-ul web ANSI (www.ansi.org). Arcul ANSI OID pentru organizaţii este 2.16.840.1. ANSI va aloca un număr (NEWNUM), creând un nou arc OID: 2.16.840.1.NEWNUM.

În cele mai multe ţări sau regiuni, asociaţia naţională de standarde întreţine un registru OID. Ca şi cu arcul ANSI, acestea sunt în general arce alocate sub OID 2.16. Ar putea fi nevoie de investigare pentru a găsi autoritatea OID pentru o anumită ţară sau regiune. Asociaţia naţională de standarde din ţara sau regiunea dumneavoastră ar putea fi un membru ISO. Numele şi informaţiile de contact ale membriilor ISO pot fi găsite la site-ul web ISO (www.iso.ch).

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

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

Informaţii înrudite

Situl web ANSI

Situl web ISO

Situl web IANA

Intrările subschemei

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

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

Clasa obiect IBMsubschema

Clasa de obiecte IBMsubschema este o clasă de obiecte specifică care memorează toate atributele şi clasele de obiecte pentru un server de director dat.

Clasa de obiecte IBMsubschema este folosită în intrarea subschemei după cum urmează:

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

Interogările schemei

API-ul ldap_search() poate fi utilizat pentru a interoga intrarea subschemei.

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

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

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

Concepte înrudite

API-urile LDAP (Lightweight Directory Access Protocol)
Vedeţi API-urile LDAP (Lightweight Directory Access Protocol) pentru informaţii suplimentare despre API Directory Server

Schemă dinamică

Este posibil să modificaţi dinamic schema.

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

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

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

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

Pentru a adăuga sau înlocui o entitate dintr-o schemă, TREBUIE să furnizaţi o definiţie a Versiunii 3 LDAP şi AŢI PUTEA furniza definiţia IBM. În toate cazurile, trebuie să furnizaţi doar definiţia sau definiţiile entităţii schemei pe care vreţi să o afectaţi.

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

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

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

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

Versiunea LDIF a celor de mai sus ar fi:

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

Controluri acces

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

Replicarea

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

Modificări de schemă nepermise

Nu sunt permise toate modificările de schemă.

Restricţiile de modificare includ următoarele:

- Orice modificare a schemei trebuie să lase schema într-o stare consistentă.
- Un tip de atribut care reprezintă un supertip al altui tip de atribut nu poate fi şters. Un tip de atribut ″MAY″ sau ″MUST″ al unei clase obiect nu poate fi şters.
- O clasă obiect care este o superclasă a altei clase nu poate fi ştearsă.
- Tipurile de atribute sau clasele obiect care se referă la entităţi inexistente (de exemplu, sintaxe sau clase obiect) nu pot fi adăugate.
- Tipurile de atribute sau clasele obiect nu pot fi modificate în aşa fel încât să ajungă să se refere la entităţi inexistente (de exemplu, sintaxe sau clase obiect).
- Atributele noi nu pot folosi tabelele bază de date existente în definiţia lor IBMattributestype.
- Atributele care sunt folosite în intrările oricărui director existent nu pot fi şterse.
- Lungimea şi sintaxa unui atribut nu pot fi modificate.
- Tabela sau coloana bazei de date asociată cu un atribut nu poate fi ştearsă.
- Atributele folosite în definiţiile claselor obiect existente nu pot fi şterse.
- Clasele obiect folosite în orice intrări ale unui director existent nu pot fi şterse.

| Puteţi mări dimensiunea coloanei prin modificarea schemei. Aceasta vă permite să măriţi lungimea maximă a
| atributelor modificând schema cu Administrarea web sau utilitarul ldapmodify.

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

Clase obiect:

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

Atribute:

- aclEntry
- aclPropagate
- aclSource
- aliasedObjectName, aliasedentryName
- businessCategory
- cn, commonName
- createTimestamp
- creatorsName

- descriere
- dn, distinguishedName
- entryOwner
- hasSubordinates
- ibm-entryChecksum
- ibm-entryChecksumOp
- ibm-entryUuid
- member
- modifiersName
- modifyTimestamp
- name
- o, organizationName, organization
- objectClass
- os400-acgcde
- os400-astlvl
- os400-atnpgm
- os400-audlvl
- os400-aut
- os400-ccsid
- os400-chridctl
- os400-cntryid
- os400-curlib
- os400-dlvry
- os400-docpwd
- os400-dspsgninf
- os400-eimassoc
- os400-gid
- os400-groupmember
- os400-grpaut
- os400-grpauttyp
- os400-grpprf
- os400-homedir
- os400-IaspStorageInformation
- os400-inlmnu
- os400-inlpgm
- os400-invalidSignonCount
- os400-jobd
- os400-kbdbuf
- os400-langid
- os400-lclpwdmgt
- os400-lmtcpb
- os400-lmtdevssn
- os400-locale
- os400-maxstg
- os400-msgq

- os400-objaud
- os400-outq
- os400-owner
- os400-password
- os400-passwordExpirationDate
- os400-passwordLastChanged
- os400-previousSignon
- os400-profile
- os400-prtdev
- os400-ptylmt
- os400-pwdexp
- os400-pwdexpitv
- os400-setjobatr
- os400-sev
- os400-spcaut
- os400-spcenv
- os400-srtseq
- os400-status
- os400-storageUsed
- os400-storageUsedOnIasp
- os400-supgrpprf
- os400-sys os400-text
- os400-uid
- os400-usrcls
- os400-usropt
- ou, organizationalUnit, organizationalUnitName
- proprietar
- ownerPropagate
- ownerSource
- ref
- replicaBindDN
- replicaBindMethod
- replicaCredentials, replicaBindCredentials
- replicaHost
- replicaPort
- replicaUpdateTimeInterval
- replicaUseSSL
- seeAlso

Sintaxe:
All

Reguli de potrivire:
All

Verificare schemă

Când serverul este iniţializat, fişierele schemei sunt citite şi verificate pentru consistenţă şi corectitudine.

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

Următoarele elemente sunt verificate pentru tipuri de atribute:

- Două tipuri diferite de atribute nu pot avea acelaşi nume sau OID.
- Ierarhia moştenită a tipurilor de atribut nu are cicluri.
- Supertipul unui tip de atribut trebuie de asemenea definit, deşi definiţia sa poate fi afişată mai târziu sau într-un fişier separat.
- Dacă un tip de atribut este un subtip al altuia, amândoi au acelaşi USAGE.
- Toate tipurile de atribute au o sintaxă direct definită sau moştenită.
- Doar atributele operaţionale pot fi marcate ca NO-USER-MODIFICATION.

Următoarele articole sunt verificate pentru clase obiect:

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

Verificarea unei intrări pe baza schemei

Când o intrare este adăugată sau modificată printr-o operaţie LDAP, intrarea este verificată pe baza schemei. Implicit, sunt realizate toate verificările afişate în această secţiune. Însă puteţi dezactiva selectiv unele dintre verificările schemei modificând nivelul de verificare al schemei. Aceasta este făcută prin Navigator System i modificând valoarea câmpului **Verificare schemă** pe pagina **bază de date/Sufixe** a proprietăţilor Serverului de director.

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

Referitor la clasele de obiecte:

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

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

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

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

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

Validitatea DN-ului este verificată după cum urmează:

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

Concepte înrudite

“Schemă de configurare Directory Server” la pagina 244
Aceste informaţii descriu Directory Information Tree (DIT) şi atributele care sunt folosite pentru a configura fişierul ibmslapd.conf.

Compatibilitatea iPlanet

Parser-ul folosit de Directory Server permite valorilor de atribut ale tipurilor de atribute din schemă (objectClasses şi attributeTypes) să fie specificate folosind gramatica iPlanet.

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

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

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

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

Astfel o descrie Directory Server:

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

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

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

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

Timpul generalizat şi UTC

Directory Server suportă sintaxele cu timp generalizat şi timp universal (UTC).

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

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

la fel ca şi multe alte notaţii.

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

- Sintaxa Timp Generalizat, care ia forma:

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

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

  ```
   "19991106210627.3"
  ```

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

  ```
  "19991106210627.3Z"
  ```

  care este timpul universal coordonat.

  ```
  "19991106210627.3-0500"
  ```

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

  Dacă desemnaţi o fracţiune de secundă opţională, este necesar un punct sau o virgulă. Pentru ora locală diferenţială, a '+' or a '-' trebuie să precedeţi valoarea oră-minut.

- Sintaxa timpului universal, care ia forma:

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

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

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

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

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

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

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

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

Următoarele filtre nu sunt valide:

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

Practici recomandate pentru structura directorului

Directory Server este deseori folosit ca magazie pentru utilizatori şi grupuri. Această secţiune descrie câteva practici recomandate pentru configurarea unei structuri optimizate pentru gestionarea utilizatorilor şi a grupurilor. Această structură şi modelul de securitate asociat pot fi extinse pentru alte utilizări ale directorului.

Utilizatorii sunt de obicei memoraţi într-o singură, sau în puţine, locaţii. Aţi putea avea un singur container, cn=users, care este intrarea părinte pentru toţi utilizatorii sau containeri separaţi pentru seturi diferite de utilizatori, care sunt administrate separat. De exemplu, angajaţii, vânzătorii şi utilizatorii Internet înregistraţi singuri ar putea fi localizaţi sub obiecte numite cn=employees, cn=vendors, respectiv cn=internet users. Ar putea exista tentaţia de a plasa persoanele sub organizaţiile de care aparţin; totuşi, aceasta poate crea dificultăţi când se mută în altă organizaţie, deoarece atunci şi intrarea din director trebuie mutată, iar grupurile sau alte surse de date (atât interne, cât şi externe directorului) ar trebui actualizate pentru a reflecta noul DN. Relaţia utilizatorilor cu structura organizaţiei poate fi capurată în intrarea utilizator, folosind atribute director ca ″o″ (organization name), ″ou″ (organizational unit name) şi departmentNumber, care fac parte din schema standard pentru organizationalPerson şi inetOrgPerson.

Similar, groupurile sunt în mod obişnuit plasate într-un container separat, de exemplu un container numit ″cn=groups″.

Prin organizarea utilizatorilor şi a grupurilor în acest mod, există doar câteva locuri în care listele de control acces (ACL-uri) trebuie configurate.

În funcţie de modul de utilizare al serverului de director şi de modul în care utilizatorii şi grupurile sunt gestionate, aţi putea folosi unul din următoarele modele de control al accesului:

- Dacă directorul este folosit pentru aplicaţii de forma unei cărţi de adrese, aţi putea dori să acordaţi permisiuni de citire şi căutare grupului special cn=anybody pentru atributele ″normal″ din containerul cn=users şi obiectele sale părinte.
- Deseori, doar DN-urile folosite de anumite aplicaţii şi administratori de grup necesită acces la containerul cn=groups. Aţi putea dori să creaţi un grup ce conţine DN-urile administratorilor grupului şi să faceţi acel grup proprietarul cn=groups şi al subordonaţilor săi. Aţi putea crea alt grup care reţine DN-urile utilizate de aplicaţii la citirea informaţiilor despre grup şi să acordaţi acelui grup permisiuni de citire şi căutare în cn=groups.
- Dacă obiectele utilizator sunt actualizate direct de utilizatori, veţi dori să acordaţi id-ului special de acces cn=this permisiuni corespunzătoare de citire, scriere şi căutare.
- Dacă utilizatorii sunt actualizaţi prin intermediul aplicaţiilor, deseori aceste aplicaţii rulează propria identitate şi doar acele aplicaţii necesită autorizarea de actualizare a obiectelor utilizator. Încă o dată, este convenabil să adăugaţi aceste DN-uri la un grup, de exemplu cn=user administrators şi să acordaţi acelui grup permisiunile necesare pentru cn=users.

Aplicând acest tip de structură şi control acces, directorul dumneavoastră iniţial ar putea arăta astfel:

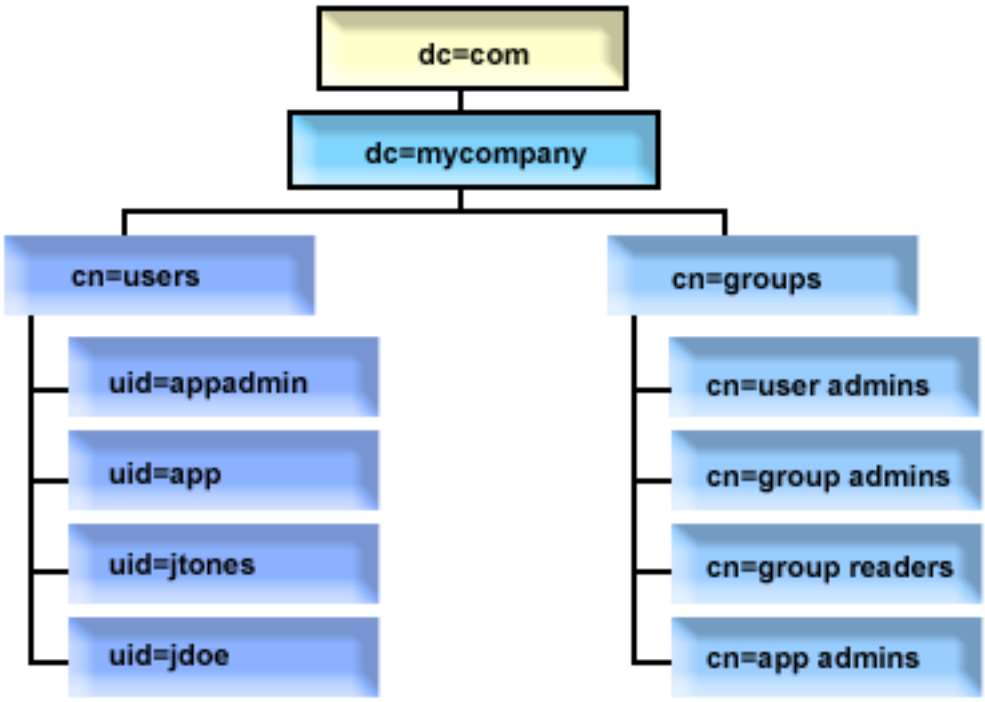


Figura 2. Exemplu de structură de director

- c=mycompany, dc=com este deţinut de administratorul directorului sau un alt utilizator sau grup cu autoritatea de a gestiona nivelul superior al directorului. Intrările suplimentare ACL oferă acces de citire atributelor normale pentru unul din cn=anybody şi cn=authenticated sau, posibil, unui alt grup, dacă este necesar un ACL mai restrictiv.
- cn=users are intrări ACL peste cele descrise mai jos, pentru a permite utilizatorilor un acces corespunzător. ACL-urile ar putea include:
  - acces de citire şi căutare la atributele normale pentru cn=anybody sau cn=authenticated
  - acces de citire şi căutare la atributele normale şi sensibile pentru administratori
  - alte intrări ACL dorite, permiţând poate accesul de scriere pentru indivizi la propriile intrări.

Observaţii:

- Pentru îmbunătăţirea proprietăţii de citire, au fost folosite RDN-urile intrărilor mai degrabă decât DN-urile complete. De exemplu, grupul ″user admins″ ar avea mai degrabă DN-ul complet uid=app,cn=users,dc=mycompany,dc=com ca membru, decât uid=app, care este mai scurt.
- Unii utilizatori şi grupuri ar putea fi combinaţi. De exemplu, dacă administratorul aplicaţiei avea autoritatea de a administra utilizatorii, aplicaţia putea rula sub DN-ul administratorului aplicaţiei. Totuşi, aceasta ar putea restricţiona posibilitatea, de exemplu, de a modifica parola de administrator a aplicaţiei, fără a mai reconfigura noua parolă în aplicaţie.
- În timp ce practicile de mai sus sunt cele mai bune pentru directoarele folosite de o singură aplicaţie, ar putea fi mai avantajos ca toate actualizările să se facă fiind autentificat ca administratorul directorului. Această practică este descurajată din motivele discutate anterior.

Publicarea

Directory Server oferă posibilitatea ca sistemul să publice anumite tipuri de informaţii într-un director LDAP. Cu alte cuvinte, sistemul va crea şi actualiza intrări LDAP reprezentând tipuri diferite de date.

i5/OS are încorporat suport pentru publicarea următoarelor informaţii pe un server LDAP:

Utilizatori

Când configuraţi sistemul de operare să publice informaţii tip Utilizatori la Directory Server, acesta exportă automat intrările din directorul de distribuţie al sistemului la Directory Server. Foloseşte API-ul QGLDSSDD pentru a face asta. Aceasta păstrează de asemenea directorul LDAP sincronizat cu modificările care sunt făcute în directorul de distribuţie sistem.

Publicarea utilizatorilor este de ajutor pentru furniz area căutării de acces LDAP la informaţii din directorul de distribuţie al sistemului (de exemplu pentru a furniza acces la agenda de adrese LDAP la clienţi mail POP3 LDAP-activat ca Netscape Communicator sau Microsoft Outlook Express).

Utilizatorii publicaţi mai pot fi folosiţi pentru a suporta autentificarea LDAP cu unii utilizatori publicaţi din directorul de distribuire sistem şi alţi utilizatori adăugaţi în director prin alte mijloace. Un utilizator publicat are un atribut uid care numeşte profilul utilizatorului şi nu are nici un atribut userPassword. Când se primeşte o cerere de legare pentru o intrare ca aceasta, serverul apelează securitatea sistemului de operare pentru a valida uid şi parola ca pe un profil utilizator şi parolă valide pentru acel profil. Dacă vreţi să utilizaţi autentificarea LDAP authentication şi aţi dori ca utilizatorii existenţi să f ie capabili să se autentifice utilizând parolele sistemelor de operare, în timp ce utilizatorii ne-i5/OS sunt adăugaţi la director manual, ar trebui să luaţi în considerare această funcţie.

Altă modalitate de a publica utilizatori este să luaţi intrările dintr-o listă de validare HTTP existentă şi să creaţi intrări LDAP corespunzătoare în serverul de director. Aceasta se realizează prin API-ul QGLDPUBVL. Acest API creează intrări director inetOrgPerson cu parole legate la intrarea listei de validare originale. API-ul poate fi rulat o dată sau poate fi planificat să ruleze periodic pentru a verifica noi intrări de adăugat în serverul de director.

Notă: Acest API suportă doar intrările listei de validare create pentru a fi utilizate cu Serverul HTTP (motorizat de Apache). Intrările existente din serverul de director nu vor fi actualizate. Nu sunt detectaţi utilizatorii care sunt şterşi din lista de validare.

Odată ce utilizatorii au fost adăugaţi în director, ei se pot autentifica atât în cadrul aplicaţiilor care folosesc validarea, cât şi în cadrul aplicaţiilor care suportă autentificarea LDAP.

Informaţii sistem

Când configuraţi sistemul de operare să publice informaţii tip Sistem la Directory Server, sunt publicate următoarele tipuri de informaţii:

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

Informaţiile despre imprimantă care pot fi publicate includ:

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

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

Partajări imprimantă

Când configuraţi sistemul de operare să publice partajările de imprimantă, informaţii despre iSeries NetServer selectat partajările de imprimantă su nt publicate laServerul de director activ configurat. Publicarea partajărilor de imprimantă la directorul activ permite utilizatorilor să adauge System i imprimante laWindows 2000 desktop cu vrăjitorul Adăugare imprimantă Windows 2000. Pent ru a face aceasta în vrăjitorul Adăugare imprimantă, specificaţi că vreţi să găsiţi o imprimantă în Directorul activ al Windows 2000. Trebuie să publicaţi partajările imprimantă pe un server de director care suportă schema Microsoft’s Active Directory.

Servicul de calitate TCP/IP

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

Puteţi de asemenea crea o aplicaţie de a publica sau căuta alte tipuri de informaţii dintr-un director LDAP folosind acest cadru de lucru definind agenţi publicare suplimentari şi folosindu-vă de API-urile publicare ale directorului.

Concepte înrudite

API-urile LDAP (Lightweight Directory Access Protocol)
Vedeţi API-urile LDAP (Lightweight Directory Access Protocol) pentru informaţii suplimentare despre API Directory Server

Operaţii înrudite

"Publicarea informaţiilor Directory Server" la pagina 124
Vedeţi cum se publică informaţiile pe Directory Server.

Replicarea

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

Pentru informaţii suplimentare despre replicare, vedeţi următoarele:

Concepte înrudite

"Taskuri de replicare" la pagina 140
Folosiţi aceste informaţii pentru a gestiona replicarea.

"Migrarea unei reţele de servere de replicare" la pagina 95
Folosiţi aceste informaţii dacă aveţi o reţea sau servere copiate.

Privire generală asupra replicării

Prin replicare, o modificare făcută la un director este propagată la unul sau mai multe directoare suplimentare. Ca efect, o modificare la un director apare pe diferite directoare multiple.

Replicarea furnizează două mari avantaje:

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

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

Directorul IBM suportă un model de replicareexpandat master-subordonat.Topologiile de replicare sunt expandate pentru a include:

- Replicarea subarborilor Arborelui de informaţii director (Directory Information Tree - DIT) la anumite servere
- O topologie multi-tier care mai este numită şi replicarea în cascadă
- Asignarea rolului serverului (master sau replică) de subarbore
- Servere master multiple, numite replicaţii peer la peer
- Replicaţii gateway de-a lungul reţelelor

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

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

Tipurile de servere aşa cum sunt definite de funcţie sunt *master/peer*, *cascadare*, *gateway* şi *replica*.

Tabela 1. Rolurile serverului

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

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

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

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

Replicare gateway

Replicarea gateway foloseşte servere gateway pentru a colecta şi distribui informaţii de replicare mai eficient de-a lungul unei reţele de replicare. Principalul avanatj al replicării gateway este reducerea traficului de reţea. Serverele gateway trebuie să fie mastere (să poată fi scrise).

Următoarea figură ilustrează modul de funcţionare a replicării gateway:

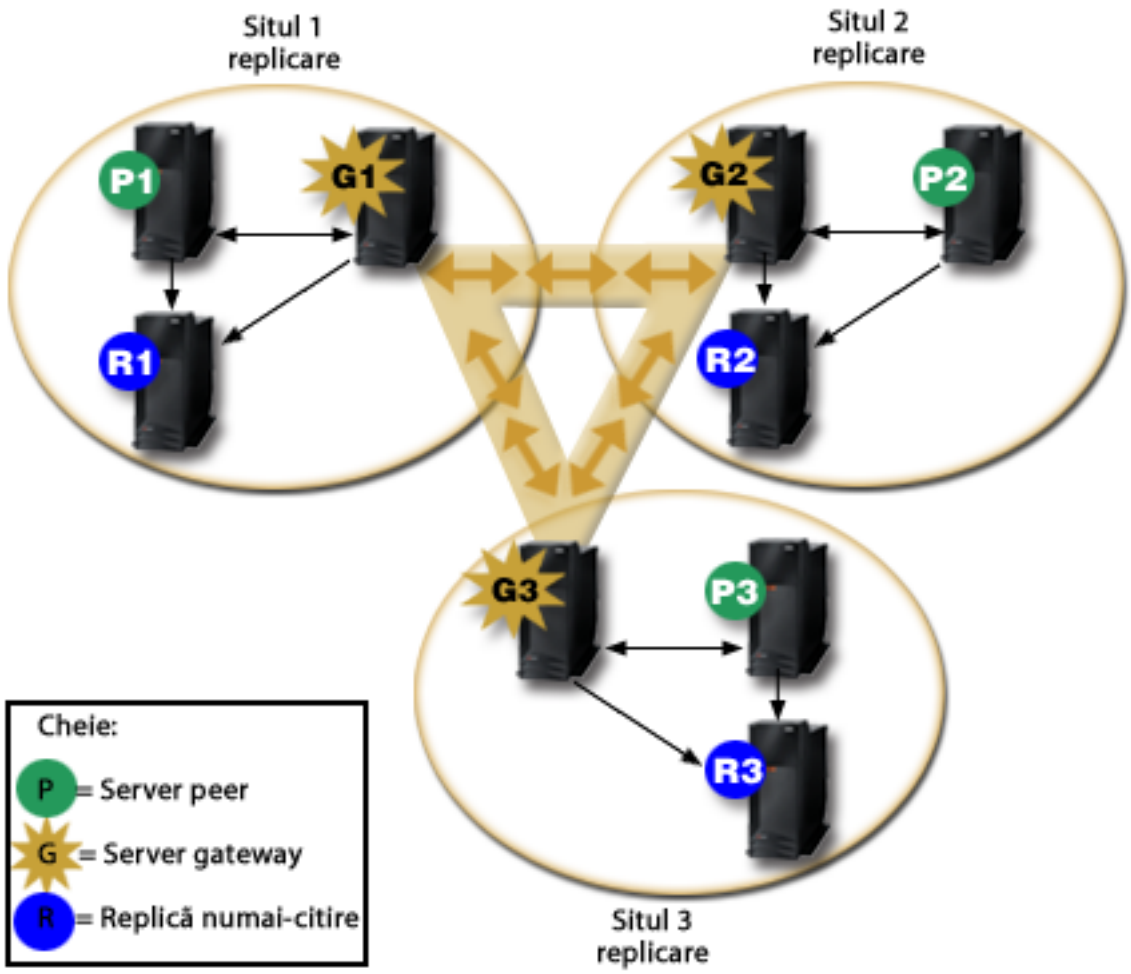


Figura 3. O reţea de replicare cu servere gateway

Reţeaua de replicare din figura precedentă conţine trei site-uri de replicare, fiecare conţinând câte un servergateway. Serverul gateway colectează actualizări de replicare de la serverele peer/master din locaţia de replicare unde se găseşte şi trimite actualizările tuturor celorlalte servere gateway din reţeaua de replicare. De asemenea colectează actualizări de replicare de la alte servere gateway din reţeaua de replicare şi trimite acele actualizări la serverele peer/master şi replică din locaţia de replicare unde se găseşte.

Serverele gateway folosesc ID-uri server şi utilizator pentru a determina ce actualizări sunt trimise la alte servere gateway din reţeaua de replicare şi ce actualizări sunt trimise serverelor locale din locaţia de replicare.

Pentru a configura replicarea gateway, trebuie să creaţi cel puţin două servere gateway. Crearea unui server gateway stabileşte o locaţie (site) de replicare. Trebuie apoi să creaţi acorduri de replicare între gateway şi serverele master/peer şi replică pe care doriţi să le includeţi în locaţia de replicare pentru gateway.

Serverele gateway trebuie să fie mastere (să poată fi scrise). Dacă încercaţi să adăugaţi clasa obiect gateway, ibm-replicaGateway la o subintrare care nu este master, este returnat un mesaj de eroare.

Există două metode de creare a uni server gateway. Puteţi:

- Creaţi un nou server gateway
- Convertiţi un server peer existent într-un server gateway

Notă: Este foarte important să asignaţi un singur server gateway pe locaţie de replicare.

Rezoluţie replicare conflict

Într-o reţea cu servere master multiple, este posibil să efectuaţi modificări conflictuale unei intrări ce poate cauza serverelor să aibe date diferite pentru intrare după ce se copiază modificările. Modificările conflictuale sunt întâlnite mai rar din moment ce necesită ca modificarea să fie făcută pe servere master diferite la închidere la aceeaşi oră. Câteva exemple de modificări conflictuale includ:

- Adăugarea aceleiaţi intrări cu atribute diferite pe două servere.
- Resetarea parolei pentru o intrare ce utilizează parole diferite pe două servere.
- Redenumirea unei intrări pe un server în timpul modificării intrării pe alt server.

IBM Tivoli Directory Server are abilitatea de a detecta automat şi de a rezolva modificări conflictuale astfel încât directoarele de pe toate serverele să rămână consistente. Când sunt detectate conflictele de replicare, modificarea conflictuală este raportată în istoricul serverului şi înregistrată, de asemenea, într-un fişier istoric ″pierdute şi găsite″ astfel încât un administrator să poată recupera orice date pierdute.

Conflict rezoluţie pantru operaţii de adăugare şi modificare în replicarea peer la peer este bazat pe intrare şi modificare timestamps. Actualizarea cu cel mai recent timestamp pe orice server într-un mediu replicaţie multi master este cea care ia precedenţă. Când un conflict de replicare este detectat intrarea înlocuită este arhivată pentru scopuri de recuperare în istoricul pierdute şi găsite.

Ştergerea replicată şi redenumire cerere sunt acceptate în ordinea primită fără rezoluţie de conflict. Dacă conflictele de replicare ce implică ştergerea sau operaţii de modificareDN (redenumire sau mutare) au loc, pot apărea erori ce necesită intervenţia umană. Spre exemplu, dacă o intrare este redenumită pe un server în timp ce este modificată pe un al doilea server, operaţia redenumire modificareDN poate sosi la o replică înainte de operaţia de modificare. Atunci, când operaţia de modificare soseşte, eşuează. În această situaţie, administratorul trebuie să răspundă erorii aplicând modificările intrătii utilizând noul DN. Toate informaţiile necesare pentru refacerea modificărilor cu numele corect sunt păstrate în istoricele de replicare şi eroare. Asemenea erori de replicare sunt apariţii rare într-o topologie de replicare configurată corect, dar nu este bine de presupus că nu au apărut niciodată.

Actualizările aduse aceleiaşi intrări efectuate de mai multe servere pot cauza inconsistenţe în datele directorului pentru că rezoluţia conflict este bazată pe amprentele de timp ale intrărilor. Cea mai recentă amprentă de timp ia precedenţă. Dacă datele de pe serverele dumneavoastră devin inconsistente, vedeţi subiectul ldapdiff în legătura înrudită de mai jos pentru informaţii despre resincronizarea serverelor.

Rezoluţie replicare conflict necesită ca furnizorul să furnizeze amprenta de timp a intrării înainte ca intrarea să fie actualizată pe furnizor. IBM Tivoli Directory Server pentru i5/OS în V5R4 şi versiunile mai vechi nu are capabilitatea să furnizeze acest tip de informaţii. Aşadar, rezoluţia de replicare conflict nu este aplicabilă pentru cazurile în care furnizorul este un server de nivel inferior. În V6R1, serverul consumator IBM Tivoli Directory Server pentru i5/OS, în acest caz, ia amprenta de timp replicată şi actualizează şi o aplică fără verificarea privind conflictele.

Notă: Versiunile mai vechi de IBM Tivoli Directory Server pentru i5/OS nu suportă rezolvarea conflictelor de amprentă de timp. Dacă topologia dumneavoastră conţine versiuni mai vechi de IBM Tivoli Directory Server pentru i5/OS, nu este asigurată consistenţa datelor pentru reţea.

Modificările conflictuale pot fi evitate utilizând un echilibrator de încărcare, preluarea adresei IP virtuale sau alte metode pentru a asigura că modificările de director sunt efectuate către un singur server, în timp ce se furnizează preluare de eroare automată altor servere dacă serverul preferat nu este disponibil.

Un echilibrator de încărcare, cum ar fi IBM WebSphere Edge Server, are un nume de gazdă virtual pe care aplicaţiile îl utilizează când trimit actualizări la director. Echilibratorul de încărcare este configurat pentru a trimite acele actualizări doar unui singur server. Dacă serverul este oprit sau nu este disponibil din cauza unei erori de reţea, echilibratorul de încărcare trimite actualizările următorului server peer disponibil, până când primul server este înapoi pe linie şi disponibil. Vedeţi documentaţia produsului dumneavoastră de echilibrator de încărcare pentru informaţii despre cum să instalaţi şi să configuraţi serverul de echilibrare a încărcării.

Operaţii înrudite

"Modificarea setărilor istoricului pierdute şi găsite" la pagina 157
Istoricul pierdute şi găsite (LostAndFound.log este numele fişierului implicit) înregistrează erorile survenite ca rezultat al conflictelor de replicare. Sunt setări pentru a controla istoricul pierdute şi găsite incluzând locaţia şi dimensiunea maximă a fişierului şi arhivarea fişierelor istoric vechi.

"Crearea unei tipologii simple cu replicare peer" la pagina 147
Replicarea peer este o topologie de replicare în care mai multe servere sunt masteri. Folosiţi replicare peer doar în mediile în care vectorii de actualizare sunt bine cunoscuţi.

Referinţe înrudite

"ldapdiff" la pagina 235
Utilitarul pentru linie de comandă de sincronizare a replicii LDAP.

Terminologia replicării

Definiţii a câtorva terminologii utilizate în replicarea de descriere.

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

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

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

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

Server gateway
Un server care înaintează tot traficul de replicare de la locaţia de replicare locală unde se găseşte la alte servere gateway din reţeaua de replicare. Un server gateway primeşte traficul de replicare de la celelalte servere gateway din reţeaua de replicare, pe care îl înaintează tuturor serverelor din zona de replicare locală. Serverele gateway trebuie să fie mastere (să poată fi scrise).

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

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

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

Grup replică
Prima intrare creată sub un context de replicare are objectclass ibm-replicaGroup şi reprezintă o colecţie de

servere participante la replicare. Furnizează o locaţie de dorit pentru setarea ACL's pentru protejarea informaţiilor topologiei de replicare. Uneltele de administrare suportă în mod curent un grup replică sub fiecare conţinut de replicare, numit **ibm-replicagroup=default**.

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

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

Reţea de replicare
O reţea care conţine locaţii de replicare conectate.

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

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

Locaţie de replicare
Un server gateway şi orice master, servere peer şi replică ce sunt configurate să replicheze împreună.

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

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

Replicare fir de execuţie multiplu

Utilizând replicarea firului de execuţie multiplu (asincron), administratorii pot copia folosind fire de execuţie multiple îmbunătăţind debitul general al replicării.

Când se utilizează replicarea unui singur fir de execuţie (sincron), este posibil ca clienţii ar putea face actualizări într-un mod consistent mai rapid decât replicarea care poate trimite schimbările altor servere.Aceasta este din cauză că standardul modelului replicării utilizează un singur fir de execuţie pentru a replica toate schimbările în ordinea primită.

Standardul modelului replicării se blochează de asemenea când apar anumite tipuri de erori, de exemplu, dacă o cerere copiată modificată eşuează din cauză că intrarea destinaţiei nu există pe serverul consumatorului. În timp ce acest comportament atrage atenţia discrepanţelor între servere care ar trebui corectate, poate de asemenea să conducă la creşterea backlog a modificărilor în aşteptare.În unele aplicaţii, acest backlog al modificărilor nereplicate poate fi nedorit.

Pentru a vă referi la aceasta, replicarea firului de execuţie multiplu furnizează de asemenea abilitatea de a înregistra informaţii despre modificările eşuate într-un istoric de eroare şi pe urmă continuă cu modificările rămase.Istoricul furnizează informţii suficiente pentru a determina care intrări au discrepanţe şi schimbările modificările care sunt sărite odată cu uneltele pentru a reîncarca modificările după corectarea erorilor.Pentur a preveni sărirea unui număr mare de modificări datorită discrepanţelor, un prag de eroare configurabilă este furnizat; când este atins, replicarea se va bloca până când erorile sunt corectate şi istoricul replicării erorii este curăţat.

- Replicarea firului de execuţie multiplu (asincron) poate fi dificil de administrat dacă serverele sau reţelele nu sunt de încredere, cauzând multe modificări copiate pentru a fi sărite.

Când apar erori, erorile sunt înregistrate şi pot fi reluate de către adminstrator dar istoricul erorilor trebuie monitorizat cu atenţie. Următoarea este o căutare pentru a arăta replicarea backlog pentru toate acordurile livrate de un singur server:

```
ldapsearch -h supplier-host -D cn=admin -w ? -s sub
   clasa obiect=ibm-acordul replicării
   ibm-replicationpendingchangecount ibm-replicationstate
```

Dacă starea replicării este activă şi numărătoarea în aşteptare creşte, este un backlog care nu va descreşte decât dacă rata actualizării descreşte sau modul replicării este schimbat de la sincron la asincron.

Replicarea se adaugă de asemenea la încărcarea de lucru la serverul master unde actualizările sunt aplicate primele. În plus la actulizarea copiei sale la datele directorului, serverul master trebuie sa trimită modificările la toate serverele replică. Dacă aplicaţia dumneavoastră sau utilizatorii nu depind de replicarea imediată, atunci planificaţi cu atenţie replicarea pentru a evita dăţile activitatăţii de vârf vă va ajta minimizaţi impactul la debit pe serverul master.

Pentru replicarea firului de execuţie muliplu, când o eroare de replicare survine, apar următoarele:

- ibm-slapdReplMaxErrors: 0 insemnă ca nici o eroare nu trebuie să fie înregistrată în instoricul erorii de replicare dar orice eroare este înregistrată în istoricul serverului şi replicarea este suspendată până toate erorile sunt curăţate.
- Dacă numărul de rori pentru un acord depăşeşte limita, replicarea este suspendată până când cel puţin o eroare este ştearsă sau numărul de erori pentru limita acordului este în creştere.
- Starea pentru acordul replicării este:

```
ibm-replicationStatus: istoricul replicării plin
```

Tabela cu erori de replicare

Tabela cu erori de replicare înregistrează actualizările eşuate, pentru recuperarea ulterioară. Când începe replicarea, este contorizat numărul de eşuări înregistrate pentru fiecare acord de replicare. Acest număr creşte dacă o eşuează o actualizare, fiind adăugată o nouă intrare în tabelă.

Fiecare intrare din tabela erorilor de replicare conţine următoarele:

- ID-ul acordului de replicare.
- ID-ul modificării replicaţei.
- Amprenta de timp pentru când a fost încercată actualizarea.
- Numărul de încercări făcute (această valoare este implicit 1 şi se incrementează pentru fiecare încercare făcută).
- Codul rezultat de la consumator.
- Toate informaţiile de la aplicarea operaţiilor de replicare la actualizare, spre exemplu, DN-ul, datele actuale, elementele de control, steguleţele şi aşa mai departe.

Dacă valoarea specificată de atributul ibm-slapdReplMaxErrors în configuraţia serverului este 0, replicarea continuă să proceseze actualizări. Atributul ibm-slapdReplMaxErrors este un atribut în intrarea de configurare replicare şi poate fi modificat dinamic.

Dacă valoarea specificată de atributul ibm-slapdReplMaxErrors este mai mare decât 0, atunci când numărătoarea de eroare pentru un acord de replicare depăşeşte această valoare, replicarea face unul din următoarele:

- **Un singur fir de execuţie**: Replicarea intră într-o buclă încercând să copieze actualizarea eşuată.
- **Mai multe fire de execuţie**: Replicarea este suspendată.

Dacă serverul este configurat să utilizeze o singură conexiune, replicarea încearcă să trimită aceeaşi actualizare după ce aşteaptă pentru 60 de secunde şi continuă să încerce până când replicarea reuşeşte sau administratorul sare peste actualizare.

Pentru un server configurat să utilizeze conexiuni multiple, replicaţia este suspendată pentru acest acrod. Firul de execuţie receptor continuă sondarea pentru stările oricăror actualizări ce au fost trimise, dar nici o actualizare nu mai este replicată. Pentru a rezuma replicarea, administratorul directorului trebuie să cureţe măcar o eroare pentru acest acord sau să mărească limita cu o modificare dinamică a configuraţiei serverului.

Pentru informaţii suplimentare, vedeţi subiectul Gestionarea cozilor de replicare în legăturile înrudite de mai jos. De asemenea, vedeţi opţiunea -op controlreplerr în subiectul ldapexop în legăturile înrudite de mai jos.

Operaţii înrudite

"Gestionarea cozilor de replicare" la pagina 156
Folosiţi aceste informaţii pentru a monitoriza starea replicării pentru fiecare acord de replicare (coadă) utilizat de acest server.

Referinţe înrudite

"ldapexop" la pagina 214
Utilitarul pentru linie de comandă de operaţie extinsă LDAP.

Acorduri de replicare

Un acord de replicare este o intrare în directorul cu clasa obiect **ibm-replicationAgreement** creată sub o subintrare replică pentru a defini replicarea de la server reprezentată de către subintrare la un alt server.

Aceste obiecte sunt similare cu intrările replicaObject folosite de versiunile de dinainte Directory Server. Acordul de replicare conţine următoarele elemente:

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

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

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

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

Clasele obiect sunt definite pentru fiecare dintre metodele de autentificare suportate:

- legătură simplă
- SASL
- mecanism EXTERN cu SSL
- Autentificare Kerberos

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

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

Pentru un acord de replicare utilizând metoda de replicare cu un singur fir de execuţie, numărul de conexiuni consumator este întotdeauna unul, valoarea atributului este ignorată. Pentru un acord utilizând replicarea cu fire de execuţie multiple, numărul de conexiuni poate fi configurat de la 1 la 32. Dacă nici o valoare nu este specificată pe acord, numărul de conexiuni consumator este setat la unu.

Notă: Pentru subarborele cn=ibmpolicies, toate acordu rile de replicare vor folosi metoda de replicare cu un singur fir de execuţie şi o conexiune consumator, ignorând valorile atributului.

Cum sunt memorate în server informaţiile de replicare

Informaţiile de replicare sunt memorate în director în anumite locuri.

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

Considerente de securitate pentru informaţii de replicare

Treceţi în revistă considerentele de securitate pentru anumite obiecte.

- ibm-replicagroup=default: Accesul controlează pe acest control al obiectului cine poate vizualiza sau modifica informaţiile de replicare memorate aici. Implicit, acest obiect moşteneşte controlul accesului de la părintele său. Ar trebui să consideraţi setarea controlului de acces pe acest obiect pentru a restricţiona accesul la informaţiile de replicare. De exemplu, puteţi defini un grup care conţine utilizatori care vor gestiona replicarea. Acest grup poate fi făcut proprietarul obiectului ″ibm-replicagroup=default″ şi altor utilizatori cărora nu li s-a dat acces la obiect.
- cn=replication,cn=localhost: Există două considerente de securitate pentru acest obiect:
  - Controlul accesului pe acest obiect controlează cine are permisiunea de a vizualiza sau actualiza obiectele memorate aici. Controlul de acces implicit permite utilizatorilor anonimi să citească majoritatea informaţiilor cu excepţia parolelor şi necesită autoritate de administrator pentru a adăuga, modifica sau şterge obiecte.
  - Obiectele memorate în ″cn=localhost″ nusunt niciodată replicate pe alte servere. Puteţi pune acreditările de replicare în acest container de pe serverul care foloseşte acreditările şi ele nu vor fi accesibile altor servere. Alternativ, puteţi alege să puneţi acreditările sub obiectul ″ibm-replicagroup=default″, astfel încât mai multe servere să partajeze aceleaşi acreditări.
- cn=IBMpolicies: Puteţi plasa acreditările de replicare în acest container, însă datele din el sunt replicate către orice consumator din server. Plasarea acreditărilor în cn=replication,cn=localhost este considerată mai sigură.

Replicarea într-un mediu cu o disponibilitate înaltă

Directory Server este deseori utilizat în soluţii cu semnare unică, ceea ce poate avea ca rezultat un singur punct de defectare.

Serverul de director poate fi făcut foarte disponibil utilizând replicarea în două moduri: utilizând Balanţă încărcare sau preluare adresă IPIBM. Informaţii suplimentare despre acest subiect pot fi găsite în Capitolul 13.2 al publicaţiei IBM Cărţi roşii *IBM WebSphere V5.1 Performanţă, Scalabilitate şi disponibilitate înaltă*.

Informaţii înrudite

IBM WebSphere V5.1 Performance, Scalability, and High Availability

Regiuni şi şabloane utilizator

Regiunea şi obiectele şablon ale utilizatorului găsite în unalta de administrare web sunt utilizate pentru a scăpa utiliza torul de nevoia de a învăţa unele din problemele LDAP subliniate.

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

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

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

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

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

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

Concepte înrudite

“Taskuri ale şablonului utilizator şi ale regiunii” la pagina 195
Folosiţi aceste informaţii pentru a gestiona şabloane ale utilizatorului şi regiunii.

Operaţii înrudite

“Crearea unei regiuni” la pagina 195
Folosiţi aceste informaţii pentru a crea o regiune.

Parametrii de căutare

Pentru a limita cantitatea de resurse folosite de server, un administrator poate configura parametrii de căutare pentru a restricţiona posibilităţile de căutare ale utilizatorilor. Posibilităţile de căutare pot fi şi extinse pentru utilizatori speciali.

Căutările utilizatorului pot fi restricţionate sau extinse folosind aceste metode:

Căutare restrictivă

- Căutare paginată
- Căutare sortată
- Dezactivare dereferenţiere alias

Extindere căutare

- Grupuri cu limită de căutare

Căutare paginată

Rezultatele căutării paginate permit unui client să gestioneze cantitatea de date returnată dintr-o cerere de căutare. Un client poate cere un subset de intrări (o pagină) în loc să primească de-odată toate rezultatele de la server. Cererile de căutare consecutivă returnează următoarea pagină de rezultate până când operaţia este anulată sau este returnat şi ultimul rezultat. Administratorul poate restricţiona folosirea acesteia, permiţând utilizarea doar de către administratori.

Căutare sortată

Căutarea sortată permite unui client să primească rezultatele căutării sortate după o listă de criterii, în care fiecare criteriu reprezintă o cheie de sortare. Aceasta mută responsabilitatea de sortare de la aplicaţia clientului la server. Administratorul poate restricţiona folosirea acesteia, permiţând utilizarea doar de către administratori.

Dezactivare dereferenţiere alias

O intrare director cu aliasul objectclass sau aliasObject conţine atributul aliasedObjectName, care este folosit ca referinţă pentru altă intrare din director. Doar cererile de căutare pot specifica dacă aliasurile sunt dereferenţiate. *Dereferenţierea* înseamnă urmărirea aliasului înapoi la intrarea originală. Timpul de răspuns al IBM Directory Server pentru căutări cu opţiunea de dereferenţiere alias setată la **întotdeauna** sau **căutare** poate fi cu mult peste timpul de răspuns la căutările cu opţiunea de dereferenţiere setată la **niciodată**, chiar dacă în director nu există intrări alias. Două setări determină comportamentul de dereferenţiere alias al serverului: opţiunea de dereferenţiere specificată de cererea de căutare a clientului şi opţiunea de dereferenţiere aşa cum este configurată în server de către administrator. Dacă este configurată să facă acest lucru, serverul poate ocoli automat dereferenţierea alias dacă nu există obiecte alias în director sau poate să nu ţină seama de opţiunea de dereferenţiere specificată în cererile de căutare client. Următoarea tabelă descrie modul în care are loc dereferenţierea alias între client şi server.

Tabela 2. Dereferenţiere alias reală bazată pe setările client şi server

Server	Client	Real
niciodată	orice setare	niciodată
întotdeauna	orice setare	setările clientului
orice setare	întotdeauna	setarea serverului
căutare	găsire	niciodată
găsire	căutare	niciodată

Grupuri cu limită de căutare

Un administrator poate crea grupuri cu limită de căutare care pot avea limite de căutare mai flexibile decât utilizatorul obişnuit. Pentru grupurile sau membrii individuali conţinuţi în grupul cu limită de căutare, limitele de căutare sunt mai restrictive decât cele impuse utilizatorilor obişnuiţi.

Când un utilizator iniţiază o căutare, prima dată sunt verificate limitările cererii de căutare. Dacă un utilizator este membru al unui grup cu limită de căutare, se compară limitările. Dacă limitările grupului cu limită de căutare sunt mai mari decât ale cererii de căutare, se utilizează limitările cererii de căutare. Dacă limitările cererii de căutare sunt mai mari decât ale grupului cu limită de căutare, se utilizează limitările grupului. Dacă nu se găsesc intrări ale grupului cu limită de căutare, aceeaşi comparaţie se realizează între limitele de căutare ale serverului. Dacă nu au fost setate limitări de căutare ale serverului, comparaţia se realizează între setările implicite ale serverului. Limitările utilizate sunt întotdeauna cele mai slabe setări ale comparaţiei.

Dacă un utilizator aparţine mai multor grupuri cu limită de căutare, utilizatorului i se acordă cel mai înalt nivel de căutare. De exemplu, utilizatorul aparţine grupului de căutare 1, care acordă limite de căutare cu dimensiunea de

căutare de 2000 de intrări şi un timp de căutare de 4000 de secunde şi grupului de căutare 2, care îi acordă limite de căutare cu intrări nelimitate ale dimensiunii de căutare şi un timp de căutare de 3000 de secunde. Utilizatorul va avea limitările de căutare cu dimensiunea căutării nelimitată şi un timp de căutare de 4000 de secunde.

Grupurile cu limită de căutare pot fi memorate fie sub localhost, fie sub IBMpolicies. Grupurile de căutare aflate sub IBMpolicies sunt replicate; acelea de sub localhost nu sunt replicate. Puteţi memora acelaşi grup cu limită de căutare atât sub localhost, cât şi sub IBMpolicies. Dacă grupul cu limită de căutare nu este memorat sub unul din aceste DN-uri, serverul ignoră partea cu limita de căutare a grupului şi o tratează ca pe un grup obişnuit.

Când un utilizator iniţiază o căutare, prima dată sunt verificate intrările grupului cu limită de căutare de sub localhost. Dacă nu se găsesc intrări pentru utilizator, se caută apoi intrările grupului cu limită de căutare de sub IBMpolicies. Dacă se găsesc intrări sub localhost, intrările grupului cu limită de căutare de sub IBMpolicies nu sunt verificate. Intrările grupului cu limită de căutare de sub localhost au prioritate faţă de cele sub IBMpolicies.

Concepte înrudite

“Taskuri ale grupului de limitare a căutării” la pagina 130
Folosiţi aceste informaţii pentru a gestiona grupurile de limitare a căutării.

Operaţii înrudite

“Ajustarea setărilor de căutare” la pagina 123
Folosiţi aceste informaţii pentru a controla capabilităţiile de căutare ale utilizatorului.

“Căutarea intrărilor directorului” la pagina 189
Folosiţi aceste informaţii pentru a căuta intrările directorului.

Considerente privind suportul de limbă naţională (NLS)

Cosiderentele NLS includ formate de date, caractere, metode de mapare şi şi casetă şir.

Trebuie să luaţi în considerare următoarele cu privire la NLS:

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

Informaţii înrudite

Globalizarea i5/OS
Globalizarea i5/OS vă oferă informaţii suplimentare pentru considerentele privind limba naţională.

Tagurile de limbă

Termenul *taguri de limbă* defineşte un mecanism care permite ca Directory Server să asocieze codurile de limbă cu valori ţinute într-un director şi permite clienţilor să interogheze directorul pentru valorile care îndeplinesc anumite cerinţe de limbă.

Tagul de limbă este o componentă a unei descrieri de atribut. Tagul de limbă este un şir cu prefixul lang-, un sub-tag primar al caracterelor alfabetice şi, opţional, taguri consecutive conectate printr-o liniuţă de despărţire (-). Tagurile următoare pot fi în orice combinaţie de caractere alfanumerice; doar sub-tagurile primare trebuie să fie alfabetice. Sub-tagurile pot avea orice lungime; singura limitare este că lungimea totală a tagului nu poate să depăşească 240 de caractere. Tagurile de limbă nu sunt sensibile la majuscule; en-us, en-US şi EN-US sunt identice. Tagurile de limbă nu sunt permise în componentele DN sau RDN. Este permis un singur tag de limbă la o descriere atribut.

Notă: Într-o bază pe atribut, tagurile de limbă sunt mutual exclusive, cu atribute unice. Dacă aţi desemnat un anumit atribut ca fiind atribut unic, acesta nu poate avea taguri de limbă asociate cu el.

Dacă tagurile de limbă sunt incluse când datele sunt adăugate într-un director, acestea pot fi folosite cu operaţii de căutare pentru a extrage selectiv valori de atribute în anumite limbaje. Dacă se oferă un tag de limbă într-o descriere

atribut din lista de atribute necesare dintr-o căutare, atunci trebuie returnate doar valorile atributelor dintr-o intrare director care au acelaşi tag de limbă cu cel furnizat. Aşadar pentru o căutare de tipul:

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

serverul returnează valori ale unui atribut ″description;lang-en″, însă nu returnează valori ale unui atribut″description″ sau ″description;lang-fr″.

Dacă se efectuează o cerere, specificând un atribut fără a oferi un tag de limbă, atunci sunt returnate toate valorile atributelor, indiferent de tagul lor de limbă.

Tipul de atribut şi tagul de limbă sunt separate printr-un caracter punct şi virgulă (;).

Notă: Caracterul punct şi virgulă poate fi folosit în partea ″NAME″ a unui AttributeType. Totuşi, deoarece acest caracter este folosit pentru a separa AttributeType din tagul de limbă, utilizarea acestuia în partea ″NAME″ a unuiAttributeType nu este permisă.

De exemplu, dacă un client cere un atribut ″description″ şi o intrare de potrivire conţine:

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

serverul returnează:

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

În cazul în care căutarea necesită un atribut ″description;lang-de″, atunci serverul returnează:

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

Utilizarea tagurilor de limbă permite date multilingve în directoarele care suportă clienţi ce operează în mai multe limbi. Folosind tagurile de limbă, o aplicaţie poate fi scrisă astfel încât un client german să vadă doar datele introduse pentru atributul lang-de, iar un client francez să vadă doar datele introduse pentru atributul lang-fr.

Pentru a determina dacă funcţia tagului de limbă este activată, lansaţi o căutare DSE în rădăcină, specificând atributul ″ibm-enabledCapabilities″.

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

Dacă este returnat OID-ul ″1.3.6.1.4.1.4203.1.5.4″, funcţia este activată.

Dacă suportul pentru tagul de limbă nu este activat, orice operaţie LDAP care asociază un tag de limbă cu un atribut este respinsă, cu un mesaj de eroare.

Unele atribute pot avea taguri de limbă asociate cu ele, în timp ce altele nu pot. Pentru a determina dacă un atribut permite sau nu taguri de limbă, utilizaţi comanda ldapexop:

- Pentru atributele care permit taguri de limbă: ldapexop -op getattributes -attrType language_tag -matches true
- Pentru atributele care nu permit taguri de limbă: ldapexop -op getattributes -attrType language_tag -matches false

Operaţii înrudite

“Adăugarea unei intrări ce conţine atribute cu taguri de limbaj” la pagina 186
Folosiţi aceste informaţii pentru a crea o intrare ce conţine atribute cu taguri de limbaj.

Referral-ii directorului LDAP

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

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

Notă: Cu serverul de director, obiectele referral trebuie să conţină numai nume distinctive (dn), un atributobjectClass (objectClass) şi un atribut referral (ref). Vedeţi comanda ldapsearch pentru un exemplucare ilustrează această restricţie.

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

Operaţii înrudite

"Specificarea unui server pentru referral-ii directorului" la pagina 119
Folosiţi aceste informaţii pentru a specifica servere referral.

Referinţe înrudite

"ldapsearch" la pagina 224
Utilitarul pentru linie de comandă de căutare LDAP.

Tranzacţiile

Puteţi configura Directory Server pentru a peemite clienţilor să folosească tranzacţii. 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, celelalte operaţii sunt anulate. Această capabilitate poate ajuta utilizatorii să-şi păstreze 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 face parte dintr-o tranzacţie:

- 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 director să întâmpine probleme impredictibile.

Operaţii înrudite

"Specificarea setărilor de tranzacţie" la pagina 118
Folosiţi aceste informaţii pentru a configura setările de tranzacţie ale Directory Server.

Securitatea Directory Server

Vedeţi cum puteţi să folosiţi o varietate de funcţii pentru a securiza Directory Server.

Vedeţi următoarele pentru informaţii suplimentare despre securitatea Directory Server:

Concepte înrudite

"Directoare" la pagina 4
Serverul de director permite accesul la un tip de bază de date care memorează informaţii intr-o structură ierarhică similară modului în care i5/OS sistemul de fişiere integrat este organizat.

"Nume distinctive (DN-uri)" la pagina 9
Fiecare intrare din director are un nume distinctiv (DN). DN-ul este numele care identifică în mod unic o intrare din director. Prima componentă a DN-ului se numeşte nume distinctiv relativ (RDN - Relative Distinguished Name).

"Taskuri ale proprietăţii securitate" la pagina 167
Folosiţi aceste informaţii pentru a gestiona taskurile proprietăţii securitate.

Operaţii înrudite

"Activarea auditării obiectelor pentru Directory Server" la pagina 122
Folosiţi aceste informaţii pentru a activa auditarea obiectului pentru Directory Server.

Auditarea

Auditarea vă permite să depistaţi detaliile anumitor tranzacţii Directory Server.

Directory Server suportă auditarea de securitate i5/OS. Printre elementele care pot fi auditate se numără:

- Legări şi dezlegări de la serverul de director.
- Modificări la permisiunile obiectelor directoarelor LDAP.
- Modificări la proprietatea obiectelor directoarelor.
- Crearea, ştergerea, căutarea şi modificarea obiectelor directoarelor LDAP.
- Modificări ale parolei administratorului şi actualizare nume distinctive (DNs).
- Modificări ale parolelor utilizatorilor.
- Importări şi exportări de fişiere.

Puteţi avea nevoie să faceţi modificări la setările de auditare înainte ca auditarea intrărilor din director să funcţioneze. Dacă variabila de sistem QAUDCTL are specificat *OBJAUD, puteţi activa auditarea obiectului prin Navigator System i.

Numele grupului pot fi specificate pentru auditare. Clienţii autorizaţi pot cere ca o operaţie să fie realizată utilizând autoritatea grupurilor specificată de client mai degrabă decât grupurile pe care serverul le-a asociat cu identitatea clientului. Această setare controlează dacă auditarea acestor cereri indică doar dacă clientul a specificat grupurile ce urmează să fie utilizate sau include, de asemenea, lista grupurilor specificată. Auditarea listei de grupuri creează intrări de auditare adiţionale ce reţin lista de grupuri pentru fiecare cerere.

Pentru a specifica dacă numele de grupuri ar trebui auditate, executaţi ce urmează:

1. În Navigator System i, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Faceţi clic pe **TCP/IP**.
4. Faceţi clic dreapta pe **IBM Directory Server** şi selectaţi**Proprietăţi**.
5. Pe fişa **Auditare**, verificaţi caseta de bifare **Includere nume grupuri când are loc auditarea grupurilor caller-specified**.

Concepte înrudite

"Directoarele distribuite" la pagina 7
Un director distribuit este un mediu de lucru în care datele sunt partiţionate pe mai multe servere de director. Pentru a face ca directorul distribuit să apară ca un director unic în aplicaţiile client, se foloseşte un server proxy (sau mai multe) care conţine informaţii despre toate serverele şi datele pe care le păstrează.

Operaţii înrudite

"Activarea auditării obiectelor pentru Directory Server" la pagina 122
Folosiţi aceste informaţii pentru a activa auditarea obiectului pentru Directory Server.

Informaţii înrudite

Referinţe de securitate

Auditările securităţii
Pentru informaţii suplimentare despre auditare, vedeţi subiectul Auditarea securităţii.

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

Pentru comunicarea mai sigură cu Directory Server, se poate folosi securitatea SSL şi TLS.

SSL este standardul pentru securitatea Internet. Puteţi folosi SSL pentru a comunica cu clienţi LDAP la fel şi cu servere replică LDAP. Puteţi folosi autentificarea client în plus la autentificarea server pentru a furniza securitate suplimentară la conexiunile dumneavoastră SSL. Autentificarea client necesită ca un client LDAP să prezinte certificatul digital care confirmă identitatea clientului pe server înainte să se stabilească o conexiune.

Pentru a folosi SSL, trebuie să aveţi instalat pe sistem Digital Certificate Manager (DCM), opţiunea 34 din i5/OS. DCM furnizează o interfaţă pentru ca să creaţi şi să gestionaţi certificatele digitale şi memorările de certificate.

TLS este proiectat ca un succesor al SSL şi foloseşte aceleaşi metode criptografice, însă suportă mai mulţi algoritmi criptografici. TLS permite serverului să primească comunicaţii sigure şi nesigure de la client prin portul implicit, 389. Pentru comunicaţii sigure, clientul trebuie să folosească operaţia extinsă StartTLS.

Pentru ca un client să folosească TLS:

1. Directory Server trebuie să fie configurat pentru a folosi TLS sau SSLTLS.
2. Opţiunea -Y trebuie să fie specificată în utilitarele de linie de comandă a clientului.

Notă: TLS şi SSL nu sunt interoperabile. Lansarea unei cereri de pornire TLS (opţiunea -Y) printr-un port SSL duce la o eroare de operare.

Un client se poate conecta la portul securizat (636) folsoind fie TLS, fie SSL. StartTLS este o caracteristică LDAP care vă permite să porniţi o comunicaţie sigură printr-o conexiune nesigură existentă (i.e. port 389). De exemplu, puteţi folosi StartTLS (sau opţiunea -Y a utilitarelor de linie de comandă) cu portul nesigur standard (389); nu puteţi folosiStartTLS cu o conexiune sigură.

Operaţii înrudite

"Activarea SSL şi Transport Layer Security pe Directory Server" la pagina 173
Folosiţi aceste informaţii pentru a activa SSL şi Transport Layer Security pentru Directory Server.

"Activarea SSL şi Transport Layer Security pe Directory Server" la pagina 173
Folosiţi aceste informaţii pentru a activa SSL şi Transport Layer Security pentru Directory Server.

"Folosirea SSL cu utilitarele liniei de comandă LDAP" la pagina 237
Folosiţi aceste informaţii pentru a înţelege cum să utilizaţi SSL împreună cu utilitarele de linie de comandă LDAP.

Informaţii înrudite

DCM (Digital Certificate Manager)

SSL (Secure Sockets Layer)

Protocoale suportate SSL şi TLS (Transport Layer Security)

Autentificarea Kerberos cu Directory Server

Server de director vă permite să utilizaţi autentificarea Kerberos. Kerberos este un protocol de autentificare reţea ca re utilizează criptografie chei secrete pentru a furniza autentificare tare la aplicaţii client şi aplicaţii server.

Pentru a activa autentificarea Kerberos, trebuie să aveţi configurat serviciul de autentificare reţea.

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

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

```
nume-serviciu/nume-gazdă@regiune
```

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

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

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

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

Trebuie să aveţi un fişier tabelă de chei (keytab) care conţine o cheie pentru principalul serviciului LDAP.

Informaţii înrudite

Serviciul de autentificare în reţea
Vedeţi subiectul Serviciul de autentificare în reţea pentru mai multe informaţii despre Kerberos.

Configurarea serviciului de autentificare în reţea
Vedeţi subiectul Configurarea serviciului de autentificare în reţea pentru informaţii despre adăugarea informaţiilor în fişierele tabelă de chei (keytab).

Criptarea parolei

IBM Tivoli Directory Server vă permite să împiedicaţi accesul neautorizat la parolele de utilizator. Administratorul poate configura serverul pentru a cripta valorile atributului userPassword fie într-un format de criptare într-un mod fie intr-un mod de criptare în două moduri. Parolele criptate sunt marcate cu algoritmul de nume criptat astfel încât parolele criptate în formate diferite pot coexis ta în director. Când configuraţia de criptare este schimbată, parolele criptate existente rămân neschimbate şi continuă să funcţioneze.

Utilizând formaturile de criptare într-un singur mod, parolele de utilizator pot fi criptate şi memorate în director, prevenind ca parolele clare să fie accesate de orice utilizatori, incluzând si adinistratorii de sistem. Utilizând formaturile de criptare într-un singur mod, parolele sunt criptate în timp ce sunt memorate în baza de date şi decriptate când sunt returnate unui client autorizat.Utilizarea criptării în două moduri protejează parola memorată în baza de date, în timp ce metodele de autentificare ale utilizării ca DIGEST-MDS care cere serverului să aibă acces la parola textului în clar si să suporte aplicaţii care să aibă nevoie de parola textului în clar.

Parolele criptate într-un singur mod pot fi utilizate pentru potrivirea parolei dar nu pot fi decriptate. În timpul logării utlizatorului, parola de logare este criptată si comparată cu versiunea memorată pentru verificarea potrivirii.

Chiar dacă serverul este configurat să stocheze noi parole într-un format particular, va accepta parole anterioare cri ptate utilizând o altă metodă. De exemplu serverul poate fi configurat pentru a utiliza parola criptată AES256 dar încă sa permită unui administrator sa incarce date dintr-un alt server care conţine parole criptate SHA+1.Ambele seturi de parole pot fi utilizate pentru a autentifica la server utilizând o simplă parolă de autentificare, dar parolele SHA-1 vor fi returnate ca siruri criptate şi nu pot fi utilizate cu autentificarea DISGEST-MD5.

Formaturile criptate într-un singur mod sunt:

- SHA-1
- MD5
- crypt

| După ce serverul este configurat, orice parole noi (pentru noi utilizyatori) sau parolele modificate (pentru utilizatorii
| existenţi) sunt criptate înainte de a fi memorate în directorul baze de date.Următoarele căutări LDAP vor returna o
| valoare marcată si criptată.

| Pentru aplicaţiile care necesită retragerea parolelor clare, ca şi agenţii autentificării nivelului, administratorul
| directorului are nevoie sa configureze serverul pentru a realiza fie o criptare criptată în două moduri pe parolele
| utilizatorului. În aceasta instanţă, parolele clare returnate de server sunt protejate de mecanismul directorului ACL.

| Formatele criptate în două moduri sunt:

- | Fără
- | AES

| Optiunea criptării în două moduri, AES, este furnizată să permită valorile atributului userPassword să fie criptate în
| director şi extrase ca parte componentă a unei intrări în formatul original clar.Este configurat să utilizeze lungimile
| cheilor de 128, 192 si 256 de biţi. Unele aplicaţii ca şi autentificare serverelor de nivel intermediar necesită parole
| pentru a fi extrase în formatul textului în clar; totuşi, politicile de securitate pot interzice memorarea parolelor clare
| într-un spaţiu secund de stocare permanent.Această opţiune satisface ambele cerinte.

| În adăugare, când parola criptată AES este utilizată într-o reţea replicată, dacă toate serverele sunt configurate cu
| aceeaşi frază-parolă si salt, datele parolă vor fi copiate în formele sale criptate, protejând mai bine datele parolă.Daca
| un server nu suportă AES sau este configurat cu o informaţie AES diferită, parolele vor fi decriptate şi copiate ca şi text
| clar.

| **Notă:**

1. | AES nu este suportat de serverele pre-V6R1 LDAP. În mod specific, replicarea datelor criptate AES nu sunt
   | suporate de serverul pre-V6R1 LDAP.
2. | Pe alte platforme, când opţiunea ″Nimic″ este selectată, parolele textului în clar sunt memorate in baza de
   | date. Dacă serverul participă într-o reţea care include IBM Tivoli Directory Server pe alte platforme, se
   | recomndă folosirea uneia dintre opţiunile de criptare AES.

| O simplă legătură va reuşi dacă parola furnizată în legătura cerută se potriveşte cu una dintre valorile multiple ale
| atributului userPassword.

| Când configuraţi serverul folosind Administrare Web, puteţi selecta una din următoarele opţiuni de criptare:

| **Fără** Parolele sunt memorate criptate în două moduri într-o listă de validare şi sunt extrase ca parte a unei intrări în
| formatul textului în clar original. Valoarea sistemului QRETSVRSEC trebuie setată la 1 pentru a folosi această
| setare.

| **crypt** Parolele sunt criptate de algoritmul de criptare UNIX înainte de a fi memorate în director. Când criptarea este
| folosită, doar primul din cele 8 caractere a unei parole este folosit. Parolele mai lungi de 8 caractere sunt
| trunchiate.

| **MD5** Parolele sunt criptate de către algoritmul hash MD5 înainte ca acestea să fie memorate în director.

| **SHA-1** Parolele sunt criptate de algoritmul de criptare SHA-1 înainte ca acestea să fie memorate în director.

| **AES128**
| Parolele sunt criptate de către algoritmul AES128 înainte ca acestea să fie memorate în director şi extrase ca
| parte a unei intrări în formatul clar original.

| **AES192**
| Parolele sunt criptate de către algoritmul AES192 înainte ca acestea să fie memorate în director şi extrase ca
| parte a unei intrări în formatul clar original.

| **AES256**
| Parolele sunt criptate de către algoritmul AES256 înainte ca acestea să fie memorate în director şi extrase ca
| parte a unei intrări în formatul clar original.

Notă: Formatul imask care a fost disponibil în ediţiile anterioare nu mai este o opţiune de criptare.Totuşi, orice valori criptate imask existente încă funcţinează.

Opţiunea implicită pentru Tivoli Directory Server pentru i5/OS este SHA-1, care este compatibil cu ediţii anterioare şi nu este necesar să setaţi o frază-parolă şi salt AES.

În plus lauserPassword, valorile atributuluisecretKey sunt în totdeauna AES256 criptate în director. Spre deosebire deuserPassword, această criptare este impusă pentru valorilesecretKey. Nici o altă opţiune nu este furnizată. Atributul secretKey este o schemă definită IBM. Aplicaţiile pot utiliza acest atribut pentru a memora date sensibile care necesită să fie întotdeauna criptate în director şi să extragă datele în formatul textului în clar utilizând elementul de control de accesare al directorului.

Pentru a schimba tipul criptării utilizând linia de comandă, de exemplu pentru a schimba la**criptare**, lansăm următoarea comandă:

ldapmodify -D <adminDN> -w <adminPW> -i <nume fişier>

unde <nume fişier> conţine:

```
dn: cn=configuraţie
changetype: modificare
înlocuieşte: ibm-slapdPWEncryption
ibm-slapdPWEncryption: crypt
```

Pentru a cauza setările actualizate să aibă efect dinamic, lansăm următoarea ldapexop comandă:

```
ldapexop -D <adminDN> -w <adminPW> -op readconfig -singurul domeniu
"cn=configuraţie" ibm-slapdPWEncryption
```

Notă: Pentru a schimba configuraţia, trebuie sa autentificaţi utilizând un utilizator proiectat DN şi o parolă pentru profilul utilizatoruluii5/OScare are o autoritate specială *ALLOBJ şi *IOSYSCFG. Aceasta este acceaşi autoritate necesară pentru a schimba configuratţia serverului prin alte interfeţe.

Operaţii înrudite

"Setare proprietăţi politică parolă" la pagina 167
Folosiţi aceste informaţii pentru a seta proprietăţile politicii parolei.

Grupurile şi rolurile

Folosiţi grupurile şi rolurile pentru a organiza şi controla accesul sau permisiunile membrilor.

Un grup este o listă, o colecţie de nume. Un grup poate fi utilizat în atributele **aclentry**, **ibm-filterAclEntry** şi **entryowner** pentru a controla accesul sau în utilizări specifice aplicaţiilor, cum ar fi o listă de poştă. Grupurile pot fi definite ca statice, dinamice sau imbricate.

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

Vedeţi următoarele pentru informaţii suplimentare:

Concepte înrudite

"Listele de control al accesului" la pagina 63
Listele de control al accesului (Access control list - ACL) oferă un mijloc de a proteja informaţiile stocate într-un director LDAP. Administratorii folosesc ACL-urile pentru a restricţiona accesul la diverse porţiuni ale directorului sau la anumite intrări din director.

"Taskuri de grup şi de utilizator" la pagina 192
Folosiţi aceste informaţii pentru a gestiona grupuri şi utilizatori.

Operaţii înrudite

"Adăugarea grupurilor" la pagina 193
Folosiţi aceste informaţii pentru a adăuga grupuri.

"Creare grupuri" la pagina 198
Folosiţi aceste informaţii pentru a crea grupuri.

Grupuri statice:

Un grup static defineşte membrii săi listându-i individual.

Un grup static defineşte fiecare membru individual folosind clasa obiect structurală **groupOfNames**, **groupOfUniqueNames**, **accessGroup** sau **accessRole**; sau clasa obiect auxiliară **ibm-staticgroup**. Un grup static folosind clasele obiect structurale **groupOfNames** sau **groupOfUniqueNames** trebuie să aibă cel puţin un membru. Un grup folosind clasele obiect structurale **accessGroup** sau **accessRole** poate fi gol. Un grup static poate fi de asemenea definit folosind clasa obiect auxiliară: **ibm-staticGroup**, care nu necesită atributul **member** şi, prin urmare, poate să fie goală.

O intrare grup tipică este:

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

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

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

Grupuri dinamice:

Un grup dinamic defineşte membrii săi utilizând o căutare LDAP.

Grupul dinamic foloseşte clasa obiect structurală **groupOfURLs** (sau clasa obiect auxiliară **ibm-dynamicGroup**) şi atributul, **memberURL** pentru a defini căutarea folosind o sintaxă LDAP URL simplificată.

```
ldap:///<DN de bază a căutării> ? ? <scopul căutării> ? <searchfilter>
```

Notă: Aşa cum se vede în exemplu, numele de gazdă nu trebuie să fie prezent în sintaxă. Parametrii rămaşi sunt ca o sintaxă URL LDAP normală. Fiecare câmp de parametru trebuie să fie separat de un ?, chiar dacă nu este specificat nici un parametru. Normal, o listă de atribute de returnat ar fi inclusă între DN-ul de bază şi domeniul căutării. Nici acest parametru nu este folosit de server la determinarea apartenenţei dinamice şi poate fi omis, însă separatorul **?** trebuie să fie prezent.

unde:

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

scopul căutării
Specifică extensia căutării. Scopul implicit este baza.

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

filtru căutare
Este filtru pe care doriţi să-l aplicaţi intrărilor din scopul căutării. Vedeţi opţiunea filtru ldapsearch pentru mai multe informaţii despre sinataxa searchfilter. Implicit este objectclass=*

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

Exemple

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

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

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

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

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

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

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

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

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

Iată un exemplu de membru al cn=GROUP1,ou=Austin:

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

Grupuri imbricate:

Imbricarea grupurilor permite crearea de relaţii ierarhice care pot fi folosite pentru a defini apartenenţa de grup moştenită.

Un grup imbricat este definit ca o intrare grup fiu al cărei DN este referit de un atribut conţinut într-o intrare de grup părinte. Un grup părinte este creat prin extinderea unei clase de obiecte grup structurală (**groupOfNames**, **groupOfUniqueNames**, **accessGroup**, **accessRole** sau **groupOfURLs**) împreună cu clasa obiect auxiliară **ibm-nestedGroup**. După extensia grupurilor imbricate, zero sau mai multe atribute **ibm-memberGroup** pot fi adăugate, cu valorile setate la DN-urile grupurilor fiu imbricate. De exemplu:

```
dn: cn=Group 2, cn=Groups, o=IBM, c=US
 objectclass: groupOfNames
 objectclass: ibm-nestedGroup
 objectclass: top
 cn: Group 2
 description: Group composed of static, and nested members.
 member: cn=Person 2.1, cn=Dept 2, cn=Employees, o=IBM, c=US
 member: cn=Person 2.2, cn=Dept 2, cn=Employees, o=IBM, c=US
 ibm-memberGroup: cn=Group 8, cn=Nested Static, cn=Groups, o=IBM, c=US
```

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

Grupuri hibride:

Apartanenţa membrului hibrid este descrisă de o combinaţie de tipuri membru static, dinamic şi imbricat.

De exemplu:

```
dn: cn=Group 10, cn=Groups, o=IBM, c=US
 objectclass: groupOfURLs
 objectclass: ibm-nestedGroup
 objectclass: ibm-staticGroup
 objectclass: top
 cn: Group 10
 description: Group composed of static, dynamic, and nested members.
 memberURL: ldap:///cn=Austin, cn=Employees, o=IBM, c=US??one?objectClass=person
 ibm-memberGroup: cn=Group 9, cn=Nested Dynamic, cn=Groups, o=IBM, c=US
 member: cn=Person 10.1, cn=Dept 2, cn=Employees, o=IBM, c=US
 member: cn=Person 10.2, cn=Dept 2, cn=Employees, o=IBM, c=US
```

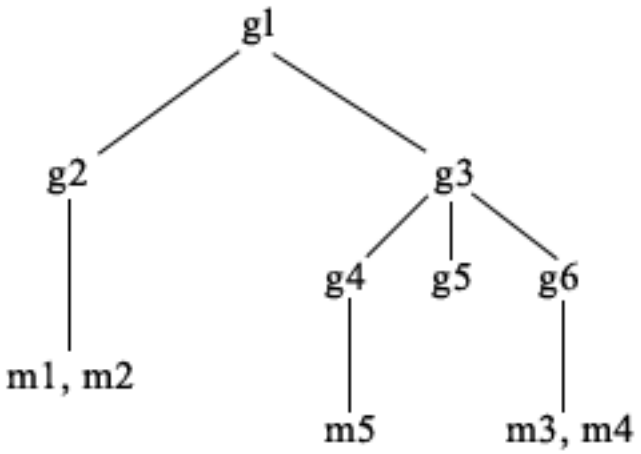
Determinarea apartenenţei la grup:

Pot fi folosite două atribute operaţionale pentru a interoga apartenenţa la un grup agregat.

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

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

Exemple de ierarhie



Pentru acest exemplu, **m1** şi **m2** sunt în atributul membru al **g2**. ACL-ul pentru **g2** permite **utilizatorului1** să citească atributul membru, dar **utiliaztorul2** nu are acces la atributul membru. Intrarea LDIF pentru intrarea **g2** este următoarea:

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

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

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

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

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

Intrările **m3** şi **m4** sunt membri ai grupului **g5** deoarece se potrivesc cu **memberURL** ACL-ul pentru intrarea **m3** permite căutarea atât **utilizatorului1**, cât şi **utilizatorului2**. ACL-ul pentru intrările **m4** nu permite lui **user2** să o caute. LDIF-ul pentru **m4** este următorul:

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

Exemplul 1:

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

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


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

Exemplul 2:

Utilizatorul 2 face o căutare pentru a obţine toţi membrii grupului **g1**. Utilizatorul 2 nu are acces la membrii **m1** sau **m2** deoarece ei nu au acces la atributul membru pentru grupul **g2**. Utilizatorul 2 are acces la atributul membru pentru **g4** şi de aceea are acces la membrul **m5**. Utilizatorul 2 poate efectua căutarea în grupul **g5** memberURL pentru intrarea **m3**, pentru ca membrii să fie menţionaţi, dar nu poate efectua căutarea lui **m4**.

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


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

Exemplul 3:

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

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


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

Exemplul 4:

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

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


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

Clasele de obiecte de grup pentru grupuri imbricate şi dinamice:

O listă de clase de obiecte grup pentru grupuri dinamice şi imbricate.

ibm-dynamicGroup

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

ibm-dynamicMember

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

ibm-nestedGroup

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

ibm-staticGroup

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

Notă: **ibm-staticGroup** este singura clasă pentru care **member** este *opţional*,toate celelalte clase care iau **member** necesită cel puţin 1 membru.

Tipurile de atribut de grup:

O listă de tipuri de atribut grup.

ibm-allGroups

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

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

ibm-allMembers

Arată toţi membrii unui grup. O intrare poate fi un membru direct prin atributele **member**, **uniqueMember** sau **memberURL** sau indirect prin atributul **ibm-memberGroup**. Acest atribut operaţional **Read-only** nu este permis într-un filtru de căutare. Atributul **ibm-allMembers** poate fi folosit într-o cerere de comparaţie pentru

a determoina dacă un DN este membru al grupului dat. De exemplu, pentru a determina dacă ″cn=john smith,cn=users,o=my company″ este membru al grupului ″cn=system administrators, o=my company″:

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

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

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

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

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

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

Rolurile:

Autorizarea bazată pe rol este un complement conceptual al autorizării bazate pe grup.

Ca membru al unui rol, aveţi autoritatea să faceţi tot ce este necesar pentru rol pentru a realiza sarcina. Spre deosebire de un grup, un rol vine cu un set implicit de permisiuni. Nu există vreo presupunere încorporată legată de permisiunile care sunt obţinute (sau pierdute) prin apartenenţa la un grup.

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

De exemplu, dacă există o colecţie de DN-uri ca ’sys admin’, prima dumneavoastră reacţie ar putea fi să vă gândiţi la ele ca la ’sys admin group’ - grup administrator sistem (de vreme ce grupurile şi utilizatorii sunt cele mai familiare tipuri de atribute pirvilegiate). Touşi, din moment ce există un set de permisiuni pe care v-aţi aştepta să le primiţi ca membru al ’sys admin’, colecţia de DN-uri poate fi definită mai exact ca ’sys admin role’ (rol administrator sistem).

Accesul administrativ

Folosiţi accesul administrativ pentru a controla accesul la anumite taskuri administrative.

IBM Directory Server permite următoarele tipuri de acces administrativ:

- **Administrator i5/OS proiectat:** Un client autentificat ca un utilizator proiectat (o intrare LDAP ce reprezintă profilul unui utilizator de sistem de operare) cu autorizările speciale *ALLOBJ şi *IOSYSCFG are autoritatea de a modifica configuraţia directorului utilizând interfeţe LDAP (subarborele cn=configuration sau taskurile ″Administrare server″ ale uneltei de administrare web), precum şi un administrator LDAP pentru alte intrări de director (intrări memorate în unul din sufixele DB2 sau din schemă). Doar administratorii proiectaţi i5/OS pot modifica configuraţia serverului.

- **Administrator LDAP:** Directory Server permite ca un singur ID de utilizator (DN) să fie administratorul primar de server LDAP. Permite de asemenea profilurilor de utilizator proiectate ale sistemului de operare să fie administratori LDAP. Administratorii serverului LDAP pot realiza o listă lungă de taskuri administrative, ca de exemplu gestionarea replicării, a schemei şi a intrărilor de director.
- **Grup de utilizatori administrativi:** Un administrator i5/OS proiectat poate numi mai mulţi utilizatori care să facă parte din grupul administrativ. Membrii acestui grup pot realiza mai multe taskuri deoarece au acelaşi acces administrativ ca un administrator de server LDAP.

  Notă: La folosirea administrării Web, taskurile ce nu au fost oferite membrilor grupului administrativ sunt dezactivate.

Un administrator LDAP sau un membru al unui grup administrativ poate realiza următoarele taskuri de administrare server:

- Modificarea propriilor parole.
- Terminarea conexiunilor.
- Activarea şi modificarea politicii parolei, exceptând criptarea parolei ce poate fi modificată doar de i5/OS administratorul proiectat.
- Gestionarea atributelor unice.
- Gestionarea schemei serverului.
- Gestionarea replicării, exceptând taskul proprietăţilor de replicare (ce include legătura server master DN şi parola şi referral implicit), ce poate fi realizat doar de un i5/OS administrator proiectat.

Concepte înrudite

"Taskurile grupurilor administrative" la pagina 129
Folosiţi aceste informaţii pentru a gestiona grupuri administrative.

"DN-uri administrator şi legare replică" la pagina 87
Puteţi specifica un profil de utilizator proiectat ca DN de legare configurat pentru administrator sau replică. Este utilizată parola profilului de utilizator.

Operaţii înrudite

"Acordarea accesului de administrator utilizatorilor proiectaţi (la filtre)" la pagina 121
Folosiţi aceste informaţii pentru a acorda acces de administrator profilelor utilizatorilor.

Autorizarea proxy

Autorizarea proxy este o formă specială de autentificare. Prin utilizarea acestui mecanism de autorizare proxy, o aplicaţie client se poate lega la director folosind propria identitate, dar îi este permis să realizeze operaţii din partea altui utilizator pentru a accesa directorul destinaţie. Un set de aplicaţii sau utilizatori de încredere poate accesa Directory Server din partea mai multor utilizatori.

Membrii grupului de autorizare proxy îşi pot asuma orice identităţi autentificate, cu excepţia celei de administrator sau a membrilor din grupul administrativ.

Grupul de autorizare proxy poate fi memorat fie sub localhost, fie sub IBMpolicies. Un grup de autorizare proxy sub IBMpolicies este replicat; un grup de autorizare proxy sub localhost nu este. Puteţi memora grupul de autorizare proxy atât sub localhost, cât şi sub IBMpolicies. Dacă grupul proxy nu este memorat sub unul din aceste DN-uri, serverul ignoră partea proxy a grupului şi o tratează ca pe un grup obişnuit.

Ca exemplu, o aplicaţie client, client1, se poate lega la Directory Server cu un nivel înalt al permisiunilor de acces. UtilizatorulA cu permisiuni limitate trimite o cerere aplicaţiei client. Dacă acest client este membru al grupului de autorizare proxy, în loc să transmită cererea către Directory Server pe postul de client1, poate transmite cererea ca UtilizatorulA, folosind nivelul mai limitat de permisiuni. Acest lucru înseamnă că în loc să realizeze cererea pe postul de client1, serverul de aplicaţii poate accesa doar acele informaţii sau să realizeze numai acele acţiuni pe care UtilizatorulA le poate accesa sau realiza. Acesta realizează cererea din partea sau ca proxy pentru UtilizatorulA.

Notă: Valoarea membrului atribut trebuie să fie sub forma unui DN. Altfel, este returnat un mesaj de sintaxă DN nevalidă. Unui DN de grup nu îi este permis să fie un membru al grupului de autorizare proxy.

Administratorii şi membrii grupului administrativ nu pot fi membrii ai grupului de autorizare proxy. Istoricul de auditare înregistrează atât DN-ul de legătură, cât şi DN-ul proxy pentru fiecare acţiune realizată folosind autorizaţia proxy.

Concepte înrudite

"Taskuri ale grupului de autorizare proxy" la pagina 133
Folosiţi aceste informaţii pentru a gestiona grupurile de autentificare proxy.

Listele de control al accesului

Listele de control al accesului (Access control list - ACL) oferă un mijloc de a proteja informaţiile stocate într-un director LDAP. Administratorii folosesc ACL-urile pentru a restricţiona accesul la diverse porţiuni ale directorului sau la anumite intrări din director.

Schimbările făcute asupra fiecărei intrări sau atribut din director pot fi controlate prin folosirea ACL-urilor. Un ACL pentru o intrare sau un atribut date pot fi moştenite de la intrarea ei părinte sau pot fi definite în mod explicit.

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

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

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

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

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

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

Pentru informaţii suplimentare, vedeţi următoarele:

Concepte înrudite

"Grupurile şi rolurile" la pagina 55
Folosiţi grupurile şi rolurile pentru a organiza şi controla accesul sau permisiunile membrilor.

"Listă control acces taskuri (ACL)" la pagina 203
utilizaţi aceste informaţii pentru a gestiona liste de control acces (ACL-uri).

"Atributele operaţionale" la pagina 89
Există mai multe atribute care au o semnificaţie specială pentru Directory Server cunoscute ca atribute operaţionale. Acestea sunt atribute care sunt menţinute de către server şi ori reflectă informaţiile pe care serverul le administrează legate de o intrare, ori afectează operarea serverului.

"Editarea listelor de control al accesului" la pagina 188
Folosiţi aceste informaţii pentru a gestiona liste de control acces (ACL-uri).

"Editarea ACL-urilor pe regiune" la pagina 200
Folosiţi aceste informaţii pentru a edita ACL-urile pe regiune.

Operaţii înrudite

"Editarea ACL-urilor pentru şablon" la pagina 202
Folosiţi aceste informaţii pentru a edita ACL-uri pentru şablon.

Liste de control acces filtrate:

ACL bazate pe filtru (liste de control acces) chemaţi o comparare bazată pe filtru,utilizând un filtru obiect specificat, pentru a potrivi obiectele destinaţie cu accesul efectiv care se aplică lor.

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

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

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

- ibm-filterAclEntry
- ibm-filterAclInherit

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

Concepte înrudite

"Propagare" la pagina 68
Când o intrare nu are explicit definit aclEntry sau entryOwner, este moştenit de la un strămoş sau a propagat jos arborele.

Sintaxa atributului de control acces:

Atributele ACL-ului (access control list) pot fi gestionate utilizând utilizând notaţia LDIF (data interchange format) LDAP. Sintaxa pentru noile atribute ACL bazate pe filtre sunt versiuni modificate ale atributelor ACL curente, nebazate pe filtre.

Următoarele definesc sintaxa pentru ACI (access control information) şi atributele entryOwner utilizând BNF (baccus naur form).

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

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

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

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

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

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

<subjectDn> ::= <DN>

<DN> ::= nume distinctiv după cum e descris în RFC 2251, secţiunea 4.1.3.

<pseudoDn> ::= "group:cn=anybody" | "group:cn=authenticated" |
                       "access-id:cn=this"
<object filter> ::= filtru de căutare şir cupă cum este definit în RFC 2254, secţiunea 4
                               (potrivire extensibilă nu este suportată).
<rights> ::= <accessList> [":" <rights> ]

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

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

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

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

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

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

<attributeName> ::= nume attributeType după cum este descris în RFC 2251, secţiunea 4.1.4.
                       (OID sau şir alpha-numeric cu conducere
                        alfabet, "-" and ";" permis)

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

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

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

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

Subiect

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

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

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

Toate grupurile director pot fi folosite în controlul accesului.

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

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

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

Pseudo DN

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

În prezent, sunt definite trei pseudo DN-uri:

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

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

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

Filtru de obiecte

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

Drepturi

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

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

Permisiune:
Există şase operaţii de bază care pot fi realizate asupra unui obiect din director. Din aceste operaţii, este preluat setul de bază de permisiuni ACI. Acestea sunt: adăugare intrare, ştergere intrare, citire valoare atribut, scriere valoare atribut, căutare atribut şi comparare valoare atribut.

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

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

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

Notă: Pentru operaţiile de căutare, subiectul trebuie să aibă acces de căutare pentru toate atributele din filtrul de căutare sau nu este returnată nici o intrare. Pentru intrările returnate dintr-o căutare, subiectul trebuie să aibă acces de căutare şi de citire la toate atributele din RDN ale intrărilor returnate sau aceste intrări nu sunt returnate.

Destinaţie acces:

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

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

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

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

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

Acestea sunt atribute păstrate de către serverul LDAP şi sunt numai-citire pentru utilizatorii directorului. **OwnerSource** şi **aclSource** sunt descrise în subiectul Propagare.

Clasa de atribute restricţionate care definesc controlul accesului sunt:

- **aclEntry**
- **aclPropagate**
- **entryOwner**
- **ownerPropagate**

- **ibm-filterAclEntry**
- **ibm-filterAclInherit**
- **ibm-effectiveAcl**

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

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

Concepte înrudite

"Propagare"
Când o intrare nu are explicit definit aclEntry sau entryOwner, este moştenit de la un strămoş sau a propagat jos arborele.

EntryOwner:

Proprietarii intrării au permisiuni complete pentru a efectua orice operaţie asupra obiectului indiferent de aclEntry.

În plus, proprietarii intrării sunt singurii cărora le este permis să administreze aclEntries pentru acel obiect. EntryOwner este un subiect de control acces, el poate fi definit ca indivizi, grupuri sau roluri.

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

Propagare:

Când o intrare nu are explicit definit aclEntry sau entryOwner, este moştenit de la un strămoş sau a propagat jos arborele.

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

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

Notă: ACL-urile bazate pe filtru nu se propagă în acelaşi mod în care se propagă ACL-urile care nu sunt bazate pe filtru. Ele se propagă asupra oricăror obiecte care corespund în urma comparaţiei din subarborele asociat.

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

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

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

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

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

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

Concepte înrudite

"Liste de control acces filtrate" la pagina 64
ACL bazate pe filtru (liste de control acces) chemaţi o comparare bazată pe filtru,utilizând un filtru obiect specificat, pentru a potrivi obiectele destinaţie cu accesul efectiv care se aplică lor.

Evaluare acces:

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

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

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

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

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

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

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

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

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

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

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

Regulă specificitate

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

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

Regulă combinatorie

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

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

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

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

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

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

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

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

Acest utilizator obţine:

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

Alt exemplu, cu următoarele aclEntries:

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

Utilizatorul are:

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

Considerente de replicare subarbore:

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

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

Exemplu de definire a ACI-urilor şi a deţinătorilor de intrări:

Următoarele două exemple afişează un subdomeniu administrativ ce este stabilit folosind utilitarele de linie de comandă.

Primul exemplu arată asignarea unui singur utilizator ca entryOwner pentru întregul domeniu. Al doilea exemplu arată un grup asignat ca entryOwner.

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

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

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

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

ibm-filterAclInherit: false
```

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

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

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

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

Exemplu de modificare a ACI şi valorile de intrare proprietar:

Mai multe exemple de modificare a ACI-ului şi a valorilor de intrare proprietar folosind utilitarele de linie de comandă.

Modificare-înlocuire

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

Date fiind următoarele ACI-uri pentru o intrare:

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

realizaţi următoarea modificare:

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

ACI-ul rezultat este:

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

Valorile ACI pentru Dept ABC se pierd prin înlocuire.

Date fiind următoarele ACI-uri pentru o intrare:

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

realizaţi următoarele modificări:

```
dn: cn=some entry
changetype: modify
replace: ibm-filterAclEntry
ibm-filterAclEntry:
group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
                  :grant:rsc

dn: cn=some entry
changetype: modify
replace: ibm-filterAclInherit
ibm-filterAclInherit: false
```

ACI-ul rezultat este:

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

Valorile ACI pentru Dept ABC se pierd prin înlocuire.

Modificare-adăugare

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

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

cu o modificare:

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

ar oferi o aclEntry multi-valoare de:

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

De exemplu, fiind dat ACI-ul:

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

cu o modificare:

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

ar oferi o aclEntry multi-valoare de:

```
Ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
                  :grant:rsc
ibm-filterAclEntry: group:cn=Dept ABC,o=IBM:(cn=Manager ABC):at.attribute1
                  :grant:rsc
```

Permisiunile de sub acelaşi atribut sau clasă de atribut sunt considerate ca fiind blocurile de bază şi acţiunile sunt considerate ca fiind calificative. Dacă este adăugată aceeaşi valoare de permisiune de mai multe ori, doar o valoare este stocată. Dacă aceeaşi valoare de permisiune este adăugată de mai multe ori cu diverse valori de acţiune, este folosită ultima valoare de acţiune. Dacă este gol câmpul permisiunii rezultante (″″), această valoare a per misiunii este setată la null şi valoarea acţiunii este setată la **permisiune**.

De exemplu, fiind dat următorul ACI:

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

cu o modificare:

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

furnizează o aclEntry de:

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

De exemplu, fiind dat următorul ACI:

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

cu o modificare:

```
dn: cn=some entry
changetype: modify
add: ibm-filterAclEntry
ibm-filterAclEntry:
group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
                  :deny:r:critical:deny::sensitive:grant:r
```

furnizează o aclEntry de:

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

Modificare-ştergere

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

Fie dat un ACI de:

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

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

furnizează un ACI care rămâne pe server de:

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

Fie dat un ACI de:

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

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

furnizează un ACI care rămâne pe server de:

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

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

Exemplu de ştergere ACI şi valori deţinător intrare:

Un exemplu de ştergere ACI şi valori de intrare proprietar folosind utilitarele de linie de comandă.

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

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

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

Acelaşi lucru poate fi făcut pentru a şterge aclEntry complet:

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

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

Exemplu de extragere a ACI şi a valorilor de intrare proprietar:

Un exemplu de ştergere ACI şi valori intrare proprietar folosind utilitarele de linie de comandă.

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

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

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

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

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

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

Drept de proprietate asupra obiectelor direcorului LDAP

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

Pentru a aloca dreptul de proprietate puteţi face unul din următoarele:

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

Serverul de 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 obiecte. De exemplu, asumaţi că obiectul cn=A are proprietarul cn=this. Orice utilizator are acces de proprietar la obiectul cn=A dacă se conectează la server ca cn=A.

Concepte înrudite

“Taskuri de intrări de director” la pagina 185
Folosiţi aceste informaţii pentru a gestiona intrările directorului.

Politica de parolă

Cu folosirea serverelor LDAP pentru autentificare, este important ca un server LDAP să suporte politici cu privire la expirarea parolei, încercările de înregistrare eşuate şi reguli de parolă. Directory Server furnizează suport configurabil pentru toate cele trei tipuri de politici.

Politica de parolă este aplicată la toate intrările directorului având un atribut userPassword. Nu puteţi defini o politică pentru un set de utilizatori şi politici diferite pentru alte seturi de utilizatori. Directory Server furnizează de asemenea un mecanism pentru ca clienţii să fie informaţi de condiţiile înrudite cu politica de parolă (parola expiră în trei zile) şi un set de atribute operaţionale pe care un administrator îl poate folosi pentru a căuta lucruri precum utilizatori cu parole expirate sau conturi blocate.

Configurarea

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

- Un comutator ″on/off″ global pentru activarea sau dezactivarea politicii de parolă
- Reguli pentru schimbarea parolelor, inclusiv:
  - Utilizatorii pot schimba propriile parole. Ţineţi cont că această politică se aplică în plus faţă de orice control de acces. Adică, controlul de acces trebuie să dea unui utilizator autorizarea de modificare a atributului userPassword, cât şi politica de parolă care permite utilizatorilor să-şi schimbe parola. Dacă această politică este

dezactivată, utilizatorii nu îşi pot schimba parola. Doar un administrator sau alt utilizator cu autorizare de schimbare a atributului userPassword poate schimba parola pentru o intrare.

- Parolele trebuie să fie schimbate după reset. Dacă această politică este activată, când o parolă este schimbată de oricine altcineva decât acel utilizator, parola este marcată ca reset şi trebuie să fie schimbată de utilizator ănainte de a putea realiza alte operaţii director. O cerere de legare cu o parolă reset este realizată cu succes. Pentru a fi notificată de faptul că parola trebuie resetată, aplicaţia trebuie să ţină cont de politica de parolă.
- Utilizatorii trebuie să trimită parolele vechi la schimbarea parolei. Dacă această politică este activată, o parolă poate fi schimbată doar prin cerere de modificare care include o ştergere a atributului userPassword (cu valoarea veche) şi o adăugare a noii valori userPassword. Aceasta asigură că doar cine îşi cunoaşte parola o poate modifica. Administratorul sau alţi utilizatori autorizaţi să schimbe atributul userPassword pot întotdeauna seta parola.

- Regulile pentru expirarea parolei includ:
  - Parolele nu expiră niciodată sau parolele expiră după un timp configurabil după ce au schimbate ultima dată.
  - Nu se atenţionează utilizatorii când expiră o parolă sau se atenţionează utilizatorii înainte de expirarea parolei cu o perioadă de timp configurabilă. Pentru a fi atenţionată de apropierea expirării parolei, aplicaţia trebuie să ţină cont de politica de parolă.
  - Permiterea unui număr configurabil de înregistrări de graţie după ce parola utilizatorului a expirat. O aplicaţie care ţine cont de politica de parolă va fi notificată de numărul de înregistrări de graţie rămase. Dacă nu sunt permise înregistrări de graţie, un utilizator nu poate autentifica sau schimba parola după ce a expirat.
- Reguli pentru validarea parolei, inclusiv:
  - O dimensiune istorie de parolă configurabilă, care spune serverului să ţină o istorie a ultimelor N parole şi să refuze parolele care au fost folosite anterior.
  - Verificarea sintaxei parolei, inclusiv o setare pentru cum ar trebui să se comporte serverul când parolele sunt hashed. Această setare afectează dacă serverul ar trebui să ignore politica în una din următoarele condiţii:
    - Serverul stochează parolele hash.
    - Un client prezintă o parolă hash către server (aceasta se poate întâmpla la transferul intrărilor între servere folosind un fişier LDIF dacă serverul sursă memorează parole hash).

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

Setările politicii de parolă pentru serverul de director sunt memorate în obiectul ″cn=pwdpolicy″, care arată astfel:

```
cn=pwdpolicy
objectclass=container
objectclass=pwdPolicy
objectclass=ibm-pwdPolicyExt
objectclass=top
cn=pwdPolicy
pwdExpireWarning=0
pwdGraceLoginLimit=0
passwordMaxRepeatedChars=0
pwdSafeModify=false
pwdattribute=userpassword
```

```
pwdinhistory=0
pwdchecksyntax=0
passwordminotherchars=0
passwordminalphachars=0
pwdminlength=0
passwordmindiffchars=0
pwdminage=0
pwdmaxage=0
pwdallowuserchange=true
pwdlockoutduration=0
ibm-pwdpolicy=true
pwdlockout=true
pwdmaxfailure=2
pwdfailurecountinterval=0
pwdmustchange=false
```

Aplicaţii care recunosc politica de parolă

Suportul politicii de parolă pentru serverul de director include un set de controale LDAP care pot fi utilizate de o aplicaţie care recunoaşte politica de parolă pentru a primi notificarea condiţiilor înrudite politicii de parolă.

O aplicaţie poate fi informată cu privire la următoarele condiţii de avertizare:

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

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

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

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

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

- ldap_parse_pwdpolicy_response
- ldap_pwdpolicy_err2string

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

Controlul cererii în politica de parolă

```
Control name: 1.3.6.1.4.1.42.2.27.8.5.1
Control criticality: FALSE
Control value: None
```

Controlul răspunsului în politica de parolă

```
Control name: 1.3.6.1.4.1.42.2.27.8.5.1 (ca la controlul cererii)
Control criticality: FALSE
Control value: O valoare codată BER definită în ASN.1 după cum urmează:
  PasswordPolicyResponseValue ::= SEQUENCE {
  warning [0] CHOICE OPTIONAL {
  timeBeforeExpiration [0] INTEGER (0 .. MaxInt),
  graceLoginsRemaining [1] INTEGER (0 .. maxInt) }
  error  [1] ENUMERATED OPTIONAL {
  passwordExpired   (0),
  accountLocked    (1),
  changeAfterReset   (2),
  passwordModNotAllowed (3),
  mustSupplyOldPassword (4),
  invalidPasswordSyntax (5),
  passwordTooShort   (6),
  passwordTooYoung   (7),
  passwordInHistory   (8) } }
```

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

Atributele operaţionale ale politicii de parolă

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

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

Replicarea politicii de parolă

Informaţiile politicii de parolă sunt replicate de serverele furnizor consumatorilor. Modificările intrării cn=pwdpolicy sunt replicate ca modificări globale, cum sunt modificările schemei. Informaţiile de stare politică parolă pentru intrările individuale sunt de asemenea replicate, astfel încât, de exemplu, dacă o intrare este blocată pe un server furnizor, acea acţiune va fi replicată la orice consumator. Modificările stării politicii de parolă de pe o replică numai citire nu se replică pe nici un alt server.

Concepte înrudite

“Taskuri de parolă” la pagina 167
Folosiţi aceste informaţii pentru a gestiona taskurile parolei.

“Atributele operaţionale” la pagina 89
Există mai multe atribute care au o semnificaţie specială pentru Directory Server cunoscute ca atribute operaţionale. Acestea sunt atribute care sunt menţinute de către server şi ori reflectă informaţiile pe care serverul le administrează legate de o intrare, ori afectează operarea serverului.

Sugestii privind politica de parolă

Politica de parolă nu se potcomporta întotdeauna cum se aşteaptă.

Există două zone în care implementarea unei politici de parole se poate comporta neaşteptat:

1. Dacă atributul pwdReset a fost setat pentru o intrare, un client se poate lega pe timp nedefinit folosind DN-ul de intrare şi parola de resetare. Cu Controlul cererii de politică parolă prezent, aceasta duce la o legare reuşită, cu un avertisment în controlul răspunsului. În cazul în care clientul nu specifică controlul cererii, acest client ″care nu ţine cont de politica de parolă″ vede o legătură reuşită, fără vreo indicaţie că parola trebuie schimbată. Operaţiile ulterioare de sub acel DN vor eşua în continuare, cu o eroare ″nedoritoare de a realiza″; doar rezultatul legăturii iniţiale poate părea înşelător. Aceasta ar putea fi o problemă dacă legătura s-a realizat doar pentru autentificare, cum ar fi cazul unei aplicaţii Web folosind direcorul pentru autentificare.
2. Politicile pwdSafeModify şi pwdMustChange nu se comportă aşa cum v-aţi fi aşteptat cu o aplicaţie care schimbă parolele sub o identitate diferită de DN-ul intrării pentru care parola este schimbată. În acest scenariu, o modificare sigură a parolei efectuată sub o identitate administrativă, de exemplu, va duce la setarea atributului pwdReset. Aplicaţia care schimbă parola poate folosi un cont de administrator şi poate înlătura atributul pwdReset, după cum a fost descris mai devreme.

Autentificarea

Folosiţi o metodă de autentificare pentru a controla accesul la Directory Server.

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

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

- Anonim
- Administratorul directorului (implicit cn=administrator)
- Un profil de utilizator proiectat (la filtre) i5/OS

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

Dintr-o perspectivă LDAP, urmează cadrele de lucru pentru autentificarea LDAP:

- Legătură simplă în care o aplicaţie furnizează un DN şi parola text în clar pentru acel DN.
- SASL (Simple Authentication and Security Layer - Autentificare simplă şi cadru de securitate), care oferă mai multe metode suplimentare de autentificare, inclusiv CRAM-MD5, DIGEST-MD5, EXTERNAL, GSSAPI şi OS400-PRFTKN.

Legătură simplă, DIGEST-MD5 şi CRAM-MD5

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

```
sample.ldif:
        dn: cn=John Smith,cn=users,o=acme,c=us
        objectclass: inetorgperson
        cn: John Smith
        sn: smith
        userPassword: mypassword

ldapadd -D cn=administrator -w secret -f sample.ldif
```

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

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

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

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

Metoda CRAM-MD5 necesită ca serverul să aibă acces la parola text clar (protecţia parolei este setată la nici una, ceea ce înseamnă de fapt că parola este memorată într-o formă decriptabilă şi returnată la căutări sub formă de text clar), iar valoarea de sistem QRETSVRSEC (Retain server security data - Reţinere date de securitate server) trebuie să fie 1 (Reţinere date). Clientul trimite DN-ul către server. Serverul primeşte valoarea userPassword pentru intrare şi generează un şir de caractere aleator. Şirul de caractere aleator este trimis către client. Atât clientul cât şi serverul dispersează (hash) şirul aleator folosind parola drept cheie şi clientul trimite rezultatul către server. Dacă cele două şiruri hashed se potrivesc, cererea de legare are succes şi parola nu a fost trimisă niciodată la server.

Metoda DIGEST-MD5 este similară metodei CRAM-MD5. Necesită ca serverul să aibe acces la parola text în clar (protecţia parolei este setată la nimic) şi ca valoarea de sistem QRETSVRSEC să fie setată la 1. În locul trimiterii DN-ului serverului, DIGEST-MD5 necesită ca clientul să trimită valoarea numelui utilizatorului serverului. Pentru ca un utilizator obişnuit să poată folosi DIGEST-MD5 (nu un administrator) este necesar ca nici o altă intrare din director să aibă aceeaşi valoare cu atributul numeutilizator. Alte diferenţe din DIGEST-MD5 includ mai multe opţiuni de configurare: regiune server, atribut numeutilizator şi parolă administrator. Directory Server permite utilizatorilor să se lege ca utilizatori proiectaţi sau publicaţi, serverul verificând parola prin compararea cu parola unui profil de utilizator din sistem. Din moment ce parola text clar pentru profiluri utilizator nu este disponibilă pentru server, DIGEST-MD5 nu poate fi folosit cu utilizatori proiectaţi sau publicaţi.

Legare ca un utilizator publicat

Directory Server oferă o cale de a avea o intrare LDAP a cărei parole este cea a unui profil utilizator din sistemul de operare de pe acelaşi sistem. Pentru a face aceasta, intrarea trebuie să:

- Să aibă un atribut UID, a cărui valoare este numele unui profil utilizator din sistemul de operare
- Să nu aibă un atribut userPassword

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

Legare ca un utilizator proiectat (la filtre)

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

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

Legătură SASL EXTERNAL

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

De exemplu, fiind dat un certificat asignat lui:

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

DN-ul subiect ar fi:

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

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

Legătură SASL GSSAPI

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

- Generează un pseudo DN al formularului ibm-kn=jsmith@acme.com.
- Căutaţi o intrare având clasele auxiliare ibm-securityidentities şi o valoare altsecurityidenties a formularului KERBEROS:<principal>@<realm>.

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

```
dn: cn=John Smith,cn=users,o=acme,c=us
objectclass: inetorgperson
objectclass: ibm-securityidentities
cn: John Smith
sn: Smith
altsecurityidentities: kerberos:jsmith@acme.com
```

Legătură OS400-PRFTKN

Mecanismul de legare OS400-PRFTKN SASL este folosit pentru autentificarea la server folosind un jeton de profil (vedeţi API-ul Generate Profile Token). Când este folosit acest mecanism, serverul validează jetonul de profil şi asociază DN-ul profilului de utilizator proiectat cu conexiunea (de exemplu, os400-profile=JSMITH,cn=accounts,os400-system=my-as400.mycompany.com). Dacă aplicaţia are deja un jeton de profil, acest mecanism evită nevoia de a obţine numele profilului de utilizator şi parola pentru a efectua o legare simplă. Pentru a utiliza acest mecanism, folosiţi API-ul ldap_sasl_bind_s, specificând un DN, OS400-PRFTKN pentru mecanism şi un berval (date binare ce sunt codate utilizând reguli de codificare simplificate de bază) ce conţine profilul pe 32 pe biţi token pentru acreditări. Când utilizaţi API-urile LDAP în i5/OS sau folosiţi utilitarele de comandă QSH (cum ar fi ldapsearch) pentru a accesa serverul de director local, puteţi omite parola şi API-urile clientului se vor autentifica pe server ca profilul de utilizator curent pentru job. De exemplu:

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

va realiza căutarea sub autorizarea profilului utilizator curent ca şi cum aţi fi folosit:

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

LDAP ca un serviciu de autentificare

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

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

Serverul Web poate de asemenea să reţină DN-ul care a fost utilizat, astfel încât o aplicaţie dată să poată folosi acel DN, probabil prin memorarea datelor personalizate din acea intrare, altă intrare asociată cu ea sau dintr-o bază de date separată folosind DN-ul ca pe o cheie pentru găsirea informaţiilor.

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

Concepte înrudite

"Back-end proiectat de sistem de operare" la pagina 83
Back-end-ul proiectat al sistemului are capacitatea de a mapa obiectei5/OS ca intrări ale arborelui director accesibil-LDAP. Obiectele proiectate sunt reprezentări (proiecţii) LDAP ale obiectelor sistemului de operare în locul intrărilor reale, memorate în baza de date a serverului LDAP.

"Taskuri utilizator" la pagina 192
Folosiţi aceste informaţii pentru a gestiona utilizatori.

API-urile LDAP (Lightweight Directory Access Protocol)
Vedeţi API-urile LDAP (Lightweight Directory Access Protocol) pentru informaţii suplimentare despre API Directory Server

Operaţii înrudite

"Configurarea autentificării DIGEST-MD5 pe Directory Server" la pagina 175
Folosiţi aceste informaţii epntru a configura autentificarea DIGEST-MD5 pe Directory Server.

"Activarea autentificării Kerberos pentru Directory Server" la pagina 175
Folosiţi aceste informaţii pentru a activa autentificarea Kerberos pe Directory Server.

Refuzarea serviciului

Folosiţi opţiunea de configurare negare serviciu pentru a proteja împotriva atacurilor de negare.

Serverul de director oferă protecţie împotriva următoarelor tipuri de atac prin refuzarea serviciului:

- Clienţii care trimit date încet, trimit date parţiale sau nu trimit deloc date
- Clienţii care nu citesc rezultate de date sau care citesc încet rezultatele
- Clienţii care nu se dezleagă
- Clienţii care efectuează cereri care produc cereri în baza de date de lungă durată (long-running)
- Clienţii care se leagă anonim
- Încărcările serverului care împiedică administratorul să administreze serverul

Serverul de director oferă unui administrator mai multe metode de a împiedica atacurile de refuzare a serviciului. Un administrator are întotdeauna acces la server prin intermediul unui fir de execuţie de urgenţă, chiar dacă serverul este

ocupat cu operaţii de lungă durată. În plus, administratorul are controlul asupra accesului la server, inclusiv posibilitatea de a deconecta clienţii cu un anumit DN de legătură sau o adresă IP şi de a configura serverul astfel încât să nu permită accesul anonim. Alte opţiuni de configurare pot fi activate pentru a permite serverului să împiedice în mod activ atacurile de refuzare a serviciului.

Operaţii înrudite

"Gestionarea conexiunilor serverului" la pagina 114
Folosiţi aceste informaţii pentru a vizualiza conexiunile la server şi operaţiile realizate de aceste conexiuni.

"Gestionarea proprietăţilor conexiunii" la pagina 115
Folosiţi aceste informaţii pentru a seta proprietăţile conexiunii, cum ar fi acelea care împiedică clienţii să blocheze serverul.

Back-end proiectat de sistem de operare

Back-end-ul proiectat al sistemului are capacitatea de a mapa obiectei5/OS ca intrări ale arborelui director accesibil-LDAP. Obiectele proiectate sunt reprezentări (proiecţii) LDAP ale obiectelor sistemului de operare în locul intrărilor reale, memorate în baza de date a serverului LDAP.

Profilurile de utilizator sunt singurele obiecte care sunt asociate sau proiectate ca intrări în cadrul arborelui director. Maparea obiectelor profil de utilizator este numită back-end proiectat de utilizatori al sistemului de operare.

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

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

Operaţii înrudite

"Acordarea accesului de administrator utilizatorilor proiectaţi (la filtre)" la pagina 121
Folosiţi aceste informaţii pentru a acorda acces de administrator profilelor utilizatorilor.

Referinţe înrudite

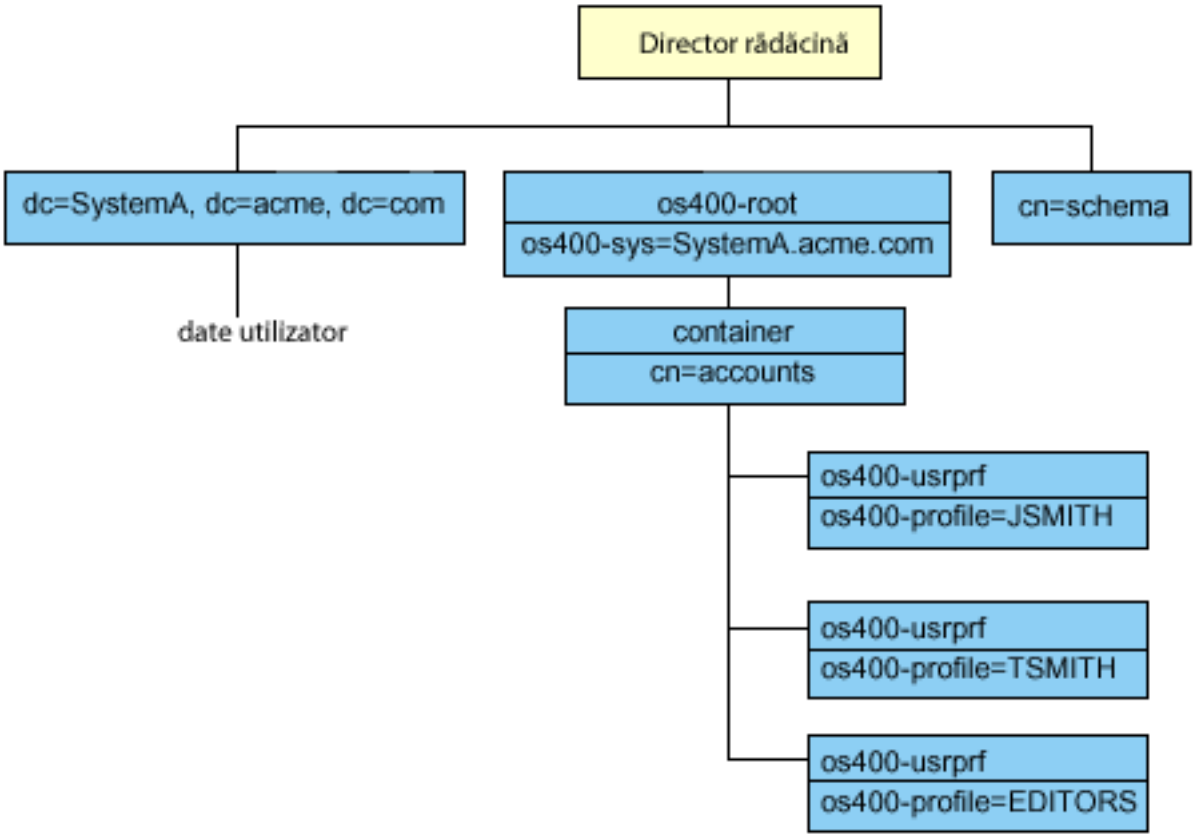
"Autentificarea" la pagina 79
Folosiţi o metodă de autentificare pentru a controla accesul la Directory Server.

Arborele de informaţii al directorului proiectat de utilizatori

Înţelegeţi cum sufixul şi profilele utilizator sunt reprezentate într-un arbore de informaţii de director utilizator.

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

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



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

În figura anterioară, containerul, cn=accounts, este afişat sub rădăcină. Acest obiect nu poate fi modificat. Un container este situat la acest nivel pentru a anticipa alte tipuri de informaţii sau obiecte care ar putea fi proiectate în viitor de sistemul de operare. Mai jos, în containerul cn=accounts sunt profilurile utilizator care sunt proiectate ca objectclass=os400-usrprf. Profilurile utilizator sunt referite ca profiluri de utilizator proiectate şi sunt cunoscute la LDAP în forma os400-profile=JSMITH,cn=accounts,os400-sys=SystemA.acme.com.

Operaţii LDAP

Înţelegeţi ce operaţii LDAP ce operaţii pot fi relizate pe back-end-ul proiectat.

Pot fi realizate următoarele operaţii LDAP folosind profilurile de utilizator proiectate.

Legătură

Un client LDAP se poate lega (autentifica) la serverul LDAP folosind un profil de utilizator proiectat. Aceasta este realizată prin specificarea numelui distinctiv (distinguished name - DN) al profilului utilizator proiectat pentru DN-ul de legare şi parola corectă 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.

Sunt disponibile două mecanisme suplimentare pentru autentificarea în serverul de director ca utilizator proiectat:

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

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

Căutare

Backend-ul proiectat al sistemului 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.

Administratorii LDAPpot interzice toate operaţiile de căutare direcţionată la back-end-ul proiectat al utilizatorului. Pentru informaţii suplimentare, referiţi-vă la subiectul Citire acces la utilizatori proiectaţi în legătura înrudită de mai jos.

Următoarea tabelă prezintă comportamentul backend-ului proiectat al sistemului pentru asemenea operaţii.

Tabela 3. Comportamentul backend-ului proiectat de sistem pentru operaţii de căutare

Cerere de căutare	Baza de căutare	Scopul de căutare	Filtrul de căutare	Comentarii
Întoarce informaţii pentru os400-sys=SystemA, (opţional) pentru containerele de sub acesta şi (opţional) pentru obiectele din acele containere.	os400-sys=SystemA.acme.com	base, sub sau one	objectclass=* objectclass=os400-root objectclass=container objectclass=os400-usrprf	Întoarce atributele corespunzătoare şi valorile lor pe baza scopului şi filtrului specificat. Atributele codate hardware şi valorile lor sunt întoarse pentru sufixele obiectelor sistem şi pentru containerul de sub acesta.
Returnarea tuturor profilurilor 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 profiluri utilizator proiectate. Dacă orice alt filtru este specificat, LDAP_UNWILLING_TO_PERFORM este returnată.
Returnarea tuturor profilurilor 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 profiluri utilizator proiectate. Dacă orice alt filtru este specificat, LDAP_UNWILLING_TO_PERFORM este returnată.
Returnarea tuturor profilurilor de utilizator şi de grup.	cn=accounts, os400-sys=SystemA.acme.com	one sau sub	os400-profile=*	Doar valorile nume distinctiv (DN), objectclass şi profil-os400 sunt returnate pentru profiluri utilizator proiectate. Dacă orice alt filtru este specificat, LDAP_UNWILLING_TO_PERFORM este returnată.
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 profilurilor 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 profiluri utilizator proiectate. Dacă orice alt filtru este specificat, LDAP_UNWILLING_TO_PERFORM este returnată.

Tabela 3. Comportamentul backend-ului proiectat de sistem pentru operaţii de căutare (continuare)

Cerere de căutare	Baza de căutare	Scopul de căutare	Filtrul de căutare	Comentarii
Returnarea tuturor profilurilor 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 profiluri utilizator proiectate. Dacă orice alt filtru este specificat, LDAP_UNWILLING_TO_PERFORM este returnată.
Returnarea tuturor profilurilor 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 profiluri utilizator proiectate. Dacă orice alt filtru este specificat, LDAP_UNWILLING_TO_PERFORM este returnată.

Comparaţie

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.

Administratorii LDAP pot interzice toate operaţiile de comparare direcţionate la back-end-ul proiectat al utilizatorului. Pentru informaţii suplimentare, referiţi-vă la subiectul Citire acces la utilizatori proiectaţi în legătura înrudită de mai jos.

Adăugare şi modificare

Puteţi crea profiluri utilizator folosind operaţia de adăugare LDAP şi puteţi de asemenea să schimbaţi profilurile utilizator folosind operaţia de modificare LDAP.

Ştergere

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

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

- os400-dltusrprf-ownobjopt 1.3.18.0.2.10.8

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

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

  Valoarea de control ownObjOpt specifică acţiunea care trebuie realizată dacă profilul utilizator deţine vreun obiect. Valoarea *NODLT indică să nu se şteargă profilul utilizator dacă profilul utilizator deţine vreun obiect. Valoarea *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 valori de control sunt următoarele:

  – *NODLT: specifică că acel profil nu poate fi şters dacă deţine vreun obiect.
  – *CHGOWN SMITH: specifică că se transfere dreptul de proprietate al oricărui obiect la profilul de utilizator SMITH.
- Identificatorul obiect (OID) este definit în ldap.h as LDAP_OS400_OWNOBJOPT_CONTROL_OID.
  – os400-dltusrprf-pgpopt 1.3.18.0.2.10.9

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

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

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

Exemple de valori 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 profilurile utilizator proiectate deoarece aceasta nu este suportată de sistemul de operare.

API-urile de import şi export

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

Concepte înrudite

EIM (Enterprise Identity Mapping)

“Accesul la citire pentru utilizatorii proiectaţi” la pagina 88
Implicit, proiectarea sistemului back-end furnizează utilizatorilor autorizaţi acces cu citire pentru informaţiile profilului de utilizator prin căutare LDAP şi operaţii de căutare. Accesul cu citire pentru utilizatorii proiectaţi poate fi activat sau dezactivat utilizând Navigator System i sau printr-o setare configurare în fişierul /QIBM/UserData/OS400/DirSrv/idsslapd-instance/etc/ibmslapd.conf (/QIBM/UserData/OS400/DirSrv/idsslapd-QUSRDIR/etc/ibmslapd.conf fişier pentru instanţa serverului implicit).

DN-uri administrator şi legare replică

Puteţi specifica un profil de utilizator proiectat ca DN de legare configurat pentru administrator sau replică. Este utilizată parola profilului de utilizator.

Profilurile de utilizator proiectate pot deveni de asemenea administratori LDAP dacă sunt autorizate la identificatorul funcţiei Directory Server Administrator (QIBM_DIRSRV_ADMIN). Profilurilor multiple de utilizator le pot fi acordate acces de administrator.

Concepte înrudite

“Accesul administrativ” la pagina 61
Folosiţi accesul administrativ pentru a controla accesul la anumite taskuri administrative.

Schema proiectată a utilizatorului

Clasele de obiecte şi atributele de la backend-ul proiectat pot fi găsite în schema de întindere server.

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

Accesul la citire pentru utilizatorii proiectaţi

Implicit, proiectarea sistemului back-end furnizează utilizatorilor autorizaţi acces cu citire pentru informaţiile profilului de utilizator prin căutare LDAP şi operaţii de căutare. Accesul cu citire pentru utilizatorii proiectaţi poate fi activat sau dezactivat utilizând Navigator System i sau printr-o setare configurare în fişierul /QIBM/UserData/OS400/DirSrv/idsslapd-instance/etc/ibmslapd.conf (/QIBM/UserData/OS400/DirSrv/idsslapd-QUSRDIR/etc/ibmslapd.conf fişier pentru instanţa serverului implicit).

Pentru a dezactiva accesul de citire la informaţiile profilului utilizator, urmaţi aceşti paşi:

1. În Navigator System i, expandaţi **Reţea**.
2. Expandaţi **Servere>TCP/IP**.
3. Faceţi clic dreapta pe **IBM Tivoli Directory Server** şi selectaţi **Proprietăţi**.
4. Selectaţi fişa **Bază de date/Sufixe**.
5. Debifaţi caseta de bifare **Permitere acces citire la informaţiile utilizatorului**.

Următoarea linie poate fi modificată în stanţa cn=Front End, cn=Configuration a fişierului de configurare pentru a dezactiva operaţiile de comparare şi căutare la back-end-ul utilizatorului proiectat:

```
ibm-slapdOs400UsrprjRead: TRUE
```

Modificaţi valoarea de la TRUE la FALSE pentru a dezactiva accesul de citire. Dacă valoarea este TRUE sau setarea nu este prezentă în fişierul de configurare, este activat accesul cu citire pentru utilizatorii proiectaţi.

Operaţii înrudite

"Activarea sau dezactivarea accesului cu citire pentru utilizatorii proiectaţi" la pagina 124
Folosiţi aceste informaţii pentru a interzice operaţiile de comparare şi căutare la back-end-ul utilizatorului proiectat.

Referinţe înrudite

"Operaţii LDAP" la pagina 84
Înţelegeţi ce operaţii LDAP ce operaţii pot fi relizate pe back-end-ul proiectat.

Directory Server şi suportul de jurnalizare i5/OS

Directory Server foloseşte suportul de bază de date i5/OS pentru a stoca informaţiile directorului. Directory Server foloseşte controlul comiterii pentru a memora intrările de director în baza de date. Pentru aceasta este necesar suportul de jurnalizare i5/OS.

Când porneşte prima dată serverul sau unealta de import LDIF, sunt construite următoarele:

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

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

Mediul dumneavoastră, mărimea şi structura directorului sau strategia de salvare şi restaurare pot dicta unele diferenţe de la valorile implicite, inclusiv modul de gestionare al acestor obiecte şi starea pragului folosit. Puteţi modifica parametrii comenzii de jurnalizare dacă este necesar. Jurnalizarea LDAP este setată implicit pentru a şterge receptorii vechi. Dacă istoricul de modificare este configurat şi doriţi să păstraţi receptorii vechi, executaţi următoarea linie de comandă:

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

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

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

Informaţii înrudite

CHGJRN (Change Journal - Modificare jurnal)

Atributele unice

Funcţia de atribute unice asigură faptul că atributele specificate au întotdeauna valori unice într-un director.

Aceste atribute pot fi specificate doar în două intrări, cn=uniqueattribute,cn=localhost şi cn=uniqueattribute,cn=IBMpolicies. Rezultatele căutării atributelor unice sunt unice numai pentru acea bază de date a serverului. Rezultatele căutării care includ rezultate de la referinţe ar putea să nu fie unice.

Notă: Atributele binare, atributele operaţionale, atributele de configurare şi atributul objectclass nu pot fi proiectate ca fiind unice.

Nu toate atributele pot fi specificate ca fiind unice. Pentru a determina dacă un atribut poate fi specificat ca fiind unic, folosiţi comanda ldapexop:

- Pentru atributele care pot fi unice: ldapexop -op getattributes -attrType unique -matches true
- Pentru atributele care nu pot fi unice: ldapexop -op getattributes -attrType unique -matches false

Concepte înrudite

"Taskuri cu atribut unic" la pagina 135
Folosiţi aceste informaţii pentru a gestiona atributele unice.

Atributele operaţionale

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

Aceste atribute au caracteristici speciale:

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

Următoarele seturi de atribute operaţionale fac parte din atributele operaţionale suportate de Directory Server:

- creatorsName, createTimestamp, modifiersName, modifyTimestamp sunt prezente la fiecare intrare. Aceste atribute arată DN-ul şi momentul legării când o intrare a fost creată sau modificată ultima dată. Puteţi folosi aceste atribute în filtre de căutare, de exemplu, pentru a găsi toate intrările modificate după un moment de timp specificat. Aceste atribute nu pot fi modificate de nici un utilizator. Aceste atribute sunt replicate la serverele consumatorilor şi sunt importate şi exportare în fişiere LDIF.
- ibm-entryuuid. Prezent la fiecare intrare care este creată când serverul este la V5R3 sau ulterior. Acest atribut este un identificator şir de caractere unic universal asignat fiecărei intrări de către server când este creată o intrare. Este folositor pentru aplicaţiile care trebuie să distingă între intrări cu acelaşi nume de pe servere diferite. Atributul foloseşte algoritmul DCE UUID pentru a genera un ID care este unic peste toate intrările de pe toate serverele folosind o amprentă de timp, adresă de adaptor şi alte informaţii.
- entryowner, ownersource, ownerpropagate, aclentry, aclsource, aclpropagate, ibm-filteracl, ibm-filteraclinherit, ibm-effectiveAcl.
- hasSubordinates. Prezent la fiecare intrare şi are valoarea TRUE dacă intrarea are subordonări.
- numSubordinates. Prezent la fiecare intrare şi conţine numărul de intrări care sunt fii ai acestei intrări.
- pwdChangedTime, pwdAccountLockedTime, pwdExpirationWarned, pwdFailureTime, pwdGraceUseTime, pwdReset, pwdHistory.
- subschemasubentry - Prezent la fiecare intrare şi identifică locaţia schemei pentru acea parte a arborelui. Acesta este util pentru serverele cu mai multe scheme dacă vreţi să găsiţi schema pe care vreţi să o folosiţi în acea parte a arborelui.

Pentru o listă a atributelor operaţionale, folosiţi următoarea operaţie extinsă: ldapexop -op getattributes -attrType operational -matches true.

Concepte înrudite

"Directoare" la pagina 4
Serverul de director permite accesul la un tip de bază de date care memorează informaţii intr-o structură ierarhică similară modului în care i5/OS sistemul de fişiere integrat este organizat.

"Listele de control al accesului" la pagina 63
Listele de control al accesului (Access control list - ACL) oferă un mijloc de a proteja informaţiile stocate într-un director LDAP. Administratorii folosesc ACL-urile pentru a restricţiona accesul la diverse porţiuni ale directorului sau la anumite intrări din director.

"Politica de parolă" la pagina 75
Cu folosirea serverelor LDAP pentru autentificare, este important ca un server LDAP să suporte politici cu privire la expirarea parolei, încercările de înregistrare eşuate şi reguli de parolă. Directory Server furnizează suport configurabil pentru toate cele trei tipuri de politici.

Cache-urile de server

Cache-urile LDAP sunt buffer-e cu spaţiu de stocare rapid în memorie, utilizate pentru a memora informaţii LDAP ca de exemplu interogări, răspunsuri şi autentificarea utilizatorului pentru o viitoare folosire. Ajustarea cache-urilor LDAP este crucială pentru îmbunătăţirea performanţei.

O căutare LDAP care accesează cache-ul LDAP poate fi mai rapidă decât una care necesită o conexiune la DB2, chiar dacă informaţiile sunt prinse înDB2. De aceea, ajustarea cache-urilor LDAP poate îmbunătăţi performanţa, prin evitarea apelurilor către baza de date. Cache-urile LDAP sunt deosebit de folositoare pentru aplicaţiile care extrag frecvent informaţii repetate din cache.

Următoarele secţiuni discută despre fiecare din cache-urile LDAP şi demonstrează cum să determinaţi şi să configuraţi cele mai bune setări ale cache-ului pentru sistemul dumneavoastră.

Concepte înrudite

"Taskuri de performanţă" la pagina 137
Folosiţi aceste informaţii pentru a ajuta setările performanţei.

Cache-ul de atribute

Cache-ul de atribute are avantajul de a fi capabil să rezolve filtrele în memorie, nu în baza de date. Are de asemenea avantajul de a fi actualizat de fiecare dată când se realizează o operaţie LDAP de adăugare, ştergere, modificare sau modrdn.

Pentru a decide ce atribute doriţi să stocaţi în memorie, trebuie să luaţi în considerare:

- Cantitatea de memorie disponibilă pentru server
- Dimensiunea directorului
- Tipurile de filtre de căutare pe care aplicaţia le foloseşte de obicei

Notă: Administratorul cache-ului de atribute poate rezolva următoarele tipuri de filtre simple: filtre cu potrivire exactă şi filtre de prezenţă. Poate rezolva filtre complexe care sunt conjunctive sau disjunctive, iar subfiltrele trebuie să fie cu potrivire exactă, de prezenţă, conjunctive sau disjunctive.

Nu toate atributele pot fi adăugate în cache-ul de atribute. Pentru a determina dacă un atribut poate sau nu să fie adăugat în cache, folosiţi comanda ldapexop:

- Pentru atributele care pot fi adăugate: ldapexop -op getattributes -attrType attribute_cache -matches true
- Pentru atributele care nu pot fi adăugate: ldapexop -op getattributes -attrType attribute_cache -matches false

Memorarea atributelor în cache poate fi configurată în două moduri: manual sau automat. Pentru a configura manual memorarea atributelor în cache, administratorul ar trebuie să realizeze căutări cn=monitor pentru a înţelege cum să realizeze o memorare mai eficientă a atributelor în cache. Aceste căutări întorc informaţiile curente care prezintă ce

atribute sunt în cache, cantitatea de memorie folosită de fiecare cache de atribute, cantitatea totală de memorie folosită de memorarea în cache a atributelor, cantitatea de memorie configurată pentru reţinerea în cache a atributelor şi o listă de atribute folosită cel mai des în filtrele de căutare. Utilizând aceste informaţii, un administrator poate schimba cantitatea de memorie permisă pentru a fi utilizată de către operaţia de memorare în cache a atributelor şi, de asemenea, ce atribute să fie reţinute în cache oricând este necesar, bazându-se pe noi căutări cn=monitor.

Alternativ, un administrator poate configura memorarea în cache automată a atributelor. Când memorarea automată în cache este activată, Directory Server urmăreşte combinaţia de atribute care ar putea fi cel mai util de memorat în cache în limitele de memorie definite de administrator. După aceea actualizează memorarea în cache la un moment dat şi intervalul de timp configurat de administrator.

Cache-ul de filtrare

Când un client emite o interogare a datelor şi aceasta nu poate fi rezolvată în memorie de către administratorul cache-ului de atribute, interogarea este redirecţionată către cache-ul de filtru. Acest cache conţine ID-uri de intrări reţinute în cache.

Se pot întâmpla două lucruri atunci când o interogare ajunge la cache-ul de filtru:

- **ID-urile care se potrivesc cu setările filtrului utilizat în interogare sunt localizate în cache-ul de filtru.** Dacă este aşa, lista cu ID-urile intrărilor care se potrivesc este trimisă la cache-ul intrării.
- **ID-urile intrărilor potrivite nu sunt memorate în cache-ul de filtru.** În acest caz, interogarea trebuie să acceseze DB2 pentru a căuta datele dorite.

Pentru a determina cât de mare trebuie să fie cache-ul de filtru, rulaţi sarcina dumneavoastră de lucru cu cache-ul de filtru setat la diferite valori şi măsuraţi diferenţele în operaţii pe secundă.

Variabila de configurare a limitei de ocolire a cache-ului de filtru limitează numărul de intrări care pot fi adăugate în cache-ul de filtru. De exemplu, dacă variabila limită de ocolire este setată la 1,000, filtrele de căutare care se potrivesc cu peste 1,000 de intrări nu sunt adăugate în cache-ul de filtru. Aceasta împiedică suprascrierea intrărilor folositoare de cache de către căutările de mare amploare şi neobişnuite. Pentru a determina cea mai bună limită de ocolire din cache-ul de filtru pentru sarcina dumneavoastră de lucru, rulaţi sarcina de lucru în mod repetat şi măsuraţi transferul.

Cache-ul de intrare

Cache-ul de intrări conţine date de intrări memorate în cache. ID-urile intrărilor sunt trimise în cache-ul de intrări.

Dacă intrările care se potrivesc cu ID-urile de intrări sunt în cache-ul de intrări, atunci rezultatele sunt returnate clientului. În cazul în care cache-ul de intrări nu conţine intrările care corespund cu ID-urile de intrare, interogarea este direcţionată către DB2 în căutarea intrărilor potrivite.

Pentru a determina cât de mare trebuie să fie cache-ul de intrări, rulaţi sarcina dumneavoastră de lucru cu cache-ul de intrări setat la diferite dimensiuni şi măsuraţi diferenţele în operaţii pe secundă.

Cache-ul ACL

Cache-ul ACL conţine informaţii de control acces ca de exemplu deţinătorul intrării şi permisiunile de intrare pentru intrările accesate recent. Acest cache este folosit pentru a îmbunătăţi performanţa de evaluare a accesului la intrările de adăugare, ştergere, modificare sau căutare.

Dacă o intrare nu se găseşte în cache-ul ACL, informaţiile de control acces sunt extrase din baza de date. Pentru a determina o dimensiune potrivită a cache-ului ACL, măsuraţi performanţa serverului folosind o sarcină de lucru obişnuită cu mărimi variate ale cache-ului ACL.

Controalele şi operaţiile extinse

Controalele şi operaţiile extinse permit extinderea protocolului LDAP fără a-l modifica.

Controale

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

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

Operaţii extinse

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

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

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

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

Concepte înrudite

“Nume distinctive (DN-uri)” la pagina 9
Fiecare intrare din director are un nume distinctiv (DN). DN-ul este numele care identifică în mod unic o intrare din director. Prima componentă a DN-ului se numeşte nume distinctiv relativ (RDN - Relative Distinguished Name).

Referinţe înrudite

“Identificatorii de obiecte (OID)” la pagina 287
Aceste informaţii conţin identificatorii de obiect (OID) utilizaţi în Directory Server.

Considerente privind salvarea şi restaurarea

Directory Server stochează datele şi informaţiile de configuraţie în mai multe locaţii.

Directory Server stochează informaţii în următoarele locaţii:

- Biblioteca de baze de date (implicit QUSRDIRDB), care conţine conţinutul serverelor de director.

  Notă: Puteţi să vedeţi ce bibliotecă de baze de date utilizaţi pe fişa **Database/Suffixes** panou de proprietăţi ale Serverului de director IBM în Navigator System i.
- 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 director 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.

Informaţii înrudite

Salvarea de rezervă şi recuperarea

Iniţierea în Directory Server

Vă iniţiaţi în instalarea, migrarea, planificarea, personalizarea şi administrare Directory Server.

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

Considerente privind migrarea

Dacă instalaţi V5R4 şi aţi folosit Directory Server pe o ediţie anterioară, atunci revedeţi considerentele legate de migrare.

Serverul de director este instalat automat când instalaţi i5/OS. Prima dată când serverul este pornit, el migrează automat orice configuraţii şi date existente. Aceasta poate determina o întârziere lungă înainte ca serverul să fie pornit pentru prima dată.

Notă: Migrarea fişierelor schemă şi de configurare se realizează în timpul instalării şi a primei porniri a serverului. Odată ce această primă pornire a serverului s-a realizat, dacă fişierele schemă şi de configurare din /qibm/userdata/os400/dirsrv sunt restaurate dintr-o copie de rezervă a unei ediţii anterioare, schema şi configurarea unei noi ediţii va fi suprapusă cu fişierele ediţiei anterioare, care nu vor fi migrate din nou. Restaurarea schemei şi configuraţiei unei ediţii anterioare după ce a avut loc migrarea poate determina ca serverul dumneavoastră să nu pornească şi alte erori neaşteptate. Dacă se doreşte o copie de rezervă a schemei şi configuraţiei serverului, aceste date ar trebui salvate după ce serverul a fost pornit cu succes.

Migrarea la V6R1 de la V5R4 sau V5R3

| Folosiţi aceste informaţii dacă aveţi un Directory Server ce rulează sub V5R4 sau V5R3.

| i5/OS V6R1 introduce funcţii noi şi capabilităţi la Serverul de director. Aceste modificări afectează şi serverul de
| director LDAP, şi interfaţa grafică utilizator (GUI) a Navigator System i. Pentru a profita de noile funcţii ale GUI-ului,
| aveţi nevoie să instalaţi Navigator System i pe un PC ce poate comunica peste conexiunea TCP/IP pe server iSeries
| dumneavoastră. Navigator System i este o componentă a System i Access pentru Windows. Dacă aveţi o versiune
| anterioară de Navigator System i instalată, ar trebui să modernizaţi la V6R1.

| i5/OS V6R1 suportă modernizări directe de la V5R4 şi V5R3. Serverul de director este modernizat la V6R1 prima dată
| când serverul este pornit. Datele de director LDAP şi fişierele schemă director sunt migrate automat conform la
| formatele V6R1.

| Când modernizaţi la i5/OS V6R1, ar trebui să fiţi conştient de câteva probleme legate de migrare:

| • Când modernizaţi la V6R1 şi porniţi serverul de director, Serverul de director vă migrează automat fişierele schemă
| la V6R1 şi şterge fişierele schemă vechi. Totuşi, dacă aţi şters sau aţi redenumit fişierele schemă, Serverul de
| director nu le poate migra. Aţi putea primi o eroare sau Serverul de director ar putea presupune că fişierele au fost
| deja migrate.
| • După ce modernizaţi la V6R1, ar trebui mai întâi să vă porniţi serverul o dată să migreze datele existente înainte să
| importe date noi. Dacă încercaţi să importaţi date înainte de a porni o dată serverul şi nu aveţi suficientă autoritate,

importarea poate eşua. Serverul de director migrează datele de director către formatul V6R1 prima dată când porniţi serverul sau importaţi un fişier LDIF. Planificaţi să alocaţi ceva timp pentru ca această migrare să fie completă.

- V6R1introduce abilitatea de a avea instanţe de server de director multiple pe sistemul dumneavoastră i5/OS. Dacă utilizaţi serverul de director înainte de a moderniza la V6R1, serverul dumneavoastră de director va fi migrat la o instanţă. Aceasta include mutarea configuraţiei şi fişierelor schemă de la directorul /QIBM/UserData/OS400/DirSrv la directorul /QIBM/UserData/OS400/DirSrv/idsslapd-QUSRDIR. Se referă la aceasta ca la instanţa serverului de director şi va fi numită instanţa QUSRDIR. De asemenea, două obiecte din biblioteca QUSRSYS sunt mutate la o bibliotecă nouă, QUSRDIRCF. Această migraţie va avea loc când serverul de director este pornit pentru prima dată după modernizarea la V6R1.
- Urmând migrarea, serverul de director LDAP va porni automat când porneşte TCP/IP. Dacă nu vreţi ca serverul de director să pornească automat, folosiţi Navigator System i pentru a schimba setarea.

Migrarea datelor de la V4R4 ,V4R5, V5R1, or V5R2 la V6R1

Folosiţi aceste informaţii dacă aveţi un Server de director tulând sub V4R4, V4R5 sau V5R1.

i5/OS V5R4 nu suportă modernizări de la V4R4, V4R5 la V5R1.

Notă: Când modernizaţi de la V4R4 la orice ediţie ulterioară, ar trebui să ţineţi cont de următoarele probleme:

- V4R4 şi ediţii anterioare a Serverului de director nu iau în seamă zonele de timp când creează intrările marcărilor timpului. Începând cu V4R5, fusul orar este folosit în toate adăugările şi modificările la director. De aceea, dacă modernizaţi datele de la V4R4 sau anterior, Serverul de director ajustează atributele existentecreatetimestamp şi modifytimestamp pentru a reflecta zona de timp corectă. Face aceasta scăzând f usul orar care este definit curent pe sistem de la mărcile timpului care sunt memorate în director. Notaţi că dacă fusul orar curent nu este aceelaşi fus orar care a fost activ când intrările au fost create sau modificate original, noile valori amprentă de timp nu vor reflecta fusul orar original.
- Dacă modernizaţi datele de la V4R4 sau anterior, trebuie să ţineţi cont că pentru datele de director va fi necesar un spaţiu de stocare aproximativ de două ori mai mare decât cel necesar anterior. Aceasta este în V4R4 sau versiuni anterioare, Serverul de director a suportat numai setul de caractere IA5 şi datele salvate în ccsid 37 (format octet singur). Server ul de director suportă setul de caractere complet ISO 10646. După ce modernizaţi, ar trebui să porniţi serverul o dată pentru a migra datele existente înainte de a importa noile date. Dacă încercaţi să importaţi date înainte de a porni serverul o dată şi nu aveţi suficientă autoritate, importarea ar putea eşua.

Dacă vreţi să migraţi aceste ediţii V5R4, puteţi urma oricare dintre următoarele proceduri.

Modernizarea de la V4R4, V4R5 sau V5R1 la o ediţie interimară:

Puteţi migra Directory Server pentru a realiza modernizarea la o ediţie interimară (V5R2 sau V5R3) şi apoi la V6R1.

Modernizările de la V4R4, V4R5, V5R1 şi V5R2 la V6R1 nu sunt suportate, dar sunt suportate următoarele modernizări:

- V4R4 şi V4R5 modernizate la V5R1
- V4R5 şi V5R1 modernizate la V5R2
- V5R1 şi V5R2 modernizate la V5R3
- V5R2 şi V5R3 modernizate la V5R4
- V5R3 şi V5R4 modernizate la V6R1

Pentru informaţii detaliate despre procedurile de instalare i5/OS, vedeţi Instalarea, modernizarea sau ştergerea i5/OS şi a software-ului înrudit. Urmaţi paşii de mai jos pentru a realiza migrarea. Modificările din schemă ar trebuie să fie migrate automat. După fiecare instalare, verificaţi dacă modificările din schemă mai sunt prezente.

1. Pentru V4R4, realizaţi instalarea V5R1. Apoi, instalaţi V5R3.
2. Pentru V4R5, realizaţi instalarea V5R1 sau V5R2. Dacă instalaţi pe V5R1, trebuie apoi să instalaţi pe V5R3. Dacă instalaţi pe V5R2, trebuie apoi să instalaţi pe V5R3 sau V5R4.

3. Pentru V5R1, realizaţi instalarea V5R3.
4. Pentru V5R2, faceţi instalarea V5R3 sau V5R4.
5. După ce aţi ajuns la V5R3 sau V5R4, instalaţi V6R1.
6. Porniţi Directory Server, dacă nu este deja pornit.

Salvarea bibliotecii bazei de date şi instalarea V6R1:

Puteţi migra Serverul de director salvând biblioteca bazei de date pe care Serverul de director o utilizează în V4R4 sauV4R5 şi apoi o rstauraţi după ce aţi instalat V6R1.

Această metodă vă salvează de pasul salvării unei ediţii interimare. Oricum, setările serverului nu sunt migrate, astfel că trebuie să reconfiguraţi setările serverului. Pentru informaţii detaliate despre i5/OS procedurile de instalare, vedeţi Instalare, modernizare sau ştergere i5/OS şi software înrudit. Urmaţi aceşti paşi generali pentru a realiza migrarea:

1. Notaţi orice modificare care aţi făcut-o la fişierele schemă din directorul /QIBM/UserData/OS400/DirSrv. Fişierele schemă nu sunt migrate automatic, aşa încât dacă vreţi să vă păstraţi schimbările va trebui să le implementaţi manual din nou. Dacă au fost realizate actualizări ale schemei folosind fişiere LDIF împreună cu utilitarul ldapmodify, localizaţi aceste fişiere pentru a le putea folosi după punerea în funcţiune a serverului pentru noua ediţie. Unealta de gestionare director sau unealta de administrare web (rulând alt V6R1 sistem) poate fi utilizat pentru a vizualizadefiniţii tip tribut individual şi clase de obiecte. Dacă modificările dumneavoastră constau doar în adăugarea unor noi tipuri de atribute şi clase obiect, faceţi o copie a fişierului /qibm/userdata/os400/dirsrv/v3.modifiedschema. Puteţi folosi acest fişier pentru a construi un fişier LDIF care conţine actualizări ale schemei. Consultaţi “Schema” la pagina 14 pentru informaţii suplimentare.
2. Luaţi aminte că setările de configurare numeroase în proprietăţiile Serverului de director, inclusiv numele bibliotecii bazei de date.
3. Salvaţi biblioteca bazei de date care este specificată în configurarea Serverului de director. Dacă aţi configurat istoricul de modificări, atunci va trebui de asemenea să salvaţi biblioteca QUSRDIRCL.
4. Notaţi configuraţia de publicare. Configurarea publicată, cu excepţia informaţiilor parolei, poate fi vizualizată folosind Navigator System i selectând**Proprietăţi** pentru sistem şi făcând clic pe fişa **Directory Services**.
5. Instalaţi i5/OS V6R1 pe sistem.
6. Folosiţi vrăjitorul în Navigator System i pentru a configura Serverul de director.
7. Restauraţi biblioteca bazei de date pe care aţi salvat-o în pasul 3. Dacă aţi salvat biblioteca QUSRDIRCL în pasul 3, restauraţi-o acum.
8. Folosiţi Navigator System i pentru a reconfigura Directory Server. Specificaţi biblioteca bază de date care a fost configurată anterior şi care a fost salvată şi restaurată în paşii anteriori
9. Folosiţi Navigator System i pentru a reconfigura publicarea.
10. Reporniţi Directory Server.
11. Folosiţi unealta Administrare Web pentru a modifica fişierele schemă pentru orice modificări ale utilizatorului pe care le-aţi remarcat în pasul 1.

Migrarea unei reţele de servere de replicare

Folosiţi aceste informaţii dacă aveţi o reţea sau servere copiate.

Prima dată când este pornit serverul master, acesta migrează informaţiile din directorul care controlează replicarea. Intrările cu objectclass replicaObject sub cn=localhost sunt înlocuite cu intrările utilizate de noul model de replicare. Serverul master este configurat să replice toate sufixele din director. Intrările de acord (agreement) sunt create cu atributul ibm-replicationOnHold setat la valoarea adevărat. Aceasta permite ca actualizările făcute la master să fie acumulate pentru replică până când replica este gata.

Aceste intrări sunt denumite topologia de replicare. Noul master poate fi folosit cu replicări ce rulează versiuni anterioare; datele legate de noile funcţii nu vor fi replicate către serverele nivel-anterior. Este necesar să exportaţi intrările topologiei de replicare de la master şi să le adăugaţi la fiecare replică după ce serverul replică a fost migrat. Pentru a exporta intrările, folosiţi unealta din linia de comandă Qshell “ldapsearch” la pagina 224 şi salvaţi ieşirea într-un fişier. Comanda de căutare este similară cu următoarea:

```
ldapsearch -h master-server-host-name -p master-server-port \
 -D master-server-admin-DN -w master-server-admin-password \
 -b ibm-replicagroup=default,suffix-entry-DN \
 -L "(|(objectclass=ibm-replicaSubEntry)(objectclass=ibm-replicationAgreement))" \
     > replication.topology.ldif
```

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

Notă: Nu includeţi următoarele sufixe:

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

Includeţi doar sufixele create de utilizator.

Repetaţi comanda pentru fiecare intrare sufix pe master, dar înlocuiţi “>” cu “>>” pentru a adăuga la sfârşit datele la fişierul de ieşire pentru căutări următoare. După ce fişierul este complet, copiaţi-l la serverele replică.

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

Pentru a porni serverul, utilizaţi opţiunea **Pornire** în Navigator System i.

Pentru a opri serverul, utilizaţi opţiunea **Oprire** în Navigator System i.

Când adăugaţi fişierul la un server replică, asiguraţi-vă că serverul replică nu este pornit. Pentru a adăuga datele, utilizaţi opţiunea **Importare fişier** în Navigator System i.

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

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

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

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

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

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

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

Migrarea pentru această replică este încheiată.

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

Concepte înrudite

"Replicarea" la pagina 37
Replicarea este o tehnică folosită de serverele de director pentru a îmbunătăţi performanţa şi încrederea. Procesul de replicare ţine datele în directoare multiple sincronizate.

Operaţii înrudite

"Pornirea Directory Server" la pagina 112
Folosiţi aceste informaţii pentru a porni Directory Server.

Schimbarea numelui serviciului Kerberos

Folosiţi aceste informaţii dacă utilizaţi Kerberos mai vechi de V5R3.

Începând în V5R3, numele serviciului utilizat de serverul de director şi API-urile client pentru autentificarea GSSAPI (Kerberos) au fost schimbate. Această schimbare este incompatibilă cu numele de serviciu folosit înainte de V5R3 (V5R2M0 PTF 5722SS1-SI08487 include aceeaşi modificare).

Înainte de V5R3, serverul de director şi API-urile client au folosit un nume serviciu de forma LDAP/nume-gazdă-dns@regiune-Kerberos când era folosit mecanismul GSSAPI (Kerberos) pentru autentificare. Acest nume nu respectă standardele care definesc autentificarea GSSAPI, care spun că numele de principal ar trebui să înceapă cu literele mici ″ldap″. Drept urmare, atât serverul de director, cât şi API-urile client ar putea să nu interopereze cu produsele altor vânzători. Aceasta este adevărat în special dacă centrul de distribuţie chei Kerberos (KDC) are nume de principal sensibile la majuscule. Furnizorul de servicii LDAP pentru JNDI, un API client Java LDAP folosit în mod normal, este un exemplu de client inclus în sistemul de operare care foloseşte numele de serviciu corect.

V5R3M0 a schimbat numele de serviciu pentru a se conforma cu standardele. Aceasta introduce oricum propriile probleme de compatibilitate.

- Un server de director configurat să folosească autentificarea GSSAPI nu va începe să instaleze această ediţie. Aceasta deoarece fişierul keytab folosit de către server are acreditări care folosesc nume vechi de serviciu (LDAP/mysys.ibm.com@IBM.COM), în timp ce serverul caută acreditări care folosesc noul nume de serviciu (ldap/mysys.ibm.com@IBM.COM).
- Un server de director sau aplicaţie LDAP utilizând API_urile LDAP la V5R3M0 s-ar putea să nu fie capabile să autentifice cu se rvere mai vechi OS/400 sau clienţi. Pentru a corecta aceasta, ar trebui să faceţi următoarele:
  1. Dacă KDC foloseşte nume principal sensibile la majuscule, creaţi un cont care foloseşte numele service corect (ldap/mysys.ibm.com@IBM.COM).
  2. Actualizaţi fişierul keytab folosit de Directory Server pentru a conţine acreditări pentru noul nume de serviciu. Aţi putea dori să ştergeţi vechile acreditări. Puteţi folosi utilitarul Qshell keytab pentru a actualiza fişierul keytab. Implicit, Directory Server utilizează fişierul /QIBM/UserData/OS/400/NetworkAuthentication/keytab/krb5.keytab file. Vrăjitorul NAS (Network Authentication Service) V5R3M0 (Kerberos) din Navigator System i creează de asemenea intrări keytab care folosesc noul nume de serviciu.
  3. Actualizaţi sistemele OS/400 V5R2M0 în care este folosit GSSAPI aplicând PTF 5722SS1-SI08487.

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

```
ADDENVVAR ENVVAR(LDAP_KRB_SERVICE_NAME)
```

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

```
export LDAP_KRB_SERVICE_NAME=1
```

Planificarea pentru Directory Server

Înainte să începeţi să configuraţi Directory Server şi să creaţi structura directorului dumneavoastră LDAP, ar trebui să vă rezervaţi câteva minute pentru a crea un plan.

Luaţi în considerare următoarele înainte de a începe să configuraţi Directory Server şi să creaţi structura directorului LDAP:

- **Organizarea directorului**. Planificaţi structura directorului dumneavoastră şi determinaţi ce sufixe şi atribute va necesita serverul dumneavoastră. Pentru informaţii suplimentare, vedeţi subiectele Practicile recomandate pentru structura de director, Directoarele, Sufixul şi Atributele.
- **Decideţi cât de mare va fi directorul dumneavoastră**. 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, un director gol care utilizează schema serverului de director implicită necesită aproximativ 10 MB de spaţiu de stocare. Un director care foloseşte schema implicită şi care conţine 1000 de intrări de informaţii tipice angajat necesită aproximativ 30 MB de spaţiu de memorare. Acest nunmăr va varia depinzând de atributele exacte care le-aţi folosit. Se va mări de asemenea considerabil dacă aţi memorat obiecte mari, cum ar fi imagini, în director.
- **Decideţi ce măsuri de securitate veţi lua**.

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

  Serverul de director suportă utilizarea SSL-ului (Secure Sockets Layer) şi Certificate digitale ca şi TLS (Transport Layer Security) pentru securitatea comunicaţiei. De asemenea este suportată şi autentificarea Kerberos.

  Serverul de director vă permite să controlaţi accesul la obiectele direc torului cu liste de control acces (ACL-uri). Puteţi de asemenea folosi auditarea securităţii sistemului de operare pentru a proteja directorul.

  În plus decideţi ce politică de parolă să aplicaţi.
- **Alegeţi un DN administrator şi o parolă**. DN-ul administrator implicit este cn=administrator. Aceasta este singura identitate care vă autorizează să creaţi sau să modificaţi intrările din director când serverul este configurat iniţial. Puteţi de asemenea folosi DN-ul administrator implicit sau să selectaţi un alt DN. De asemenea trebuie să creaţi o parolă pentru DN-ul administrator.
- **Instalare software preliminar pentru unealta de administrare Web pentru Directory Server**. În ordine pentru a utiliza Unealta de administrare web a serverului de director, următoarele produse cerinţe preliminare trebuiesc instalate.
  - Server HTTP IBM pentrui5/OS (5761-DG1)
  - IBM WebSphere Server de aplicaţii 6.0 (5733-W60 Opţiuni Bază sau Explicit)
- **Planificaţi o strategie de recuperare şi copiere de rezervă**. Planificaţi cum veţi salva datele dumneavoast ră şi informaţiile de configurare.

Concepte înrudite

“Practici recomandate pentru structura directorului” la pagina 34
Directory Server este deseori folosit ca magazie pentru utilizatori şi grupuri. Această secţiune descrie câteva practici recomandate pentru configurarea unei structuri optimizate pentru gestionarea utilizatorilor şi a grupurilor. Această structură şi modelul de securitate asociat pot fi extinse pentru alte utilizări ale directorului.

“Directoare” la pagina 4
Serverul de director permite accesul la un tip de bază de date care memorează informaţii intr-o structură ierarhică similară modului în care i5/OS sistemul de fişiere integrat este organizat.

“Sufixul (contextul de numire)” la pagina 12
Un sufix (numit şi context de numire) este un DN care identifică cea mai de sus intrare dintr-o ierarhie de director păstrată local.

“Atributele” la pagina 18
Fiecare intrare din director are un set de atribute asociate cu aceasta prin clasa sa de obiecte.

"Considerente privind salvarea şi restaurarea" la pagina 92
Directory Server stochează datele şi informaţiile de configuraţie în mai multe locaţii.

Informaţii înrudite

IBM HTTP Server
Vedeţi subiectul IBM HTTP Server pentru informaţii suplimentare despre IBM HTTP Server şi IBM WebSphere Application Server

Configurarea Directory Server

Rulaţi vrăjitorul Configurare Directory Server pentru a personaliza setările Directory Server.

1. Dacă sistemul dumneavoastră nu a fost configurat pentru a publica informaţii către alt server LDAP şi niciun server LDAP nu este cunoscut serverului DNS TCP/IP, atunci Directory Server este instalat automat cu o configuraţie implicită limitată. Directory Server oferă un vrăjitor pentru a vă ajuta să realizaţi o configuraţie specifică necesităţilor dumneavoastră. Puteţi rula vrăjitorul ulterior, din Navigator System i. Folosiţi acest vrăjitor când configuraţi iniţial serverul de director. Mai puteţi folosi vrăjitorul şi pentru a reconfigura serverul de director.

   Notă: Când folosiţi vrăjitorul pentru a reconfigura serverul de director, porniţi configurarea de la zero. Configuraţia originală este ştersă, nu schimbată. Însă datele din director nu sunt şterse, ci rămân stocate în biblioteca pe care aţi selectat-o la instalare (implicit QUSRDIRDB). Istoricul modificărilor rămâne de asemenea intact, fiind creat implicit în biblioteca QUSRDIRCL.

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

   Dacă doriţi să modificaţi configuraţia serverului de director, nu să o ştergeţi complet, faceţi clic dreapta pe **Director** şi selectaţi **Proprietăţi**. În acest fel nu se şterge configuraţia iniţială.

   Pentru a configura serverul, trebuie să aveţi autorizările speciale *ALLOBJ şi *IOSYSCFG. Dacă doriţi să configuraţi auditarea de securitate, trebuie să aveţi şi autorizarea specială *AUDIT.
2. Pentru a porni vrăjitorul de configurare Directory Server, parcurgeţi paşii următori:
   a. În Navigator System i, expandaţi **Reţea**.
   b. Expandaţi **Servere**.
   c. Faceţi clic pe **TCP/IP**.
   d. Faceţi clic dreapta pe **IBM Directory Server** şi selectaţi **Configurare**.

   Notă: Dacă aţi configurat deja serverul de director, faceţi clic pe **Reconfigurare**, nu pe **Configurare**.
3. Urmaţi instrucţiunile din vrăjitorul de configurare pentru a configura Directory Server.

   Notă: Ar putea fi necesar să puneţi biblioteca ce memorează datele din director într-un ASP de utilizator, nu în ASP-ul de sistem. Însă această bibliotecă nu poate fi stocată într-un ASP independent, eşuând orice încercare de configurare, reconfigurare sau pornire a serverului cu o bibliotecă aflată într-un ASP independent.
4. Când vrăjitorul s-a terminat, Directory Server are o configuraţie de bază. Dacă rulaţi Lotus Domino pe sistemul dumneavoastră, atunci portul 389 (portul implicit pentru serverul LDAP) ar putea să fie deja folosit de funcţia LDAP Domino. Trebuie să faceţi una din următoarele:
   - Schimbaţi portul pe care Lotus Domino îl foloseşte. Pentru informaţii suplimentare, vedeţi Host Domino LDAP şi Directory Server de pe acelaşi sistem , în subiectul E-mail-ul.
   - Modificaţi portul pe care îl foloseşte Directory Server. Consultaţi "Modificarea portului sau adresei IP" la pagina 118 pentru mai multe informaţii.
   - Folosiţi adrese IP specifice. Consultaţi "Modificarea portului sau adresei IP" la pagina 118 pentru mai multe informaţii.
5. Creaţi intrări corespunzătoare pentru sufixul sau sufixele pe care le-aţi configurat. Pentru informaţii, vedeţi "Adăugarea şi înlăturarea sufixelor serverului de director" la pagina 119.
6. Puteţi dori să faceţi câteva din următoarele sau toate înainte de a continua:

- Activaţi securitatea Secure Sockets Layer (SSL), vedeţi “Activarea SSL şi Transport Layer Security pe Directory Server” la pagina 173.
- Activaţi autentificarea Kerberos, vedeţi “Activarea autentificării Kerberos pentru Directory Server” la pagina 175.
- Setaţi un referral, vedeţi “Specificarea unui server pentru referral-ii directorului” la pagina 119.

7. Porniţi Directory Server. Pentru informaţii, vedeţi “Pornirea Directory Server” la pagina 112.
8. Instanţa Directory Server existentă este numită instanţa QUSRDIR. Fişierele sale de schemă şi de configuraţie se află în directorul /QIBM/UserData/OS400/DirSrv/idsslapd-QUSRDIR. Instanţa serverului poate fi creată automat dacă încercaţi să porniţi instanţa implicită. Nicio altă instanţă nu va fi creată automat.

Concepte înrudite

“Configurarea implicită pentru Directory Server” la pagina 296
Directory Server este instalat automat când instalaţi i5/OS. Această instalare include o configuraţie implicită.

Popularea directorului

Populaţi directorul cu date.

Sunt mai multe metode de a popula directorul cu date:

- Publicaţi informaţii la Serverul de director.
- Importaţi date de la un fişier LDIF.
- Copiaţi utilizatori de la o listă de aplicaţii server HTTP la Serverul de director.

Operaţii înrudite

“Publicarea informaţiilor Directory Server” la pagina 124
Vedeţi cum se publică informaţiile pe Directory Server.

“Importarea unui fişier LDIF” la pagina 126
Folosiţi aceste informaţii pentru a importa un fişier LDIF (Data Interchange Format) LDAP.

“Copierea utilizatorilor în Directory Server dintr-o listă de validare a serverului HTTP” la pagina 127
Folosiţi aceste informaţii pentru a copia utilizatori dintr-o listă de validare a serverului HTTP în Directory Server.

Administrarea Web

Setaţi şi utilizaţi consola de administrare web pentru a administra Serverele de director.

Unul sau mai multe servere de director pot fi administrate prin intermediul consolei de administrare Web. Consola de administrare Web vă permite să:

- Adăugaţi sau modificaţi lista de servere de director care pot fi administrate.
- Administraţi un Directory Server folosind unealta de administrare Web.
- Schimbaţi atributele consolei de administrare Web.

Pentru a folosi consola de administrare Web, faceţi următoarele:

1. Dacă aceasta este prima dată când folosiţi administrarea Web pentru Directory Server, trebuie să setaţi întâi administrarea Web (vedeţi “Setarea Administrării web pentru prima dată” la pagina 101) şi apoi continuaţi cu pasul următor.
2. Înregistraţi-vă în administrarea Web din Directory Server, efectuând una din următoarele:
   - De la Navigator System i, selectaţi serverul dumneavoastră şi faceţi clic pe **Reţea → Servere → TCP/IP**, faceţi clic dreapta pe **Serverul de director IBM** şi faceţi clic pe **Administrare server**.
   - De la iSeries pagina Taskuri (http://*your_server*:2001) faceţi clic pe**Serverul de director IBM** .
3. Dacă doriţi să administraţi un Directory Server, faceţi următoarele:
   a. Selectaţi Directory Server pe care vreţi să îl administraţi în câmpul **Nume gazdă LDAP** .
   b. Introduceţi DN-ul de înregistrare administrator pe care îl folosiţi să vă legaţi la serverul de director.
   c. Introduceţi parola de administrator.

d. Faceţi clic pe **Logare**. Pagina IBM Directory Server Web Administration Tool este afişată. Pentru informaţii suplimentare despre pagina IBM Directory Server Web Administration Tool, vedeţi “Unealta de administrare Web” la pagina 102.

4. Dacă vreţi să adăugaţi sau să modificaţi lista de servere de director care pot fi administrate sau să modificaţi atributele consolei de administrare web, faceţi următoarele:
   a. Selectaţi **Console Admin** în câmpul **Nume gazdă LDAP**.
   b. Introduceţi login-ul de administrator consolă.
   c. Introduceţi parola de administrator consolă.
   d. Faceţi clic pe **Logare**. Pagina IBM Directory Server Web Administration Tool este afişată. Pentru informaţii suplimentare despre pagina IBM Directory Server Web Administration Tool, vedeţi “Unealta de administrare Web” la pagina 102.
   e. Apăsaţi **Administrare consolă** şi apoi selectaţi una din următoarele:
      - **Schimbare login administrator consolă** pentru a schimba numele login-ului de administrator consolă.
      - **Schimbare parolă administrator consolă** pentru a schimba parola administratorului de consolă.
      - **Gestionare servere consolă** pentru a schimba ce server de director pot fi administrate de către consola de administrare web.
      - **Gestionare proprietăţi consolă** pentru a schimba proprietăţile consolei de administrare web.

Setarea Administrării web pentru prima dată

Acest subiect dă instrucţiuni despre setarea uneltei de administrare web a Directory Server pentru prima dată.

1. Instalare IBM WebSphere Server de aplicaţii 6.0 (5733-W60 Base sau opţiuni Express) şi cerinţa preliminară de software asociat dacă nu este deja instalat.
2. Activaţi instanţa server a aplicaţiei sistem în serverul HTTP ADMIN. Vedeţi subiectul IBM HTTP Server pentru mai multe informaţii.
   a. Porniţi instanţa de server HTTP ADMIN, făcând una din următoarele:
      - În Navigator System i, faceţi clic pe **Servere de → reţea → TCP/IP** şi faceţi clic dreapta pe **Administrare HTTP**. Apoi faceţi clic pe **Pornire**.
      - În linia de comandă, tastaţi STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN).
   b. Înregistraţi-vă la IBM Administrare web pentru iSeries. Folosiţi un profil de utilizator sistem de operare şi parolă pentru a vă înregistra la iSeries Pagina de taskuri (http://*your_server*:2001), apoi faceţi clic pe **IBM Administrare web pentru iSeries**.
   c. De la pagina Server de administrare HTTP *your_server*, faceţi clic pe fişa **Gestionare** şi apoi faceţi clic pe fişa **Servere HTTP**. Fiţi sigur că **ADMIN ⌂?Apache** este selectat din lista derulantă **Server** şi că **Include/QIBM/UserData/HTTPA/admin/conf/admin-cust.conf** este selectat din lista derulantă **Zonă server**.
   d. Din opţiunile din panoul din stânga paginii, faceţi clic pe **Configuraţii generale server**.

      Notă: S-ar putea să fie nevoie să expandaţi secţiunea **Proprietăţi server** pentru a vedea opţiunea **Configuraţii generale server**.
   e. Setaţi **Pornire instanţă de server de aplicaţii sistem la pornirea serverului 'Admin'** la **Da**.
   f. Apăsaţi **OK**.
   g. Reporniţi instanţa de server HTTP ADMIN, făcând clic pe butonul de repornire (al doilea buton de sub fişa **Servere HTTP**). Puteţi, de asemenea, să opriţi şi să porniţi instanţa serverului HTTP ADMIN utilizând Navigator System i sau o linie de comandă.

      Puteţi opri instanţa serverului HTTP ADMIN, făcând una din următoarele:
      - În Navigator System i faceţi clic pe **Servere de → reţea → TCP/IP** şi faceţi clic dreapta pe**Administrare HTTP**. Apoi faceţi clic pe **Oprire**.
      - În linia de comandă, tastaţi ENDTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN).

      Puteţi porni instanţa serverului HTTP ADMIN, făcând una din următoarele:
      - În Navigator System i faceţi clic pe **Severe de → reţea → TCP/IP** şi faceţi clic dreapta pe **Administrare HTTP**. Apoi faceţi clic pe **Pornire**.

- În linia de comandă, tastaţi STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN).

Vedeţi subiectul IBM HTTP Server pentru mai multe informaţii.

3. Înregistraţi-vă în Directory Server Web Administration Tool.
   a. Aduceţi la vedere **pagina Logare**, făcând una din următoarele:
      - Din Navigator System i, selectaţi serverul dumneavoastră şi faceţi clic pe **Reţea → Servere → TCP/IP**, faceţi clic dreapta pe **IBM Directory Server** şi apoi faceţi clic pe **Administrare server**.
      - Din pagina Taskuri iSeries (http://*your_server*:2001), faceţi clic pe **IBM Directory Server pentru iSeries**.
   b. Selectaţi **Console Admin** în câmpul **Nume gazdă LDAP**.
   c. Introduceţi superadmin în câmpul **Nume utilizator**.
   d. Tastaţi secret în câmpul **Parolă**.
   e. Faceţi clic pe **Logare**. Este afişată pagina Unealtă de administrare Web IBM Directory Server.
4. Schimbaţi logarea administratorului de consolă.
   a. Faceţi clic pe **Administrare consolă** în panoul din stânga pentru a extinde secţiunea, apoi faceţi clic pe **Modificare logare administrator consolă**.
   b. Tastaţi un nou nume de logare administrare parolă în câmpul **Logare administrator consolă**.
   c. Tastaţi parola curentă (secret) în câmpul **Parola curentă**.
   d. Faceţi clic pe **OK**.
5. Schimbaţi parola de administrare a consolei. Faceţi clic pe **Modificare parolă administrator consolă** în panoul din stânga.
6. Adăugaţi ce Directory Server doriţi să administraţi. Faceţi clic pe **Gestionare servere consolă** în panoul din stânga.

   Notă: La adăugarea unui Directory Server, **Port administrare** nu este folosit şi va fi ignorat.
7. Dacă doriţi, puteţi să modificaţi proprietăţile consolei. Faceţi clic pe **Gestionare proprietăţi consolă** în panoul din stânga.
8. Faceţi clic pe **Delogare**. Când apare ecranul de succes al delogării, faceţi clic pe legătura **aici** pentru a reveni la pagina de logare pentru administrare web.

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

- Schimbarea logării şi a parolei administratorului de consolă.
- Schimbarea serverului de director care poate fi administrat de unealta de administrare Web.
- Schimbare proprietăţilor consolei.

Unealta de administrare Web

Odată ce v-aţi logat la unealta de administrare web, veţi găsi o fereastră aplicaţie conţinând cinci părţi.

Zona de banner
Zoan de banner se află în vârful panoului şi conţine numele aplicaţiei şi logo-ul IBM.

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

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

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

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

Gestionarea replicărilor
Acest task vă permite să lucraţi cu acreditări, topologie, planificări şi cozi.

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

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

Administrare server
Acest task vă permite să schimbaţi configuraţia serverului şi setările de securitate.

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

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

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

Scenarii pentru Directory Server

Folosiţi aceste informaţii pentru a studia scenarii care ilustrează exemple de taskuri Directory Server tipice.

Scenariu: Setarea unui Server de director

Un exemplu privind modul în care se setează un director LDAP pe Directory Server.

Situaţie

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

Obiective

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

Obiectivele acestui scenariu sunt cele ce urmează:

- Pentru a face informaţiile despre angajaţi disponibile oriunde în reţeaua companiei pentru angajaţii care folosesc un client Lotus Notes sau de poştă Microsoft Outlook Express.
- Pentru a permite managerilor să schimbe datele angajaţilor în baza de date director, în timp ce nu permiteţi celorlalţi să schimbe datele despre angajaţi.
- Pentru a permite sistemului să fie capabil să publice datele angajaţilor în baza de director.

Detalii

Serverul de director va rula pe sistemul numit mySystem.

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

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

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

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

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

Sistemul (mySystem) de asemenea necesită să aibă autorizarea ed a modifica datele angajaţilor. În acestscenariu, sistemul e plasat în arborele directorului de angajaţi şi este făcut membru a grupului de manageri.

Dac ă vreţi să păstraţi intrările angajat separat de intrarea sistemului, puteţi crea alt arbore de director (de exemplu: computere) şi să adăugaţi sistemul aici. Sistemul va trebui să aibă aceeaşi autorizare ca şi managerii.

Cerinţe preliminare şi supoziţii

Unealta de administrare Web este configurată şi rulează corespunzător. Consultaţi “Administrarea Web” la pagina 100 pentru mai multe informaţii.

Paşi setare

Efectuaţi operaţiile următoare:

Detalii scenariu: Setarea Directory Server

Pasul 1: Configuraţi Serverul de director:

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

1. În Navigator System i faceţi clic pe **Network → Servere → TCP/IP**.
2. Faceţi clic pe **Configurare sistem ca Server de director** în fereastra **Taskuri configurare server** la partea de jos din dreapta Navigator System i.
3. Va apărea **Vrăjitorul de configurare Directory Server**.
4. Faceţi clic pe **Configurarea unui server de director LDAP local** din fereastra**Vrăjitor de configurare IBM Directory Server - Bun venit**.
5. Faceţi clic pe **Următor** în fereastra **Vrăjitor de configurare IBM Directory Server - Bun venit**.

6. Selectaţi **Nu** în fereastra **Vrăjitor de configurare IBM Directory Server - Specificare setări**. Aceasta vă permite să configuraţi serverul LDAP fără setările implicite.
7. Faceţi clic pe **Următor** în fereastra **Vrăjitor de configurare IBM Directory Server - Specificare setări**.
8. Deselectaţi **Generat de sistem** în fereastra **Vrăjitor de configurare IBM Directory Server - Specificare DN administrator** şi introduceţi următoarele:

DN Administrator	cn=administrator
Parolă	secret
Confirmare parolă	secret

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

9. Faceţi clic pe **Următor** în fereastra **Vrăjitor de configurare IBM Directory Server - Specificare DN administrator**.
10. Tastaţi dc=my_co,dc=com în câmpul **Sufix** din fereastra **Vrăjitor de configurare IBM Directory Server - Specificare sufixe**.
11. Faceţi clic pe **Adăugare** în fereastra **Vrăjitor de configurare IBM Directory Server - Specificare sufixe**.
12. Faceţi clic pe **Următor** în fereastra **Vrăjitor de configurare IBM Directory Server - Specificare sufixe**.
13. Selectaţi **Da, foloseşte toate adresele IP** în fereastra **Vrăjitor de configurare IBM Directory Server - Selectare adrese IP**.
14. Faceţi clic pe **Următor** în fereastra **Vrăjitor de configurare IBM Directory Server - Selectare adrese IP**.
15. Selectaţi **Da** în fereastra **Vrăjitor de configurare IBM Directory Server - Specificare preferinţă TCP/IP**.
16. Faceţi clic pe **Următor** în fereastra **Vrăjitor de configurare IBM Directory Server - Specificare preferinţă TCP/IP**.
17. Faceţi clic pe **Sfârşit** în fereastra **Vrăjitor de configurare IBM Directory Server - Rezumat**.
18. Faceţi clic dreapta pe **IBM Directory Server** şi apăsaţi **Pornire**.

Pasul 2: Configuraţi unealta de administrare web a serverului de director:

1. Îndreptaţi-vă browserul la http://*mySystem.my_co.com*:9080/IDSWebApp/IDSjsp/Login.jsp, unde *mySystem.my_co.com* este sistemul dumneavoastră.
2. Ar trebui să apară o pagină de logare. Apăsaţi pe lista **Nume gazdă LDAP** şi selectaţi **Admin consolă**. Tastaţi superadmin pentru numele de utilizator şi secret pentru parolă. Faceţi clic pe **Logare**.
3. Configuraţi unealta de administrare web să se conecteze la serverul LDAP de pe sistemul dumneavoastră. Selectaţi **Administrare consolă → Gestionare servere consolă** în navigaţia mâina stângă.
4. Selectaţi **Adăugare**.
5. În câmpul **Adăugare server**, tastaţi mySystem.my_co.com.
6. Faceţi clic pe **Ok**. Noul server va apărea în lista de sub **Gestionare servere consolă**.
7. Apăsaţi **delogare** în cadrul de navigare din stânga.
8. Pe pagina de logare a uneltei de administrare web faceţi clic pe lista **Nume gazdă LDAP** şi selectaţi serverul pe care tocmai l-aţi configurat (**mySystem.my_co.com**).
9. În câmpul **Username** tastaţi cn=administrator şi în câmpul **Parolă** tastaţi secret. Faceţi clic pe **Logare**.Ar trebui să vedeţi pagina principală a uneltei de administrare Web a serverului de director IBM.

Detalii scenariu: Crearea bazei de date a directorului

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

Pasul 1: Creaţi un obiect DN de bază:

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

Pasul 2: Creaţi un şablon utilizator:
Veţi crea un şablon utilizator ca un ajutor la adăugarea datelor despre angajaţi ai MyCo, Inc.

1. În unealta de administrare web, faceţi clic pe **Regiuni şi şabloane → Adăugare şablon utilizator**.
2. În câmpul **Nume şablon utilizator**, tastaţi Angajat.
3. Faceţi clic pe butonul **Răsfoire...** de lângă câmpul **DN părinte**. Apăsaţi pe DN-ul de bază pe care l-aţi creat în secţiunea anterioară, **dc=my_co,dc=com** şi apăsaţi **Selectare** în dreapta ferestrei.
4. Apăsaţi **Următorul**.
5. În lista derulantă **Clase de obiecte structurale**, alegeţi **inetOrgPerson** şi faceţi clic pe **Următorul**.
6. În lista derulantă **Atribut de numire**, selectaţi **cn**.
7. În lista **Fişe**, selectaţi **Necesar** şi apăsaţi **Editare**.
8. Fereastra **Editare fişă** este unde alegeţi care câmpuri să fie incluse în şablonul utilizator. **sn** şi **cn** sunt necesare.
9. În lista **Atribute**, selectaţi **departmentNumber** şi faceţi clic pe **Adăugare >>>**.
10. Selectaţi **telephoneNumber** şi faceţi clic pe **Adăugare >>>**.
11. Selectaţi **mail** şi faceţi clic pe **Adăugare >>>**.
12. Selectaţi **userPassword** şi faceţi clic pe **Adăugare >>>**.
13. Apăsaţi **OK** şi apoi **Sfârşit** pentru a crea şablonul utilizator.

Pasul 3: Creaţi o regiune:

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

Pasul 4: Creaţi un grup de manageri:

1. Creaţi grupul de manageri.
   a. În unealta de administrare web, faceţi clic pe **Utilizatori şi grupuri → Adăugare grup** .
   b. În câmpul **Nume grup**, tastaţi manageri.
   c. Asiguraţi-vă că **angajaţi** este selectat în lista derulantă **Regiune**.
   d. Faceţi clic pe **Sfârşit**.
2. Configuraţi administratorul grupului de manageri pentru regiunea **angajaţi**.
   a. Faceţi clic pe **Regiune şi şablon → Gestionare regiuni**.
   b. Selectaţi regiunea pe care aţi creat-o, **cn=employees,dc=my_co,dc=com** şi apăsaţi **Editare**.
   c. În dreapta câmpului **Grup administrator**, apăsaţi **Răsfoire...**.

d. Selectaţi **dc=my_co,dc=com** şi apăsaţi **Expandare**.
e. Selectaţi **cn=employees** şi apăsaţi **Expandare**.
f. Selectaţi **cn=managers** şi apăsaţi **Selectare**.
g. În fereastra **Editare regiune**, apăsaţi **OK**.

3. Daţi-i grupului de manageri autorizare pentru sufixul **dc=my_co,dc=com**.
   a. Faceţi clic pe **Gestiune director → Gestiune intrări**.
   b. Selectaţi **dc=my_co,dc=com** şi apăsaţi **Editare ACL...**.
   c. În fereastra **Editare ACL**, apăsaţi pe fişa **Proprietari**.
   d. Selectaţi căsuţa de bifare **Propagare proprietar**. Oricine este membru al grupului de manageri va fi făcut proprietar al arborelui de date **dc=my_co,dc=com**.
   e. În lista derulantă **Tip**, selectaţi **Grup**.
   f. În câmpul **DN (Nume distinctiv)**, tastaţi cn=managers,cn=employees,dc=my_co,dc=com.
   g. Selectaţi **Adăugare**.
   h. Faceţi clic pe **Ok**.

Pasul 5: Adăugaţi un utilizator ca manager:

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

Detalii scenariu: Publicaţi datele System i5 la baza de date a directorului

Configuraţi publicarea pentru a permite sistemului dumneavoastră să introducă automat informaţii utili zator în directorul LDAP. Informaţiile utilizator din directorul de distribuţie sistem sunt publicate în directorul LDAP.

Notă: Uti lizatorii creaţi cuNavigator System i le sunt daţi atât un profil utilizator şi o intrare utilizator director de distribuire sistem. Dacă folosiţi comenzi CL pentru crearea utilizatorilor, trebuie să creaţi atât un profil utilizator(**CRTUSRPRF**), cât şi o intrare utilizator director de distribuţie sistem (**WRKDIRE**). Dacă utilizatorii dvs. există doar ca profiluri de utilizator şi vreţi ca ei să fie publicaţi în directorul LDAP, trebuie să creaţi intrări utilizator director distribuţie sistem pentru ei.

Pasul 1: Faceţi sistemul un utilizator server de director:

1. Logaţi-vă la unealta de administrare web (http://**mySystem.my_co.com**:9080/IDSWebApp/IDSjsp/Login.jsp) ca administratorul.
   a. Selectaţi **mySystem.my_co.com** în lista **LDAP Hostname**.
   b. tastaţi cn=administrator în câmpul **Nume utilizator**
   c. Tastaţi secret în câmpul **Parolă** .
   d. Faceţi clic pe **Logare**.

2. Faceţi clic pe **Utilizatori şi grupuri → Adăugare utilizator**.
3. Selectaţi **employees** din lista **Regiune**.
4. Apăsaţi **Următorul**.
5. Tastaţi mySystem.my_co.com în câmpul **cn**.
6. Tastaţi mySystem.my_co.com în câmpul ***sn**.
7. Tastaţi mySystem.my_co.com în câmpul ***cn**.
8. Tastaţi secret în câmpul **Parolă utilizator**.
9. Apăsaţi fişa **Grupuri utilizator**.
10. Selectaţi grupul **manageri**.
11. Selectaţi **Adăugare →** .
12. Faceţi clic pe **Sfârşit**.

pasul 2: Configuraţi sistemul să publice date:

1. În Navigator System i, faceţi clic dreapta peiSeries al dumneavoastră în navigarea mâna stângă şi selectaţi **Proprietăţi**.
2. În fereastra de dialog **Proprietăţi**, alegeţi fişa **Directory Server**.
3. Selectaţi **Utilizatori** şi apăsaţi **Detalii**.
4. Selectaţi căsuţa de bifare **Publicare informaţii utilizator**.
5. În secţiunea **Unde să se publice**, apăsaţi butonul **Editare**. Apare o fereastră.
6. Tastaţi mySystem.my_co.com.
7. În câmpul **Sub DN**, tastaţi cn=employees,dc=my_co,dc=com.
8. În secţiunea **Conexiune server**, asiguraţi-vă că este introdus numărul de port implicit, **389**, în câmpul **Port**. În lista derulantă **Metodă de autentificare**, alegeţi **Nume distinctiv** şi introduceţi cn=mySystem,cn=employees,dc=my_co,dc=com în câmpul **Nume distinctiv**.
9. Faceţi clic pe **Parolă**.
10. Tastaţi secret în câmpul **Parolă** .
11. Tastaţi secret în câmpul **Confirmare parolă** .
12. Apăsaţi **OK**.
13. Faceţi clic pe fişa **Verificare**. Aceasta asigură că aţi introdus toate informaţiile corect şi că sistemul se poate conecta la directorul LDAP.
14. Apăsaţi **OK**.
15. Apăsaţi **OK**.

Detalii scenariu: Introducerea informaţiilor în baza de date director

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

Pasul 1: Logaţivă pe unealta de administrare web:
Se înregistrează în unealta de Administrare Web. (http://**mySystem.my_co.com**:9080/IDSWebApp/IDSjsp/Login.) făcând următoarele:

1. Selectaţi **mySystem.my_co.com**, în thelista **Nume gazdă LDAP**.
2. Tastează cn=Jose Alvirez,cn=myco employees,dc=my_co,dc=com în câmpul Username.
3. Tastează secret în câmpul parolă.
4. Faceţi clic pe **Logare**.

Pasul 2: modificaţi datele angajatului:

1. Faceţi clic pe **Utilizatori şi grupuri → Gestionare utilizatori**.
2. Selectează **employees** din lista **Regiune** şi apasă **Vizualizare utilizatori**.
3. Selectează **Jane Doe** din lista de utilizatori şi apasă **Editare**.
4. tastaţi DEPTA în câmpul **departmentNumber**.
5. Apăsaţi **OK**.
6. Apăsaţi **Close**.

Pasul 3: Adăugare date angajat:

1. Faceţi clic pe **Utilizatori şi grupuri → Adăugare utilizator**.
2. Selectaţi **employees** din meniul derulant **Regiune** şi apăsaţi **Continuare**.
3. În câmpul **cn**, tastaţi John Smith.
4. În câmpul ***sn** tastaţi Smith.
5. În câmpul ***cn** tastaţi John Smith.
6. În câmpul **telephoneNumber** tastaţi 999 555 1235.
7. În câmpul **departmentNumber** tastaţi DEPTA.
8. În câmpul **mail** tastaţi jsmith@my_co.com.
9. Apăsaţi **Sfârşit** în josul ferestrei.

Detalii scenariu: Testarea bazei de date director

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

Căutaţi baza de date a directorului folosind agenda de adrese e-mail a dumneavoastră:
Informaţiile dintr-un director LDAP pot fi căutate cu uşurinţă cu programe cu posibilităţi LDAP. Mulţi clienţi de e-mail pot căuta în servere directoare LDAP ca parte a funcţiei lor de carte de adrese. Următoarele sunt exemple de proceduri de configurare Lotus Notes 6 şi Microsoft Outlook Express 6. Procedura pentru majoritatea celorlalţi clienţi de e-mail va fi similară.

Lotus Notes:

1. Deschideţi agenda de adrese.
2. Faceţi clic pe **Acţiuni → Nou → Connt**.
3. Tastaţi mySystem în câmpul **Nume cont**.
4. Tastaţi mySystem.my_co.com în câmpul **Cont nume server**.
5. Selectaţi **LDAP** în câmpul **Protocol**.
6. Faceţi clic pe fişa **Configuraţie protocol**.
7. Tastaţi dc=my_co,dc=com în câmpul **Bază de căutare**.
8. Faceţi clic pe **Salvare şi închidere**.
9. Faceţi clic pe **Creare → Mail → Memo**.
10. Faceţi clic pe **Adresă...**.
11. Selectaţi mySystem în câmpul **Alegere agendă de adrese**.
12. Tastaţi Alvirez în câmpul **Căutare pentru**.
13. Faceţi clic pe **Căutare**. Apar datele pentru Jose Alvirez.

Microsoft Outlook Express:

1. Faceţi clic pe **Unelte → Conturi**.
2. Faceţi clic pe **Adăugare → Service de director**.
3. Tastaţi adresa web a sistemului în câmpul **Server (LDAP) al directorului internetr** (mySystem.my_co.com).
4. Debifaţi caseta de bifare **Serverul meu LDAP necesită ca eu să mă loghez**.

5. Apăsaţi **Următorul**.
6. Apăsaţi **Următorul**.
7. Faceţi clic pe **Sfârşit**.
8. Selectaţi mySystem.my_co.com (the directory service pe care tocmai le-aţi configurat) şi faceţi clic pe **Proprietăţi**.
9. Apăsaţi **Avansat**.
10. Tastaţi dc=my_co,dc=com în câmpul **Bază de căutare**.
11. Faceţi clic pe **Ok**.
12. Apăsaţi **Close**.
13. Tastaţi Ctrl+E pentru a deschide fereastra **Căutare persoană**.
14. Selectaţi mySystem.my_co.com din lista **Căutare în**.
15. Tastaţi Alvirez în câmpul **Nume**.
16. Faceţi clic pe **Găsire acum**. Apar datele pentru Jose Alvirez.

Căutaţi baza de date a directorului utilizând comanda liniei de comandă ldapsearch:

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

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

   Unde:

   –h este numele maşinii gazdă care rulează serverul LDAP.

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

   objectclass=*
   întoarce toate intrările din director.

   Această comandă întoarce ceva de forma următoare:

   ```
   dc=my_co,dc=com
   dc=my_co
   objectclass=domain
   objectclass=top

   cn=MyCo employee,dc=my_co,dc=com

   .
   .
   .

   cn=Jose Alvirez,cn=MyCo Employees,dc=my_co,dc=com

   sn=Alvirez
   departmentNumber=DEPTA
   mail=jalvirez@my_co.com
   telephoneNumber=999 999 9999
   objectclass=top
   objectclass=inetOrgPerson
   objectclass=organizationalPerson
   objectclass=person
   cn=Jose Alvirez

   .
   .
   .
   ```

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

Scenariu: Copierea utilizatorilor în Directory Server dintr-o listă de validare a serverului HTTP

Un exemplu de copiere a utilizatorilor dintr-o listă de validare a serverului HTTP în Directory Server.

Situaţie şi privire generală

În prezent aveţi o aplicaţie care rulează în Serverul HTTP (motorizată de Apache), folosind utilizatorii Internet din lista de validare MYLIB/HTTPVLDL. Aţi dori să utilizaţi aceeaşi utilizatori Internet cu Serverul de aplicaţiiWebSphere (WAS)cu autentificare LDAP. Pentru a evita dubla întreţinere a informaţiilor utilizator din lista de validare şi LDAP, veţi configura, de asemenea, aplicaţia serverului HTTP pentru a folosi autentificarea LDAP.

Pentru a realiza acest lucru, trebuie să efectuaţi următorii paşi:

1. Copiaţi utilizatorii din lista de validare existentă în serverul de director local.
2. Configuraţi serverul WAS aă utilizeze autentificarea LDAP.
3. Reconfiguraţi serverul HTTP să folosească autentificarea LDAP în locul listei de validare.

Pasul 1: Copiaţi utilizatorii lista de validare existentă la serverul de director local

Se presupune că serverul de director a fost configurat anterior cu sufixul ″o=my company″ şi rulează. Utilizatorii LDAP urmează să fie memoraţi în subarborele directorului ″cn=users,o=my company″. DN-ul administratorului serverului de director este ″cn=administrator″, iar parola administratorului este ″secret″.

Apelaţi API-ul din linia de comandă, după cum urmează:

```
CALL PGM(QSYS/QGLDCPYVL) PARM('HTTPVLDL  MYLIB     ' 'cn=administrator'
X'00000000' 'secret' X'00000000' 'cn=users,o=my company' X'00000000' '' X'00000000'
X'00000000')
```

Când este gata, serverul de director va conţine intrări inetorgperson bazate pe intrările din lista de validare. De exemplu, utilizatorul listei de validare:

```
User name: jsmith
Description: John Smith
Password: ******
```

va avea ca efect următoarea intrare din director:

```
dn: uid=jsmith,cn=users,o=my company
objectclass: top
objectclass: person
objectclass: organizationalperson
objectclass: inetorgperson
uid: jsmith
sn: jsmith
cn: jsmith
description: John Smith
userpassword: ******
```

Această intrare poate fi acum folosită pentru autentificarea la serverul de director. De exemplu, realizarea acestei ldapsearch QSH va citi intrarea din rădăcina DSE a serverului:

```
> ldapsearch -D "uid=jsmith,cn=users,o=my company" -w ****** -s base "(objectclass=*)"
```

Odată create, puteţi edita intrările directorului pentru a conţine informaţii detaliate. De exemplu, puteţi dori să modificaţi valorile cn şi sn pentru a reflecta numele şi prenumele întreg al utilizatorului corespunzător sau să adăugaţi un număr de telefon şi o adresă de e-mail.

Pasul 2: Configuraţi serverul WAS pentru a utiliza autentificarea LDAP

Securitatea LDAP WAS trebuie configurată pentru a căuta intrări sub dn-ul ″cn=users,o=my company″, folosind un filtru de căutare care asociază numele utilizator introdus cu intrările inetOrgPerson care conţin acea valoare uid a

atributului. De exemplu, autentificarea în WAS folosind numele utilizator jsmith va duce la o căutare pentru intrările care se potrivesc cu filtrul de căutare ″(uid=jsmith)″. Pentru informaţii suplimentare, vedeţi Configurare filtre de căutare LDAP în serverul de aplicaţii Websphere pentru Centrul de informare iSeries.

Reconfiguraţi serverul HTTP să utilizeze autentificarea LDAP în loc de lista de validare

Notă: Procedura descrisă mai jos are rolul de a ajuta la ilustrarea exemplelor din acest scenariu, prezentând o privire generală de nivel înalt asupra configurării serverului HTTP pentru a folosi autentificarea LDAP. S-ar putea să aveţi nevoie de informaţii detaliate găsite în IBM Cărţi roşii publicaţieImplementation şi Utilizare practică a LDAP pe IBM eServer iSeries Server, SG24-6193 Secţiunea 6.3.2 ″Setare autentificare LDAP pentru alimentat de serverul Apache″ la fel de bine ca şi Setare protecţie parolă pe server HTTP (alimentat de Apache).

1. Faceţi clic pe **Autentificare de bază** de pe fişa **Configurare** pentru serverul dumneavoastră HTTP din unealta Administarre HTTP.
2. Sub metoda **Autentificare utilizator**, schimbaţi**Folosire utilizatori Internet din listele de validare** în **Folosire intrări utilizator din severul LDAP** şi faceţi clic pe **OK**.
3. Reveniţi la fişa **Configurare** şi faceţi clic pe **Acces control**. Configuraţi aceasta cum e descris în publicaţia Cărţi roşii cu legătura de mai sus şi faceţi clic pe **OK**.
4. Pe fişa **Configurare**, faceţi clic pe **Autentificare LDAP**.
   a. Introduceţi numele gazdă şi portul serverului LDAP. Pentru **Căutare utilizator DN de bază**, introduceţi cn=users,o=my company.
   b. Subr **Creare DN unic LDAP DN pentru autentificarea utilizatorului**, introduceţi filtrul (&objectclass=person)(uid=%v1)).
   c. Introduceţi informaţiile despre grup şi faceţi clic pe **OK**.
5. Configuraţi conexiunea la serverul LDAP cum este descris în publicaţia Cărţi roşii cu legătura de mai sus.

Administrarea Directory Server

Folosiţi aceste informaţii pentru a gestiona Directory Server.

Pentru a administra Directory Server, profilul utilizator pe care îl folosiţi trebuie să aibă următoarea autorizare:

- 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 director: 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-ul de administrator, fie cu un alt DN care are autorizarea corespunzătoare LDAP. Dacă este folosită integrarea autorizării, un administrator poate fi de asemenea un utilizator proiectat (vedeţi “Back-end proiectat de sistem de operare” la pagina 83), care are autorizarea pentru ID-ul funcţiei Directory Server Administrator. Majoritatea taskurilor administrative mai pot fi realizate de utilizatori din grupul administrativ (vedeţi “Accesul administrativ” la pagina 61).

Taskuri de administrare generală

Folosiţi aceste informaţii pentru a gestiona administrarea generală a Directory Server.

Pornirea Directory Server

Folosiţi aceste informaţii pentru a porni Directory Server.

1. În Navigator System i, expandaţi **Reţea**.

2. Expandaţi **Servere**.
3. Faceţi clic pe **TCP/IP**.
4. Faceţi clic dreapta pe **IBM Directory Server** şi selectaţi **Pornire**.

   Serverul de director poate avea nevoie de mai multe minute pentru a porni, în funcţie de viteza serverului dumneavoastră şi de cantitatea de memorie disponibilă. Prima pornire a serverului de director poate dura cu câteva minute mai mult decât de obicei, deoarece serverul trebuie să creeze fişiere noi. Similar, când porniţi serverul de director pentru prima dată după ce aţi actualizat de la o versiune anterioară a serverului de director, ar putea lua mai multe minute mai mult decăt de obicei deoarece serverul trebuie să migreze fişierele. Puteţi verifica starea serverului periodic (vedeţi "Modificarea stării serverului de director") pentru a vedea dacă a pornit deja.

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

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

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

Operaţii înrudite

"Oprirea Directory Server"
Folosiţi aceste informaţii pentru a opri Directory Server.

"Modificarea stării serverului de director"
Folosiţi aceste informaţii pentru a verifica starea Serverului de director.

Oprirea Directory Server

Folosiţi aceste informaţii pentru a opri Directory Server.

Notă: Oprirea Directory Server afectează toate aplicaţiile care utilizează serverul în momentul opririi. Printre acestea se numără aplicaţiile Enterprise Identity Mapping (EIM) care folosesc curent serverul de director pentru operaţii EIM. Toate aplicaţiile sunt deconectate de la serverul de director, totuşi, nu sunt prevenite de la încercarea de a se reconecta la server.

1. În Navigator System i, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Faceţi clic pe **TCP/IP**.
4. Faceţi clic dreapta pe **IBM Directory Server** şi selectaţi **Oprire**.

   Serverul de director poate avea nevoie de mai multe minute pentru a se opri, în funcţie de viteza serverului dumneavoastră, de cantitatea de activitate a serverului şi de cantitatea de memorie disponibilă. Puteţi verifica starea serverului periodic (vedeţi "Modificarea stării serverului de director") pentru a vedea dacă a pornit deja.

Directory Server poate fi de asemenea oprit din interfaţa bazată pe caractere introducând comanda ENDTCPSVR *DIRSRV, ENDTCPSVR *ALL sau ENDTCP. ENDTCPSVR *ALL şi ENDTCP afectează de asemena orice alte servere TCP/IP care rulează pe sistemul dumneavoastră. ENDTCP va opri de asemenea TCP/IP.

Operaţii înrudite

"Pornirea Directory Server" la pagina 112
Folosiţi aceste informaţii pentru a porni Directory Server.

Modificarea stării serverului de director

Folosiţi aceste informaţii pentru a verifica starea Serverului de director.

Informaţii de bază despre stare se găsesc în Navigator System i. Cu unealta de administrare Web puteţi găsi informaţii asupra stării mai avansate şi mai complete.

Navigator System iAfişează starea Serverului de director în coloana **Stare** din cadrul drept.

Pentru a verifica starea Serverului de director în Navigator System i, urmaţi aceşti paşi:

1. Expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Faceţi clic pe **TCP/IP**. Navigator System i afişează starea tuturor serverelor TCP/IP, incluzând serverul de director, 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 director, faceţi clic dreapta pe **IBM Directory Server** şi selectaţi **Stare**. Aceasta va afişa numărul de conexiuni active, ca 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 director fără să pierdeţi timp suplimentar ce este necesar pentru a verifica starea altor servere TCP/IP.

Pentru a vizualiza starea serverului de director folosind unealta de administrare Web, efectuaţi aceşti paşi:

1. Expandaţi categoria **Administrare server** din zona de navigare.

   Notă: Pentru a modifica setările de configuraţiei ale serverului utilizând taskurile din categoria Administrare de server a uneltei de administrare web, trebuie să vă autentificaţi la server ca un profil de utilizator i5/OS ce are autorităţile speciale *ALLOBJ şi IOSYSCFG. Aceasta se poate realiza prin autentificarea ca utilizator proiectat cu parola pentru acel profil. Pentru a vă lega ca utilizator proiectat din unealta de administrare Web, introduceţi un numeutilizator de forma os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, unde şirurile MYUSERNAME şi MYSYSTEM.COM sunt înlocuite cu numele profilului dumneavoastră de utilizator, respectiv cu sufixul de proiectare al sistemului configurat.
2. Faceţi clic pe **Vizualizare stare server**.
3. În panoul **Vizualizare stare server**, selectaţi diferitele fişe pentru a vizualiza informaţiile despre stare.

Verificarea joburilor de pe Directory Server

Folosiţi aceste informaţii pentru a monitoriza joburi specifice pe Directory Server.

Pentru a verifica joburi server în Navigator System i, urmaţi aceşti paşi:

1. În Navigator System i, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Faceţi clic pe **TCP/IP**.
4. Faceţi clic dreapta pe **IBM Directory Server** şi selectaţi **Joburi server**.

Gestionarea conexiunilor serverului

Folosiţi aceste informaţii pentru a vizualiza conexiunile la server şi operaţiile realizate de aceste conexiuni.

Administratorul poate lua decizii pentru a controla accesul şi a împiedica atacurilor de refuzare a serviciului bazate pe conexiuni. Aceasta se realizează prin unealta de administrare Web.

Notă: Pentru a modifica setările configuraţiei serverului utilizând taskurile din categoria Administrare server a Uneltei de administrare web, trebuie să vă autentificaţi pe server ca un profil de utilzator i5/OS care are autoritatea specială *ALLOBJ şi IOSYSCFG. Aceasta se poate realiza prin autentificarea ca utilizator proiectat cu parola pentru acel profil. Pentru a vă lega ca utilizator proiectat din unealta de administrare Web, introduceţi un numeutilizator de forma os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, unde şirurile MYUSERNAME şi MYSYSTEM.COM sunt înlocuite cu numele profilului dumneavoastră de utilizator, respectiv cu sufixul de proiectare al sistemului configurat.

1. Expandaţi categoria **Administrare server** din zona de navigare.
2. Faceţi clic pe **Gestionare conexiuni server**.

   Este afişată o tabelă ce conţine următoarele informaţii pentru fiecare conexiune:

DN Specifică DN-urile unei conexiuni client la server.

IP address (adresă IP)
Specifică adresa IP a clientului care are o conexiune la server.

Oră pornire
Specifică data şi ora (în funcţie de ora locală a serverului) când s-a realizat conexiunea.

Stare Specifică dacă acea conexiune este activă sau inactivă. O conexiune este considerată activă dacă are vreo operaţie în curs.

Ops iniţiate
Specifică numărul de operaţii necesare de la momentul stabilirii conexiunii.

Ops terminate
Specifică numărul de operaţii care s-au efectuat pentru fiecare conexiune.

Tip Specifică dacă conexiunea este securizată de SSL sau de TLS. Altfel, câmpul este gol.

Notă: Această tabelă afişează până la 20 de conexiuni o dată.

Puteţi specifica afişarea acestei tabele fie după DN, fie după adresa IP, prin expandarea meniului derulant din vârful panoului şi prin realizarea unei selecţii. Selecţia implicită este după DN. În mod similar, mai puteţi specifica dacă tabela să fie afişată în ordine crescătoare sau descrescătoare.

3. Faceţi clic pe **Reîmprospătare** pentru a actualiza informaţiile curente privind conexiunea.
4. Dacă sunteţi înregistrat ca administrator sau ca membru al grupului de administrare, aveţi selecţii suplimentare pentru a deconecta conexiunile serverului disponibile în panou. Această posibilitate de a deconecta conexiunile serverului vă permite să opriţi atacurile de refuzare a serviciului şi să controlaţi accesul la server. Puteţi deconecta o conexiune expandând meniurile derulante, selectând un DN, o adresă IP sau ambele şi făcând clic pe **Deconectare**. Pentru a deconecta toate conexiunile la server cu excepţia celei care efectuează această cerere, faceţi clic pe **Deconectare toate**. Este afişat un avertisment de confirmare. Faceţi clic pe **OK** pentru a continua acţiunea de deconectare sau apăsaţi **Anulare** pentru a opri acţiunea şi a reveni la panoul **Administrare conexiuni server**.

Pentru informaţii suplimentare despre atacurile de refuzare a serviciului, vedeţi Gestionarea proprietăţilor conexiunii.

Concepte înrudite

"Refuzarea serviciului" la pagina 82
Folosiţi opţiunea de configurare negare serviciu pentru a proteja împotriva atacurilor de negare.

Operaţii înrudite

"Gestionarea proprietăţilor conexiunii"
Folosiţi aceste informaţii pentru a seta proprietăţile conexiunii, cum ar fi acelea care împiedică clienţii să blocheze serverul.

Gestionarea proprietăţilor conexiunii

Folosiţi aceste informaţii pentru a seta proprietăţile conexiunii, cum ar fi acelea care împiedică clienţii să blocheze serverul.

Posibilitatea de a gestiona proprietăţile conexiunii vă permite să împiedicaţi clienţii să blocheze serverul. De asemenea, asigură că administratorul are întotdeauna acces la server în cazurile în care backend-ul este ţinut ocupat cu taskuri de lungă durată. Gestionarea proprietăţilor conexiunii se realizează prin unealta de administrare Web.

Notă: Aceste selecţii sunt afişate doar dacă sunteţi înregistrat ca administrator sau ca membru al grupului de administrare pe un server care suportă această funcţie.

Pentru a seta proprietăţile conexiunii, realizaţi următorii paşi:

1. Expandaţi categoria **Administrare server** din zona de navigare şi apăsaţi **Gestionare proprietăţi conexiune**.

   Notă: Pentru a modifica setările configuraţiei serverului utilizând taskurile din categoria Administrare server a Uneltei de administrare web, trebuie să vă autentificaţi pe server ca un profil de utilzator i5/OS care are

autoritatea specială *ALLOBJ şi IOSYSCFG. Aceasta se poate realiza prin autentificarea ca utilizator proiectat cu parola pentru acel profil. Pentru a vă lega ca utilizator proiectat din unealta de administrare Web, introduceţi un numeutilizator de forma os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, unde şirurile MYUSERNAME şi MYSYSTEM.COM sunt înlocuite cu numele profilului dumneavoastră de utilizator, respectiv cu sufixul de proiectare al sistemului configurat.

2. Selectaţi fişa **General**.
3. Configuraţi setarea conexiunii anonime. Caseta de bifare **Permisiune conexiuni anonime** este deja selectată, astfel încât legăturile anonime sunt permise. Aceasta este setarea implicită. Puteţi face un clic pe caseta de bifare pentru a deselecta funcţia **Permisiune conexuini anonime**. Această acţiune determină serverul să dezlege toate conexiunile anonime.

   Notă: Unele aplicaţii ar putea eşua dacă nu mai permiteţi conexiunile anonime.
4. În câmpul **Curăţare prag pentru conexiuni anonime**, setaţi valoarea pragului pentru a iniţia dezlegarea conexiunilor anonime. Puteţi specifica un număr între 0 şi 65535.

   Notă: Numărul maxim real este limitat de numărul de fişiere permise pe proces. Pe sistemele UNIX, puteţi folosi comanda**ulimit -a** pentru a determina limitele. Pe sistemele Windows, acesta este un număr fixat.

   Setarea implicită este 0. Când numărul conexiunilor anonime este depăşit, conexiunile sunt curăţate având la bază limita timeout-ului de inactivitate pe care aţi setat-o în câmpul **Timeout inactivitate**.
5. În câmpul **Curăţare prag pentru conexiuni autentificate**, setaţi valoarea pragului pentru iniţierea dezlegării conexiunilor autentificate. Puteţi specifica un număr între 0 şi 65535.

   Notă: Numărul maxim real este limitat de numărul de fişiere permise pe proces. Pe sistemele UNIX, puteţi folosi comanda ulimit -a pentru a determina limitele. Pe sistemele Windows, acesta este un număr fixat.

   Setarea implicită este 1100. Când acest număr de conexiuni autentificate este depăşit, conexiunile sunt curăţate având la bază limita timeout-ului de inactivitate pe care aţi setat-o în câmpul **Timeout de inactivitate**.
6. În câmpul **Curăţare prag pentru toate conexiunile**, setaţi valoarea pragului pentru a iniţia dezlegarea tuturor conexiunilor. Puteţi specifica un număr între 0 şi 65535.

   Notă: Numărul maxim real este limitat de numărul de fişiere permise pe proces. Pe sistemele UNIX, puteţi folosi comanda ulimit -a pentru a determina limitele. Pe sistemele Windows, acesta este un număr fixat.

   Setarea implicită este 1200. Când acest număr total de conexiuni este depăşit, conexiunile sunt curăţate având la bază limita timeout-ului de inactivitate pe care aţi setat-o în câmpul **Timeout de inactivitate**.
7. În câmpul **Limită timeout de inactivitate**, setaţi numărul de secunde în care o conexiune poate fi inactivă înainte să fie închisă de un proces de curăţare. Puteţi specifica un număr între 0 şi 65535.

   Notă: Numărul maxim real este limitat de numărul de fişiere permise pe proces. Pe sistemele UNIX, puteţi folosi comanda ulimit -a pentru a determina limitele. Pe sistemele Windows, acesta este un număr fixat.

   Setarea implicită este 300. Când un proces de curăţare este iniţiat, orice conexiuni din proces care depăşesc limita sunt închise.
8. În câmpul **Limită timeout rezultat**, setaţi numărul de secunde care este permis între încercări de scriere. Puteţi specifica un număr între 0 şi 65535. Setarea implicită este 120. Orice conexiuni care depăşesc această limită sunt închise.

   Notă: Aceasta se aplică doar sistemelor Windows. O conexiune care depăşeşte 30 de secunde este abandonată automat de sistemul de operare. Prin urmare, această setare **Limită timeout rezultat** este înlocuită de sistemul de operare după 30 de secunde.
9. Faceţi clic pe fişa **Fir de execuţie de urgenţă**.
10. Configuraţi setarea firului de execuţie de urgenţă. Caseta de bifare **Activare fir de execuţie de urgenţă** este deja selectată, astfel încât firul de execuţie de urgenţă poate fi activat. Aceasta este setarea implicită. Puteţi face un clic pe caseta de bifare pentru a deselecta funcţia **Activare fir de execuţie de urgenţă**. Această acţiune împiedică activarea firului de execuţie de urgenţă.

11. În câmpul **Cerere prag în curs**, setaţi limita valorii pentru cererile de lucru care activează pragul de urgenţă. Specificaţi un număr între 0 şi 65535 pentru a seta limita cererilor de lucru care pot fi în coadă înainte de activarea firului de execuţie de urgenţă. Valoarea implicită este 50. Când limita specificată este depăşită, firul de execuţie de urgenţă este activat.
12. În câmpul **Prag de timp**, setaţi numărul de minute care se pot scurge de când ultimul articol de lucru a fost înlăturat din coadă. Dacă sunt articole de lucru în coadă şi această limită de timp este depăşită, firul de execuţie de urgenţă este activat. Puteţi specifica un număr între 0 şi 240. Setarea implicită este 5.
13. Din meniul derulant, selectaţi criteriile care trebuie folosite la activarea firului de execuţie de urgenţă. Puteţi selecta:
    - **Numai dimensiunea:** Firul de execuţie de urgenţă este activat doar când coada depăşeşte cantitatea specificată de articole de lucru în curs.
    - **Numai timp:** Firul de execuţie de urgenţă este activat doar când limita de timp dintre articolele de lucru înlăturate depăşeşte valoarea specificată.
    - **Dimensiune sau timp:** Firul de execuţie de urgenţă este activat fie când dimensiunea cozii, fie durata pragului, depăşesc valorile specificate.
    - **Dimensiune şi timp:** Firul de execuţie de urgenţă este activat când atât dimensiunea cozii, cât şi durata pragului, depăşesc valorile specificate.

    Dimensiunea şi timpul reprezintă setarea implicită.
14. Apăsaţi **OK**.

Concepte înrudite

"Refuzarea serviciului" la pagina 82
Folosiţi opţiunea de configurare negare serviciu pentru a proteja împotriva atacurilor de negare.

Operaţii înrudite

"Gestionarea conexiunilor serverului" la pagina 114
Folosiţi aceste informaţii pentru a vizualiza conexiunile la server şi operaţiile realizate de aceste conexiuni.

Activarea notificării evenimentelor

Folosiţi aceste informaţii pentru a activa notificarea evenimentelor Directory Server.

Notificarea evenimentelor permite clienţilor să se înregistreze la Directory Server pentru a fi anunţaţi când survine un eveniment specific, de exemplu când se adaugă ceva în director.

Pentru a activa notificarea de evenimente pentru serverul dumneavoastră, urmaţi aceşti paşi:

1. Expandaţi categoria **Gestionare proprietăţi server** din zona de navigare a Uneltei de administrare Web, selectaţi fişa **Notificare eveniment**.
2. Selectaţi caseta de bifare **Activare notificare eveniment** pentru a activa notificarea evenimentelor. Dacă **Activare notificare eveniment** este dezactivată, serverul ignoră toate celelalte opţiuni din acest panou.
3. Setaţi **Numărul maxim de înregistrări pe conexiune**. Faceţi clic pe butonul radio **Înregistrări** sau **Nelimitat**. Dacă selectaţi **Înregistrări**, trebuie să specificaţi în câmp numărul maxim de înregistrări permise pentru fiecare conexiune. Numărul maxim de tranzacţii este 2,147,483,647. Setarea implicită este 100 de înregistrări.
4. Setaţi **Total număr maxim de înregistrări**. Această selecţie stabileşte câte înregistrări poate avea serverul la un moment dat. Faceţi clic pe butonul radio **Înregistrări** sau **Nelimitat**. Dacă selectaţi **Înregistrări**, trebuie să specificaţi în câmp numărul maxim de înregistrări permise pentru fiecare conexiune. Numărul maxim de tranzacţii este 2,147,483,647. Numărul implicit de înregistrări este **Nelimitat**.
5. Când aţi terminat, faceţi clic pe **Aplicare** pentru a vă salva modificările fără să ieşiţi sau apăsaţi **OK** pentru a aplica modificările şi să ieşiţi sau apăsaţi **Anulare** pentru a părăsi acest panou fără a face vreo modificare.
6. Dacă aţi activat notificare eveniment, trebuie să reporniţi serverul pentru ca modificările să aibă efect. Dacă aţi modificat doar setările, serverul nu trebuie repornit.

Notă: Pentru a dezactiva notificările de evenimente, deselectaţi caseta de bifare **Activare notificări eveniment** şi reporniţi serverul.

| Pentru informaţii suplimentare despre notificarea evenimentelor, vedeţi secţiunea Notificarea evenimentelor din IBM
| Tivoli Directory Server Version 6.0 Programming Reference.

Informaţii înrudite

Centrul de informare IBM Tivoli software
Vedeţi Centrul de informare IBM Tivoli software pentru informaţii despre IBM Tivoli Directory Server

Specificarea setărilor de tranzacţie

Folosiţi aceste informaţii pentru a configura setările de tranzacţie ale Directory Server.

Tranzacţiile Directory Server permit ca un grup de operaţii de director LDAP să fie tratat ca o singură unitate.

Pentru a configura setările de tranzacţii ale serverului dumneavoastră, urmaţi aceşti paşi:

1. Expandaţi categoria **Administrare proprietăţi server** din zona de navigare a Uneltei de administrare Web, selectaţi fişa **Tranzacţii**.
2. Selectaţi caseta de bifare **Activare procesare tranzacţie** pentru a activa procesarea tranzacţiei. Dacă **Activare procesare tranzacţie** este dezactivată, toate celelalte opţiuni din acest panou, ca de exemplu **Numărul maxim de operaţii pe tranzacţie** şi **Limita de timp în curs**, sunt ignorate de către server.
3. Setaţi **Numărul maxim de tranzacţii**. Faceţi clic pe butonul radio **Tranzacţii** sau **Nelimitat**. Dacă selectaţi **Tranzacţii**, trebuie să specificaţi în câmp numărul maxim de tranzacţii. Numărul maxim de tranzacţii este 2,147,483,647. Setarea implicită este 20 de tranzacţii.
4. Setaţi **Numărul maxim de operaţii pe tranzacţie**. Faceţi clic pe butonul radio **Operaţii** sau **Nelimitat**. Dacă selectaţi **Operaţii**, trebuie să specificaţi în câmp numărul maxim de operaţii permise pentru fiecare tranzacţie. Numărul maxim de tranzacţii este 2,147,483,647. Cu cât numărul este mai mic, cu atât creşte performanţa. Valoarea implicită este de 5 operaţii.
5. Setaţi **Limita timpului de aşteptare**. Această selecţie stabileşte valoarea maximă a timeout-ului unei tranzacţii în curs, în secunde. Faceţi clic pe butonul radio **Secunde** sau **Nelimitat**. Dacă selectaţi **Secunde**, trebuie să specificaţi în câmp numărul maxim de secunde permise pentru fiecare tranzacţie. Numărul maxim de tranzacţii este 2,147,483,647. Tranzacţiile lăsate neterminate pentru un timp mai mare decât acesta sunt anulate (date înapoi). Valoarea implicită este 300 de secunde.
6. Când aţi terminat, faceţi clic pe **Aplicare** pentru a vă salva modificările fără să ieşiţi sau apăsaţi **OK** pentru a aplica modificările şi să ieşiţi sau apăsaţi **Anulare** pentru a părăsi acest panou fără a face vreo modificare.
7. Dacă aţi activat suportul pentru tranzacţii, trebuie să reporniţi serverul pentru ca modificările să aibă efect. Dacă aţi modificat doar setările, serverul nu trebuie repornit.

Notă: Pentru a dezactiva procesarea tranzacţiei, deselectaţi caseta de bifare **Activare procesare tranzacţie** şi reporniţi serverul.

Concepte înrudite

"Tranzacţiile" la pagina 50
Puteţi configura Directory Server pentru a peemite clienţilor să folosească tranzacţii. O tranzacţie este un grup de operaţii director LDAP care sunt tratate ca o unitate.

Modificarea portului sau adresei IP

Folosiţi această procedură pentru a modifica porturile pe care Serverul de director la utilizează sau adresele IP pe care Serverul de director acceptă conexiuni.

Directory Server foloseşte următoarele porturi implicite:

- 389 pentru conexiuni nesecurizate.
- 636 pentru conexiuni securizate (dacă aţi utilizat Certificat digital manager pentru a activa Serverul de director ca o aplicaţie ce poate utiliza un port de siguranţă).

Notă: Implicit, toate adresele IP definite pe sistemul local sunt legate la server.

Dacă folosiţi deja aceste porturi pentru altă aplicaţie, puteţi aloca un port diferit pentru Directory Server sau puteţi folosi adrese IP diferite pentru cele două servere, dacă aplicaţiile suportă legarea la o anumită adresă IP.

Pentru a modifica porturile pe care le foloseşte Directory Server sau adresele IP pe care Directory Server acceptă conexiuni, faceţi aceşti paşi:

1. În Navigator System i, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Faceţi clic pe **TCP/IP**.
4. Faceţi clic dreapta pe **IBM Directory Server** şi selectaţi**Proprietăţi**.
5. Faceţi clic pe fişa **Reţea**.
6. Dacă doriţi să modificaţi numărul portului, introduceţi numerele de port corespunzătoare, apoi faceţi clic pe **OK**.
7. Dacă doriţi să modificaţi adresa IP, faceţi clic pe butonul **Adrese IP...**. Apoi continuaţi cu următorul pas.
8. Selectaţi **Utilizare adrese IP selectate** şi selectaţi adresele IP care să fie utilizate de server pentru acceptarea conexiunilor.

Informaţii înrudite

Host Domino LDAP şi Directory Server pe acelaşi sistem

Specificarea unui server pentru referral-ii directorului

Folosiţi aceste informaţii pentru a specifica servere referral.

Pentru a aloca servere referral pentru Dirctory Server, urmaţi aceşti paşi:

1. În Navigator System i, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Faceţi clic pe **TCP/IP**.
4. Faceţi clic dreapta pe **IBM Directory Server**, apoi selectaţi **Proprietăţi**.
5. Selectaţi pagina de proprietăţi **General**.
6. În câmpul **Referral nou**, specificaţi URL-ul serverului referral.
7. La prompt, specificaţi numele serverului referral 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 referral nu foloseşte portul implicit, specificaţi numărul de port corect ca parte a URL-ului, aşa cum este specificat portul 400 în exemplul al doilea de mai sus.
8. Selectaţi **Adăugare**.
9. Faceţi clic pe **OK**.

Concepte înrudite

"Referral-ii directorului LDAP" la pagina 50
Referral-ii permit mai multor servere de director să lucreze în echipe. Dacă DN-ul pe care un client îl cere nu este într-un director, serverul poate trimite automat cererea la orice alt server LDAP.

Adăugarea şi înlăturarea sufixelor serverului de director

Folosiţi aceste informaţii pentru a adăuga sau a înlătura sufixul unui server de director.

Adăugarea unui sufix la Directory Server permite serverului să gestioneze acea parte a arborelui director.

Notă: Nu puteţi adăuga un sufix care este sub un alt sufix aflat deja pe server. De exemplu, dacă o=ibm, c=us erau sufixe pe serverul dumneavoastră, nu puteţi adăuga ou=rochester, o=ibm, c=us.

Pentru a adăuga un sufix la serverul de director, urmaţi aceşti paşi:

1. În Navigator System i, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Faceţi clic pe **TCP/IP**.
4. Faceţi clic dreapta pe **IBM Directory Server** şi selectaţi **Proprietăţi**.
5. Faceţi clic pe fişa **Bază de date/Sufixe**.
6. În câmpul **Sufix nou**, introduceţi numele noului sufix.
7. Selectaţi **Adăugare**.
8. Apăsaţi **OK**.

Notă: Adăugarea unui sufix indică serverului o secţiune a directorului, dar nu creează obiecte. Dacă un obiect care corespunde noului sufix nu exista anterior, trebuie să îl creaţi la fel ca pe orice alt obiect.

Pentru a şterge un sufix din Directory Server, urmaţi aceşi paşi:

1. În Navigator System i, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Faceţi clic pe **TCP/IP**.
4. Faceţi clic dreapta pe **IBM Directory Server** şi selectaţi **Proprietăţi**.
5. Faceţi clic pe fişa **Bază de date/Sufixe**.
6. Apăsaţi sufixul pe care doriţi să îl înlăturaţi pentru a-l selecta.
7. Faceţi clic pe **Înlăturare**.

Notă: Puteţi alege să ştergeţi un sufix fără să ştergeţi obiectele directorului de sub el. Aceasta face datele inaccesibile din serverul de director. Totuşi, puteţi mai târziu recăpăta acces la date prin adăugarea înapoi a sufixului.

Concepte înrudite

"Sufixul (contextul de numire)" la pagina 12
Un sufix (numit şi context de numire) este un DN care identifică cea mai de sus intrare dintr-o ierarhie de director păstrată local.

Adăugarea unui sufix la serverul de director:

Pentru a adăuga un sufix la serverul de director, urmaţi aceşti paşi:

1. În Navigator System i, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Faceţi clic pe **TCP/IP**.
4. Faceţi clic dreapta pe **IBM Directory Server** şi selectaţi**Proprietăţi**.
5. Faceţi clic pe fişa **Bază de date/Sufixe**.
6. În câmpul **Sufix nou**, introduceţi numele noului sufix.
7. Selectaţi **Adăugare**.
8. Apăsaţi **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.

Eliminarea unui sufix din serverul de director:

Pentru a şterge un sufix din Directory Server, urmaţi aceşi paşi:

1. În Navigator System i, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Faceţi clic pe **TCP/IP**.
4. Faceţi clic dreapta pe **IBM Directory Server** şi selectaţi**Proprietăţi**.

5. Faceţi clic pe fişa **Bază de date/Sufixe**.
6. Apăsaţi sufixul pe care doriţi să îl înlăturaţi pentru a-l selecta.
7. Faceţi clic pe **Înlăturare**.

Notă: Puteţi alege să ştergeţi un sufix fără să ştergeţi obiectele directorului de sub el. Aceasta face datele inaccesibile din serverul de director. Totuşi, puteţi mai târziu recăpăta acces la date prin adăugarea înapoi a sufixului.

Acordarea accesului de administrator utilizatorilor proiectaţi (la filtre)

Folosiţi aceste informaţii pentru a acorda acces de administrator profilelor utilizatorilor.

Puteţi acorda acces de administrator pentru profilurile utilizator care au primit acces la identificatorul funcţiei Directory Server Administrator (QIBM_DIRSRV_ADMIN).

De exemplu, dacă profilul de utilizator JOHNSMITH primeşte acces la identificatorul funcţiei Directory Server Administrator şi este selectată opţiunea Acordare acces administrator la utilizatorii autorizaţi din dialogul Proprietăţi director, profilul JOHNSMITH are atunci autorizarea de administrator LDAP. Când acest profil este folosit pentru a lega la serverul de director folosind următorul DN, os400-profile=JOHNSMTH,cn=accounts,os400-sys=systemA.acme.com, utilizatorul are autoritate de administrator. Sufixul obiectului sistem din acest exemplu este os400-sys=systemA.acme.com.

Pentru a selecta opţiunea Acordarea accesului de administrator utilizatorilor autorizaţi şi ID-ul funcţiei Administrator server de director, faceţi aceşti paşi:

1. În Navigator System i, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Faceţi clic dreapta pe **Director** şi selectaţi **Proprietăţi**.
4. La fişa **General** sub **Informaţii administrator** , selectaţi opţiunea **Acordare de acces administrator utilizatorilor autorizaţi**.
5. În Navigator System i, faceţi clic-dreapta pe numele sistemului şi selectaţi **Administrare aplicaţii**.
6. Faceţi clic pe fişa **Aplicaţii gazdă**.
7. Expandaţi **Operating System/400**.
8. Apăsaţi **Administrator Directory Server** pentru a evidenţia această opţiune.
9. Faceţi clic pe butonul **Actualizare**.
10. Expandaţi **Utilizatori**, **Grupuri** sau **Utilizatori care nu fac parte dintr-un grup**, care este corespunzător pentru utilizatorul care-l doriţi.
11. Selectaţi un utilizator sau grup de adăugat la lista **Acces permis**.
12. Faceţi clic pe butonul **Adăugare**.
13. Apăsaţi **OK** pentru a salva modificările.
14. Apăsaţi **OK** pe caseta de dialog **Administrare aplicaţii**.

Concepte înrudite

"Accesul administrativ" la pagina 61
Folosiţi accesul administrativ pentru a controla accesul la anumite taskuri administrative.

"Back-end proiectat de sistem de operare" la pagina 83
Back-end-ul proiectat al sistemului are capacitatea de a mapa obiectei5/OS ca intrări ale arborelui director accesibil-LDAP. Obiectele proiectate sunt reprezentări (proiecţii) LDAP ale obiectelor sistemului de operare în locul intrărilor reale, memorate în baza de date a serverului LDAP.

Activarea tagurilor de limbă

Folosiţi aceste informaţii pentru a activa tagurile de limbă.

Pentru a activa tagurile de limbă, faceţi următoarele (sunt afişate în mod implicit):

1. Faceţi clic pe **Gestionare proprietăţi server** sub categoria **Administrare server** din zona de navigare.

   Notă: Pentru a modifica setările configuraţiei serverului utilizând taskurile din categoria Administrare server a Uneltei de administrare web, trebuie să vă autentificaţi pe server ca un profil de utilzator i5/OS care are autoritatea specială *ALLOBJ şi IOSYSCFG. Aceasta se poate realiza prin autentificarea ca utilizator proiectat cu parola pentru acel profil. Pentru a vă lega ca utilizator proiectat din unealta de administrare Web, introduceţi un numeutilizator de forma os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, unde şirurile MYUSERNAME şi MYSYSTEM.COM sunt înlocuite cu numele profilului dumneavoastră de utilizator, respectiv cu sufixul de proiectare al sistemului configurat.
2. Fişa General este preselectată. Faceţi clic pe caseta de bifare **Activare suport tag de limbă** pentru a o activa.

   Notă: După activarea opţiunii tag de limbă, dacă asociaţi taguri de limbă cu atributele unei intrări, serverul întoarce intrarea cu tagurile de limbă. Aceasta are loc chiar dacă mai târziu dezactivaţi caracteristica tag de limbă. Deoarece comportamentul serverului ar putea să nu fie potrivit pentru aplicaţie şi pentru a evita eventualele probleme, nu dezactivaţi opţiunea tag de limbă după ce a fost activată.

Urmărirea accesului şi a modificărilor la directorul LDAP

Folosiţi aceste informaţii pentru a urmări accesul şi modificările directorului dumneavoastră LDAP.

Puteţi folosi istoricul de modificări a directoarelor LDAP pentru a păstra evidenţa schimbărilor din director. Jurnalul de modificări este localizat sub sufixul special cn=changelog. Este memorat în biblioteca QUSRDIRCL.

Pentru a activa istoricul de modificări, urmaţi aceşti paşi:

1. În Navigator System i, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Faceţi clic pe **TCP/IP**.
4. Faceţi clic dreapta pe **IBM Directory Server** şi selectaţi**Proprietăţi**.
5. Faceţi clic pe fişa **Modificare istoric**.
6. Selectaţi **Înregistrare modificări directoare**.
7. Opţional: În câmpul **Intrări maxime** specificaţi numărul maxim de intrări pentru ca istoricul de modificare să-l păstreze. În câmpul **Vârsta maximă** specificaţi cât timp sunt păstrate intrările în istoricul de modificări.

   Notă: Deşi aceşti parametri sunt opţionali, ar trebuie să vă gândiţi serios dacă să specificaţi fie un număr maxim de intrări, fie o vârstă maximă. Dacă nu specificaţi nici una, nici alta, istoricul de modificări va păstra toate intrările şi ar putea deveni prea mare.

Clasa de obiecte changeLogEntry este folosită pentru a reprezenta modificările aplicate serverului de director. Setul de modificări este dat de setul ordonat al tuturor intrărilor din containerul istoric modificări, după cum este definit de changeNumber. Informaţiile istoricului de modificări sunt numai pentru citire.

Orice utilizator care se află în lista de control acces pentru sufixul cn=changelog poate căuta intrările în istoricul de modificări. Ar trebui să executaţi căutări doar pentru sufixul istoricului de modificări, cn=changelog. Nu încercaţi să adăugaţi, să modificaţi sau să ştergeţi sufixul istoricului de modificări, chiar dacă aveţi autorizarea să o faceţi. Aceasta va cauza rezultate imprevizibile.

Exemplu:

Următorul exemplu foloseşte utilitarul pentru linia de comandă **ldapsearch** pentru a extrage toate intrările istoricului de modificări înregistrate pe server:

```
ldapsearch -h ldaphost -D cn=admininistrator -w password -b cn=changelog  (changetype=*)
```

Activarea auditării obiectelor pentru Directory Server

Folosiţi aceste informaţii pentru a activa auditarea obiectului pentru Directory Server.

Directory Server suportă auditarea de securitate i5/OS. Dacă variabila de sistem QAUDCTL are specificat *OBJAUD, puteţi activa auditarea obiectului prin Navigator System i.

Pentru a activa auditarea obiectelor pentru Directory Server, urmaţi aceşti paşi:

1. În Navigator System i, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Faceţi clic pe **TCP/IP**.
4. Faceţi clic dreapta pe **IBM Directory Server** şi selectaţi**Proprietăţi**.
5. Faceţi clic pe fişa **Auditare**.
6. Selectaţi setarea de auditare pe care vreţi s-o folosiţi pentru serverul dumneavoastră.
7. Apăsaţi **OK**.

Modificările asupra setărilor de auditare vor avea efect imediat ce faceţi clic pe **OK**. Nu este nevoie să reporniţi Directory Server.

Concepte înrudite

"Auditarea" la pagina 51
Auditarea vă permite să depistaţi detaliile anumitor tranzacţii Directory Server.

"Securitatea Directory Server" la pagina 50
Vedeţi cum puteţi să folosiţi o varietate de funcţii pentru a securiza Directory Server.

Ajustarea setărilor de căutare

Folosiţi aceste informaţii pentru a controla capabilităţiile de căutare ale utilizatorului.

Puteţi seta parametrii de căutare să controleze abilităţile de căutare ale utilizatorilor, ca de exemplu căutarea paginată şi sortată, limitele de dimensiune şi de timp şi opţiunile de dereferenţiere alias, folosind unealta de administrare Web.

Rezultatele căutării paginate permit unui client să gestioneze cantitatea de date returnată dintr-o cerere de căutare. Un client poate cere un subset de intrări (o pagină) în loc să primească de-odată toate rezultatele. Cererile de căutare următoare afişează următoarea pagină de rezultate până când este anulată operaţia sau este returnat ultimul rezultat.

Căutarea sortată permite unui client să primească rezultatele căutării sortate după o listă de criterii, în care fiecare criteriu reprezintă o cheie de sortare. Aceasta mută responsabilitatea de sortare de la aplicaţia clientului la server.

Pentru a ajusta setările căutării pentru serverul de director, urmaţi aceşti paşi:

1. Expandaţi categoria **Administrare server** din zona de navigare şi selectaţi **Gestionare proprietăţi server**.

   Notă: Pentru a modifica setările configurării serverului utilizând taskurile în categoria Administrare server a uneltei de administrare web, trebuie să vă autentificaţi la server ca un profil utilizatori5/OS care are autorizările speciale *ALLOBJ şi IOSYSCFG. Aceasta se poate realiza prin autentificarea ca utilizator proiectat cu parola pentru acel profil. Pentru a vă lega ca utilizator proiectat din unealta de administrare Web, introduceţi un numeutilizator de forma os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, unde şirurile MYUSERNAME şi MYSYSTEM.COM sunt înlocuite cu numele profilului dumneavoastră de utilizator, respectiv cu sufixul de proiectare al sistemului configurat.
2. Selectaţi fişa **Setări căutare**.
3. Setaţi **Limita de mărime a căutării**. Faceţi clic pe butonul radio **Intrări** sau **Nelimitat**. Dacă selectaţi **Intrări**, trebuie să specificaţi în câmp numărul maxim de intrări pe care să le întoarcă o căutare. Setarea implicită este 500. Dacă mai multe intrări se potrivesc cu criteriile de căutare, acestea nu sunt întoarse. Această limită nu se aplică administratorilor sau membrilor grupurilor cu limită de căutare cărora li s-au acordat mărimi mai mari ale limitelor de căutare.
4. Setaţi **Limita de timp de căutare**. Faceţi clic pe butonul radio **Secunde** sau **Nelimitat**. Dacă selectaţi **Secunde**, trebuie să specificaţi în câmp durata maximă de timp pe care serverul poate să o petreacă procesând cererea. Setarea implicită este 900. Această limită nu se aplică administratorilor sau membrilor grupurilor cu limită de căutare cărora li s-au acordat durate de timp mai mari ale limitelor de căutare.

5. Pentru a restricţiona posibilităţile de sortare a căutării numai pentru administratori, selectaţi caseta de bifare **Permiteţi numai administratorilor să sorteze căutările**.
6. Pentru a restricţiona posibilităţile de paginare a căutării numai pentru administratori, selectaţi caseta de bifare **Permiteţi numai administratorilor să pagineze căutările**.
7. Expandaţi meniul derulant pentru **Dereferenţiere alias** şi selectaţi una din următoarele. Setarea implicită este **Întotdeauna**.

   Niciodată
   Alias-urile nu sunt niciodată dereferenţiate.

   Găsire Alias-urile sunt dereferenţiate la găsirea punctului de plecare pentru căutare, dar nu când se caută sub acea intrare de plecare.

   Căutare
   Alias-urile sunt dereferenţiate la căutarea intrărilor de sub punctul de plecare al căutării, dar nu la găsirea intrării de plecare.

   Întotdeauna
   Alias-urile sunt întotdeauna dereferenţiate, atât la găsirea punctului de plecare pentru căutare, cât şi la căutarea intrărilor de sub intrarea de plecare. Setarea implicită este întotdeauna.

   Operaţii înrudite

   "Căutarea intrărilor directorului" la pagina 189
   Folosiţi aceste informaţii pentru a căuta intrările directorului.

   Referinţe înrudite

   "Parametrii de căutare" la pagina 46
   Pentru a limita cantitatea de resurse folosite de server, un administrator poate configura parametrii de căutare pentru a restricţiona posibilităţile de căutare ale utilizatorilor. Posibilităţile de căutare pot fi şi extinse pentru utilizatori speciali.

Activarea sau dezactivarea accesului cu citire pentru utilizatorii proiectaţi

Folosiţi aceste informaţii pentru a interzice operaţiile de comparare şi căutare la back-end-ul utilizatorului proiectat.

Pentru a interzice operaţiile de căutare şi comparare la back-end-ul proiectat al utilizatorului,faceţi următoarele:

1. Opriţi serverul de director. Introduceţi ENDTCPSVR *DIRSRV.
2. Ediaţi fişierul /QIBM/UserData/OS400/DirSrv/ibmslapd.conf. De exemplu, introduceţi EDTF '/QIBM/UserData/OS400/DirSrv/ibmslapd.conf'.
3. Căutaţi textul cn=Frint end.
4. Inseraţi o nouă linie conţinând ibm-slapdSetEnv: IBMSLAPDOS400USRPRJREAD=FALSE imediat după ce linia care conţine textul cn=Front End. În următorul exemplu, a doua linie a fost inserată:

   ```
   dn: cn=Front End, cn=Configuration
   ibm-slapdSetEnv: IBMSLAPDOS400USRPRJREAD=FALSE
   cn: Front End
   ```

5. Salvaţi fişierul şi ieşiţi din editor. De exemplu, apăsaţi F2 pentru a salva fişierul, urmat de F3 pentru a ieşi din editor dacă utilizaţi EDTF.
6. Reporniţi server de director. Introduceţi STRTCPSVR *DIRSRV.

   Concepte înrudite

   "Accesul la citire pentru utilizatorii proiectaţi" la pagina 88
   Implicit, proiectarea sistemului back-end furnizează utilizatorilor autorizaţi acces cu citire pentru informaţiile profilului de utilizator prin căutare LDAP şi operaţii de căutare. Accesul cu citire pentru utilizatorii proiectaţi poate fi activat sau dezactivat utilizând Navigator System i sau printr-o setare configurare în fişierul /QIBM/UserData/OS400/DirSrv/idsslapd-instance/etc/ibmslapd.conf (/QIBM/UserData/OS400/DirSrv/idsslapd-QUSRDIR/etc/ibmslapd.conf fişier pentru instanţa serverului implicit).

Publicarea informaţiilor Directory Server

Vedeţi cum se publică informaţiile pe Directory Server.

Vă puteţi configura sistemul să publice anumite informaţii într-un Directory Server din acelaşi sistem sau dintr-un sistem diferit, precum şi informaţii definite de utilizator. Sistemul de operare publică automataceste informaţii la Serverul de director când utilizaţi Navigator System i pentru a modifica a ceste informaţiii5/OS. Informaţiile pe care le puteţi publica includ sistem (sisteme şi imprimante), partajări imprimantă, informaţii utilizator şi politici Calitate a serviciilor TCP/IP.

Dacă părintele DN lacare datele sunt publicate nu există, Serverul de director le creează automat. S -ar putea să fi instalat alte i5/OS aplicaţii care publică informaţii într-un director LDAP. În plus, puteţi apela interfeţele de program aplicaţie (API) din programele dvs proprii pentru a publica alte tipuri de informaţii în directorul LDAP.

Notă: Puteţi de asemenea publica i5/OS informaţii la un server de director care nu rulează pe i5/OS dacă configuraţi serverul să utilizeze schema IBM.

Pentru a configura informaţiile sistemului dumneavoastră i5/OS într-un server de director,faceţi următorii paşi:

1. În Navigator System i, apăsaţi clic-dreapta pe sistemul dumneavoastră şi selectaţi **Proprietăţi**.
2. Faceţi clic pe fişa **Directory Server**.
3. Selectaţi tipurile de informaţii pe care doriţi să le publicaţi. Selectaţi tipurile de informaţii pe care doriţi să le publicaţi.

   Indiciu: Dacă planificaţi să publicaţi mai mult de un tip de informaţie la aceeaşi locaţie, puteţi salva timp prin selectarea ami multor tipuri de informaţii de configurat la un moment dat. Navigatorul de operaţii va folosi apoi valorile care le introduceţi când configuraţi acelaşi tip de informaţii ca şi valorile implicite când configuraţi tipurile ulterioare de informaţii.
4. Faceţi clic pe **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. Apăsaţi butonul **Editare** de lângă câmpul**Directory Server (Activ)** . În dialogul care apare,introduceţi numele serverului de director unde vreţi să publicaţi i5/OS informaţiile, apoi faceţi clic pe **OK**.
8. În câmpul **Sub DN**, introduceţi numele distinctiv părinte unde doriţi ca informaţiile să fie adăugate în serverul de director.
9. Completaţi câmpurile din cadrul **Conexiune server** care sunt corespunzătoare configuraţiei.

   Notă: Pentru a publica i5/OS informaţiile serverul de director utilizând SSL sau Kerberos, trebuie mai întâi să aveţi serverul de director configurat să utilizeze protocolul corespunzător. Vedeţi “Autentificarea Kerberos cu Directory Server” la pagina 52 pentru informaţii despre SSL şi Kerberos.
10. Dacă serverul de director 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. Apăsaţi **OK**.

Notă: Puteţi de asemenea publica i5/OS informaţiilela un server de dire ctor care este pe o platformă diferită. Trebuie să publicaţi informaţii utilizator şi parolă la un server de director care utilizează o schemă compatibilă cu schema serverului de director IBM. Pentru informaţii suplimentare despre IBM Directory Schema, vedeţi “Schema serverului de director” la pagina 14.

Puteţi de asemenea utiliza API-urile de publicare şi configurare a serverului LDAP pentru a activa i5/OS programele pe care le scrieţi să publice alte tipuri de informaţii. Aceste tipuri de informaţii apar apoi şi în pagina **Directory Server**. Precum sistemele şi utilizatorii, acestea sunt iniţial dezactivate şi le configuraţi folosind aceeaşi procedură. Programul care adaugă datele la directorul LDAP este numit agentul de publicare. Tipul de informaţii care sunt publicate, după cum apare în pagina **Directory Server**, este numit nume agent.

Următoarele API-uri vă vor permite să încorporaţi publicarea în propriile dumneavoastră programe:

QgldChgDirSvrA
O aplicaţie foloseşte formatul CSVR0500 pentru a adăuga iniţial un nume de agent care este marcat ca o intrare dezactivată. Instrucţiunile pentru utilizatori din aplicaţie ar trebui să transmită utilizatorilor să folosească Navigator System i pentru a merge la pagina de proprietăţi servere de director pentru a configura agentul de publicare. Exemple de nume agent sunt numele de agent utilizatori şi sisteme disponibile automat în pagina **Directory Server**.

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

QgldPubDirObj
Folosiţi acest API pentru a face publicarea efectivă a informaţiei.

Concepte înrudite

"Publicarea" la pagina 35
Directory Server oferă posibilitatea ca sistemul să publice anumite tipuri de informaţii într-un director LDAP. Cu alte cuvinte, sistemul va crea şi actualiza intrări LDAP reprezentând tipuri diferite de date.

API-urile Directory Server

Importarea unui fişier LDIF

Folosiţi aceste informaţii pentru a importa un fişier LDIF (Data Interchange Format) LDAP.

Puteţi transfera informaţii între diferite servere de director prin folosirea fişierelor LDAP LDIF. Folosiţi unealta de import (şi API-ul corespunzător QgldImportLdif) pentru a adăuga noi intrări în director. Unealta de import nu poate fi folosită pentru a modifica sau şterge intrări, iar fişierul LDIF trebuie să utilizeze stilul de conţinut director, nu înregistrări LDIF în stilul modificare înregistrare. Dacă fişierul LDIF de intrare conţine directive changetype utilizate în înregistrări LDIF cu stilul modificare înregistrare, linia changetype este interpretată ca un alt atribut şi intrarea nu va fi adăugată în director.

De obicei, este exportat de pe un server întregul director (sau un subarbore al directorului), folosind unealta de export (sau API-ul QgldExportLdif) şi apoi este importat pe alt server.

Uneltele de export şi import nu sunt echivalente cu folsoirea utilitarelor pentru linie de comandă ldapsearch şi ldapadd. Unealta de export include mai multe atribute operaţionale (cum ar fi informaţiile de control al accesului şi amprentele de timp ale creării intrării) nereturnate normal de ldapsearch, în timp ce unealta de import poate seta atribute care nu pot fi setate de obicei de o aplicaţie client cum este ldapadd. Utilitarul ldapadd poate fi folsoit cu opţiunea -k (control administrare server) pentru a încărca aceste fişiere.

Înainte de a începe această procedură, transferaţi fişierul LDIF la sistemul dumneavoastră ca un fişier flux.

Pentru a importa un fişier LDIF în Directory Server, urmaţi aceşti paşi:

1. Dacă serverul de director este pornit, opriţi-l. Vedeţi "Pornirea Directory Server" la pagina 112 pentru informaţii despre oprirea serverului de director.
2. În Navigator System i, expandaţi **Reţea**.
3. Expandaţi **Servere**.
4. Faceţi clic pe **TCP/IP**.
5. Faceţi clic dreapta pe **IBM Directory Server** şi selectaţi **Unelte**, apoi **Importare fişier**.

   Opţional puteţi face ca serverul să replice noile date importate la următoarea pornire, prin selectarea **Replicare date importate**. Aceasta este de folos când adăugaţi noi intrări la un arbore director existent pe un server master. Dacă importaţi date pentru a iniţializa un server replică (sau peer), de obicei nu veţi dori ca datele să fie replicate, deoarece s-ar putea să existe deja pe serverele pentru care acest server este furnizor.

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

Referinţe înrudite

"Formatul pentru schimbul de date LDAP (LDIF)" la pagina 238
Formatul interschimbare date LDAP este un format text standard pentru reprezentarea obiectelor LDAP şi actualizărilor LDAP (adăugare, modificare, ştergere, modificare DN) într-un formular textual. Fişierele ce conţin înregistrări LDIF pot fi utilizate pentru trasferul datelor între serverele de director sau utilizate ca intrări de către unelte LDAP precum **ldapadd** şi **ldapmodify**.

"ldapmodify şi ldapadd" la pagina 207
Utilitarele de linie de comandă modificare-intrare LDAP şi adăugare-intrare LDAP.

Exportarea unui fişier LDIF

Folosiţi aceste informaţii pentru a exporta un fişier LDIF (Data Interchange Format) LDAP

Puteţi transfera informaţii între diferite fişiere LDIF. Puteţi exporta tot directorul sau părţi ale directorului LDAP la un fişier LDIF.

Pentru a exporta un fişier LDIF din serverul de director, urmaţi aceşti paşi:

1. În Navigator System i, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Faceţi clic pe **TCP/IP**.
4. Faceţi clic dreapta pe **IBM Directory Server** şi selectaţi **Unelte**, apoi **Exportare fişier**.

   Notă: Dacă nu specificaţi o cale complet calificată pentru fişierul LDIF în care să exportaţi datele, fişierul va fi creat în directorul home din profilul utilizator al sistemului dumneavoastră de operare.
5. Specificaţi dacă să **Exportaţi întregul director** sau să**Exportaţi subarborele selectat** şi de asemenea dacă să **Exportaţi atributele operaţionale**. Atributele operaţionale care sunt exportate sunt creatorsName, createTimestamp, modifiersName şi modifyTimestamp.

Observaţii:

1. La exportarea datelor pentru importarea în V5R3 sau în servere de director precedente, nu selectaţi**Exportare atribute operaţionale**. Aceste atribute operaţionale nu pot fi importate în V5R3 sau servere de director mai vechi.
2. De asemenea puteţi crea un fişier LDIF complet sau parţial cu utilitarul ldapsearch. Folosiţi opţiunea -L şi redirectaţi ieşirea într-un fişier.
3. Asiguraţi-vă că setaţi autoritatea fişierului LDIF pentru a preveni accesul neautorizat la datele directorului. Pentru a face asta, faceţi clic-dreapta pe fişierul din Navigator System i, apoi selectaţi **Permissions**.

Referinţe înrudite

"Formatul pentru schimbul de date LDAP (LDIF)" la pagina 238
Formatul interschimbare date LDAP este un format text standard pentru reprezentarea obiectelor LDAP şi actualizărilor LDAP (adăugare, modificare, ştergere, modificare DN) într-un formular textual. Fişierele ce conţin înregistrări LDIF pot fi utilizate pentru trasferul datelor între serverele de director sau utilizate ca intrări de către unelte LDAP precum **ldapadd** şi **ldapmodify**.

"ldapsearch" la pagina 224
Utilitarul pentru linie de comandă de căutare LDAP.

Copierea utilizatorilor în Directory Server dintr-o listă de validare a serverului HTTP

Folosiţi aceste informaţii pentru a copia utilizatori dintr-o listă de validare a serverului HTTP în Directory Server.

Dacă folosiţi în prezent serverul HTTP sau l-aţi folosit în trecut, s-ar putea să fi creat liste de validare pentru memorarea utilizatorilor de internet şi a parolelor acestora. Pe măsură ce vă îndreptaţi către WebSphere Application Server, Portal Server şi alte aplicaţii care suportă autentificarea LDAP, puteţi dori să continuaţi să folosiţi aceşti utilizatori de internet existenţi şi parolele lor. Aceasta se poate realiza folosind API-ul QGLDCPYVL (″Copy Validation List to Directory″ - Copiere listă de validare în director) .

QGLDCPYVL citeşte intrări de la o listă de validare şi creează obiecte LDAP corespunzătoare în serverul de director local. Obiectele sunt intrări inetOrgPerson scheletice cu un atribut userPassword care conţine o copie a informaţiilor parolei de la intrarea listei de validare. Puteţi decide cum şi când să se numească acest API. Îl puteţi folosi o singură dată ca operaţie pentru o listă de validare care nu se va modifica sau ca un job planificat să actualizeze serverul de director pentru a reflecta noile intrări din lista de validare.

De exemplu:

```
CALL PGM(QSYS/QGLDCPYVL) PARM('HTTPVLDL  MYLIB     ' 'cn=administrator'
X'00000000' 'secret' X'00000000' 'cn=users,o=my company' X'00000000' '' X'00000000'
X'00000000')
```

Concepte înrudite

API-urile LDAP (Lightweight Directory Access Protocol)
Vedeţi API-urile LDAP (Lightweight Directory Access Protocol) pentru informaţii suplimentare despre API Directory Server

Operaţii înrudite

"Scenariu: Copierea utilizatorilor în Directory Server dintr-o listă de validare a serverului HTTP" la pagina 111
Un exemplu de copiere a utilizatorilor dintr-o listă de validare a serverului HTTP în Directory Server.

Gestionarea instanţelor

Puteţi avea multiple servere de director pe sistemul dumneavoastră i5/OS. Fiecare server este cunoscut ca o istanţă. Dacă aţ i folosit serverul de director pe o ediţie anterioarăi5/OS, va fi migrată la o instanţă cu numele QUSRDIR. Puteţi crea multiple instanţe ale serverului de director pentru a face service aplicaţiilor dumneavoastră.

Unicitatea printre instanţele serverului de director este definită de adresa IP şi/sau portul la care instanţa este configurată dă asculte. De asemenea, fiecare instanţă a serverului de director care rulează trebuie să aibă o bază de date unică, un istoric de modificări şi un fişier de configurare. Vă va fi permis să creaţi şi să configuraţi instanţe de server cu conflicte, totuşi, dacă încercaţi să porniţi o instanţă de server care este în conflict cu altă instanţă de server activă, a doua instanţă nu va porni şi va fi lansat un mesaj de eroare.

O instanţă de server conţine toate fişierele care sunt necesare pentru ca un server de director să ruleze pe un computer.

Printre fişierele instanţei serverului de director se numără:

- Fişierul ibmslapd.conf (fişierul de configurare)
- Fişiere de schemă
- Fişiere de istoric
- Fişiere temporare de stare

Fişierele pentru o instanţă a serverului de director sunt memorate într-un director numit idsslapd-*instance_name*, unde *instance_name* este numele instanţei a serverului de director. Directorulidsslapd-*instance_name* este în directorul /QIBM/UserData/OS400/DirSrv.

Fiecare instanţă a serverului de director, când creată, înregistrează o nouă aplicaţie la Managerul de certificate digitale (DCM). Noile instanţe ale serverului de director au numele QIBM_DIRECTORY_SERVER_ <instance-name>. Trebuie să utilizaţi DCM pentru a asocia un certificat digital cu instanţa serverului de director dacă vreţi să utilizaţi SSL. Când fiecare instanţă de server porneşte, înregistrează cu Navigator System i ca unserver pentru a putea fi urmărită cu Navigator System i.

Jobul pentru instanţa serverului are setat nu mele jobului la numele instanţei. Aşa, de exemplu, instanţa QUSRDIR are un nume job complet calificat xxxxxx/QDIRSRV/QUSRDIR. 'xxxxxx'- ul este numărul jobului care este determinat când jobul porneşte. Aceasta este o diferenţă pentru utilizatorii care utilizează curent serverul de director ca şi numele jobului a fost xxxxxx/QDIRSRV/QDIRSRV.

Pentru a gestiona instanţe, faceţi următoarele:

1. În Navigator System i, expandaţi **Reţea**.

2. Expandaţi **Servere**.
3. Faceţi clic pe **TCP/IP**.
4. Faceţi clic dreapta pe **IBM Tivoli Directory Server** şi selectaţi **Gestionare instanţe**.

Dacă salvaţi periodic instanţele, trebuie să salvaţi biblioteca <*instance-name*>CF împreună cu directorul de baze de date.

Taskurile grupurilor administrative

Folosiţi aceste informaţii pentru a gestiona grupuri administrative.

Grupul administrativ dispune de posibilitatea de a oferi abilităţi administrative fără a fi nevoie de partajarea unui ID sau parolă printre administratori. Membrii grupului administrativ au propriile ID-uri şi parole unice. DN-urile membrilor grupului administrativ nu trebuie să fie aceleaşi şi nu trebuie să se potrivească nici cu DN-ul administratorului IBM Directory Server. Dimpotrivă, DN-ul administratorului IBM Directory Server nu trebuie să se potrivească cu DN-ul unui membru din alt grup administrativ.

Această regulă se aplică şi pentru administratorul ID-urilor Kerberos sau Digest-MD5 ale IBM Directory Server şi membrilor grupului administrativ. Aceste DN-uri nu trebuie să coincidă cu DN-urile vreunui furnizor de replicare a IBM Directory Server. Aceasta mai înseamnă că DN-urile furnizorului de replicare a IBM Directory Server nu trebuie să coincidă cu DN-urile vreunui membru al grupului administrativ sau cu DN-ul administratorului IBM Directory Server.

Notă: DN-urile furnizorului de replicare a IBM Directory Server pot să coincidă între ele.

Concepte înrudite

"Accesul administrativ" la pagina 61
Folosiţi accesul administrativ pentru a controla accesul la anumite taskuri administrative.

Activarea grupului administrativ

Folosiţi aceste informaţii pentru a activa grupul administrativ.

Trebuie să fiţi administratorul IBM Directory Server pentru a realiza această operaţie.

1. Expandaţi categoria **Administrare server** din zona de navigare a Uneltei de administrare Web şi apăsaţi **Gestionare grup administrativ**.

   Notă: Pentru a modifica setările configuraţiei serverului taskurile din categoria Administrare server a uneltei de administrare web, trebuie să vă autentificaţi la server ca un profil utilizator i5/OS care ar e autorizările speciale *ALLOBJ şi IOSYSCFG. Aceasta se poate realiza prin autentificarea ca utilizator proiectat cu parola pentru acel profil. Pentru a vă lega ca utilizator proiectat din unealta de administrare Web, introduceţi un numeutilizator de forma os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, unde şirurile MYUSERNAME şi MYSYSTEM.COM sunt înlocuite cu numele profilului dumneavoastră de utilizator, respectiv cu sufixul de proiectare al sistemului configurat.
2. Pentru a activa sau dezactiva grupul administrativ, faceţi clic pe caseta de bifare de lângă **Activare grup administrativ**. Dacă această casetă este bifată, grupul administrativ este activat.
3. Apăsaţi **OK**.

   Notă: Dacă dezactivaţi grupul administrativ, orice membru care este logat poate continua operaţiile administrative până când i se cere să se reconecteze.

Adăugarea, editarea şi înlăturarea membrilor grupului administrativ

Folosiţi aceste informaţii pentru a adăuga, edita sau înlătura membrii grupului administrativ.

Cerinţă preliminară: Trebuie să fiţi administratorul IBM Directory Server pentru a realiza această operaţie.

1. Expandaţi categoria **Administrare server** din zona de navigare a Uneltei de administrare Web şi apăsaţi **Gestionare grup administrativ**.

Notă: Pentru a modifica setările configuraţiei serverului utilizând taskurile în categoria Administrare server a Uneltei de administ rare Web, trebuie să vă autetificaţi la server ca un profil utilizator i5/OS care are autorizările speciale *ALLOBJ şi IOSYSCFG. Aceasta se poate realiza prin autentificarea ca utilizator proiectat cu parola pentru acel profil. Pentru a vă lega ca utilizator proiectat din unealta de administrare Web, introduceţi un numeutilizator de forma os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, unde şirurile MYUSERNAME şi MYSYSTEM.COM sunt înlocuite cu numele profilului dumneavoastră de utilizator, respectiv cu sufixul de proiectare al sistemului configurat.

2. În panoul **Gestionare grup administrativ**, apăsaţi **Adăugare**.
3. În panoul **Adăugare membru grup administrativ**:
   a. Introduceţi DN-ul de administrator al membrului (acesta trebuie să aibă o sintaxă DN validă).
   b. Introduceţi parola membrului.
   c. Introduceţi din nou parola membrului pentru a o confirma.
   d. Opţional: Introduceţi ID-ul membrului Kerberos. ID-ul Kerberos trebuie să fie în format ibm-kn sau ibm-KerberosName. Valorile nu sunt sensibile la majuscule, de exemplu, ibm-kn=root@TEST.ROCHESTER.IBM.COM este echivalent cu ibm-kn=ROOT@TEST.ROCHESTER.IBM.COM.
4. Opţional: introduceţi numele utilizator al membrului **Digest-MD5**.

   Notă: Numele utilizator Digest-MD5 este sensibil la majuscule.
5. Apăsaţi **OK**.
6. Repetaţi această procedură pentru fiecare membru pe care doriţi să îl adăugaţi în grupul administrativ.

DN-ul de administrator al membrului, numele utilizator Digest-MD5, dacă este specificat şi ID-ul Kerberos, dacă este specificat, sunt afişate în caseta listei membrilor grupului administrativ.

Pentru a modifica sau înlătura membrii grupului administrativ, urmaţi aceeaşi procedură ca cea de mai sus, dar folosiţi butoanele **Editare** şi **Ştergere** din panoul **Gestionare grup administrativ**.

| Parola ăentru un membru gr up administrativ poate de asemenea să fie modificat utilizând comanda Modificare server
| de director Attr (CHGDIRSVRA). Pentru a modi fica parola membrului grupului administrativ cu legătură DN
| cn=adminuser1 la newpassword, utilizaţi această parolă:

```
| CHGDIRSVRA INSTANCE(QUSRDIR) DN('cn=adminuser1' 'newpassword')
```

| Taskuri ale grupului de limitare a căutării

Folosiţi aceste informaţii pentru a gestiona grupurile de limitare a căutării.

Pentru a împiedica un consum prea mare de resurse şi, în consecinţă, slăbirea performanţei serverului datorate cererilor de căutare ale unui utilizator, sunt impuse limite de căutare pentru aceste cereri pentru orice server dat. Administratorul stabileşte aceste limite de căutare prin dimensiunea şi durata căutărilor la configurarea serverului.

Doar administratorul şi membrii grupului administrativ sunt scutiţi de aceste limite de căutare, care se aplică tuturor celorlalţi utilizatori. Totuşi, în funcţie de necesităţi, un administrator poate crea grupuri cu limită de căutare care pot avea mai multe llimite de căutare flexibile decât pentru un utilizator obişnuit. Astfel, administratorul poate oferi privilegii speciale de căutare pentru un grup de utilizatori.

Unealta de administrare Web este folosită pentru a gestiona grupurile cu limită de căutare.

Referinţe înrudite

“Parametrii de căutare” la pagina 46
Pentru a limita cantitatea de resurse folosite de server, un administrator poate configura parametrii de căutare pentru a restricţiona posibilităţile de căutare ale utilizatorilor. Posibilităţile de căutare pot fi şi extinse pentru utilizatori speciali.

Crearea unui grup de limitare a căutării

Folosiţi aceste informaţii pentru a crea un grup de limitare a căutării.

Pentru a crea un grup cu limită de căutare, trebuie creată o intrare grup folosind unealta de administrare Web.

1. Expandaţi categoria **Gestionare director** din zona de navigare şi apăsaţi **Adăugare intrare**. Sau faceţi clic pe **Gestionare intrări** şi selectaţi locaţia (cn=IBMpolicies sau cn=localhost), apoi apăsaţi **Adăugare**. Intrările sub cn=IBMpolicies vor fi replicate, cele de sub cn=localhost nu vor fi.
2. Selectaţi una din clasele obiect ale grupului din meniul **Clasă de obiecte structurale**.
3. Apăsaţi **Următorul**.
4. Selectaţi o clasă obiect auxiliară **ibm-searchLimits** din meniul **Disponibilă** şi apăsaţi **Adăugare**. Repetaţi acest proces pentru fiecare clasă obiect auxiliară suplimentară care trebuie adăugată. O clasă obiect auxiliară din meniul **Selectată** poate fi înlăturată selectând-o şi apăsând **Înlăturare**.
5. Apăsaţi **Următorul**.
6. În câmpul **DN corespunzător**, introduceţi numele distinctiv corespunzător (RDN) al grupului care este adăugat. De exemplu, cn=Search Group1.
7. În câmpul **DN părinte**, introduceţi numele distinctiv al intrării din arbore care este selectată. De exemplu, cn=localhost. Puteţi de asemenea să apăsaţi pe **Răsfoire** pentru a selecta DN-ul părinte din listă. Faceţi o alegere şi apăsaţi **Selectare** pentru a specifica un DN părinte. **DN-ul părinte** are valoare implicită intrarea selectată în arbore.

   Notă: Dacă aţi pornit acest task din panoul **Gestionare intrări**, acest câmp este completat pentru dumneavoastră. **DN-ul părinte** a fost selectat înainte de a apăsa **Adăugare** pentru a porni procesul de adăugare intrare.
8. În fişa **Atribute necesare**, introduceţi valorile pentru atributele necesare.
   - **cn** este DN-ul corespunzător pe care l-aţi specificat mai devreme.
   - În câmpul **ibm-searchSizeLimit**, specificaţi numărul de intrări cu care să limitaţi dimensiunea căutării. Acest număr poate fi în intervalul de la 0 până la 2,147,483,647. O setare 0 este aceeaşi cu **Nelimitat**.
   - În câmpul **ibm-searchTimeLimit**, specificaţi numărul de secunde cu care să limitaţi durata căutării. Acest număr poate fi în intervalul de la 0 până la 2,147,483,647. O setare 0 este aceeaşi cu **Nelimitat**.
   - În funcţie de clasa obiect pe care aţi selectat-o, puteţi vedea un câmp **Membru** sau **uniqueMember**. Aceştia sunt membrii grupului pe care îl creaţi. Intrarea este sub forma unui DN, de exemplu, cn=Bob Garcia,ou=austin,o=ibm,c=us.
9. Dacă vreţi să adăugaţi mai mult de o valoare pentru un anumit atribut, apăsaţi **Valori multiple** şi apoi adăugaţi valorile pe rând. Apăsaţi **OK** când aţi terminat de editat valorile multiple. Valorile sunt adăugate într-un meniu expandabil afişat la atribut.
10. Dacă serverul dumneavoastră are tagurile de limbă activate, faceţi clic pe **Valoare tag limbă** pentru a adăuga sau înlătura descriptorii tagului de limbă.
11. Faceţi clic pe **Alte atribute**.
12. În fişa **Alte atribute**, introduceţi valorile corespunzătoare pentru atribute. Consultaţi “Modificarea atributelor binare” la pagina 191 pentru mai multe informaţii.
13. Faceţi clic pe **Sfârşit** pentru a crea intrarea.

Modificarea unui grup de limitare a căutării

Folosiţi aceste informaţii pentru a modifica un grup de limitare a căutării.

Puteţi modifica atributele limită de dimensiune sau de timp ale unui grup cu limită de căutare. Puteţi de asemenea să adăugaţi şi să ştergeţi membrii unui grup. Folosiţi unealta de administrare Web pentru a modifica un grup cu limită de căutare.

1. Dacă nu aţi făcut asta deja, expandaţi categoria **Gestionare director** din zona de navigare, apoi apăsaţi pe **Gestionare intrări**. Puteţi expanda diverşi subarbori şi selecta intrarea cu care vreţi să lucraţi. Apăsaţi **Editare atribute** din bara de unelte din partea dreaptă.

2. În fişa **Atribute obligatorii** introduceţi valorile pentru atributele obligatorii. Vedeţi “Modificarea atributelor binare” la pagina 191 pentru informaţii despre adăugarea valorilor binare. Dacă vreţi să adăugaţi mai mult de o valoare pentru un anumit atribut, apăsaţi **Valori multiple** şi apoi adăugaţi valorile pe rând.
3. Apăsaţi **Atribute opţionale**.
4. În fişa **Atribute opţionale** introduceţi valorile corespunzătoare pentru atributele opţionale. Dacă vreţi să adăugaţi mai mult de o valoare pentru un anumit atribut, apăsaţi **Valori multiple** şi apoi adăugaţi valorile pe rând.
5. Faceţi clic pe **Apartenenţă**.
6. Dacă aţi creat vreun grup, la fişa **Apartenenţă**:
   - Selectaţi un grup din **Grupuri disponibile** şi apăsaţi **Adăugare** pentru a face intrarea membru al **Apartenenţei la grupul static** selectate.
   - Selectaţi un grup din **Apartenenţe grup spatic** şi faceţi clic pe **Înlăturare** pentru a înlătura intrarea din grupul selectat.
7. Dacă intrarea este o intrare grup, o fişă **Membri** este disponibilă. Fişa **Membri** afişează membrii grupului selectat. Puteţi adăuga şi înlătura membrii din grup.
   - Pentru a adăuga un membru la grup:
     a. Fie faceţi clic pe **Valori multiple** din fişa **Membri** sau la fişa **Membri**, faceţi clic pe **Membri**.
     b. În câmpul Membru, introduceţi DN-ul intrării pe care doriţi să o adăugaţi.
     c. Selectaţi **Adăugare**.
     d. Apăsaţi **OK**.
   - Pentru a înlătura un membru din grup:
     a. Fie faceţi clic pe **Valori multiple** din fişa **Membri** sau la fişa **Membri**, faceţi clic pe **Membri**.
     b. Selectaţi intrarea pe care doriţi să o înlăturaţi:
     c. Faceţi clic pe **Înlăturare**.
     d. Apăsaţi **OK**.
   - Pentru a reîmprospăta lista de membri, faceţi clic pe **Actualizare**.
8. Faceţi clic pe **OK** pentru a modifica intrarea.

Copierea unui grup de limitare a căutării

Folosiţi aceste informaţii pentru a copia un grup de limitare a căutării.

Este folositor să copiaţi un grup cu limită de căutare dacă doriţi să aveţi acelaşi grup cu limită de căutare atât sub localhost, cât şi sub IBMpolicies. Este de asemenea util dacă doriţi să creaţi un nou grup care are informaţii similare cu un grup existent, dar are diferenţe minore.

1. Dacă nu aţi făcut asta deja, expandaţi categoria **Gestionare director** din zona de navigare, apoi apăsaţi pe **Gestionare intrări**. Puteţi expanda diverşi subarbori şi selecta intrarea, precum John Doe, cu care vreţi să lucraţi. Apăsaţi **Copiere** din bara de unelte din partea dreaptă.
2. Modificaţi intrarea RDN din câmpul DN. De exemplu modificaţi cn=John Doe cu cn=Jim Smith.
3. În fişa de atribute necesară, modificaţi intrarea cn la noua RDN. În acest exemplu Jim Smith.
4. Modificaţi corespunzător celelalte atribute necesare. În acest exemplu modificaţi atributul sn de la Doe la Smith.
5. Când aţi terminat de modificat faceţi clic pe **OK** pentru a crea noua intrare. Noua intrare Jim Smith este adăugată în josul listei de intrare.

Înlăturarea unui grup de limitare a căutării

Folosiţi aceste informaţii pentru a înlătura un grup de limitare a căutării.

1. Dacă nu aţi făcut asta deja, expandaţi categoria **Gestionare director** din zona de navigare, apoi apăsaţi pe **Gestionare intrări**. Puteţi expanda diverşi subarbori şi selecta subarborele, sufixul sau intrarea cu care vreţi să lucraţi. Apăsaţi **Şterge** din bara de unelte din partea dreaptă.
2. Vi se va cere să confirmaţi ştergerea. Apăsaţi **OK**. Intrarea este ştearsă din director şi reveniţi la lista de intrări.

Taskuri ale grupului de autorizare proxy

Folosiţi aceste informaţii pentru a gestiona grupurile de autentificare proxy.

Membrii unui grup cu autorizare proxy pot accesa Directory Server şi să realizeze multe taskuri din partea mai multor utilizatori fără a trebuie să se reconecteze pentru fiecare utilizator. Membrii grupului de autorizare proxy îşi pot asuma orice identităţi autentificate, cu excepţia celei de administrator sau a membrilor din grupul administrativ.

Unealta de administrare Web este folosită pentru a gestiona autorizarea proxy.

Concepte înrudite

"Autorizarea proxy" la pagina 62
Autorizarea proxy este o formă specială de autentificare. Prin utilizarea acestui mecanism de autorizare proxy, o aplicaţie client se poate lega la director folosind propria identitate, dar îi este permis să realizeze operaţii din partea altui utilizator pentru a accesa directorul destinaţie. Un set de aplicaţii sau utilizatori de încredere poate accesa Directory Server din partea mai multor utilizatori.

Crearea unui grup de autorizare proxy

Folosiţi aceste informaţii pentru a crea un grup de autorizare proxy.

1. Expandaţi categoria **Gestionare director** din zona de navigare şi apăsaţi **Adăugare intrare**. Sau faceţi clic pe **Gestionare intrări** şi selectaţi locaţia (cn=ibmPolicies sau cn=localhost), apoi apăsaţi **Adăugare**.
2. Selectaţi clasele obiect **groupof Names** din meniul **Clasă de obiecte structurale**.
3. Apăsaţi **Următorul**.
4. Selectaţi o clasă obiect auxiliară **ibm-proxyGroup** din meniul**Disponibilă** şi apăsaţi **Adăugare**. Repetaţi acest proces pentru fiecare clasă obiect auxiliară suplimentară pe care doriţi să o adăugaţi.
5. Apăsaţi **Următorul**.
6. În câmpul **DN corespunzător**, tastaţi cn=proxyGroup.
7. În câmpul **DN părinte**, introduceţi numele distinctiv al intrării din arbore pe care o selectaţi, de exemplu, cn=localhost. Puteţi de asemenea să faceţi clic pe **Răsfoire** pentru a selecta **DN-ul părinte** din listă. Selectaţi-vă opţiunea şi faceţi clic pe **Selectare** pentru aspecifica părintele DN pe care îl vreţi. Valoarea implicită a DN-ului părinte este intrarea selectată în arbore.

   Notă: Dacă aţi pornit acest task din panoul Gestionare intrări, acest câmp este deja completat pentru dumneavoastră. Aţi selectat DN-ul părinte înainte de a face clic pe Adăugare pentru a începe procesul de adăugare intrare .
8. În fişa **Atribute necesare**, tastaţi valorile pentru atributele necesare.
   - **cn** este proxyGroup.
   - **Membru** este sub forma unui DN, de exemplu, cn=Bob Garcia,ou=austin,o=ibm,c=us.

     Vedeţi "Modificarea atributelor binare" la pagina 191 pentru informaţii suplimentare despre adăugarea valorilor binare.
9. Dacă vreţi să adăugaţi mai mult de o valoare pentru un anumit atribut, apăsaţi **Valori multiple** şi apoi adăugaţi valorile pe rând.

   Notă: Nu creaţi valori multiple pentru o valoare cn. Grupul de autorizare proxy trebuie să aibă bine-cunoscutul nume proxyGroup.

   Apăsaţi **OK** când aţi terminat de editat valorile multiple. Valorile sunt adăugate într-un meniu expandabil afişat la atribut.
10. Dacă serverul dumneavoastră are tagurile de limbă activate, faceţi clic pe **Valoare tag limbă** pentru a adăuga sau înlătura descriptorii tagului de limbă.
11. Faceţi clic pe **Alte atribute**.
12. În fişa **Alte atribute**, introduceţi valorile corespunzătoare pentru atribute. Vedeţi "Modificarea atributelor binare" la pagina 191 pentru informaţii suplimentare despre adăugarea valorilor binare.

13. Dacă vreţi să adăugaţi mai mult de o valoare pentru un anumit atribut, apăsaţi **Valori multiple** şi apoi adăugaţi valorile pe rând. Apăsaţi **OK** când aţi terminat de editat valorile multiple. Valorile sunt adăugate într-un meniu expandabil afişat la atribut.
14. Dacă serverul dumneavoastră are tagurile de limbă activate, faceţi clic pe **Valoare tag limbă** pentru a adăuga sau înlătura descriptorii tagului de limbă.
15. Faceţi clic pe **Sfârşit** pentru a crea intrarea.

Modificarea unui grup de autentificare proxy

Folosiţi aceste informaţii pentru a modifica un grup de autentificare proxy.

Puteţi modifica grupul cu autorizare proxy, cum ar fi adăugarea sau ştergerea membrilor grupului, folosind unealta de administrare Web.

1. Dacă nu aţi făcut asta deja, expandaţi categoria **Gestionare director** din zona de navigare, apoi apăsaţi pe **Gestionare intrări**. Puteţi expanda diverşi subarbori şi selecta intrarea cu care vreţi să lucraţi. Apăsaţi **Editare atribute** din bara de unelte din partea dreaptă.
2. În fişa **Atribute obligatorii** introduceţi valorile pentru atributele obligatorii. Vedeţi “Modificarea atributelor binare” la pagina 191 pentru informaţii despre adăugarea valorilor binare. Dacă vreţi să adăugaţi mai mult de o valoare pentru un anumit atribut, apăsaţi **Valori multiple** şi apoi adăugaţi valorile pe rând.
3. Apăsaţi **Atribute opţionale**.
4. În fişa **Atribute opţionale** introduceţi valorile corespunzătoare pentru atributele opţionale. Dacă vreţi să adăugaţi mai mult de o valoare pentru un anumit atribut, apăsaţi **Valori multiple** şi apoi adăugaţi valorile pe rând.
5. Faceţi clic pe **Apartenenţă**.
6. Dacă aţi creat vreun grup, la fişa **Apartenenţă**:
   - Selectaţi un grup din **Grupuri disponibile** şi apăsaţi **Adăugare** pentru a face intrarea membru al **Apartenenţei la grupul static** selectate.
   - Selectaţi un grup din **Apartenenţe grup spatic** şi faceţi clic pe **Înlăturare** pentru a înlătura intrarea din grupul selectat.
7. Dacă intrarea este o intrare grup, o fişă **Membri** este disponibilă. Fişa **Membri** afişează membrii grupului selectat. Puteţi adăuga şi înlătura membrii din grup.
   - Pentru a adăuga un membru la grup:
     a. Fie faceţi clic pe **Valori multiple** din fişa **Membri** sau la fişa **Membri**, faceţi clic pe **Membri**.
     b. În câmpul Membru, introduceţi DN-ul intrării pe care doriţi să o adăugaţi.
     c. Selectaţi **Adăugare**.
     d. Apăsaţi **OK**.
   - Pentru a înlătura un membru din grup:
     a. Fie faceţi clic pe **Valori multiple** din fişa **Membri** sau la fişa **Membri**, faceţi clic pe **Membri**.
     b. Selectaţi intrarea pe care doriţi să o înlăturaţi:
     c. Faceţi clic pe **Înlăturare**.
     d. Apăsaţi **OK**.
   - Pentru a reîmprospăta lista de membri, faceţi clic pe **Actualizare**.
8. Faceţi clic pe **OK** pentru a modifica intrarea.

Copierea unui grup de autorizare proxy

Folosiţi aceste informaţii pentru a copia un grup de autorizare proxy.

Este folositor să copiaţi un grup cu autorizare proxy dacă doriţi ca acelaşi grup de autorizare proxy să se găsească atât sub localhost, cât şi sub IBMpolicies.

1. Dacă nu aţi făcut asta deja, expandaţi categoria **Gestionare director** din zona de navigare, apoi apăsaţi pe **Gestionare intrări**. Puteţi expanda diverşi subarbori şi selecta intrarea, precum John Doe, cu care vreţi să lucraţi. Apăsaţi **Copiere** din bara de unelte din partea dreaptă.

2. Modificaţi intrarea RDN din câmpul DN. De exemplu modificaţi cn=John Doe cu cn=Jim Smith.
3. În fişa de atribute necesară, modificaţi intrarea cn la noua RDN. În acest exemplu Jim Smith.
4. Modificaţi corespunzător celelalte atribute necesare. În acest exemplu modificaţi atributul sn de la Doe la Smith.
5. Când aţi terminat de modificat faceţi clic pe **OK** pentru a crea noua intrare. Noua intrare Jim Smith este adăugată în josul listei de intrare.

Înlăturarea unui grup de autorizare proxy

Folosiţi aceste informaţii pentru a înlătura un grup de autorizare proxy.

1. Dacă nu aţi făcut asta deja, expandaţi categoria **Gestionare director** din zona de navigare, apoi apăsaţi pe **Gestionare intrări**. Puteţi expanda diverşi subarbori şi selecta subarborele, sufixul sau intrarea cu care vreţi să lucraţi. Apăsaţi **Şterge** din bara de unelte din partea dreaptă.
2. Vi se va cere să confirmaţi ştergerea. Apăsaţi **OK**. Intrarea este ştearsă din director şi reveniţi la lista de intrări.

Taskuri cu atribut unic

Folosiţi aceste informaţii pentru a gestiona atributele unice.

Gestionarea atributelor unice este realizată prin categoria **Administrare server** din unealta de administrare Web.

Notă: Pe o bază pe atribut, tagurile de limbă sunt mutual exclusive, cu atribute unice. Dacă desemnaţi un anumit atribut ca fiind atribut unic, nu poate avea taguri de limbă asociate cu el.

Notă: Pentru a modifica setările configuraţiei serverului utilizând taskurile din categoria Administrare server a Uneltei de administrare web , trebuie să vă autentificaţi pe server ca un profil utilzator i5/OS care are a utorizările speciale *ALLOBJ şi IOSYSCFG. Aceasta se poate realiza prin autentificarea ca utilizator proiectat cu parola pentru acel profil. Pentru a vă lega ca utilizator proiectat din unealta de administrare Web, introduceţi un numeutilizator de forma os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, unde şirurile MYUSERNAME şi MYSYSTEM.COM sunt înlocuite cu numele profilului dumneavoastră de utilizator, respectiv cu sufixul de proiectare al sistemului configurat.

Concepte înrudite

“Atributele unice” la pagina 89
Funcţia de atribute unice asigură faptul că atributele specificate au întotdeauna valori unice într-un director.

Operaţii înrudite

“Crearea unei liste de atribute unice” la pagina 136
Folosiţi aceste informaţii pentru a crea o listă unică de atribute.

“Înlăturarea unei intrări din lista de atribute unice” la pagina 136
Folosiţi aceste informaţii pentru a înlătura o intrare din lista de atribute unice.

Determinarea posibilităţii de a specifica un atribut ca unic

Folosiţi aceste informaţii pentru a determina dacă un atribut poate fi specificat ca unic.

Nu toate atributele pot fi specificate ca fiind unice. Vedeţi următoarele pentru o listă de condiţii când un atribut nu poate fi desemnat ca unic:

- Atributele binare, atributele operaţionale, atributele de configurare şi atributul objectclass nu pot fi proiectate ca fiind unice.
- Atributele cu valori conflictuale existente nu pot fi făcute unice.
- Pe o bază pe atribut, tagurile de limbă sunt mutual exclusive, cu atribute unice. Dacă desemnaţi un atribut particular ca find un atribut unic,nu poate avea taguri de limbă asociate.

Taskul Unealta de administrare web gestionează atribute unice vă arată numai atributelecare satisfac prima condiţie. Puteţi lua aceeaşi listă de atribute executând comanda ldapexop după ce vă legaţi ca administrator. Pentru a obţine o listă de atribute care pot fi unice, specificaţi următoarele:

```
ldapexop -op getattributes -attrType unique -matches true
```

Pentru a obţine o listă de atribute care nu pot fi unice, specificaţi următoarele:

```
ldapexop -op getattributes -attrType unique -matches false
```

Unele din atributele menţionate ca permise pentru atribute unice pot avea valori conflictuale şi acestea nu pot fi făcute unice. Pentru a determina dacă un atribut poate fi specificat ca unic, utilizaţi comanda ldapexop. De exemplu, comanda:

```
ldapexop -op uniqueattr -a uid
```

indică dacă atributul uid poate fi făcut unic. De asemenea afişează valori conflictuale, dacă există, pentru atribut.

Dacă comanda ldapexop indică valori conflictuale, comanda ldapsearch poate fi folosită să găsească intrări care au acea valoare. De exemplu, următoarea comandă listează toate intrările având uid=jsmith:

```
ldapsearch -b "" -s sub "(uid=jsmith)"
```

Crearea unei liste de atribute unice

Folosiţi aceste informaţii pentru a crea o listă unică de atribute.

1. Expandaţi categoria **Administrare server** din zona de navigare. Faceţi clic pe **Gestionare atribute unice**.
2. Selectaţi atributul pe care doriţi să îl adăugaţi ca atribut unic din meniul **Atribute disponibile**. Atributele disponibile afişate sunt cele care pot fi desemnate ca fiind unice; de exemplu, sn.
3. Faceţi clic fie pe **Adăugare în cn=localhost**, fie pe **Adăugare în cn=IBMpolicies**. Diferenţa dintre aceşti doi containeri este că intrările cn=IBMpolicies sunt replicate, iar intrările cn=localhost nu sunt replicate. Atributul este afişat în caseta listă corespunzătoare. Puteţi afişa acelaşi atribut în ambii containeri.

   Notă: Dacă o intrare este creată atât sub cn=localhost, cât şi sub cn=IBMpolicies, reuniunea rezultantă a acestor două intrări este lista atributelor unice. De exemplu, dacă atributele cn şi employeeNumber sunt desemnate ca unice în cn=localhost şi atributele cn şi telephoneNumber sunt desemnate ca unice în cn=IBMploicies, serverul tratează atributele cn, employeeNumber şi telephoneNumber ca atribute unice.
4. Repetaţi acest proces pentru fiecare atribut pe care doriţi să-l adăugaţi ca atribut unic.
5. Apăsaţi **OK** pentru a salva modificările.

La adăugarea sau modificarea unei intrări de atribut unic, dacă stabilirea unei constrângeri de unicitate pentru oricare din tipurile de atribute unice afişate duce la erori, intrarea nu este adăugată sau creată în director. Problema trebuie rezolvată şi comanda de adăugare sau modificare trebuie relansată înainte ca intrarea să poată fi creată sau modificată. De exemplu, în timpul adăugării unei intrări de atribut unic în director, dacă stabilirea unei constrângeri de unicitate pe o tabelă pentru unul din tipurile de atribute unice afişate a eşuat (adică, datorită unor valori duplicate în baza de date), intrarea de atribut unic nu este adăugată în director. Este emisă o eroare.

Când o aplicaţie încercă să adauge o intrare în director cu o valoare atribut care este duplicata unei intrări existente din director, se emite o eroare cu codul rezultat 20 (LDAP: cod eroare 20 - Atributul sau valoarea există) de la serverul LDAP.

Când serverul porneşte, acesta verifică lista de atribute unice şi determină dacă restricţiile DB2 există pentru fiecare din ele. Dacă nu există restricţia pentru un atribut deoarece a fost înlăturată de utilitarul bulkload sau deoarece a fost înlăturată manual de către utilizator, acesta este înlăturat din lista de atribute unice şi un mesaj de eroare este înregistrat în istoricul de erori ibmslapd.log. De exemplu, dacă atributul cn este desemnat ca unic încn=uniqueattributes,cn=localhost şi nu există o restricţie DB2 pentru el, se înregistrează următorul mesaj:

```
Valorile pentru atributul CN nu sunt unice.
Atributul CN a fost înlăturat din intrarea atribute unice
: CN=UNIQUEATTRIBUTES,CN=LOCALHOST
```

Concepte înrudite

“Taskuri cu atribut unic” la pagina 135
Folosiţi aceste informaţii pentru a gestiona atributele unice.

Înlăturarea unei intrări din lista de atribute unice

Folosiţi aceste informaţii pentru a înlătura o intrare din lista de atribute unice.

Dacă un atribut unic există atât în cn=uniqueattribute,cn=localhost, cât şi în cn=uniqueattribute,cn=IBMpolicies şi este înlăturat dintr-o singură intrare, serverul continuă să trateze acel atribut ca atribut unic. Atributul nu mai este unic atunci când a fost înlăturat din ambele intrări.

1. Expandaţi categoria **Administrare server** din zona de navigare şi apăsaţi **Gestionare atribute unice**.
2. Selectaţi atributul pe care doriţi să îl înlăturaţi din lista de atribute unice, făcând clic pe atributul din caseta listei corespunzătoare.
3. Faceţi clic pe **Înlăturare**.
4. Repetaţi acest proces pentru fiecare atribut pe care doriţi să-l înlăturaţi din listă.
5. Apăsaţi **OK** pentru a salva modificările.

Notă: Dacă înlăturaţi ultimul atribut unic din casetele listă cn=localhost sau cn=IBMpolicies, intrarea container pentru acea casetă listă, cn=uniqueattribute, cn=localhost sau cn=uniqueattribute, cn=IBMpolicies, este ştearsă automat.

Concepte înrudite

"Taskuri cu atribut unic" la pagina 135
Folosiţi aceste informaţii pentru a gestiona atributele unice.

Taskuri de performanţă

Folosiţi aceste informaţii pentru a ajuta setările performanţei.

Puteţi ajusta setările de performanţă ale serverului dumneavoastră de director prin modificarea uneia din următoarele:

- Dimensiunea cache-ului ACL, dimensiunea cache-ului de intrări, numărul maxim de căutări de stocat în cache-ul de filtru şi cea mai mare căutare de memorat în cache-ul de filtru.
- Numărul de conexiuni la baza de date şi fire de execuţie server
- Setările cache-ului de atribut
- Setările tranzacţiei serverului

Concepte înrudite

"Cache-urile de server" la pagina 90
Cache-urile LDAP sunt buffer-e cu spaţiu de stocare rapid în memorie, utilizate pentru a memora informaţii LDAP ca de exemplu interogări, răspunsuri şi autentificarea utilizatorului pentru o viitoare folosire. Ajustarea cache-urilor LDAP este crucială pentru îmbunătăţirea performanţei.

Setarea conexiunilor bazei de date şi setările de cache

Folosiţi aceste informaţii pentru a seta conexiunile bază de date şi cache-ul.

Pentru a configura conexiunile la baza de date şi setările cache, faceţi următoarele:

1. Expandaţi categoria **Gestionare proprietăţi server** din zona de navigare a Uneltei de administrare Web, apoi apăsaţi fişa **Performanţă** a panoului din dreapta.
2. Specificaţi **Numărul de conexiuni la baza de date**. Aceasta setează numărul de conexiuni la DB2 folosite de server. Numărul minim pe care trebuie să-l specificaţi este 4. Setarea implicită este 15. Dacă serverul dumneavoastră LDAP primeşte un volum mare de cereri client sau clienţii primesc erorile ″conexiune refuzată″, aţi putea obţine rezultate mai bune prin creşterea setării numărului de conexiuni ale serverului la DB2. Numărul maxim de conexiuni este determinat de setarea din baza dumneavoastră de date DB2. În perioada în care nu există limitări ale serverului până la numărul de conexiuni pe care îl specificaţi, fiecare conexiune consumă resurse.
3. Specificaţi **Numărul de conexiuni la baza de date pentru replicare**. Aceasta setează numărul de conexiuni la DB2 folosite de server la replicare. Numărul minim pe care trebuie să-l specificaţi este 1. Setarea implicită este 4.

   Notă: Numărul total de conexiuni specificate pentru conexiunile la baza de date, incluzând conexiunile la baza de date pentru replicare, nu poate depăşi numărul de conexiuni setate în baza dumneavoastră de date DB2.
4. Selectaţi **Informaţii cache ACL** pentru a folosi următoarele setări ale cache-ului ACL.
5. Specificaţi **Numărul maxim de elemente în cache-ul ACL**. Implicit este 25 000.

6. Specificaţi **Numărul maxim de elemente în cache-ul intrare**. Implicit este 25 000.
7. Specificaţi **Numărul maxim de elemente în cache-ul filtru de căutare**. Implicit este 25 000.Cache-ul filtrului de căutare conţine interogări reale despre filtrele atribut cerute şi identificatorii intrare rezultaţi care s-au potrivit. Într-o operaţie de actualizare, toate intrările de cache filtru sunt nevalide.
8. Specificaţi **Numărul maxim de elemente dintr-o singură căutare adăugate la cache-ul filtru de căutare.** . Dacă selectaţi **Elemente**, trebuie să introduceţi un număr. Valoarea implicită este 100. Altfel, selectaţi **Nelimitat**. Intrările din căutare care se potrivesc cu mai multe intrări decât numărul specificat aici nu sunt adăugate în cache-ul filtru de căutare.
9. Când terminaţi, apăsaţi **OK**.
10. Dacă setaţi numărul de conexiuni la baza de date, reporniţi serverul pentru ca modificările să aibă efect. Dacă aţi modificat doar setările cache, serverul nu necesită să fie repornit.

Configurarea cache-ului de atribute

Folosiţi aceste informaţii pentru setările cache-ului de atribute.

Setările pentru cache-ul de atribute sunt configurate atât în unealta de administrare Web, cât şi în Navigator System i.

Pentru a ajusta manual stările cache-ului de atribute din unealta de administrare Web, urmaţi aceşti paşi:

1. Expandaţi categoria **Administrare server** din zona de navigare a Uneltei de administrare Web, apoi selectaţi fişa **Cache de atribut** a panoului din dreapta.

   Notă: Pentru a modifica setările de configuraţiei ale serverului utilizând taskurile din categoria Administrare de server a uneltei de administrare web, trebuie să vă autentificaţi la server ca un profil de utilizator i5/OS ce are autorităţile speciale *ALLOBJ şi IOSYSCFG. Aceasta se poate realiza prin autentificarea ca utilizator proiectat cu parola pentru acel profil. Pentru a vă lega ca utilizator proiectat din unealta de administrare Web, introduceţi un numeutilizator de forma os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, unde şirurile MYUSERNAME şi MYSYSTEM.COM sunt înlocuite cu numele profilului dumneavoastră de utilizator, respectiv cu sufixul de proiectare al sistemului configurat.
2. Modificaţi cantitatea de memorie în kiloocteţi disponibilă în cache-ul directorului. Valoarea implicită este 16 384 kiloocteţi (16 MB).
3. Modificaţi cantitatea de memorie în kiloocteţi disponibilă în cache-ul istoric modificări. Valoarea implicită este 16 384 kiloocteţi (16 MB).

   Notă: Această selecţie este dezactivată dacă istoricul de modificări nu a fost configurat. Punerea în cache a atributului pentru istoricul de modificări ar trebui setată la 0 şi nici un atribut nu ar trebui să fie configurat decât dacă efectuaţi căutări frecvente în istoricul de modificări şi performanţa acestor căutări este critică.
4. Selectaţi atributul pe care doriţi să îl puneţi în cache din meniul **Atribute disponibile**. În acest meniu sunt afişate numai acele atribute care pot fi puse în cache; de exemplu, sn.

   Notă: Un atribut rămâne în lista de atribute disponibile până când a fost pus în ambii containeri cn=directory şi cn=changelog.
5. Faceţi clic pe **Adăugare în cn=directory** sau **Adăugare în cn=changelog**. Atributul este afişat în caseta listă corespunzătoare. Puteţi afişa acelaşi atribut în ambii containeri.

   Notă: **Adăugare în cn=changelog** este dezactivat dacă istoricul de modificări nu a fost configurat. Punerea în cache a atributului pentru istoricul de modificări ar trebui setată la 0 şi nici un atribut nu ar trebui să fie configurat decât dacă efectuaţi căutări frecvente în istoricul de modificări şi performanţa acestor căutări este critică.
6. Repetaţi acest proces pentru fiecare atribut pe care doriţi să-l adăugaţi în cache-ul de atribut.
7. Când terminaţi, apăsaţi **OK**.

Pentru a activa punerea în cache automată a atributelor în Navigator System i, parcurgeţi aceşti paşi:

1. În Navigator System i, expandaţi **Reţea**.

2. Expandaţi **Servere**.
3. Faceţi clic pe **TCP/IP**.
4. Faceţi clic dreapta pe **IBM Directory Server** şi selectaţi**Proprietăţi**.
5. Faceţi clic pe **Performanţă**.
6. Selectaţi **Activare punere automată în cache a atributelor** pentru una dintre **Baza de date** şi **Modificare istoric** sau ambele. Punerea în cache automată a atributului pentru istoricul de modificări nu ar trebui să fie activată decât dacă efectuaţi căutări frecvente în istoricul de modificări şi performanţa acestor căutări este critică.
7. Specificaţi **Ora de pornire** (în funcţie de ora locală a serverului) şi **Intervalul** pentru fiecare tip de punere în cache pe care alegeţi să o activaţi. De exemplu, dacă activaţi punerea în cache a bazei de date şi setaţi ora de pornire la 6.00 a.m. şi intervalul să fie de şase ore, cache-ul va fi ajustat automat la 6 a.m., la prânz, la 6 p.m. şi la miezul nopţii, indiferent când a fost pornit serverul sau când a fost configurată ajustarea automată.

Notă: Punerea în cache automată a atributelor va pune în cache atribute până când se atinge cantitatea maximă de memorie pentru punere în cache specificată în unealta de administrare Web, după cum a fost descris mai sus.

Tabela 4. Interacţiunea setărilor cache de atribut

Activitate	Ce apare
Pornire server	Dacă punerea în cache automată a atributelor este în prezent activă şi punerea în cache automată a fost activată la ultima oprire a serverului, aceleaşi atribute care au fost puse în cache când serverul a fost oprit vor fi create la repornirea serverului. Dacă mai este disponibilă memorie suplimentară pentru punerea în cache a atributelor, atributele care au fost configurate manual vor şi ele puse în cache. Dacă punerea în cache automată a atributelor este în prezent activă şi nu a fost activată la ultima oprire a serverului, atributele care sunt configurate manual pentru punerea în cache vor fi reţinute în cache. În oricare din cazuri, serverul va ajusta apoi automat cache-urile de atribute, bazându-se pe ora de pornire şi intervalul de timp specificate. Dacă punerea în cache automată nu este activată, setările de cache ajustate manual vor avea efect.
Activare punere automată în cache după pornirea serverului	Punerea automată în cache a atributelor va avea loc după cum a fost descrisă la pornirea serverului. Orice cache-uri de atribut configurate manual care nu se încadrează în cantitatea de memorie configurată pentru punerea în cache a atributelor vor fi şterse.
Dezactivare punere în cache automată a atributelor după pornirea serverului	Doar atributele care au fost configurate manual vor fi puse în cache.
Modificare atribute puse în cache manual în timp ce punerea în cache automată este activată după pornirea serverului	Nu se va întâmpla nimic. Configuraţia manuală va avea efect când punerea în cache automată este dezactivată.
Modificare cantitate de memorie disponibilă pentru punerea în cache după pornirea serverului	Dacă modificarea automată este activată, serverul va începe imediat să pună din nou în cache, bazându-se pe noua dimensiune. Dacă modificarea automată este dezactivată, serverul va pune în cache atributele configurate manual până ajunge la noua dimensiune.
Modificare oră de pornire şi interval după pornirea serverului	Dacă punerea în cache automată este activată, noile setări vor avea efect la ora de pornire şi intervalul specificate. Dacă punerea în cache automată este dezactivată, setările sunt memorate şi au efect când punerea în cache automată este activată.

Configurarea setărilor de tranzacţie

Folosiţi aceste informaţii pentru a specifica setările tranzacţiei.

Pentru a configura setările tranzacţiei, faceţi următoarele:

1. Expandaţi categoria **Gestionare proprietăţi server** din zona de navigare a Uneltei de administrare Web şi apoi selectaţi fişa **Tranzacţii** a panoului din dreapta.

2. Selectaţi caseta de bifare **Activare procesare tranzacţie** pentru a activa procesarea tranzacţiei. Dacă **Activare procesare tranzacţie** este dezactivată, toate celelalte opţiuni din acest panou sunt ignorate de către server.
3. Setaţi **Numărul maxim de tranzacţii**. Faceţi clic pe butonul radio **Tranzacţii** sau **Nelimitat**. Dacă selectaţi **Tranzacţii**, specificaţi numărul maxim de tranzacţii. Numărul maxim de tranzacţii este 2 147 483 647. Setarea implicită este 20 de tranzacţii.
4. Setaţi **Numărul maxim de operaţii pe tranzacţie**. Faceţi clic pe butonul radio **Operaţii** sau **Nelimitat**. Dacă selectaţi **Operaţii**, specificaţi numărul maxim de operaţii permise pentru fiecare tranzacţie. Numărul maxim de operaţii este 2 147 483 647. Cu cât numărul este mai mic, cu atât creşte performanţa. Valoarea implicită este de 5 operaţii.
5. Setaţi **Limita timpului de aşteptare**. Această selecţie stabileşte valoarea maximă a timeout-ului unei tranzacţii în curs, în secunde. Faceţi clic pe butonul radio **Secunde** sau **Nelimitat**. Dacă selectaţi **Secunde**, specificaţi numărul maxim de secunde permise pentru fiecare tranzacţie. Numărul maxim de secunde este 2 147 483 647. Tranzacţiile lăsate neterminate pentru un timp mai mare decât acesta sunt anulate (date înapoi). Valoarea implicită este 300 de secunde.
6. Când terminaţi, apăsaţi **OK**.
7. Dacă aţi activat suportul pentru tranzacţii, trebuie să reporniţi serverul pentru ca modificările să aibă efect. Dacă aţi modificat doar setările, serverul nu trebuie repornit.

Taskuri de replicare

Folosiţi aceste informaţii pentru a gestiona replicarea.

Pentru a gestiona replicarea, expandaţi categoria **Gestionare replicare** din unealta de administrare web.

Concepte înrudite

"Replicarea" la pagina 37
Replicarea este o tehnică folosită de serverele de director pentru a îmbunătăţi performanţa şi încrederea. Procesul de replicare ţine datele în directoare multiple sincronizate.

Crearea unei topologii master-replica

Folosiţi aceste informaţii pentru a crea o topologie master-replica.

Pentru a defini o topologie de bază master-replică trebuie să:

1. Creaţi un server master şi să definiţi ce conţine el. Selectaţi subarborele care vreţi să fie replicat şi să specificaţi serverul ca master. Vedeţi"Crearea unui server master (subarbore replicat)" la pagina 141.
2. Creaţi acreditări de folosit de către furnizor. Vedeţi"Crearea acreditărilor de replicare" la pagina 143.
3. Creaţi un server replică. Vedeţi"Crearea unui server replică" la pagina 144.
4. Exportaţi topologia de la master către replică. Vedeţi"Copierea datelor la replică" la pagina 145.
5. Modificaţi configuraţia replicii pentru a identifica cine este autorizat să replice modificările făcute asupra ei şi adăugaţi un referral la un master. Vedeţi"Adăugarea informaţiilor furnizorului la replica nouă" la pagina 146.

Notă:

Dacă intrarea de la rădăcina subarborelui care vreţi să fie replicat nu este un sufix în server, înainte de a putea folosi funcţia **Adăugare subarbore**, trebuie să vă asiguraţi că ACL-urile lui sunt definite după cum urmează:

Pentru ACL-uri nefiltrate:

```
ownersource: <la fel ca intrarea DN>
ownerpropagate: TRUE

aclsource: <la fel ca intrarea DN>
aclpropagate: TRUE
```

Pentru ACL-uri filtrate:

```
ibm-filteraclinherit: FALSE
```

Pentru a satisface cerinţele de ACL, dacă intrarea nu este un sufix în server, editaţi ACL-ul pentru acea intrare în panoul **Gestionare intrări**. Selectaţi intrarea şi apăsaţi **Editare ACL**. Dacă vreţi să adăugaţi ACL-uri nefiltrate selectaţi acea fişă şi selectaţi căsuţa de bifare pentru a specifica dacă ACL-urile sunt explicite sau nu, atât pentru ACL-uri, cât şi pentru proprietari. Asiguraţi-vă că **Propagare ACL-uri** şi **Propagare proprietar** sunt bifate. Dacă vreţi să adăugaţi ACL-uri filtrate, selectaţi acea fişa şi adăugaţi o intrare **cn=this** cu rolul **access-id** pentru ACL-uri şi proprietari. Asiguraţi-vă că **Acumulare ACL-uri filtrate** este nebifat şi că **Propagare proprietar** este bifat. Vedeţi “Listă control acces taskuri (ACL)” la pagina 203 pentru mai multe informaţii detaliate.

Iniţial, obiectul **ibm-replicagroup** creat de acest proces moşteneşte ACL-ul intrării rădăcină pentru subarborele replicat. Aceste ACL-uri ar putea să nu fie potrivite pentru controlul accesului la informaţiile de replicare din director.

Crearea unei topologii master-forwarder-replica

Folosiţi aceste informaţii pentru a crea o topologie master-forwarder-replica.

Pentru a defini o topologie master-forwarder-replica, trebuie să:

1. Creaţi un server master şi un server replică. Vedeţi“Crearea unei topologii master-replica” la pagina 140.
2. Creaţi un nou server replică pentru replica originală. Vedeţi“Crearea unui nou server replică”.
3. Copiaţi datele la replici. Vedeţi“Copierea datelor la replică” la pagina 145.

Crearea unui server master (subarbore replicat)

Folosiţi aceste informaţii pentru a crea un server master subarbore replicat.

Notă: Serverul trebuie să ruleze pentru a efectua această operaţie.

Această operaţie desemnează o intrare ca rădăcină a unui subarbore replicat în mod independent şi creează un **ibm-replicasubentry** care reprezintă acest server drept singurul master pentru subarbore. Pentru a crea un subarbore replicat, trebuie să desemnaţi subarborele pe care vreţi să îl replice serverul.

Expandaţi categoria Gestionare replicare din zona de navigare şi apăsaţi **Gestionare topologie**.

1. Faceţi clic pe **Adăugare subarbore**.
2. Introduceţi DN-ul intrării rădăcină a subarborelui pe care vreţi să îl replicaţi sau apăsaţi **Răsfoire** pentru a expanda intrările pentru a selecta intrarea care va fi rădăcina subarborelui.
3. URL-ul referral al serverului master este afişat în forma unui URL LDAP, de exemplu:

   ```
   ldap://<myservername>.<mylocation>.<mycompany>.com
   ```

   Notă: URl-ul referral al serverului master este opţional. Este folosit doar:
   - Dacă serverul conţine (sau va conţine) orice subarbore numai citire.
   - Pentru a defini un URL referral care este returnat pentru actualizări la orice subarbore numai citire de pe server.
4. Apăsaţi **OK**.
5. Noul server este afişat în panoul Gestionare topologie sub antetul **Subarbori replicaţi**.

Crearea unui nou server replică

Folosiţi aceste informaţii pentru a crea un nou server replică.

Dacă aţi setat o topologie de replicre (vedeţi Crearea unui server master (subarbore copiat)) cu un master (server1) şi o replică (server2), puteţi modifica rolul lui server2 cu cel al unui server dinainte. Pentru a face aceasta trebuie să creaţi o nouă replică (server3) sub server2.

1. Conectaţi Administrarea Web la master (server1)
2. Expandaţi categoria Gestionare replicare din zona de navigare şi apăsaţi **Gestionare topologie**.
3. Selectaţi subarborele pe care vreţi să îl replicaţi şi apăsaţi **Arată topologie**.
4. Apăsaţi săgeata de lângă selecţia **Topologie de replicare** pentru a expanda lista de servere furnizor.

5. Apăsaţi săgeata de lângă selecţia **server1** pentru a expanda lista de servere.
6. Selectaţi server2 şi apăsaţi **Adăugare replică**.
7. În fişa **Server** din fereastra **Adăugare replică**:
   - Introduceţi numele gazdă şi numărul de port pentru replica (server3) pe care o creaţi. Portul implicit este 389 pentru non-SSL şi 636 pentru SSL. Acestea sunt câmpuri necesare.
   - Selectaţi dacă să activaţi comunicaţiile SSL.
   - Introduceţi numele replicii sau lăsaţi acest câmp gol pentru a folosi numele gazdă.
   - Introduceţi ID replică. Dacă serverul pe care creaţi replica rulează, apăsaţi **Obţinere ID replică** pentru a completa automat acest câmp. Acesta este un câmp obligatoriu, dacă serverul pe care îl adăugaţi va fi server peer sau de înaintare (forwarding). Este recomandat ca toate serverele să aibă aceeaşi ediţie.
   - Introduceţi o descriere a serverului replică.

   În fişa **Adiţional**:
   - Specificaţi acreditările pe care le foloseşte replica pentru a comunica cu masterul.

     Notă: Unealta de administrare web vă permite să definiţi acreditări în două locuri:
     - **cn=replication,cn=localhost**, care păstrează acreditările doar pe serverul care le foloseşte.
     - În subarborele replicat, caz în care acreditările sunt replicate cu restul subarborelui.

     Plasarea acreditărilor în cn=replication,cn=localhost este considerată mai sigură. Acreditările plasate în subarborele replicat sunt create sub intrarea **ibm-replicagroup=default** pentru acel subarbore.
   - Faceţi clic pe **Selectare**.
     - Selectaţi locaţia pentru acreditările pe care vreţi să le folosiţi. De preferat aceasta este cn=replication,cn=localhost.
     - Apăsaţi **Arată acreditări**.
     - Expandaţi lista de acreditări şi selectaţi-o pe aceea pe care vreţi să o folosiţi.
     - Apăsaţi **OK**.

       Vedeţi Creare acreditări replicare pentru informaţii adiţionale despre acreditările acordului.
   - Specificaţi o planificare de replicare din meniul derulant sau apăsaţi **Adăugare** pentru a crea una. Vedeţi Crearea planificărilor de replicare.
   - Din lista de capabilităţi furnizor puteţi deselecta orice capabilităţi pe care nu vreţi să le replicaţi la consumator.

     Dacă reţeaua dvs. are un amestec de servere la diferite ediţii, sunt disponibile capabilităţi pe ediţii ulterioare care nu sunt disponibile pe ediţii mai vechi. Unele capabilităţi, precum ACL-uri filtrate şi politica de parolă, folosesc atribute operaţionale care sunt replicate cu alte modificări. În majoritatea cazurilor, dacă aceste funcţii sunt folosite, este de dorit ca toate serverele să le suporte. Dacă toate serverele nu suportă capabilitatea, atunci nu vreţi să o folosiţi. De exemplu, nu aţi dori ACL-uri diferite care să fie active pe fiecare server. Oricum, ar putea fi cazuri în care aţi dori să folosiţi o capabilitate de pe serverele care o suportă şi modificările legate de această capabilitate să nu fie replicate la serverele care nu suportă capabilitatea. În astfel de cazuri, puteţi folosi lista de capabilităţi pentru a marca anumite capabilităţi care să nu fie replicate.
   - Selectaţi fie firul singur de execuţie sau firul de execuţie multiplu pentru metoda replicaţiei. Dacă specificaţi fir de execuţie multiplu, trebuie de asemenea, să specificaţi numărul (între 2 şi 32) de conexiuni de utilizat pentru replicare. Numărul implicit de conexiuni este 2.
   - Apăsaţi **OK** pentru a crea replica.
8. Copie date de la server2 la noua replică server3. Vedeţi Copiere date la replică pentru informaţii despre cum să faceţi aceasta.
9. Adăugaţi acordul furnizorului la server3 care face server2 ca furnizor pentru server 3 şi server 3 drept consumator pentru server2. Vedeţi Adăugare informaţii furnizor la noua replică pentru informaţii despre cum se face aceasta.

Rolurile serverelor sunt reprezentate de iconuri în unealta de administrare Web. Topologia dvs. este acum:

- server1 (master)

– server2 (forwarder)
  - server3 (replica)

Crearea acreditărilor de replicare

Folosiţi aceste informaţii pentru a crea acreditări de replicare.

Expandaţi categoria de Gestionare replicare în zona de navigare a uneltei de administrare web şi faceţi clic pe **Gestionare acreditări**.

1. Selectaţi locaţia pe care vreţi să o folosiţi pentru a stoca acreditările din lista de subarbori. Unealta de administrare web vă permite să definiţi acreditări în aceste locaţii:
   - **cn=replication,cn=localhost**, care păstrează acreditările doar pe serverul curent.

     Notă: În majoritatea cazurilor de replicare, este preferată localizarea acreditărilor în cn=replication,cn=localhost deoarece oferă o securitate mai mare decât acreditările localizate în subarbore. Oricum, există anumite situaţii în care acreditările localizate în cn=replication,cn=localhost nu sunt disponibile.

     Dacă încercaţi să adăugaţi o replică sub un server, de exemplu, serverA şi sunteţi conectat la un alt server cu unealta de administrare web, serverB, câmpul **Selectare acreditări** nu afişează opţiunea **cn=replication,cn=localhost**. Aceasta deoarece nu poate citi informaţiile sau actualiza vreo informaţie de sub **cn=localhost** de pe serverA când sunteţi conectat la serverB.

     Opţiunea cn=replication,cn=localhost este disponibilă doar când serverul sub care încercaţi să adăugaţi o replică este acelaşi server la care sunteţi conectat cu unealta de administrare web.
   - În subarborele replicat, caz în care acreditările sunt replicate cu restul subarborelui. Acreditările plasate în subarborele replicat sunt create sub intrarea **ibm-replicagroup=default** pentru acel subarbore.

     Notă: Dacă nu este afişat nici un subarbore mergeţi la “Crearea unui server master (subarbore replicat)” la pagina 141 pentru instrucţiuni despre crearea subarborelui pe care vreţi să îl replicaţi.
2. Selectaţi **Adăugare**.
3. Introduceţi numele pentru acreditările pe care le creaţi, de exemplu **mycreds**, cn= este completat dinainte pentru dvs.
4. Selectaţi tipul de metodă de autentificare pe care vreţi să o folosiţi şi apăsaţi **Următor**.
   - Dacă aţi selectat autentificarea cu legare simplă:
     a. Introduceţi DN-ul pe care îl foloseşte serverul pentru a se lega la replică, de exemplu cn=any
     b. Introduceţi parola pe care serverul o foloseşte când se leagă la replică, de exemplu secret.
     c. Introduceţi parola din nou pentru a confirma că nu există erori tipografice.
     d. Dacă vreţi, introduceţi o descriere scurtă a acreditărilor.
     e. Faceţi clic pe **Sfârşit**.

     Notă: Aţi putea dori să înregistraţi DN-ul de legare a acreditării şi parola pentru referiri ulterioare. Vă va trebui această parolă când creaţi acordul de replică.
   - Dacă aţi selectat autentificarea Kerberos:
     a. Introduceţi DN-ul de legare Kerberos.
     b. Introduceţi numele fişierului keytab.
     c. Dacă vreţi, introduceţi o descriere scurtă a acreditărilor. Nu sunt necesare alte informaţii. Vedeţi “Activarea autentificării Kerberos pentru Directory Server” la pagina 175 pentru informaţii suplimentare.
     d. Faceţi clic pe **Sfârşit**.

     Panoul **Adăugare acreditări Kerberos** primeşte un DN de legare opţional de forma ibm-kn=user@realm şi un nume fişier keytab opţional (referit ca fişier cheie). Dacă este specificat un DN de legare, serverul foloseşte numele director specificat pentru a se autentifica în serverul consumatorului. Altfel, este folosit numele de serviciu Kerberos al serverului (ldap/host-name@realm). Dacă este fol osit un fişier keytab, serverul îl utilizează

pentru a obţine acreditările pentru numele director specificat. Dacă nu este specificat un fişier keytab, serverul foloseşte fişierul keytab specificat în configuraţia Kerberos a serverului. Dacă există mai mult de un furnizor, trebuie să specificaţi numele director şi fişierul keytab care să fie folosit de toţi furnizorii.

Pe serverul pe care aţi creat acreditările:

a. Expandaţi **Gestionare director** şi apăsaţi **Gestionare intrări**.
b. Selectaţi subarborele unde aţi stocat acreditările, de exemplu **cn=localhost** şi apăsaţi **Expandare**.
c. Selectaţi **cn=replication** şi apăsaţi **Expandare**.
d. Selectaţi acreditările Kerberos (ibm-replicationCredentialsKerberos) şi apăsaţi **Editare atribute**.
e. Faceţi clic pe fişa **Alte atribute**.
f. Introduceţi **replicaBindDN**, de exemplu, **ibm-kn=myprincipal@SOME.REALM**.
g. Introduceţi **replicaCredentials**. Acesta este un nume de fişier keytab folosit pentru **myprincipal**.

Notă: Acest principal şi parolă ar trebui să fie aceleaşi cu cele folosite pentru a rula **kinit** de la linia de comandă.

Pe replică

a. Apăsaţi pe **Gestionare proprietăţi de replicare** în zona de navigare.
b. Selectaţi un furnizor din meniul derulant **Informaţii despre furnizor** sau introduceţi numele subarborelui replicat pentru care vreţi să configuraţi acreditările de furnizor.
c. Faceţi clic pe **Editare**.
d. Introduceţi DN-ul de legare de replicare. În acest exemplu, **ibm-kn=myprincipal@SOME.REALM**.
e. Introduceţi şi confirmaţi **Parola de legare replicare**. Aceasta este parola KDC folosită pentru **myprincipal**.

- Dacă aţi selectat SSL cu autentificare cu certificat nu este nevoie să furnizaţi vreo informaţie suplimentară, dacă folosiţi certificatul serverului. Dacă alegeţi să folosiţi un certificat diferit de cel al serverului:
  a. Introduceţi numele fişierului cheie.
  b. Introduceţi parola fişierului cheie.
  c. Reintroduceţi parola fişierului cheie pentru a o confirma.
  d. Introuceţi eticheta cheii.
  e. Dacă doriţi, introduceţi o scurtă descriere.
  f. Faceţi clic pe **Sfârşit**.

  Vedeţi “Activarea SSL şi Transport Layer Security pe Directory Server” la pagina 173 pentru informaţii suplimentare.

5. Pe serverul unde aţi creat acreditările, setaţi valoarea sistem Permite reţinerea informaţiilor de securitate server (QRETSVRSEC) la 1 (reţinere date). Deoarece acreditările de replicare sunt stocate într-o listă de validare, aceasta permite serverului să extragă acreditările din lista de validare când se conectează la replică.

Crearea unui server replică

Folosiţi aceste informaţii pentru a crea un server replică.

Notă: Serverul trebuie să ruleze pentru a efectua această operaţie.

Expandaţi categoria **Gestionare replicare** din zona de navigare şi apăsaţi **Gestionare topologie**.

1. Selectaţi subarborele pe care vreţi să îl replicaţi şi apăsaţi **Arată topologie**.
2. Apăsaţi săgeata de lângă selecţia **Topologie de replicare** pentru a expanda lista de servere furnizor.
3. Selectaţi serverul furnizor şi apăsaţi **Adăugare replică**.
4. În fişa **Server** din fereastra **Adăugare replică**:
   a. Introduceţi numele gazdă şi numărul de port pentru replica pe care o creaţi. Portul implicit este 389 pentru non-SSL şi 636 pentru SSL. Acestea sunt câmpuri necesare.

b. Selectaţi dacă să activaţi comunicaţiile SSL.
c. Introduceţi numele replicii sau lăsaţi acest câmp gol pentru a folosi numele gazdă.
d. Introduceţi ID replică. Dacă serverul pe care creaţi replica rulează, apăsaţi **Obţinere ID replică** pentru a completa automat acest câmp. Acesta este un câmp obligatoriu, dacă serverul pe care îl adăugaţi va fi server peer sau de înaintare (forwarding). Este recomandat ca toate serverele să aibă aceeaşi ediţie.
e. Introduceţi o descriere a serverului replică.

5. În fişa **Adiţional**,
   - Specificaţi acreditările pe care le foloseşte replica pentru a comunica cu masterul.

     Notă: Unealta de administrare web vă permite să definiţi acreditări în aceste locuri:
     - **cn=replication,cn=localhost**, care păstrează acreditările doar pe serverul care le foloseşte.
     - În subarborele replicat, caz în care acreditările sunt replicate cu restul subarborelui. Acreditările plasate în subarborele replicat sunt create sub intrarea **ibm-replicagroup=default** pentru acel subarbore.

     Plasarea acreditărilor în cn=replication,cn=localhost este considerată mai sigură. Acreditările plasate în subarborele replicat sunt create pe lângă intrarea ibm-replicagroup=default pentru acel subarbore.
   - Faceţi clic pe **Selectare**.
     - Selectaţi locaţia pentru acreditările pe care vreţi să le folosiţi. De preferat aceasta este cn=replication,cn=localhost.
     - Apăsaţi **Arată acreditări**.
     - Expandaţi lista de acreditări şi selectaţi-o pe aceea pe care vreţi să o folosiţi.
     - Apăsaţi **OK**.

       Vedeţi Creare acreditări replicare pentru informaţii adiţionale despre acord acreditări.
   - Specificaţi o planificare de replicare din meniul derulant sau apăsaţi **Adăugare** pentru a crea una. Vedeţi Creare programe replicare.
   - Din lista de capabilităţi furnizor puteţi deselecta orice capabilităţi pe care nu vreţi să le replicaţi la consumator.

     Dacă reţeaua dvs. are un amestec de servere la diferite ediţii, sunt disponibile capabilităţi pe ediţii ulterioare care nu sunt disponibile pe ediţii mai vechi. Unele capabilităţi, precum ACL-uri filtrate şi politica de parolă, folosesc atribute operaţionale care sunt replicate cu alte modificări. În majoritatea cazurilor, dacă aceste funcţii sunt folosite, este de dorit ca toate serverele să le suporte. Dacă toate serverele nu suportă capabilitatea, atunci nu vreţi să o folosiţi. De exemplu, nu aţi dori ACL-uri diferite care să fie active pe fiecare server. Oricum, ar putea fi cazuri în care aţi dori să folosiţi o capabilitate de pe serverele care o suportă şi modificările legate de această capabilitate să nu fie replicate la serverele care nu suportă capabilitatea. În astfel de cazuri, puteţi folosi lista de capabilităţi pentru a marca anumite capabilităţi care să nu fie replicate.
   - Selectaţi fie firul de execuţie Singular sau firul de execuţie Multiplu pentru metoda de replicare. Dacă specificaţi fir de execuţie Multiplu, trebuie, de asemenea, să specificaţi numărul de conexiuni (între 2 şi 32) de utilizat pentru replicare. Numărul implicit de conexiuni este 2.
   - Faceţi clic pe **OK** pentru a crea replica.

6. Este afişat un mesaj care spune că trebuie făcute acţiuni suplimentare. Faceţi clic pe **OK**.

   Notă: Dacă adăugaţi mai multe servere ca replice adiţionale sau creaţi o tipologie complexă, nu continuaţi cu Copiere date la replică sau Adăugare informaţii furnizor la replica nouă până când nu aţi terminat să definiţi topologia din serverul master. Dacă creaţi *masterfile.ldif* după ce aţi încheiat topologia, aceasta conţine intrările director ale serverului master şi o copie completă a acordurilor de topologie. Când încărcaţi acest fişier pe fiecare din servere, fiecare server are aceeaşi informaţie.

Copierea datelor la replică

Folosiţi aceste informaţii pentru a copia datele la replică.

După ce creaţi replica, trebuie să exportaţi topologia de la master către replică.

1. Pe serverul master creaţi un fişier LDIF pentru date. Pentru a copia toate datele conţinute pe serverul master, faceţi următoarele:
   a. În Navigator System i, expandaţi **Reţea**.
   b. Expandaţi **Servere**.
   c. Faceţi clic pe **TCP/IP**.
   d. Faceţi clic dreapta pe **IBM Directory Server** şi selectaţi **Unelte**, apoi **Exportare fişier**.
   e. Specificaţi numele fişierului de ieşire LDIF (de exemplu masterfile.ldif), opţional specificaţi un subarbore pentru a exporta (de exemplu subtreeDN) şi apăsaţi **OK**.
2. Pe maşina unde creaţi replica, faceţi următoarele:
   a. Asiguraţi-vă că sufixele replicate sunt definite în configuraţia serverului replică.
   b. Opriţi serverul replică.
   c. Copiaţi fişierul LDIF pe replică şi faceţi următoarele:
      1) În Navigator System i, expandaţi **Reţea**.
      2) Expandaţi **Servere**.
      3) Faceţi clic pe **TCP/IP**.
      4) Faceţi clic dreapta pe **IBM Directory Server** şi selectaţi **Unelte**, apoi **Importare fişier**.
      5) Specificaţi numele fişierului de intrare LDIF (de exemplu masterfile.ldif), opţional specificaţi dacă vreţi să replicaţi datele şi apăsaţi **OK**.

      Acordurile de replicare, planificările, acreditările (dacă sunt stocate în subarborele replicat) şi datele intrării sunt încărcate pe replică.
   d. Porniţi serverul.

Adăugarea informaţiilor furnizorului la replica nouă

Folosiţi aceste informaţii pentru a adăuga informaţiile furnizorului la replica nouă.

Trebuie să modificaţi configuraţia replicii pentru a identifica cine este autorizat să replice modificările făcute asupra ei şi adăugaţi un referral la un master.

Pe maşina unde creaţi replica:

1. Expandaţi **Gestionare replicare** din zona de navigare şi apăsaţi **Gestionare proprietăţi de replicare**.

   Notă: Trebuie să vă înregistraţi în unealta de administrarea web ca un utilizator proiectat OS/400 cu autorizările speciale *ALLOBJ şi *IOSYSCFG pentru a modifica setările în panourile **Gestionare prorietăţi replicare** .
2. Selectaţi **Adăugare**.
3. Selectaţi un furnizor din meniul derulant **Subarbore replicat** sau introduceţi numele subarborelui replicat pentru care vreţi să configuraţi acreditările de furnizor. Dacă editaţi acreditările de furnizor, acest câmp nu este editabil.
4. Introduceţi DN-ul de legare de replicare. În acest exemplu, cn=any.

   Notă: Puteţi folosi oricare dintre aceste două opţiuni, în funcţie de situaţia dvs.
   - Setaţi DN-ul de legare replicare (şi parola) şi un referral implicit pentru toate subarborele replicate pe un server folosind 'acreditările şi referral-ul implicite'. Acestea ar putea fi folosite când toţi subarborii sunt replicaţi de la acelaşi furnizor.
   - Setaţi DN-ul de legare replicare şi parola independent pentru fiecare subarbore replicat prin adăugarea informaţiilor despre furnizor pentru fiecare subarbore. Acesta ar putea fi folosit când fiecare subarbore are alt furnizor (adică un server master diferit pentru fiecare subarbore).
5. În funcţie de tipul de acreditare, introduceţi şi confirmaţi parola acreditării. (Aţi înregistrat aceasta anterior pentru folosiri ulterioare.)
   - **Legare simplă** - Specificaţi DN-ul şi parola

- **Kerberos** - Dacă acreditările de pe furnizor nu identifică principalul şi parola, ce sunt, serviciile principal proprii ale serverului ce urmează a fi folosite, atunci legătura DN este ibm-kn=ldap/<*yourservername@yourrealm*>. Dacă acreditările au un nume principal cum ar fi <*myprincipal@myrealm*>, utilizaţi-l ca pe DN. În orice caz, nu este necesară o parolă.
- **SSL w/ EXTERNAL bind** - Specificaţi DN-ul subiect pentru certificat şi nici o parolă

Vedeţi"Crearea acreditărilor de replicare" la pagina 143.

6. Apăsaţi **OK**.
7. Trebuie să reporniţi replica pentru ca schimbările să aibă efect.

Vedeţi "Modificarea proprietăţilor replicării" la pagina 153 pentru informaţii adiţionale.

Replica este într-o stare suspendată şi nu apare nici o replicare. După ce aţi terminat de setat topologia dumneavoastră de replicare, trebuie să apăsaţi pe **Gestionare cozi**, să selectaţi replica şi să apăsaţi **Suspendare/reluare** pentru a porni replicarea. Vedeţi "Gestionarea cozilor de replicare" la pagina 156 pentru mai multe informaţii detaliate. Replica primeşte acum actualizări de la master.

Crearea unei tipologii simple cu replicare peer

Replicarea peer este o topologie de replicare în care mai multe servere sunt masteri. Folosiţi replicare peer doar în mediile în care vectorii de actualizare sunt bine cunoscuţi.

Actualizările la obiecte particulare din cadrul directorului trebuie să fie făcute doar de către un server peer. Aceasta este intenţionată pentru a preveni un scenariu în care un server şterge un obiect, urmat de un alt server ce modifică obiectul. Acest scenariu creează posibilitatea ca un server peer să primească o comandă ştearsă urmată de o comandă modificată pentru acelaşi obiect, ceea ce creează un conflict. Ştergerea replicată şi redenumire cerere sunt acceptate în ordinea primită fără rezoluţie de conflict. Vedeţi legăturile înrudite de mai jos pentru a învăţa mai multe despre Rezoluţie replicare conflict.

Expandaţi categoria **Gestionare replicare** din zona de navigare şi apăsaţi **Gestionare topologie**.

1. Selectaţi subarborele pe care vreţi să îl replicaţi şi apăsaţi **Arată topologie**.
2. Faceţi clic pe caseta de lângă serverele existente pentru a expanda lista serverelor furnizoare, dacă doriţi să vizualizaţi topologia existentă.
3. Faceţi clic pe **Adăugare master**.

Pe fişa **Server** a ferestrei **Adăugare master**:

- Introduceţi numele gazdei şi numărul portului pentru serverul pe care îl creaţi. Portul implicit este 389 pentru non-SSL şi 636 pentru SSL. Acestea sunt câmpuri necesare.
- Selectaţi dacă să activaţi comunicaţiile SSL.
- Selectaţi dacă doriţi să creaţi serverul ca un server gateway.
- Introduceţi numele serverului sau lăsaţi acest câmp blanc pentru a utiliza numele gazdei.
- Introduceţi ID server. Dacă serverul pe care creaţi peer-master rulează, faceţi clic pe **Obţinere ID server** pentru a completa automat implicit acest câmp. Dacă nu ştiţi ID-ul serverului, introduceţi **necunoscut**.
- Introduceţi o descriere a serverului.
- Trebuie să specificaţi acreditările pe care serverul le foloseşte pentru a comunica cu celelalte servere master.Faceţi clic pe **Alegere**

Notă: Unealta de administrare web vă permite să definiţi acreditări în următoarele locuri:

- **cn=replication,cn=localhost**, care păstrează acreditările doar pe serverul care le foloseşte. Plasarea acreditărilor în cn=replication,cn=localhost este considerată mai sigură.
- **cn=replication,cn=IBMpolicies**, ce sunt disponibile chiar şi atunci când serverul sub care încercaţi să adăugaţi o replică nu este acelaşi server la care sunteţi conectat cu unealta de administrarea web. Acreditările amplasate sub această locaţie sunt copiate la server.

Notă: Locaţia, cn=replication,cn=IBMpolicies este disponibilă doar dacă suportul IBMpolicies OID, 1.3.18.0.2.32.18, este prezent sub ibm-supportedcapabilities a rădăcinii DSE.

– În subarborele replicat, caz în care acreditările sunt replicate cu restul subarborelui. Acreditările plasate în subarborele replicat sunt create sub intrarea **ibm-replicagroup=default** pentru acel subarbore.

1. Selectaţi locaţia pentru acreditările pe care vreţi să le folosiţi. De preferat aceasta este cn=replication,cn=localhost.
2. Dacă aţi creat deja un set de acreditări, faceţi clic pe Afişare acreditări.
3. Expandaţi lista de acreditări şi selectaţi-o pe aceea pe care vreţi să o folosiţi.
4. Faceţi clic pe OK.
5. Dacă nu aveţi acreditări preexistente, faceţi clic pe Adăugare pentru a crea acreditările.

În fişa **Adiţional**:

1. Specificaţi o planificare de replicare din meniul derulant sau apăsaţi **Adăugare** pentru a crea una. Vedeţi Crearea planificărilor de replicare.
2. Din lista de capabilităţi furnizor puteţi deselecta orice capabilităţi pe care nu vreţi să le replicaţi la consumator.

   Dacă reţeaua dvs. are un amestec de servere la diferite ediţii, sunt disponibile capabilităţi pe ediţii ulterioare care nu sunt disponibile pe ediţii mai vechi. Unele capabilităţi, precum ACL-uri filtrate şi politica de parolă, folosesc atribute operaţionale care sunt replicate cu alte modificări. În cele mai multe cazuri dacă aceste caracteristici sunt utilizate, doriţi ca toate serverele să le suporte. Dacă toate serverele nu suportă capabilitatea, atunci nu vreţi să o folosiţi. De exemplu, nu aţi dori ACL-uri diferite care să fie active pe fiecare server. Oricum, ar putea fi cazuri în care aţi dori să folosiţi o capabilitate de pe serverele care o suportă şi modificările legate de această capabilitate să nu fie replicate la serverele care nu suportă capabilitatea. În astfel de cazuri, puteţi folosi lista de capabilităţi pentru a marca anumite capabilităţi care să nu fie replicate.
3. Verificaţi caseta de bifare **Adăugare de informaţii de acreditare pe consumator** , dacă doriţi să activaţi actualizările dinamice a acreditărilor furnizorului. Această selecţie actualizează în mod automat acreditările furnizorului în fişierul de configuraţie a serverului consumator. Aceasta dă posibilitatea informaţiilor de topologie să fie copiate pe server.
   - Tastaţi Administrare DN pentru serverul consumator. Spre exemplu cn=root.

     Notă: Dacă administratorul DN ce a fost creat în timpul procesului de configuraţie de server a fost cn=root, atunci introduceţi întregul administrator DN. Să nu folosiţi doar root.
   - Tastaţi Administrare parolă pentru serverul consumator. Spre exemplu secret.
4. Faceţi clic pe **OK**.
5. Acordurile furnizorului şi ale consumatorului sunt listate între un nou server master şi oricare server deja existent. Debifaţi oricare acord ce nu doriţi să fie creat. Acesta este în mod special important dacă creaţi un server gateway.
6. Selectaţi **Continuare**.
7. E posibil să se afişeze mesaje pentru a aduce aminte că trebuie luate acţiuni suplimentare. Realizaţi sau luaţi la cunoştinţă acţiunile corespunzătoare. Când terminaţi, apăsaţi **OK**.
8. Adăugaţi acreditările corespunzătoare.

   Notă: În unele situaţii panoul Selectare acreditări va întreba despre o acreditare ce este localizată într-un alt loc înafară de cn=replication,cn=localhost. În astfel de situaţii trebuie să furnizaţi un obiect de acreditare care se află în alt loc decât cn=replication,cn=localhost. Selectaţi acreditările pe care subarborele urmează să le folosească din setul existent de acreditări sau creaţi noi acreditări.
9. Faceţi clic pe **OK** pentru a crea cheia.
10. E posibil să se afişeze mesaje pentru a aduce aminte că trebuie luate acţiuni suplimentare. Realizaţi sau luaţi la cunoştinţă acţiunile corespunzătoare. Când terminaţi, apăsaţi **OK**.

Referinţe înrudite

“Privire generală asupra replicării” la pagina 37
Prin replicare, o modificare făcută la un director este propagată la unul sau mai multe directoare suplimentare. Ca efect, o modificare la un director apare pe diferite directoare multiple.

Crearea unei topologii de replicare complexă

Folosiţi această privire de ansamblu de nivel înalt ca un ghid pentru setarea unei topologii complexe de replicare.

1. Porniţi toate serverele peer sau viitoare replici. Acest lucru este necesar pentru unealta de administrare Web pentru a culege informaţii de la servere.
2. Porniţi 'primul' master şi configuraţi-l ca master pentru context.
3. Încărcaţi datele pentru subarborele de replicat pe 'primul' master, dacă datele nu sunt deja încărcate.
4. Selectaţi subarborele care va fi replicat.
5. Adăugaţi toate potenţialele servere master peer ca replici ale 'primului' master.
6. Adăugaţi toate celelalte replici.
7. Mutaţi celelalte servere master peer pentru a le promova.
8. Adăugaţi acorduri replică pentru replicile către fiecare masteri de peer.

   Notă: Dacă acreditările urmează să fie create în **cn=replication,cn=localhost**, atunci acreditările trebuie să fie create pe fiecare server după ce ele sunt restartate. Replicarea de către perechi eşuează până când sunt create obiectele de acreditare.
9. Adăugaţi acorduri replică pentru alţi masteri către fiecare masteri de peer. 'Primul' master are deja acele informaţii.
10. Dezactivaţi subarborele replicat. Aceasta împiedică efectuarea de actualizări în timp ce se copiază date către celelalte servere.
11. Folosiţi Gestionare cozi pentru a sări peste toate pentru fiecare coadă.
12. Exportaţi datele pentru subarborele replicat de la 'primul' master.
13. Activaţi subarborele.
14. Opriţi serverele replică şi importaţi datele pentru subarborele replicat de pe fiecare replică şi master peer. Apoi reporniţi serverele.
15. Gestionaţi proprietăţile de replicare de pe fiecare replică şi master peer pentru a seta acreditările care vor fi folosite de furnizori.

Crearea unei topologii complexe cu replicare peer

Folosiţi aceste informaţii pentru a crea o topologie complexă cu replicare peer.

Replicarea peer este o topologie de replicare în care mai multe servere sunt masteri. Totuşi, spre deosebire de un mediu multi-master, nu este făcută rezoluţie de conflicte între serverele peer. Serverele LDAP acceptă actualizările furnizate de serverele peer şi actualizează propriile copii ale datelor. Nu este ţinut cont de ordinea în care sunt primite actualizările sau dacă mai multe actualizări intră în conflict.

Pentru a adăuga masteri (peer) suplimentari, trebuie întâi să adăugaţi serverul ca o replică numai citire a masterilor existenţi (vedeţi "Crearea unui server replică" la pagina 144), să iniţializaţi datele director şi apoi să promovaţi serverul să fie master (vedeţi "Mutarea sau promovarea unui server" la pagina 165).

Iniţial, obiectul **ibm-replicagroup** creat de acest proces moşteneşte ACL-ul intrării rădăcină pentru subarborele replicat. Aceste ACL-uri ar putea să nu fie potrivite pentru controlul accesului la informaţiile de replicare din director.

Pentru ca operaţia Adăugare subarbore să aibă succes, intrarea DN pe careo adăugaţi trebuie să aibă ACL-uri corecte, dacă nu este un sufix în server.

Pentru ACL-uri nefiltrate:

- ownersource : <*intrarea DN*>
- ownerpropagate: TRUE
- aclsource : <*intrarea DN*>
- aclpropagate: TRUE

ACL-uri filtrate:

- ownersource : <*intrarea DN*>
- ownerpropagate: TRUE
- ibm-filteraclinherit: FALSE
- ibm-filteraclentry : <*orice valoare*>

Folosiţi funcţia **Editare ACL-uri** din unealta de administrare web pentru a seta ACL-urile pentru informaţiile de replicare asociate cu subarborele de replicare nou creat (vedeţi “Editarea listei de control acces” la pagina 167).

Replica este într-o stare suspendată şi nu apare nici o replicare. După ce aţi terminat de setat topologia dumneavoastră de replicare, trebuie să apăsaţi pe **Gestionare cozi**, să selectaţi replica şi să apăsaţi **Suspendare/reluare** pentru a porni replicarea. Vedeţi “Gestionarea cozilor de replicare” la pagina 156 pentru mai multe informaţii detaliate. Replica primeşte acum actualizări de la master.

Folosiţi replicarea peer doar în mediile unde şablonul de actualizări director este bine cunoscut. Actualizările la obiecte particulare din cadrul directorului trebuie să fie făcute doar de către un server peer. Acesta are scopul de a împiedica scenariul în care un server şterge un obiect, după care alt server modifică obiectul. Acest scenariu creează posibilitatea ca un server peer să primească o comandă de ştergere urmată de o comandă de modificare, ceea ce creează un conflict.

Pentru a defini o topologie peer-forwarder-replica, constând în două servere peer-master, două servere forwarding şi patru replici trebuie să:

1. Creaţi un server master şi un server replică. Vedeţi“Crearea unei topologii master-replica” la pagina 140.
2. Creaţi două servere replică suplimentare pentru serverul master. Vedeţi“Crearea unui server replică” la pagina 144.
3. Creaţi două replici sub fiecare din cele două servere replică nou create.
4. Promovaţi replica originală la un master. Vedeţi“Promovarea unui server să fie un peer”.

   Notă: Serverul pe care vreţi să îl promovaţi la master trebuie să fie o replică frunză fără nici o replică subordonată.
5. Copiaţi datele de la master la noul master şi noile replici. Vedeţi“Copierea datelor la replică” la pagina 145.

Operaţii înrudite

“Mutarea sau promovarea unui server” la pagina 165
Folosiţi aceste informaţii pentru a muta sau promova un server.

Promovarea unui server să fie un peer

Folosiţi aceste informaţii pentru a promova un server să fie peer.

Folosind topologia de forwarding creată în “Crearea unei topologii master-forwarder-replica” la pagina 141, puteţi promova un server să fie peer. În acest exemplu, veţi promova replica (server3) să fie peer pentru serverul master (server1).

1. Conectaţi Administrarea Web la master (server1).
2. Expandaţi categoria Gestionare replicare din zona de navigare şi apăsaţi **Gestionare topologie**.
3. Selectaţi subarborele pe care vreţi să îl replicaţi şi apăsaţi **Arată topologie**.
4. Apăsaţi săgeata de lângă selecţia **Topologie de replicare** pentru a expanda lista de servere.
5. Apăsaţi săgeata de lângă selecţia **server1** pentru a expanda lista de servere.
6. Apăsaţi săgeata de lângă selecţia **server2** pentru a expanda lista de servere.
7. Apăsaţi **server1** şi apăsaţi **Adăugare replică**. Creaţi server4. Vedeţi“Crearea unui server replică” la pagina 144. Urmaţi aceeaşi procedură pentru a crea server5. Rolurile serverelor sunt reprezentate de iconuri în unealta de administrare Web. Topologia dvs. este acum:
   - server1 (master)
     - server2 (forwarder)
       - server3 (replica)
     - server4 (replica)
     - server5 (replica)

8. Apăsaţi **server2** şi apăsaţi **Adăugare replică** pentru a crea server6.
9. Apăsaţi **server4** şi apăsaţi **Adăugare replică** pentru a crea server7. Urmaţi aceeaşi procedură pentru a crea server8. Topologia dvs. este acum:
   - server1 (master)
     - server2 (forwarder)
       - server3 (replica)
       - server6 (replica)
     - server4 (forwarder)
       - server7 (replica)
       - server8 (replica)
     - server5 (replica)
10. Selectaţi **server5** şi faceţi clic pe **Mutare**.

    Notă: Serverul pe care vreţi să îl mutaţi trebuie să fie o replică frunză fără nici o replică subordonată.
11. Selectaţi **Topologie de replicare** pentru a promova replica la un master. Faceţi clic pe **Mutare**.
12. Este afişat panoul **Creare acorduri furnizor suplimentare**. Replicarea peer necesită ca fiecare master să fie un furnizor şi consumator pentru fiecare din ceilalţi masteri din topologie şi pentru fiecare din replicile de pe primul nivel, server2 şi server 4. Server5 este deja un consumator al server1, el are acum nevoie să devină furnizor pentru server1, server2 şi server4. Asiguraţi-vă că casetele de acord furnizor sunt bifate pentru:

Tabela 5.

	Furnizor	Consumator
✔	server5	server1
✔	server5	server2
✔	server5	server4

Selectaţi **Continuare**.

Notă: În unele cazuri va apare panoul Selectare acreditări care să vă ceară o acreditare care se află în alt loc decât cn=replication,cn=localhost. În astfel de situaţii trebuie să furnizaţi un obiect de acreditare care se află în alt loc decât cn=replication,cn=localhost. Selectaţi acreditările pe care subarborele urmează să le folosească din setul existent de acreditări sau creaţi noi acreditări. Vedeţi“Crearea acreditărilor de replicare” la pagina 143.

13. Apăsaţi **OK**. Topologia dvs. este acum:
    - server1 (master)
      - server2 (forwarder)
        - server3 (replica)
        - server6 (replica)
      - server4 (forwarder)
        - server7 (replica)
        - server8 (replica)
      - server5 (master)
    - server5 (master)
      - server1 (master)
      - server2 (forwarder)
      - server4 (forwarder)
14. Copie date de la server1 la toate serverele. Vedeţi “Copierea datelor la replică” la pagina 145 pentru informaţii despre cum să faceţi aceasta.

Setarea unei topologii de gateway

Folosiţi aceste informaţii pentru a seta o topologie de gateway.

Înainte de a începe să vă setaţi topologia de replicare, faceţi o copie de rezervă a fişierului original ibmslapd.conf. Puteţi folosi această copie de rezervă pentru a restaura configuraţia originală dacă întâmpinaţi dificultăţi în replicare.

Pent ru a seta o gateway cu topologie complexă cu replicare de la procedura în Promovare server la a fi un peer, trebuie să finalizaţi următorii paşii:

- Convertiţi un server peer existent (peer 1) într-un server gateway pentru a crea locaţia 1 de replicare.
- Creaţi un nou server gateway pentru locaţia de replicare 2 şi acordurile cu peer 1.
- Creaţi topologia pentru locaţia de replicare 2 (nu este ilustrată în acest exemplu).
- Copiaţi datele din master la toate maşinile din topologie.

1. Folosiţi unealta de administrare Web pentru a vă loga în master (server1).
2. Expandaţi categoria **Gestionare replicare** din zona de navigare şi apăsaţi **Gestionare topologie**.
3. Selectaţi subarborele pe care vreţi să îl replicaţi şi apăsaţi **Arată topologie**.
4. Pentru a converti un server existent la un server gateway, selectaţi **Gestionare servere gateway** . Selectaţi **server1** sau peer-ul său **server5**. Pentru acest exemplu utilizaţi **server1** şi faceţi clic pe**Creare gateway**.
5. Apăsaţi **OK**.

   Notă: Dacă serverul pe care doriţi să îl folosiţi ca gateway nu este deja master, trebuie să fie o replică frunză (leaf) fără replici subordonate, pe care îl puteţi promova mai întâi să fie master şi apoi să îl desemnaţi să fie gateway.

6. 6. Pentru a crea un nou server gateway, faceţi clic pe **Adăugare server**.
7. Creaţi noul server, **server9** ca un server gateway. Vedeţi “Adăugarea unui peer-master sau a unui server gateway” la pagina 161 pentru informaţii despre cum să faceţi aceasta.
8. Este afişat panoul **Creare acorduri cu furnizorul suplimentare**. În acest panou, asiguraţi-vă că acele casete de acorduri furnizor sunt bifate doar pentru server1. Deselectaţi celelalte acorduri.

	Furnizor	Consumator
✓	server1	server9
✓	server9	server1
	server2	server9
	server9	server2
	server4	server9
	server9	server4
	server9	server5
	server5	server9

9. Selectaţi **Continuare**.
10. Apăsaţi **OK**.
11. Adăugaţi acreditările corespunzătoare şi informaţiile consumatorului.

    Notă: În unele cazuri, panoul **Selectare acreditări** este afişat, cerând o acreditare care se află în alt loc decât cn=replication,cn=localhost. În astfel de situaţii trebuie să furnizaţi un obiect de acreditare care se află în alt loc decât cn=replication,cn=localhost. Selectaţi acreditările pe care subarborele urmează să le folosească din setul existent de acreditări sau creaţi noi acreditări. Vedeţi Creare acreditări replicare.

12. Apăsaţi **OK**. Rolurile serverelor sunt reprezentate de iconuri în unealta de administrare Web. Topologia dvs. este acum:
    - server1 (master-gateway pentru locaţia de replicare 1)

- server2 (forwarder)
  - server3 (replica)
  - server6 (replica)
- server4 (forwarder)
  - server7 (replica)
  - server8 (replica)
- server5 (master)
- server9 (master-gateway pentru locaţia de replicare 2)

• server5 (master)
- server1 (master)
- server2 (forwarder)
  - server3 (replica)
  - server6 (replica)
- server4 (forwarder)
  - server7 (replica)
  - server8 (replica)

• server9 (master-gatway)
- server1 (master-gateway)

13. Adăugare server la **server9** pentru a crea topologiapentru site-ul de replicare 2. Aduceţi-vă aminte să deselectaţi orice acord pentru noile servere la orice server în afară de site-ul de plicare 2.
14. Repetaţi acest proces pentru a crea locaţii de replicare suplimentare. Amintiţi-vă să creaţi un singur server gateway pentru o locaţie de replicare. Totuşi,fiecare server gateway trebuie să fie pre zent în topologiile cu acordurile la alte servere gateway.
15. Când aţi terminat de creat topologia, copiaţi datele de la server1 la toate serverele noi din toate locaţiile de replicare şi adăugaţi informaţiile despre furnizor pentru toate serverele noi. Vedeţi Copiere date la replică şi Adăugare informaţii furnizor la noua replică pentru informaţii despre cum se face aceasta.

Operaţii înrudite

“Adăugarea unei replici” la pagina 159
Folosiţi aceste informaţii pentru a crea o replică.

“Adăugarea unui peer-master sau a unui server gateway” la pagina 161
Acest subiect furnizează informaţii despre cum se creează un nou peer-master sau un server gateway.

“Gestionarea serverelor gateway” la pagina 163
Acest subiect furnizează informaţii despre gestionarea serverelor gateway. Puteţi desemna dacă un server master este de a avea rolul unui server gateway în site-ul de replicare.

Modificarea proprietăţilor replicării

Folosiţi aceste informaţii pentru a modifica proprietăţilor de replicare.

Trebuie să vă înregistraţi la unealta de administrare Web ca un utilizator proiectat cu autorizările speciale *ALLOBJ şi *IOSYSCFG pentru a modifica setările din panourile **Gestionare proprietăţi replicare**.

1. Expandaţi categoria **Gestiune replicare** în zona de navigare şi faceţi clic pe **Gestionare proprietăţi replicare**
2. În acest panou puteţi:
   a. Schimba numărul maxim de modificări în aşteptare care vor fi întoarse de interogările de stare replicare. Implicit este 200.
   b. Setaţi numărul maxim de erori de replicare pe care un server le va înregistra în timp ce replicaţi actualizările la un consumator. Dacă serverul utilizează replicarea cu un singur fir de execuţie şi maximul este depăşit, actualizarea este reîncerc ată periodic până când reuşeşte sau până când administratorul curăţă istoricul pentru ca eşuarea să poată fi adăugată. Dacă serverul utilizează replicare cu mai multe fire de execuţie şi maximul este depăşit, orice erori de replicare care survin pentru actualizări î n progres sunt logate şi replicarea pentru

administratorpentru a curăţa istoricul. Istoricul poate fi curăţat reîncercând sau înlăturând actualizările eşuate. Istoricele separate suntmenţinute pentru fiecare utilizator. Implicit este zeroca în nimic.

Notă: Logarea este activată dacă o valoare mai mare decât zero este specificată.

c. Modificaţi dimensiunea în octeţi a cache-ului contextului de replicare. Implicit este 100,000 octeţi.

d. Setaţi dimensiunea intrării maxime a conflictului de replicare în octeţi. Dacă dimensiunea totală a unei intrări în octeţi depăşeşte valoarea din acest câmp, intrarea nu este trimisă din nou de furnizor pentru a rezolva un conflict de replicare pe consumator. Implicit este 0 pentru nelimitat.

e. Adăugaţi, editaţi sau ştergeţi informaţiile de furnizor.

Notă: Furnizorul DN poate fi DN-ul unui profil utilizator proiectat i5/OS. Profi lul utilizatorul protejat i5/OS trebuie să nu aibă autorizare administrativă LDAP. Utilizatorul nu poate fi un utilizator cu autorizările speciale *ALLOBJ şi *IOSYSCFG şi nu poate să îi fi fost acordată autoritate administrativă prin ID-ul de aplicaţie administrator server de director.

Pentru informaţii suplimentare, vedeţi următoarele:

- “Adăugarea informaţiilor furnizorului”
- “Editarea informaţiilor furnizorului”
- “Înlăturarea informaţiilor furnizorului” la pagina 155

Adăugarea informaţiilor furnizorului

Folosiţi aceste informaţii pentru a adăuga informaţiile furnizorului.

1. Selectaţi **Adăugare**.
2. Selectaţi un furnizor din meniul derulant sau introduceţi numele subarborelui replicat pe care vreţi să îl adăugaţi ca furnizor .
3. Introduceţi DN-ul de legare de replicare pentru acreditări.

   Notă: Puteţi folosi oricare dintre aceste două opţiuni, în funcţie de situaţia dvs.

   - Setaţi DN-ul de legare replicare (şi parola) şi un referral implicit pentru toate subarborele replicate pe un server folosind ’acreditările şi referral-ul implicite’. Acestea ar putea fi folosite când toţi subarborii sunt replicaţi de la acelaşi furnizor.
   - Setaţi DN-ul de legare replicare şi parola independent pentru fiecare subarbore replicat prin adăugarea informaţiilor despre furnizor pentru fiecare subarbore. Acesta ar putea fi folosit când fiecare subarbore are alt furnizor (adică un server master diferit pentru fiecare subarbore).
4. În funcţie de tipul de acreditare, introduceţi şi confirmaţi parola acreditării. (Aţi înregistrat aceasta anterior pentru folosiri ulterioare.)
   - **Legare simplă** - specificaţi DN-ul şi parola
   - **Kerberos** - specificaţi un pseudo DN de forma ’ibm-kn=LDAP-service-name@realm’ fără o parolă
   - **SSL w/ EXTERNAL bind** - specificaţi DN-ul subiect pentru certificat şi nici o parolă

   Vedeţi“Crearea acreditărilor de replicare” la pagina 143.
5. Apăsaţi **OK**.

Subarborele furnizorului este adăugat la lista cu informaţii despre furnizor.

Editarea informaţiilor furnizorului

Folosiţi aceste informaţii pentru a modifica informaţiile furnizorului.

1. Selectaţi subarborele furnizor pe care vreţi să îl editaţi.
2. Faceţi clic pe **Editare**.
3. Dacă editaţi **Referral şi acreditări implicite**, care sunt folosite pentru a crea intrarea cn=Master Server sub cn=configuration, introduceţi URL-ul serverului de la care clientul vrea să primească actualizări replică în câmpul URL LDAP al Furnizorului implicit. Acesta trebuie să fie un URL LDAP valid (ldap://). Altfel, săriţi la pasul 4 la pagina 155.

4. Introduceţi DN-ul de legare de replicare pentru noile acreditări pe care vreţi să le folosiţi.
5. Introduceţi şi confirmaţi parola de acreditare.
6. Apăsaţi **OK**.

Parola pentru un furnizor replicare DN poate fi de asemenea modificat utilizând comanda Modificare ser ver de director Attr (CHGDIRSVRA). Pentru a modifica parola pentru replicarea cu legătură DN cn=master la parolănouă,utilizaţi această comandă:

```
CHGDIRSVRA INSTANCE(QUSRDIR) DN('cn=master' 'newpassword')
```

Înlăturarea informaţiilor furnizorului

Folosiţi aceste informaţii pentru a înlătura informaţiile furnizorului.

1. Selectaţi subarborele furnizor pe care vreţi să îl ştergeţi.
2. Faceţi clic pe **Ştergere**
3. Când vi se cere să confirmaţi ştergerea, apăsaţi **OK**.

Subarborele este şters din lista Informaţii furnizor.

Crearea planificărilor de replicare

Folosiţi aceste informaţii pentru a crea planificările de replicare.

Puteţi defini opţional planificări pentru a planifica replicarea la anumite momente de timp sau să nu se facă replicarea la anumite momente de timp. Dacă nu folosiţi o planificare, serverul planifică replicarea oricând se face o schimbare. Aceasta este echivalentă cu specificarea unei planificări cu replicare imediată începând la 12:00 AM în toate zilele.

Expandaţi categoria **Gestionare replicare** din zona de navigare şi apăsaţi **Gestionare planificări**.

În fişa **Planificare săptămânală**, selectaţi subarborele pentru care vreţi să creaţi planificarea şi apăsaţi **Arată planificări**. Dacă există vreo planificare, ele sunt afişate în căsuţa **Planificări săptămânale**. Pentru a crea sau adăuga o nouă planificare:

1. Selectaţi **Adăugare**.
2. Introduceţi un nume pentru planificare. De exemplu **schedule1**.
3. Pentru fiecare zi, planificarea zilnică este specificată ca **Nici una**. Aceasta înseamnă că nu este planificat nici un eveniment de replicare. Ultimul eveniment de replicare, dacă există, are încă efect. Deoarece aceasta este o replică nouă, nu există evenimente de replicare anterioare, de aceea, planificarea este implicit pe replicare imediată.
4. Puteţi selecta o zi şi să apăsaţi **Adăugare planificare zilnică** pentru a crea o planificare de replicare zilnică pentru ea. Dacă creaţi o planificare zilnică aceasta devine planificarea implicită pentru fiecare zi a săptămânii. Puteţi:
   - Păstraţi planificarea zilnică ca cea implicită pentru fiecare zi sau să selectaţi o anumită zi şi să modificaţi planificarea la Nici una. Ţineţi minte că ultimul eveniment de replicare care a apărut are încă efect pentru o zi care nu are planificate evenimente de replicare.
   - Modificaţi planificarea zilnică, selectând o zi şi apăsând **Editare planificare zilnică**. Reţineţi că schimbările la o planificare zilnică afectează toate zilele care folosesc acea planificare, nu doar ziua pe care aţi selectat-o.
   - Creaţi o altă planificare zilnică prin selectarea unei zile şi apăsarea pe **Adăugare planificare zilnică**. După ce aţi creat această planificare, ea este adăugată la meniul derulant **Planificare zilnică**. Trebuie să selectaţi această planificare pentru fiecare zi pentru care vreţi să fie folosită planificarea.

   Vedeţi “Crearea unei planificări de replicare zilnice” la pagina 156 pentru mai multe informaţii despre setarea planificărilor zilnice.
5. Când terminaţi, apăsaţi **OK**.

Operaţii înrudite

“Vizualizarea planificării replicării” la pagina 164
Pentru a vizualiza planificarea replicării utilizând unealta de administrare web,urmaţi aceşti paşi.

Crearea unei planificări de replicare zilnice

Folosiţi aceste informaţii pentru a crea o planificare de replicare zilnică.

Expandaţi categoria **Gestionare replicare** din zona de navigare şi apăsaţi **Gestionare planificări**.

În fişa **Planificare zilnică**, selectaţi subarborele pentru care vreţi să creaţi planificarea şi apăsaţi **Arată planificări**. Dacă există vreo planificare, ele sunt afişate în căsuţa **Planificări zilnice**. Pentru a crea sau adăuga o nouă planificare:

1. Selectaţi **Adăugare**.
2. Introduceţi un nume pentru planificare. De exemplu, **monday1**.
3. Selectaţi setarea de fus orar, fie UTC sau local.
4. Selectaţi un tip de replicare din meniul derulant.

   Imediat
   Realizează orice actualizări de intrare în aşteptare de la ultimul eveniment de replicare şi apoi actualizează intrările în mod continuu până când apare următorul eveniment de actualizare planificat.

   O dată Realizează toate actualizările în aşteptare anterioare momentului de start. Orice actualizări făcute după momentul de start, aşteaptă până la următorul eveniment de replicare planificat.
5. Selectaţi o oră de începere (în funcţie de ora locală a serverului) pentru evenimentul de replicare.
6. Selectaţi **Adăugare**. Sunt afişate tipul evenimentului de replicare şi timpul.
7. Adăugaţi sau ştergeţi evenimente pentru a completa planificarea. Lista de evenimente este reîmprospătată în ordine cronologică.
8. Când terminaţi, apăsaţi **OK**.

De exemplu:

Tip replicare	Oră pornire
Imediat	12:00 AM
O dată	10:00 AM
O dată	2:00 PM
Imediat	4:00 PM
O dată	8:00 PM

În această planificare, primul eveniment de replicare apare la miezul nopţii şi actualizează orice modificări în aşteptare anterioare acelui moment. Actualizările de replicare continuă să fie făcute până la 10:00 AM. Actualizările făcute între 10:00 AM şi 2:00 PM aşteaptă până la 2:00 PM pentru a fi replicate. Orice actualizări făcute între 2:00 PM şi 4:00 PM aşteaptă evenimentul de replicare planificat la 4:00 PM, după care actualizările de replicare continuă până la următorul eveniment de replicare planificat la 8:00 PM. Orice actualizări făcute după 8:00 PM, aşteaptă până la următorul eveniment de replicare planificat.

Notă: Dacă evenimentele de replicare sunt planificate prea apropiate unele de altele, un eveniment de replicare ar putea fi sărit dacă actualizările de la evenimentul anterior sunt încă în desfăşurare când este planificat următorul eveniment.

Gestionarea cozilor de replicare

Folosiţi aceste informaţii pentru a monitoriza starea replicării pentru fiecare acord de replicare (coadă) utilizat de acest server.

1. Expandaţi categoria **Gestionare replicare** din zona de navigare şi apăsaţi **Gestionare cozi**.
2. Selectaţi replica pentru care vreţi să gestionaţi coada.
3. În funcţie de starea replicii, puteţi apăsa pe **Suspendare/reluare** pentru a opri sau porni replicarea.
4. Apăsaţi **Forţare replicare** pentru a replica toate modificările în aşteptare indiferent de când este planificată următoarea replicare.

5. Apăsaţi **Detalii coadă**, pentru informaţii mai complete despre coada replicii. Puteţi de asemenea gestiona coada de la această selecţie.
6. Faceţi clic pe **Vizualizare erori** pentru a ajunge la panoul de gestionare a erorilor de replicare. De aici puteţi vizualiza istoricul erorilor de replicare, reîncercaţi modificări eşuate sau înlătura intrări din istoric.
7. Apăsaţi **Reîmprospătare** pentru a actualiza cozile şi pentru a şterge mesajele serverului.

Dacă aţi apăsat **Detalii coadă**, sunt afişate trei fişe:

- Stare
- Ultimele detalii încercate
- Schimbări în aşteptare

Fişa **Stare** afişează numele replicii, subarborele ei, starea ei şi o înregistrare a momentelor de replicare. Din acest panou puteţi suspenda sau relua replicarea apăsând pe **Reluare**. Apăsaţi **Reîmprospătare** pentru a actualiza informaţiile despre coadă.

Fişa **Ultimele detalii încercate** oferă informaţii despre ultima încercare de actualizare. Dacă nu poate fi încărcată o intrare apăsaţi **Sărire intrare blocantă** pentru a continua replicarea cu următoarea intrare în aşteptare. Apăsaţi **Reîmprospătare** pentru a actualiza informaţiile despre coadă.

Fişa **Schimbări în aşteptare** arată toate schimbările la replică în aşteptare. Dacă replicarea este blocată puteţi şterge toate schimbările în aşteptare apăsând pe **Sărire toate**. Apăsaţi pe **Reîmprospătare** pentru a actualiza lista de schimbări în aşteptare ca să reflecte orice noi actualizări sau actualizări care au fost procesate.

Notă: Dacă alegeţi să săriţi modificările blocante, trebuie să vă asiguraţi că serverul consumator este în cele din urmă actualizat.

Concepte înrudite

"Tabela cu erori de replicare" la pagina 43
Tabela cu erori de replicare înregistrează actualizările eşuate, pentru recuperarea ulterioară. Când începe replicarea, este contorizat numărul de eşuări înregistrate pentru fiecare acord de replicare. Acest număr creşte dacă o eşuează o actualizare, fiind adăugată o nouă intrare în tabelă.

Referinţe înrudite

"ldapdiff" la pagina 235
Utilitarul pentru linie de comandă de sincronizare a replicii LDAP.

Modificarea setărilor istoricului pierdute şi găsite

Istoricul pierdute şi găsite (LostAndFound.log este numele fişierului implicit) înregistrează erorile survenite ca rezultat al conflictelor de replicare. Sunt setări pentru a controla istoricul pierdute şi găsite incluzând locaţia şi dimensiunea maximă a fişierului şi arhivarea fişierelor istoric vechi.

Pentru a modifica setările istoricului pierdute şi găsite, executaţi următoarele:

1. În unealta Web de administrare IBM Tivoli Directory Server, expandaţi **Administrare server** şi apoi **Istorice** în zona de navigare şi faceţi clic pe **Modificare setări istoric**.
2. 2. Faceţi clic pe **Istoric pierdute şi găsite**.
3. 3. Itroduceţi calea şi numele fişierului pentru istoricul eroare. Asiguraţi-vă că fişierul există pe serverul ldap şi că calea este validă. calea istoricului implicită este *<unitate>**idsslapd-<nume-instanţă>**istorice*, unde *unitate* este unitatea pe care o specificaţi când creaţi instanţa unui server de director şi *nume instanţă* este numele instanţei serverului de director. Dacă specificaţi un fişier ce nu este un nume de fişier acceptabil (spre exemplu, sintaxă invalidă sau dacă serverul nu are drepturile să creeze şi/sau să modifice fişierul), tentativa eşuează cu eroarea următoare: Serverul LDAP nu este doritor să realizeze operaţia .
4. Sub **Prag dimensiune istoric (MB)** selectaţi primul buton radio şi introduceţi dimens iunea istoricului maximă în Megaocteţi. Dacă nu doriţi să limitaţi dimensiunea istoricului, selectaţi butonul radio **nelimitat**.
5. Sub **Arhivări istoric maxime**, selectaţi una din următoarele:

- Dacă doriţi să specificaţi un număr maxim de istorice de arhivare, selectaţi butonul radio cu o fereastră de editare lângă el. Introduceţi numărul maxim de arhivări pe care doriţi să le salvaţi. Un istoric de arhivare este un istoric recent ce şi-a atins progul său de dimensiune.
- Dacă nu doriţi să arhivaţi istorice, selectaţi Fără arhive.
- Dacă nu doriţi să limitaţi numărul de istorice de arhivare, selectaţi Nelimitat.

6. Sub **Cale istoric de arhivare**, faceţi una din următoarele:
   - Dacă doriţi să săecificaţi calea unde sunt ţinute arhivele, selectaţi butonul radio cu o fereastră de editare lângă el şi introduceţi calea dorită.
   - Dacă doriţi să păstraţi arhivele în directorul unde este localizat fişierul istoric, selectaţi butonul radio **Acelaşi director ca fişierul istoric**.
7. Faceţi clic pe **Aplicare** pentru a vă aplica modificările şi să continuaţi să lucraţi cu istorice sau faceţi clic pe **OK** pentru a vă salva modificările şi a reveni în panoul Introducere administrare Web IBM Tivoli Directory Server. Faceţi clic pe **Anulare** pentru a vă întoarce la panoul Introducere administrare Web IBM Tivoli Directory Server fără să salvaţi modificările.

Referinţe înrudite

"Privire generală asupra replicării" la pagina 37
Prin replicare, o modificare făcută la un director este propagată la unul sau mai multe directoare suplimentare. Ca efect, o modificare la un director apare pe diferite directoare multiple.

Vizualizarea fişierului istoric pierdute şi găsite

Fişierul istoric pierdute şi găsite de replicare poate fi vizualizat utilizând unealta de administrare Web IBM Tivoli Directory Server, folosind opţiunile fişierului istoric al utilitarului ldapexop sau vizualizând fişierul direct.

Pentru a vizualiza fişierul istoric pierdute şi găsite utilizând unealta de administrare Web, expandaţi **Administrare server** în zona de navigare Administrare web şi apoi **Istorice** în lista expandată.

1. Faceţi clic pe **Vizualizare istoric**.
2. În panoul **Vizualizare istorice**, selectaţi **Istoric pierdute şi găsite** şi faceţi clic pe butonul **Vizualizare**.

Notă: Administratorul de director şi membrii grupului administrativ sunt numai utilizatorii care pot accesa acest panou.

Pentru a vizualiza istoricul pierdute şi găsite utilizând utilitarul ldapexop, faceţi următoarele de la Qshell:

```
ldapexop -D  -w  -op readlog -log pierdute şi găsite -aliniere toate
```

Faceţi următoarele pentru a curăţa istoricul pierdute şi găsite:

```
ldapexop -D  -w  -op clearlog -log LostAndFound
```

Notă: Dacă sunteţi semnat pe sistemul i5/OS ca utilizator cu autorizarea specială *ALLOBJ şi *IOSYSCFG sau ca utilizator căruia i-a fost dat acces de administrator la serverul de director, puteţi folosi utilitarul ldapexop cu opţiunea -m OS400-PRFTKN în loc de a furniza DN-ul de administrator şi parola. De exemplu,

```
ldapexop -m OS400-PRFTKN -op readlog -log LostAndFound -lines all
```

Referinţe înrudite

"ldapexop" la pagina 214
Utilitarul pentru linie de comandă de operaţie extinsă LDAP.

Setarea replicării peste o conexiune sigură

Folosiţi aceste informaţii pentru a seta replicarea peste o conexiune sigură.

Replicarea peste SSL ar trebui setată pe etape, astfel încât să puteţi verifica totul pe măsură ce treceţi prin proces.

Înainte de a încerca să configuraţi replicarea peste o conexiune sigură, ar trebui să realizaţi următoarele taskuri (în orice ordine):

- Configuraţi replicarea peste o conexiune ne-sigură.

- Configuraţi serverul consumatorului să accepte conexiuni sigure prin portul sigur. Verificaţi dacă un client poate folosi o conexiune sigură la serverul consumatorului, de exemplu, folosind utilitarul ldapsearch. Dacă doriţi ca un server furnizor să folosească un certificat pentru autentificare, cum este legătura externă SASL peste SSL, ar trebui mai întâi să setaţi autentificare server şi apoi autentificare client şi server, unde ″serverul″ este serverul consumator, iar clientul este serverul furnizor.

  Notă: Când serverul este configurat să folosească autentificarea client şi server, toţi clienţii care folosesc SSL trebuie să aibă un certificat de client.
- Configuraţi serverul furnizor să aibă încredere în autoritatea de certificare care a emis certificatul consumatorului.

1. În unealta de administrare Web, faceţi clic pe **Gestionare topologie** din categoria **Gestionare replicare**.
2. Alegeţi unul din acordurile existente pe care vreţi să-l securizaţi.
3. Alegeţi **Editare acord...** şi selectaţi folosirea SSL, asigurându-vă că utilizaţi numărul corect al portului. 636 este numărul portului securizat standard.
4. Verificaţi că replicarea din acord funcţionează corespunzător.

Dacă încercaţi doar să setaţi replicarea pentru a vă autentifica folosind un DN şi o parolă peste o conexiune sigură, paşii anteriori au realizat deja acest lucru pentru dumneavoastră. Autentificarea folosind un certificat de client necesită un obiect diferit de acreditări care să fie folosit de serverul furnizor la acordul său, ca şi configurarea consumatorului pentru a accepta acel certificat ca server furnizor.

Taskuri ale topologiei de replicare

Folosiţi aceste informaţii pentru a gestiona topologiile subarborilor replicaţi.

Topologiile sunt specifice pentru subarborii replicaţi.

Vizualizarea topologiei

Folosiţi aceste informaţii pentru a vizualiza topologia subarbore.

Notă: Serverul trebuie să ruleze pentru a efectua această operaţie.

Expandaţi categoria **Gestionare replicare** din zona de navigare şi apăsaţi **Gestionare topologie**.

Selectaţi subarborele pe care vreţi să îl vizualizaţi şi apăsaţi **Arată topologie**.

Topologia este afişată în lista de Replicare topologie. Expandaţi topologiile apăsând pe triunghiurile albastre. Din această listă puteţi să:

- Adăugaţi o replică.
- Editaţi informaţiile de pe o replică existentă.
- Vă mutaţi la un server furnizor pentru replică sau promovaţi replica la un server master.
- Ştergeţi o replică.
- Vizualizaţi planificarea replicării

Adăugarea unei replici

Folosiţi aceste informaţii pentru a crea o replică.

Notă: Paşii descrişi aici explică cum să adăugaţi o replică prin taskul de administrare web şi fac parte dintr-un proces general ce include alţi paşi necesari pentru a iniţializa corect noul server. Referiţi-vă la subiect în legăturile înrudite de mai jos.

Notă: Serverul trebuie să ruleze pentru a efectua această operaţie.

Expandaţi categoria **Gestionare replicare** din zona de navigare şi apăsaţi **Gestionare topologie**.

1. Selectaţi subarborele pe care vreţi să îl replicaţi şi apăsaţi **Arată topologie**.

2. Apăsaţi săgeata de lângă selecţia **Topologie de replicare** pentru a expanda lista de servere furnizor.
3. Selectaţi serverul furnizor şi apăsaţi **Adăugare replică**.
4. În fişa **Server** din fereastra **Adăugare replică**:
   a. Introduceţi numele gazdă şi numărul de port pentru replica pe care o creaţi. Portul implicit este 389 pentru non-SSL şi 636 pentru SSL. Acestea sunt câmpuri necesare.
   b. Selectaţi dacă să activaţi comunicaţiile SSL.
   c. Introduceţi numele replicii sau lăsaţi acest câmp gol pentru a folosi numele gazdă.
   d. Introduceţi ID replică. Dacă serverul pe care creaţi replica rulează, apăsaţi **Obţinere ID replică** pentru a completa automat acest câmp. Acesta este un câmp obligatoriu, dacă serverul pe care îl adăugaţi va fi server peer sau de înaintare (forwarding). Este recomandat ca toate serverele să aibă aceeaşi ediţie.
   e. Introduceţi o descriere a serverului replică.
5. În fişa **Adiţional**,
   - Specificaţi acreditările pe care le foloseşte replica pentru a comunica cu masterul.

     Notă: Unealta de administrare web vă permite să definiţi acreditări în aceste locuri:
     - **cn=replication,cn=localhost**, care păstrează acreditările doar pe serverul care le foloseşte.
     - În subarborele replicat, caz în care acreditările sunt replicate cu restul subarborelui. Acreditările plasate în subarborele replicat sunt create sub intrarea **ibm-replicagroup=default** pentru acel subarbore.

     Plasarea acreditărilor în cn=replication,cn=localhost este considerată mai sigură. Acreditările plasate în subarborele replicat sunt create pe lângă intrarea ibm-replicagroup=default pentru acel subarbore.
   - Faceţi clic pe **Selectare**.
     - Selectaţi locaţia pentru acreditările pe care vreţi să le folosiţi. De preferat aceasta este cn=replication,cn=localhost.
     - Apăsaţi **Arată acreditări**.
     - Expandaţi lista de acreditări şi selectaţi-o pe aceea pe care vreţi să o folosiţi.
     - Apăsaţi **OK**.

       Vedeţi Creare acreditări replicare pentru informaţii adiţionale despre acord acreditări.
   - Specificaţi o planificare de replicare din meniul derulant sau apăsaţi **Adăugare** pentru a crea una. Vedeţi Creare programe replicare.
   - Din lista de capabilităţi furnizor puteţi deselecta orice capabilităţi pe care nu vreţi să le replicaţi la consumator.

     Dacă reţeaua dvs. are un amestec de servere la diferite ediţii, sunt disponibile capabilităţi pe ediţii ulterioare care nu sunt disponibile pe ediţii mai vechi. Unele capabilităţi, precum ACL-uri filtrate şi politica de parolă, folosesc atribute operaţionale care sunt replicate cu alte modificări. În majoritatea cazurilor, dacă aceste funcţii sunt folosite, este de dorit ca toate serverele să le suporte. Dacă toate serverele nu suportă capabilitatea, atunci nu vreţi să o folosiţi. De exemplu, nu aţi dori ACL-uri diferite care să fie active pe fiecare server. Oricum, ar putea fi cazuri în care aţi dori să folosiţi o capabilitate de pe serverele care o suportă şi modificările legate de această capabilitate să nu fie replicate la serverele care nu suportă capabilitatea. În astfel de cazuri, puteţi folosi lista de capabilităţi pentru a marca anumite capabilităţi care să nu fie replicate.
   - Selectaţi fie firul de execuţie Singular sau firul de execuţie Multiplu pentru metoda de replicare. Dacă specificaţi fir de execuţie Multiplu, trebuie, de asemenea, să specificaţi numărul de conexiuni (între 2 şi 32) de utilizat pentru replicare. Numărul implicit de conexiuni este 2.
   - Faceţi clic pe **OK** pentru a crea replica.
6. Este afişat un mesaj care spune că trebuie făcute acţiuni suplimentare. Faceţi clic pe **OK**.

   Notă: Dacă adăugaţi mai multe servere ca replice adiţionale sau creaţi o tipologie complexă, nu continuaţi cu Copiere date la replică sau Adăugare informaţii furnizor la replica nouă până când nu aţi terminat să definiţi topologia din serverul master. Dacă creaţi *masterfile.ldif* după ce aţi încheiat topologia, aceasta conţine

intrările director ale serverului master şi o copie completă a acordurilor de topologie. Când încărcaţi acest fişier pe fiecare din servere, fiecare server are aceeaşi informaţie.

Operaţii înrudite

"Setarea unei topologii de gateway" la pagina 152
Folosiţi aceste informaţii pentru a seta o topologie de gateway.

Adăugarea unui peer-master sau a unui server gateway

Acest subiect furnizează informaţii despre cum se creează un nou peer-master sau un server gateway.

Notă: Aceşti paşi descrişi aici explică cum se execută adăugarea unui peer-master sau a unui server gateway prin taskul de administrare web şi fac parte dintr-un proces general ce include alţi paşi necesari pentru a iniţializa corect noul server. Referiţi-vă la subiect în legăturile înrudite de mai jos.

Expandaţi categoria **Gestionare replicare** din zona de navigare şi apăsaţi **Gestionare topologie**.

1. Selectaţi subarborele pe care vreţi să îl replicaţi şi apăsaţi **Arată topologie**.
2. Faceţi clic pe caseta după **Replicare topologie** pentru a expanda lista de servere furnizate, dacă doriţi să vizualizaţi topologia existentă.
3. Faceţi clic pe **Adăugare master**.

Pe fişa **Server** a ferestrei **Adăugare master**:

- Introduceţi numele gazdă şi numărul portului pentru serverul pe care îl creaţi. Portul implicit este 389 pentru non-SSL şi 636 pentru SSL. Acestea sunt câmpuri necesare.
- Selectaţi dacă să activaţi comunicaţiile SSL.
- Selectaţi dacă doriţi să creaţi serverul ca un server gateway.
- Introduceţi numele server sau lăsaţi acest câmp blanc pentru a utiliza numele gazdă.
- Introduceţi **ID server**. Dacă serverul pe care creaţi peer-master rulează, faceţi clic pe Obţinere ID server pentru a completa implicit, automat acest câmp.
- Introduceţi o descriere a serverului.
- Trebuie să specificaţi acreditările pe care serverul le foloseşte pentru a comunica cu celelalte servere master. Faceţi clic pe **Alegere**.

  Notă: Unealta de administrare web vă permite să definiţi acreditări în următoarele locuri:
  - **cn=replication,cn=localhost**, care păstrează acreditările doar pe serverul care le foloseşte. Plasarea acreditărilor în cn=replication,cn=localhost este considerată mai sigură.
  - **cn=replication,cn=IBMpolicies**, ce sunt disponibile chiar şi atunci când serverul sub care încercaţi să adăugaţi o replică nu este acelaşi server la care sunteţi conectat cu Administrarea web de unelte. Acreditările amplasate sub această locaţie sunt copiate la server.

    Notă: Locaţia, cn=replication,cn=IBMpolicies este disponibilă doar dacă suportul IBMpolicies OID, 1.3.18.0.2.32.18, este prezent sub ibm-supportedcapabilities a rădăcinii DSE.
  - În subarborele replicat, caz în care acreditările sunt replicate cu restul subarborelui. Acreditările plasate în subarborele replicat sunt create sub intrarea **ibm-replicagroup=default** pentru acel subarbore.

  1. Selectaţi locaţia pentru acreditările pe care vreţi să le folosiţi. De preferat aceasta este cn=replication,cn=localhost.
  2. Dacă aţi creat deja un set de acreditări, faceţi clic pe Afişare acreditări.
  3. Expandaţi lista de acreditări şi selectaţi-o pe aceea pe care vreţi să o folosiţi.
  4. Faceţi clic pe OK.
  5. Dacă nu aveţi acreditări preexistente, faceţi clic pe Adăugare pentru a crea acreditările.

În fişa **Adiţional**:

1. Specificaţi o planificare de replicare din meniul derulant sau apăsaţi **Adăugare** pentru a crea una. Vedeţi Crearea planificărilor de replicare.
2. Din lista de capabilităţi furnizor puteţi deselecta orice capabilităţi pe care nu vreţi să le replicaţi la consumator.

   Dacă reţeaua dvs. are un amestec de servere la diferite ediţii, sunt disponibile capabilităţi pe ediţii ulterioare care nu sunt disponibile pe ediţii mai vechi. Unele capabilităţi, cum ar fi filtru ACLs (Filtrează listele de control acces) şi politica de parolă (Setează proprietăţiile politicii de parolă), se folosesc de atributele operaţionale ce sunt copiate cu alte modificări. În cele mai multe cazuri dacă aceste caracteristici sunt utilizate, doriţi ca toate serverele să le suporte. Dacă toate serverele nu suportă capabilitatea, atunci nu vreţi să o folosiţi. De exemplu, nu aţi dori ACL-uri diferite care să fie active pe fiecare server. Oricum, ar putea fi cazuri în care aţi dori să folosiţi o capabilitate de pe serverele care o suportă şi modificările legate de această capabilitate să nu fie replicate la serverele care nu suportă capabilitatea. În astfel de cazuri, puteţi folosi lista de capabilităţi pentru a marca anumite capabilităţi care să nu fie replicate.
3. Verificaţi casetă de bifare **Adăugare de informaţii de acreditare pe consumator** , dacă doriţi să activaţi actualizările dinamice a acreditărilor furnizorului. Această selecţie actualizează în mod automat informaţiile furnizorului în fişierul de configuraţie a serverului pe care îl creaţi. Aceasta dă posibilitatea informaţiilor de topologie să fie copiate pe server.
   - Tastaţi Administrare DN pentru acesta, serverul consumator. Spre exemplu cn=root.

     Notă: Dacă administratorul DN ce a fost creat în timpul procesului de configuraţie de server a fost cn=root, atunci introduceţi întregul administrator DN. Să nu folosiţi doar root.
   - Tastaţi Administrare parolă pentru acesta, serverul consumator. Spre exemplu secret.
4. Apăsaţi **OK**.
5. Acordurile furnizorului şi ale consumatorului sunt listate între un nou server master şi oricare server deja existent. Debifaţi oricare acord ce nu doriţi să fie creat. Acesta este în mod special important dacă creaţi un server gateway.
6. Selectaţi **Continuare**.
7. E posibil să se afişeze mesaje pentru a aduce aminte că trebuie luate acţiuni suplimentare. Realizaţi sau luaţi la cunoştinţă acţiunile corespunzătoare. Când aţi terminat faceţi clic pe **OK**.
8. Adăugaţi acreditările corespunzătoare.

   Notă: În unele situaţii panoul Selectare acreditări va întreba despre o acreditare ce este localizată într-un alt loc înafară de cn=replication,cn=localhost. În astfel de situaţii trebuie să furnizaţi un obiect de acreditare care se află în alt loc decât cn=replication,cn=localhost. Selectaţi acreditările pe care subarborele urmează să le folosească din setul existent de acreditări sau creaţi noi acreditări.
9. Verificaţi caseta de bifare **Adăugare de informaţii de acreditare pe consumator** , dacă doriţi să activaţi actualizările dinamice a acreditărilor furnizorului. Această selecţie actualizează în mod automat informaţiile furnizorului în fişierul de configuraţie a serverului pe care îl creaţi. Aceasta dă posibilitatea informaţiilor de topologie să fie copiate pe server.
   - Tastaţi Administrare DN pentru acesta, serverul consumator. Spre exemplu cn=root.

     Notă: Dacă administratorul DN ce a fost creat în timpul procesului de configuraţie de server a fost cn=root, atunci introduceţi întregul administrator DN. Să nu folosiţi doar root.
   - Tastaţi Administrare parolă pentru acesta, serverul consumator. Spre exemplu secret.
10. Faceţi clic pe **OK** pentru a crea cheia.
11. E posibil să se afişeze mesaje pentru a aduce aminte că trebuie luate acţiuni suplimentare. Realizaţi sau luaţi la cunoştinţă acţiunile corespunzătoare. Când aţi terminat faceţi clic pe **OK**.

Notă: Dacă un obiect extern acreditat este selectat în timp ce adăugaţi acreditări pe consumatori în timpul unei operaţii de Adăugare master utilizând Administrare web de unelte, atunci următoarele setări trebuie să fie configurate pe maşina pe care rulează IBM WebSphere Server de aplicaţii:

- WAS_HOME\java\jre\lib\ext\ are următoarele fişiere jar:
  - ibmjceprovider.jar

- ibmpkcs.jar
- ibmjcefw.jar
- local_policy.jar
- US_export_policy.jar
- ibmjlog.jar
- gsk7cls.jar

• Fişierul WAS_HOME\java\jre\lib\security\java.security trebuie să aibe următoarele două linii pentru a registra furnizorul CMS şi furnizorul JCE:

```
security.provider.2=com.ibm.spi.IBMCMSProvider
security.provider.3=com.ibm.crypto.provider.IBMJCE
```

• Reporniţi IBM WebSphere server de aplicaţii.

• Trebuie instalat Gskit şi gsk7\lib trebuie să fie în calea sistemului.

• Pentru ca unealta de administrare web să citească fişierul de chei ce conţine informaţiile de acreditări pe care serverul master le utilizează pentru a se conecata la replică şi să creeze acreditări pe replică, fişierul de chei trebuie să fie prezent în C:\temp pe plaformele Windows şi în /tmp pe UNIX.

Operaţii înrudite

"Setarea unei topologii de gateway" la pagina 152
Folosiţi aceste informaţii pentru a seta o topologie de gateway.

Gestionarea serverelor gateway

Acest subiect furnizează informaţii despre gestionarea serverelor gateway. Puteţi desemna dacă un server master este de a avea rolul unui server gateway în site-ul de replicare.

Pentru a desemna un master să fie un server gateway, expandaţi categoria **Gestionare replicare** în zona de navigare şi faceţi clic pe **Topologie gestionare**.

1. Selectaţi subarborele pe care vreţi să îl vizualizaţi şi apăsaţi **Arată topologie**.
2. Faceţi clic pe **Gestionare servere gateway**.
3. Selectaţi serverul din caseta **Servere master** pe care vreţi să îl faceţi server gateway.
4. Faceţi clic pe **Creare gateway**. Serverul este mutat din caseta **Servere master** l a caseta **Servere gateway**.
5. Apăsaţi **OK**.

Pentru a înlătura rolul unui server gateway de la un server master.

1. Faceţi clic pe **Gestionare servere gateway**.
2. Selectaţi serverul din caseta **Servere gateway** pe care vreţi să îl faceţi un server master.
3. Faceţi clic pe **Creare master**. Serverul este mutat din caseta **Servere gateway** la caseta **Servere master** .
4. Faceţi clic pe **OK**.

Notă: Reţineţi că nu poate fi decât un server gateway per sit de replicare. Când creaţi servere gateway suplimentare în topologia dumneavoastră, unealta de administrare web tratează gateway-ul ca server peer şi creează acorduri la toate serverele din topologie. Asiguraţi-vă că deselectaţi orice acorduri care nu sunt altele decât servere gateway sau nu sunt în site-ul de replicare gateway-uri propriu.

Vedeţi subiectul Setarea unei topologii gateway în legătu rile înrudite de mai jos pentru informaţii suplimentare.

Operaţii înrudite

"Setarea unei topologii de gateway" la pagina 152
Folosiţi aceste informaţii pentru a seta o topologie de gateway.

Vizualizarea informaţiilor serverului

Puteţi vedea numele serverului, numele gazdă, port, ID server, rol, mod configurare, nume instanţă şi securitate de la panoul Vizualizare al serverului.

Expandaţi categoria **Gestiune replicare** în zona de navigare a Uneltei de administrare web ş i faceţi clic pe **Gestionare topologie**.

1. Selectaţi subarborele pe care vreţi să îl vizualizaţi şi apăsaţi **Arată topologie**.
2. Selectaţi serverul pe care vreţi să îl utilizaţi.
3. Faceţi clic pe **Vizualizare server** pentru a afişa panoul server vizualizare.

Panoul de vizualizare afişează următoarele informaţii:

Nume server
Acest câmp afişează numele serverului pe care instanţa directorului rulează. Aceste informaţii sunt afişate în nume gazdă:format port.

Nume gazdă
Acest câmp afişează numele gazdă al maşinii pe care instanţa serverului de director.

Port Acest câmp afişează portul nesifur pe care serverul este ascultat.

ID server
Acest câmp afişează ID-ul unic semnat pe server la prima pornire a serverului. Acest ID este utilizat în topologia de replicare pentru a determina rolul unui server.

Role Acest câmp afişează rolul configurat al serverului într-o topologie de replicare.

Mod configurare
Acest câmp identifică dacă serverul rulează în moduld e configurare. Dacă ADEVĂRAT, serverul este în mod de configurare. Dacă FALS, serverul nu este în mod de configurare.

Nume instanţă
Acest câmp afişează numele serverului pe care instanţa directorului rulează pe server.

Securitate
Acest câmp afişează portul sigur SSL la care serverul ascultă.

Numele serverului, ID şi rol şi informaţii consumator sunt afişate.

Vizualizarea planificării replicării

Pentru a vizualiza planificarea replicării utilizând unealta de administrare web,urmaţi aceşti paşi.

Expandaţi categoria **Gestiune replicare** în zona de navigare a uneltei de administrare reţea ş i faceţi clic pe **Gestionare topologie**.

1. Selectaţi subarborele pe care vreţi să îl vizualizaţi şi apăsaţi **Arată topologie**.
2. Selectaţi masterul sau serverul gateway pe care vreţi să îl vizualizaţi.
3. Faceţi clic pe **Vizualizare planificare**.

Dacă o planificare replicare există între serverul selectat şi consumatorii săi, ei sunt afişaţi. Puteţi modifica sau şterge aceste planificări. Dacă nu există planificări şi vreţi să creaţi una, trebuie să utilizaţi funcţia **Gestionare planificări** din zona de navigare unealta de administrare web . Vedeţi Crearea planificărilor de replicare în legăturile înrudite de mai jos pentru nformaţii despre gestionare planificări.

Operaţii înrudite

“Crearea planificărilor de replicare” la pagina 155
Folosiţi aceste informaţii pentru a crea planificările de replicare.

Editarea acordului

Folosiţi aceste informaţii pentru a edita un acord replicare.

Puteţi modifica următoarele informaţii pentru replică:

1. În fişa **Server** puteţi modifica numai:
   - Nume gazdă

- Port
- Activare SSL
- Descriere

2. În fişa **Adiţional** puteţi schimba:
   - Acreditări - vedeţi “Crearea acreditărilor de replicare” la pagina 143.
   - Planificări replicare - vedeţi “Crearea planificărilor de replicare” la pagina 155.
   - Schimbaţi capabilităţile replicate la replica consumator. Din lista de capabilităţi furnizor puteţi deselecta orice capabilităţi pe care nu vreţi să le replicaţi la consumator.
3. Când terminaţi, apăsaţi **OK**.

Mutarea sau promovarea unui server

Folosiţi aceste informaţii pentru a muta sau promova un server.

1. Selectaţi serverul dorit şi apăsaţi **Mutare**.
2. Selectaţi serverul pe care vreţi să mutaţi replica sau selectaţi **Topologie de replicare** pentru a promova replica la un master. Faceţi clic pe **Mutare**.
3. În unele cazuri va apare panoul Selectare acreditări care să vă ceară o acreditare care se află în alt loc decât cn=replication,cn=localhost. În astfel de situaţii trebuie să furnizaţi un obiect de acreditare care se află în alt loc decât cn=replication,cn=localhost. Selectaţi acreditările pe care subarborele urmează să le folosească din setul existent de acreditări sau creaţi noi acreditări. Vedeţi“Crearea acreditărilor de replicare” la pagina 143.
4. Se afişează **Creare acorduri furnizor suplimentare**. Selectaţi acordurile de furnizor corespunzătoare pentru rolul serverului. De exemplu, dacă un server replică este promovat să fie un server peer, trebuie să selectaţi să creaţi acorduri furnizor cu toate celelalte servere şi cu replicile lor de pe primul nivel. Aceste acorduri permit serverului promovat să funcţioneze ca furnizor pentru celelalte servere şi pentru replicile lor. Acordurile de furnizor existente de la celelalte servere către serverul nou promovat au încă efect şi nu trebuie să fie recreate.
5. Apăsaţi **OK**.

Modificarea din arborele topologiei reflectă mutarea serverului.

Operaţii înrudite

“Crearea unei topologii complexe cu replicare peer” la pagina 149
Folosiţi aceste informaţii pentru a crea o topologie complexă cu replicare peer.

Retrogadarea unui master

Folosiţi aceste informaţii pentru a schimba rolul unui server de la master la replică.

Pentru a schimba rolul unui server de la master la replică faceţi următoarele:

1. Conectaţi unealta de administrare web la serverul pe care vreţi să îl retrogradaţi.
2. Apăsaţi **Gestionare topologie**.
3. Selectaţi subarborele şi apăsaţi **Arată topologie**.
4. Ştergeţi toate acordurile pentru serverul pe care vreţi să îl retrogradaţi.
5. Selectaţi serverul pe care îl retrogradaţi şi apăsaţi **Mutare**.
6. Selectaţi serverul sub care veţi plasa serverul retrogradat şi apăsaţi **Mutare**.
7. La fel ca pentru o replică nouă, creaţi noi acorduri de furnizor între serverul retrogradat şi furnizorul lui. Vedeţi “Crearea unui server replică” la pagina 144 pentru instrucţiuni.

Copierea unui subarbore

Folosiţi aceste informaţii pentru a copia un subarbore.

Notă: Serverul trebuie să ruleze pentru a efectua această operaţie.

Expandaţi categoria **Gestionare replicare** din zona de navigare şi apăsaţi **Gestionare topologie**.

1. Apăsaţi **Adăugare subarbore**.

2. Introduceţi DN-ul subarborelui pe care vreţi să îl replicaţi sau apăsaţi **Răsfoire** pentru a expanda intrările pentru a selecta intrarea care va fi rădăcina subarborelui.
3. Introduceţi URL-ul referral al serverului master. Acesta trebuie să fie în forma unui URL LDAP, de exemplu:
   `ldap://<myservername>.<mylocation>.<mycompany>.com`
4. Apăsaţi **OK**.

Noul server este afişat pe panoul Gestionare topologie sub antetetul **Subarbori copiaţi**

Editarea unui subarbore

Folosiţi aceste informaţii pentru a modifica URL-ul serverului master la care acest subarbore şi replicile sale trimit actualizări. Trebuie să faceţi aceasta pentru a modifica numărul portului sau numele gazdă al serverului master sau modifica masterul la un server diferit.

1. Selectaţi subarborele pe care vreţi să îl editaţi.
2. Faceţi clic pe **Editare subarbore**.
3. Introduceţi URL-ul referral al serverului master. Acesta trebuie să fie în forma unui URL LDAP, de exemplu:
   `ldap://<mynewservername>.<locaţiamea>.<companiamea>.com`

În funcţie de rolul jucat de către server în acest subarbore (indiferent dacă este master, replică sau forwarding), vor apărea etichete şi butoane diferite în panou.

- Când rolul subarborelui este replică, este afişată o etichetă care indică cum că serverul funcţionează ca replică sau forwarder împreună cu butonul **Faceţi serverul master**. Dacă se apasă pe acest buton atunci serverul la care este conectată unealta de administrare web devine un master.
- Când subarborele este configurat doar pentru replicare prin adăugarea clasei auxiliare (nu există nici un grup şi subintrare implicite), atunci eticheta **Acest subarbore nu este replicat** este afişată împreună cu butonul **Replicare subarbore**. Dacă se apasă pe acest buton sunt adăugate grupul şi subintrarea implicite, astfel încât serverul cu care este conectată unealta de administrare web devine un master.
- Dacă nu sunt găsite subintrări pentru serverele master, atunci este afişată eticheta **Nu este definit nici un server master pentru acest subarbore** împreună cu butonul **Faceţi serverul master**. Dacă se apasă pe acest buton, este adăugată subintrarea lipsă astfel încât serverul cu care este conectată unealta de administrare web devine un master.

Înlăturarea unui subarbore

Folosiţi aceste informaţii pentru a înlătura un subarbore.

1. Selectaţi subarborele pe care vreţi să îl înlăturaţi.
2. Faceţi clic pe **Ştergere subarbore**.
3. Când vi se cere să confirmaţi ştergerea, apăsaţi **OK**.

Subarborele este şters din lista **Subarbore replicat**.

Notă: Această operaţie are succes doar dacă intrarea ibm-replicaGroup=default este goală.

Dezactivarea arborelui

Folosiţi aceste informaţii pentru a dezactiva arborele.

Această funcţie este folositoare când doriţi să realizaţi mentenanţă sau să schimbaţi topologia. Minimizează numărul de actualizări care pot fi făcute la server. Un server activat nu acceptă cereri client. El acceptă cereri doar de la un administrator care foloseşte controlul Administrare server.

Această funcţie este Boolean.

1. Apăsaţi **Quiesce/Unquiesce** pentru a dezactiva subarborele.
2. Când vi se cere să confirmaţi acţiunea, apăsaţi **OK**.
3. Apăsaţi **Quiesce/Unquiesce** pentru a reactiva subarborele.
4. Când vi se cere să confirmaţi acţiunea, apăsaţi **OK**.

Editarea listei de control acces

Acest subiect furnizează informaţii despre autorizările necesare pentru editarea listelor de control acces(ACL-uri) şi de asemnea furnizează informaţii despre lucrul cu ACL-uri.

Informaţiile de replicare (subintrări replică, acorduri de replicare, planificări, posibile acreditări) sunt stocate sub un obiect special, **ibm-replicagroup=default**. Obiectul ibm-replicagroup se află imediat sub intrarea rădăcină a subarborelui replicat. Implicit, acest subarbore moşteneşte ACL-ul de la intrarea rădăcină a subarborelui replicat. Acest ACL ar putea să nu fie potrivit pentru controlul accesului la informaţiile de replicare.

Autorizări necesare:

- Replicare control - Trebuie să aveţi acces de scriere la obiectul ibm-replicagroup=default (sau să fiţi proprietar/administrator).
- Cascadare replicare control - Trebuie să aveţi acces de scriere la obiectul ibm-replicagroup=default (sau să fiţi proprietar/administrator).
- Coadă de control - Trebuie să aveţi acces de scriere la acordul de replicare.

Pentru a vedea proprietăţile ACL folosind unealta de administrare Web şi să lucraţi cu ACL-uri, vedeţi “Listă control acces taskuri (ACL)” la pagina 203.

Vedeţi “Listele de control al accesului” la pagina 63 pentru informaţii suplimentare.

Taskuri ale proprietăţii securitate

Folosiţi aceste informaţii pentru a gestiona taskurile proprietăţii securitate.

Directory Server are multe mecanisme pentru a asigura securitatea datelor dumneavoastră. Acestea includ gestionarea parolei, criptarea folosind SSL şi TLS, autentificarea Kerberos şi autentificarea DIGEST-MD5. Pentru informaţii suplimentare despre conceptele de securitate, vedeţi “Securitatea Directory Server” la pagina 50.

Concepte înrudite

“Securitatea Directory Server” la pagina 50
Vedeţi cum puteţi să folosiţi o varietate de funcţii pentru a securiza Directory Server.

Taskuri de parolă

Folosiţi aceste informaţii pentru a gestiona taskurile parolei.

Pentru a gestiona parolele, expandaţi categoria **Gestionare proprietăţi securitate** din zona de navigare a Uneltei de administrare Web şi selectaţi fişa **Politică parolă**.

Concepte înrudite

“Politica de parolă” la pagina 75
Cu folosirea serverelor LDAP pentru autentificare, este important ca un server LDAP să suporte politici cu privire la expirarea parolei, încercările de înregistrare eşuate şi reguli de parolă. Directory Server furnizează suport configurabil pentru toate cele trei tipuri de politici.

Setare proprietăţi politică parolă:

Folosiţi aceste informaţii pentru a seta proprietăţile politicii parolei.

Pentru a seta politica de parolă, urmaţi aceşti paşi:

Notă: Aceşti paşi vă explică cum să setaţi politica parolei utilizatorului. Faceţi referire la Setare parolă de administrare şi subiect politică de blocare în legăturile înrudite de mai jos pentru a învăţa despre politica parolei administrative ce se aplică membrilor grupului administrativ.

1. Expandaţi categoria **Gestionare proprietăţi securitate** din zona de navigare a Uneltei de administrare Web şi selectaţi fişa **Politică parolă**. Panoul afişează un câmp **Atribut parolă** care nu poate fi editat şi care conţine numele atributului folosit de politica de parolă.
2. Selectaţi tipul de criptare parolă din lista derulantă:

   Fără Parolele sunt memorate criptate în două moduri într-o listă de validare şi sunt extrase ca fiind parte a unei intrări în formatul text clar original. Valoarea de sistem QRETSVRSEC trebuie setată la 1 pentru a utiliza această setare.

   crypt Parolele sunt codate de către algoritmul de codare criptat UNIX înainte să fie memorate în director.

   SHA-1 Parolele sunt codate folosind algoritmul de codare SHA-1 înainte de a fi reţinute în director.

   MD5 Parolele sunt codate pe baza algoritmului de codare MD5 înainte să fie memorate în director.

   AES128
   Parolele sunt criptate pe baza algoritmului AES128 înainte să fie memorate în director şi sunt extrase ca fiind parte a unei intrări în formatul de curăţare original.

   AES192
   Parolele sunt criptate pe baza algoritmului AES192 înainte să fie memorate în director şi sunt extrase ca fiind parte a unei intrări în formatul de curăţare original.

   AES256
   Parolele sunt criptate pe baza algoritmului AES256 înainte să fie memorate în director şi sunt extrase ca fiind parte a unei intrări în formatul de curăţare original.

   Notă: AES nu este suportat pe serverele pre-V6R1 LDAP. Dacă parolele criptate AES sunt exportate şi apoi importate către un server pre-V6R1, parolele nu vor fi utilizabile.

   Dacă utilizaţi criptarea AES când serverele multiple sunt utilizate, toate serverele ar trebui să utilizeze aceaşi frază-parolă AES passphrase şi salt. Administratorul trebuie să ţină urma frazelor-parolă în timp ce configuraţia serverului afişează saltul configurat disponibil. Administratorul trebuie să introducă frazele-parolă AES corespunzătoare când setează un server suplimentar să utilizeze AES.

   Pentru informaţii suplimentare, vedeţi subiectul Criptare parolă în legăturile înrudite de mai jos.
3. Selectaţi caseta de bifare **Politică parolă activată** pentru a activa politica de parolă.

   Notă: Dacă politica de parolă nu este activată, nici una din celelalte funcţii din acest panou de parole sau din alt panou nu este disponibilă până când caseta de bifare nu este activată. Implicit, politica de parolă este dezactivată.
4. Selectaţi caseta de bifare **Utilizatorul poate modifica parola** pentru a specifica dacă utilizatorul poate schimba parola.
5. Selectaţi caseta de bifare **Utilizatorul trebuie să schimbe parola după resetare** pentru a specifica dacă utilizatorul trebuie să schimbe parola după logarea cu o parolă de reset.
6. Selectaţi caseta de bifare **Utilizatorul trebuie să trimită parola la schimbare** pentru a specifica dacă utilizatorul, după logarea iniţială, trebuie să specifice din nou parola înainte să o poată modifica.
7. Setaţi limita de expirare a parolei. Faceţi clic pe butonul radio **Parola nu expiră niciodată** pentru a specifica faptul că nu este nevoie ca parola să fie schimbată la anumite intervale de timp sau faceţi clic pe butonul radio **Zile** şi specificaţi intervalul de timp în zile, când parola trebuie resetată.
8. Specificaţi dacă sistemul să emită un avertismnet de expirare parolă înainte ca parola să expire.

   Dacă faceţi clic pe butonul radio **Nu avertizaţi niciodată**, utilizatorul nu este avertizat înainte ca parola anterioară să expire. Utilizatorul nu poate accesa directorul până când administratorul nu a creat o nouă parolă.

   Dacă faceţi clic pe butonul radio **Zile înainte de expirare** şi specificaţi un număr de zile (n), utilizatorul primeşte o un prompt de avertizare pentru a schimba parola de fiecare dată când se loghează, începând cu n zile înainte de parola să expire. Utilizatorul încă mai poate accesa directorul până când parola expiră.
9. Specificaţi de câte ori, dacă este cazul, utilizatorul se poate loga după ce parola a expirat. Această selecţie permite utilizatorului să acceseze directorul cu o parolă expirată.

10. Apăsaţi **OK**.

Notă: Puteţi de asemenea folosi utilitarul ldapmodify (vedeţi “ldapmodify şi ldapadd” la pagina 207) pentru a seta politica de parolă.

Pentru mai multe informaţii despre politica de parolă, vedeţi “Politica de parolă” la pagina 75.

Concepte înrudite

“Criptarea parolei” la pagina 53
IBM Tivoli Directory Server vă permite să împiedicaţi accesul neautorizat la parolele de utilizator. Administratorul poate configura serverul pentru a cripta valorile atributului userPassword fie într-un format de criptare într-un mod fie intr-un mod de criptare în două moduri. Parolele criptate sunt marcate cu algoritmul de nume criptat astfel încât parolele criptate în formate diferite pot coexis ta în director. Când configuraţia de criptare este schimbată, parolele criptate existente rămân neschimbate şi continuă să funcţioneze.

Operaţii înrudite

“Setarea parolei de administrare şi politicii de căutare”
Politica parolei de administrare este setată utilizând numai linia de comandă. Unealta de administrare web nu suportă politica parolei de administrare.

Setarea parolei de administrare şi politicii de căutare:

Politica parolei de administrare este setată utilizând numai linia de comandă. Unealta de administrare web nu suportă politica parolei de administrare.

Notă: Trebuie să vă autentificaţi ca un profil de utilizator i5/OS cu autorizările speciale *ALLOBJ şi *IOSYSCFG.

Pentru a activa politica parolei de administrare cu o configuraţie sigură EAL4, emiteţi următoarea comandă:

```
ldapmodify -D <adminDN> -w
<adminPW> -i <nume fişier>
```

unde <nume fişier> conţine:

```
dn: cn=pwdPolicy Admin,cn=Configuration
changetype: modify
replace: ibm-slapdConfigPwdPolicyOn
ibm-slapdConfigPwdPolicyOn: true
```

Pentru a activa politica parolei de administrare şi pentru a modifica setările implicite, lansaţi următoarea comandă:

```
ldapmodify -D
<adminDN> -w <adminPW>  -i <nume fişier>
```

unde <nume fişier> conţine:

```
dn: cn=pwdPolicyAdmin,cn=Configuration
changetype: modify
replace: ibm-slapdConfigPwdPolicyOn
ibm-slapdConfigPwdPolicyOn: TRUE
-
replace: pwdlockout
pwdlockout: TRUE
#select TRUE to enable, FALSE to disable
-
replace:pwdmaxfailure
pwdmaxfailure: 10
-
replace:pwdlockoutduration
pwdlockoutduration: 300
-
replace:pwdfailurecountinterval
pwdfailurecountinterval: 0
-
```

```
replace:pwdminlength
pwdminlength: 8
-
replace:passwordminalphachars
passwordminalphachars: 2
-
replace:passwordminotherchars
passwordminotherchars: 2
-
replace:passwordmaxrepeatedchars
passwordmaxrepeatedchars: 2
-
replace:passwordmindiffchars
passwordmindiffchars: 2
```

Notă: Conturile administrative pot fi blocate ca urmare a unui număr prea mare de autentificări eşuate. Aceast se aplică numai conexiunilor client la distanţă. Contul este resetat la pornirea serverului.

Operaţii înrudite

"Setare proprietăţi politică parolă" la pagina 167
Folosiţi aceste informaţii pentru a seta proprietăţile politicii parolei.

Setarea proprietăţilor de căutare parolă:

Folosiţi aceste informaţii pentru a seta proprietăţile de căutare parolă.

1. Expandaţi categoria **Gestionare proprietăţi securitate** din zona de navigare a Uneltei de administrare Web, apoi selectaţi fişa **Blocare parolă**.

   Notă: Dacă politica de parolă nu este activată pe server, funcţiile din acest panou nu au efect.
2. Specificaţi numărul de secunde, minute, ore sau zile care trebuie să expire înainte ca o parolă să poată fi schimbată.
3. Specificaţi dacă logările incorecte au blocat parola.
   - Selectaţi butonul radio **Parolele nu sunt niciodată blocate** dacă doriţi să permiteţi încercări nelimitate de logare. Acestă selecţie dezactivează funcţia de blocare parolă.
   - Selectaţi butonul radio Încercări şi specificaţi numărul de încercări de înregistrare care sunt permise înainte de blocarea parolei. Această selecţie activează funcţia de blocare parolă.
4. Specificaţi durata blocării. Selectaţi butonul radio **Blocările nu expiră niciodată** pentru a specifica faptul că administratorul de sistem trebuie să reseteze parola sau selectaţi butonul radio**Secunde** şi specificaţi numărul de secunde până când blocarea expiră şi încercările de înregistrare pot fi reluate.
5. Specificaţi ora de expirare pentru o înregistrare incorectă. Faceţi clic pe butonul radio **Înregistrări incorecte înlăturate doar printr-o parolă corectă** pentru a specifica faptul că înregistrările incorecte sunt înlăturate doar printr-o înregistrare reuşită sau faceţi clic pe butonul radio **Secunde** şi specificaţi numărul de secunde până când o încercare nereuşită de înregistrare poate fi ştearsă din memorie.

   Notă: Această opţiune funcţionează doar dacă parola nu este blocată.
6. Când aţi terminat, faceţi clic pe **Aplicare** pentru a vă salva modificările fără să ieşiţi sau apăsaţi **OK** pentru a aplica modificările şi să ieşiţi sau apăsaţi **Anulare** pentru a părăsi acest panou fără a face vreo modificare.

Setare proprietăţi validare parolă:

Folosiţi aceste informaţii pentru a seta proprietăţile de validare parolă.

1. Expandaţi categoria **Gestionare proprietăţi securitate** din zona de navigare a Uneltei de administrare Web, apoi selectaţi fişa **Validare parolă**.

   Notă: Dacă politica de parolă nu este activată pe server, funcţiile din acest panou nu au efect.
2. Setaţi numărul de parole care trebuie folosite înainte ca o parolă să poată fi refolosită. Introduceţi un număr între 0 şi 30. Dacă introduceţi zero, o parolă poate fi folosită fără restricţii.

3. Din meniul derulant, selectaţi dacă parola este bifată pentru sintaxa definită în următoarele câmpuri de intrări. Puteţi selecta:

   Nu bifaţi sintaxa
   Nu se realizează nici o verificare a sintaxei.

   Verificaţi sintaxa (cu excepţia celei criptate)
   Verificarea sintaxei este realizată pentru toate parolele necriptate.

   Verificaţi sintaxa
   Verificarea sintaxei este realizată pentru toate parolele.
4. Specificaţi o valoare număr pentru a seta dimensiunea minimă a parolei. Dacă valoarea este setată la zero, nu se realizează nici o verificare a sintaxei.
   - Specificaţi o valoare număr pentru a seta numărul minim de caractere alfabetice necesare pentru parolă.
   - Specificaţi o valoare număr pentru a seta numărul minim de caractere numerice şi speciale necesare pentru parolă.

   Notă: Suma numărului minim de caractere alfabetice, numerice şi speciale trebuie să fie mai mică sau egală cu numărul specificat ca fiind lungimea minimă a parolei.
5. Specificaţi numărul maximum de caractere care pot fi repetate în parolă. Această opţiune limitează de câte ori un anumit caracter poate apare în parolă. Dacă valoarea este setată la zero, numărul de caractere care se repetă nu este verificat.
6. Specificaţi numărul minim de caractere care trebuie să fie diferite de parola anterioară şi numărul de parole anterioare specificat în câmpul **Numărul minim de parole înainte de reutilizare**. Dacă valoarea este setată la zero, numărul de caractere diferite nu este verificat.
7. Când aţi terminat, faceţi clic pe **Aplicare** pentru a vă salva modificările fără să ieşiţi sau apăsaţi **OK** pentru a aplica modificările şi să ieşiţi sau apăsaţi **Anulare** pentru a părăsi acest panou fără a face vreo modificare.

Vizualizarea atributelor politicii de parolă:

Folosiţi aceste informaţii pentru a vizualiza atributele politicii de parolă.

Atributele operaţionale sunt întoarse la o cerere de căutare doar când este cerut în mod special de client. Pentru a folosi aceste atribute în operaţiile de căutare, trebuie să aveţi permisiune la atributele critice sau permisiune la atributele specifice utilizate.

1. Pentru a vizualiza toate atributele politicii de parolă pentru o intrare dată:
   ```
   > ldapsearch -b "uid=user1,cn=users,o=ibm" -s base "(objectclass=*)"
    pwdChangedTime pwdAccountLockedTime pwdExpirationWarned
    pwdFailureTime pwdGraceUseTime pwdReset
   ```
2. Pentru a căuta intrări pentru care parola este pe cale să expire, utilizaţi atributul pwdChangedTime. De exemplu, pentru a găsi parolele care expiră pe 26 august 2004, având o politică de expirare parolă de 186 de zile, verificaţi intrările pentru care parola s-a schimbat cel puţin cu 186 de zile în urmă (22 februarie 2004):
   ```
   > ldapsearch -b "cn=users,o=ibm" -s sub
    "(!(pwdChangedTime>20040222000000Z))" 1.1
   ```
   unde filtrul este echivalent cu pwdChangedTime la miezul nopţii, 22 februarie 2004.
3. Pentru interogarea privind conturile blocate, folosiţi atribututl pwdAccountLockedTime:
   ```
   > ldapsearch -b "cn=users,o=ibm" -s sub "(pwdAccountLockedTime=*)" 1.1
   ```
   unde ″1.1″ indică faptul că numai DN-urile intrare trebuie returnate.
4. Pentru interogarea privind conturile pentru care parola trebuie modificată deoarece a fost resetată, folosiţi atributul pwdReset:
   ```
   > ldapsearch -b "cn=users,o=ibm" -s sub "(pwdReset=TRUE)" 1.1
   ```

Înlocuirea atributelor politicii parolei:

Folosiţi aceste informaţii pentru a înlocui atributele politicii de parolă.

Trebuie să faceţi asta mai întâi.

Un administrator de director poate înlocui comportamentul normal al politicii de parolă pentru intrări specifice, modificând atributele operaţionale ale politicii de parolă şi folosind controlul de administrare server (opţiunea -k a utilitarelor de linie de comandă LDAP).

1. Puteţi împiedica expirarea parolei unui anumit cont prin setarea atributului pwdChangedTime la o dată îndepărtată când configuraţi atributul userPassword. Următorul exemplu setează ora la miezul nopţii, 1 ianuarie 2200.

   ```
   > ldapmodify -D cn=root -w ? -k
   dn: uid=wasadmin,cn=users,o=ibm
   changetype: modify
   replace: pwdChangedTime
   pwdChangedTime: 22000101000000Z
   ```

2. Puteţi debloca un cont care a fost blocat datorită unor eşuări excesive ale înregistrării prin înlăturarea atributelor pwdAccountLockedTime şi pwdFailureTime:

   ```
   > ldapmodify -D cn=root -w ? -k
   dn: uid=user1,cn=users,o=ibm
   changetype: modify
   delete: pwdAccountLockedTime
   -
   delete: pwdFailureTime
   ```

3. Puteţi debloca un cont expirat prin modificarea pwdChangedTime şi ştergând atributele pwdExpirationWarned şipwdGraceUseTime:

   ```
   > ldapmodify -D cn=root -w ? -k
   dn: uid=user1,cn=users,o=ibm
   changetype: modify
   replace: pwdChangedTime
   pwdChangedTime: 20040826000000Z
   -
   delete: pwdExpirationWarned
   -
   delete: pwdGraceUseTime
   ```

4. Puteţi înlătura sau seta starea ″parola trebuie schimbată″ prin setarea atributului pwdReset:

   ```
   > ldapmodify -D cn=root -w ? -k
   dn: uid=user1,cn=users,o=ibm
   changetype: modify
   delete: pwdReset

   > ldapmodify -D cn=root -w ? -k
   dn: uid=user2,cn=users,o=ibm
   changetype: modify
   replace: pwdReset
   pwdReset: TRUE
   ```

5. Un cont poate fi blocat administrativ prin setarea atributului operaţional ibm-pwdAccountLocked la TRUE.

   Setarea utilizator pe care acest atribut trebuie să aibă permisiunea de a o scrie este atributul ibm-pwdAccountLocked, care este definit ca aflându-se în clasa de acces CRITICAL.

   ```
   > ldapmodify -D uid=useradmin,cn=users,o=ibm -w ?
   dn: uid=user1,cn=users,o=ibm
   changetype: modify
   replace: ibm-pwdAccountLocked
   ibm-pwdAccountLocked: TRUE
   ```

6. Contul poate fi deblocat prin setarea atributului la FALSE. Deblocarea unui cont în acest mod nu afectează starea contului, în ceea ce priveşte blocarea datorată unor eşuări excesive ale parolei sau unei parole expirate.

   Setarea utilizator pe care acest atribut trebuie să aibă permisiunea de a o scrie este atributul ibm-pwdAccountLocked, care este definit ca aflându-se în clasa de acces CRITICAL.

```
> ldapmodify -D uid=useradmin,cn=users,o=ibm -w ?
dn: uid=user1,cn=users,o=ibm
changetype: modify
replace: ibm-pwdAccountLocked
ibm-pwdAccountLocked: FALSE
```

Activarea SSL şi Transport Layer Security pe Directory Server

Folosiţi aceste informaţii pentru a activa SSL şi Transport Layer Security pentru Directory Server.

Dacă aveţi instalat Digital Certificate Manager pe sistem, puteţi folosi securitatea SSL (Secure Sockets Layer) pentru a proteja accesul la Directory Server. Înainte să activaţi SSL pe Directory Server, poate fi util să citiţi subiectul SSL şi TLS cu Directory Server.

Pentru a activa SSL pe serverul LDAP, faceţi următoarele:

1. **Asociaţi un certificat cu Directory Server**
   a. Dacă veţi să gestionaţi Directory Server printr-o conexiune SSL de la Navigator System i, vedeţi *Ghidul utilizatorului System i Access pentru Windows* (este opţional instalat pe PC-ul dumneavoastră când instalaţi Navigator System i). Dacă planificaţi să permiteţi ambele conexiuni SSL şi non-SSL în serverul de director, puteţi alege să săriţi acest pas.
   b. Porniţi IBM Digital Certificate Manager. Vedeţi Pornire Digital Certificate Manager din subiectul Digital Certificate Manager pentru mai multe informaţii.
   c. Dacă aveţi nevoie să obţineţi sau să creaţi certificate sau altfel să setaţi sau să modificaţi sistemul dumneavoastră de certificare, faceţi asta acum. Vedeţi Digital Certificate Manager pentru informaţii despre setarea unui sistem de certificate. Sunt două aplicaţii server şi o aplicaţie client asociate cu Directory Server. Acestea sunt:

      Aplicaţia Directory Server
      Aplicaţia Directory Server este serverul însuşi.

      Aplicaţia de publicare Directory Server
      Aplicaţia de publicare Directory Server identifică certificatul folosit prin publicare.

      Aplicaţia client Directory Server
      Aplicaţia client Directory Server identifică certificatul implicit folosit de aplicaţiile care folosesc API-urile ILE client LDAP.
   d. Apăsaţi **Selectare depozit de certificate**.
   e. Selectaţi ***SYSTEM**. Selectaţi **Continuare**.
   f. Introduceţi parola corespunzătoare pentru depozitul de certificate *SYSTEM. Selectaţi **Continuare**.
   g. Când meniul de navigare din stânga se reîncarcă, expandaţi **Gestiune aplicaţii**.
   h. Apăsaţi **Actualizare asignare certificat**.
   i. În ecranul următor, selectaţi aplicaţia **Server**. Selectaţi **Continuare**.
   j. Selectaţi **serverul de director**.
   k. Apăsaţi **Actualizare asignare certificat** pentru a asigna un certificat la Directory Server ca să îl folosească pentru a stabili identitatea sa către clienţii System i Access pentru Windows.

      Notă: Dacă alegeţi un certificat de la o CA ale cărei certificate CA nu este în baza de date de chei a clientului dvs. System i Access pentru Windows, va trebui să o adăugaţi pentru a putea folosi SSL. Terminaţi această procedură înainte de a o începe pe aceea.
   l. Selectaţi un certificat din listă pentru a îl asigna la server.
   m. Apăsaţi **Asignare certificat nou**.
   n. DCM se reîncarcă în pagina **Actualizare asignare certificat** cu un mesaj de confirmare. Când aţi terminat să setaţi certificatele pentru Directory Server, apăsaţi **Gata**.
2. Opţional: **Asociaţi un certificat pentru publicarea Directory Server**. Dacă de asemenea vreţi să activaţi publicarea de la sistem la un server de director printr-o conexiune SSL, s-ar putea să vreţi de asemenea să asociaţi

un certificat cu publicarea serverului de director. Aceasta identifică certificatul implicit şi CA-urile de încredere pentru aplicaţiile care folosesc API-urile ILE LDAP care nu specifică propriul ID aplicaţie sau o altă bază de date de chei.

a. Porniţi IBM Digital Certificate Manager.
b. Apăsaţi **Selectare depozit de certificate**.
c. Selectaţi ***SYSTEM**. Selectaţi **Continuare**.
d. Introduceţi parola corespunzătoare pentru depozitul de certificate *SYSTEM. Selectaţi **Continuare**.
e. Când meniul de navigare din stânga se reîncarcă, expandaţi **Gestiune aplicaţii**.
f. Apăsaţi **Actualizare asignare certificat**.
g. În ecranul următor, selectaţi aplicaţia **Client**. Selectaţi **Continuare**.
h. Selectaţi **Publicare Directory Server**.
i. Apăsaţi **Actualizare asignare certificat** pentru a asigna un certificat la publicarea Directory Server care îşi va stabili identitatea.
j. Selectaţi un certificat din listă pentru a îl asigna la server.
k. Apăsaţi **Asignare certificat nou**.
l. DCM se reîncarcă în pagina **Actualizare asignare certificat** cu un mesaj de confirmare.

Notă: Aceşti paşi presupun că publicaţi deja informaţii la Directory Server cu o conexiune non-SSL. Vedeţi "Publicarea informaţiilor Directory Server" la pagina 124 pentru informaţii complete despre setarea unei publicări.

3. Opţional: **Asocierea unui certificat pentru clientul Directory Server**. Dacă aveţi alte aplicaţii care utilizează conexiuni SSL la un server de director, trebuie de asemenea să asociaţi un certificat cu un client al serverului de director.
   a. Porniţi IBM Digital Certificate Manager.
   b. Apăsaţi **Selectare depozit de certificate**.
   c. Selectaţi ***SYSTEM**. Selectaţi **Continuare**.
   d. Introduceţi parola corespunzătoare pentru depozitul de certificate *SYSTEM. Selectaţi **Continuare**.
   e. Când meniul de navigare din stânga se reîncarcă, expandaţi **Gestiune aplicaţii**.
   f. Apăsaţi **Actualizare asignare certificat**.
   g. În ecranul următor, selectaţi aplicaţia **Client**. Selectaţi **Continuare**.
   h. Selectaţi **Clientul Directory Server**.
   i. Apăsaţi **Actualizare asignare certificat** pentru a asigna un certificat pentru clientul Directory Server care îşi va stabili identitatea.
   j. Selectaţi un certificat din listă pentru a îl asigna la server.
   k. Apăsaţi **Asignare certificat nou**.
   l. DCM se reîncarcă în pagina **Actualizare asignare certificat** cu un mesaj de confirmare.

După ce SSL este activat, puteţi schimba portul pe care îl foloseşte Directory Server pentru conexiuni securizate.

Pentru a utiliza SSL sau TLS, trebuie să le activaţi în Navigator System i.

1. În Navigator System i, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Faceţi clic dreapta pe **Director** şi selectaţi **Proprietăţi**.
4. Pe fişa **Reţea**, verificaţi caseta de bifare de lângă **Securizare**.

   Puteţi de asemenea să specificaţi numărul portului pe care doriţi să îl securizaţi. Apăsarea casetei de bifare **Securizare** este o indicaţie că o aplicaţie poate porni o conexiune SSL sau TLS peste portul securizat. De asemenea, este o indicaţie că o aplicaţie poate lansa o operaţie StartTLS pentru a permite o conexiune TLS peste

portul nesecurizat. Sau poate fi invocat TLS folosind opţiunea -Y într-un utilitar pentru linia de comandă de pe client. Dacă folosiţi linia de comandă, atributul ibm-slapdSecurity trebuie să fie egal cu TLS sau SSLTLS.

Concepte înrudite

"SSL (Secure Sockets Layer) şi TLS (Transport Layer Security) cu Directory Server" la pagina 52
Pentru comunicarea mai sigură cu Directory Server, se poate folosi securitatea SSL şi TLS.

Activarea autentificării Kerberos pentru Directory Server

Folosiţi aceste informaţii pentru a activa autentificarea Kerberos pe Directory Server.

Dacă aveţi Network Authentication Service configurat pe sistemul dvs., puteţi seta Directory Server să folosească autentificarea Kerberos. Autentificarea Kerberos se aplică la utilizatori şi la administrator. Înainte de a activa Kerberos pe serverul de director, s-ar putea să vi se pară util să citiţi o privire generală despre utilizazrea Kerberos cu Serverul de director.

Pentru a activa autentificarea Kerberos, urmaţi aceşti paşi:

1. În Navigator System i, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. Faceţi clic pe **TCP/IP**.
4. Faceţi clic dreapta pe **IBM Directory Server** şi selectaţi**Proprietăţi**.
5. Faceţi clic pe fişa **Kerberos**.
6. Bifaţi **Activare autentificare Kerberos** .
7. Specificaţi alte setări din pagina **Kerberos** corespunzător cu situaţia dumneavoastră. Vedeţi ajutorul online al paginii pentru informaţii despre câmpurile individuale.

Referinţe înrudite

"Autentificarea" la pagina 79
Folosiţi o metodă de autentificare pentru a controla accesul la Directory Server.

Configurarea autentificării DIGEST-MD5 pe Directory Server

Folosiţi aceste informaţii epntru a configura autentificarea DIGEST-MD5 pe Directory Server.

DIGEST-MD5 este un mecanism de autentificare SASL. Când un client foloseşte DIGEST-MD5, parola nu este transmisă în text clar şi protocolul împiedică atacurile prin redare. Unealta de administrare Web este folosită pentru a configura DIGEST-MD5.

1. Sub **Administrare server**, expandaţi categoria **Gestionare proprietăţi de securitate** din zona de navigare şi selectaţi fişa **DIGEST-MD5**.

   Notă: Pentru a modifica setările configuraţiei serverului utilizând taskurile de administrare server a uneltei de administrare web, trebuie să vă autentificaţi la server ca profil utilizator i5/OS care are auto rizări speciale *ALLOBJ şi IOSYSCFG. Aceasta se poate realiza prin autentificarea ca utilizator proiectat cu parola pentru acel profil. Pentru a vă lega ca utilizator proiectat din unealta de administrare Web, introduceţi un numeutilizator de forma os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, unde şirurile MYUSERNAME şi MYSYSTEM.COM sunt înlocuite cu numele profilului dumneavoastră de utilizator, respectiv cu sufixul de proiectare al sistemului configurat.
2. Sub **Regiune server**, utilizaţi setarea preselectată **Implicit**, care este numele gazdă complet calificat al serverului sau puteţi apăsa **Regiune** şi să introduceţi numele regiunii sub care doriţi să configuraţi serverul. Acest nume de regiune este utilizat de client pentru a determina ce nume utilizator şi parolă să folosiţi. Când folosiţi replicarea, este de dorit să aveţi toate serverele configurate cu aceeaşi regiune.
3. Sub atributul **Username**, folosiţi setarea preselectată **Implicit**, care este uid, sau puteţi apăsa **Atribut** şi să introduceţi numele atributului pe care doriţi ca serverul să-l folosească pentru a identifica în mod unic intrarea utilizator în timpul legărilor SASL DIGEST-MD5.

4. Dacă sunteţi logat ca administrator director, sub **Username administrator**, introduceţi username-ul administratorului. Acest câmp nu poate fi editat de membrii grupului administrativ. Dacă username-ul specificat în asocierea SASL DIGEST-MD5 se potriveşte cu acest şir, utilizatorul este administrator.

   Notă: Username-ul administratorului este sensibil la majuscule.
5. Când terminaţi, apăsaţi **OK**.

Referinţe înrudite

"Autentificarea" la pagina 79
Folosiţi o metodă de autentificare pentru a controla accesul la Directory Server.

Taskuri de schemă

Folosiţi aceste informaţii pentru a gestiona schema.

Schema poate fi gestionată folosind unealta de administrare prin web sau o aplicaţie LDAP precum ldapmodify în combinaţie cu fişierele LDIF. Când definiţi pentru prima dată noi clase obiect sau atribute, ar putea fi preferabil să folosiţi unealta de administrare Web. Dacă este necesar să copiaţi noua schemă pe alte servere (poate ca parte a implementării unui produs sau unelte), ar putea fi mai bine să folosiţi utilitarul ldapmodify; vedeţi "Copierea schemei la alte servere" la pagina 184 pentru informaţii suplimentare.

Concepte înrudite

"Sufixul (contextul de numire)" la pagina 12
Un sufix (numit şi context de numire) este un DN care identifică cea mai de sus intrare dintr-o ierarhie de director păstrată local.

"Schema" la pagina 14
O schemă este un set de reguli care controlează modalitatea prin care datele pot fi stocate în director. Schema defineşte tipul de intrări permise, structura atributelor lor şi sintaxa atributelor.

Vizualizarea claselor de obiecte

Folosiţi aceste informaţii pentru a vizualiza clasele de obiecte.

Puteţi vizualiza clasele de obiecte în schemă utilizând fie unealta de administrare web sau utilizând linia de comandă.

1. Expandaţi **Gestionare schemă** în zona de navigare şi apăsaţi pe **Gestionare clase de obiecte**. Este afişat un panou numai citire care vă permite să vedeţi clasele de obiecte din schemă şi caracteristicile lor. Clasele de obiecte sunt afişate în ordine alfabetică. Vă puteţi deplasa o pagină înapoi sau înainte apăsând pe Anterior sau Următor. Câmpul de lângă aceste butoane identifică pagina la care sunteţi. Puteţi de asemenea folosi meniul derulant al acestui câmp pentru a sări la o anumită pagină. Prima clasă de obiecte listată pe pagină este afişată cu numărul de pagină pentru a vă ajuta să localizaţi clasa de obiecte pe care vreţi să o vizualizaţi. De exemplu, dacă vreţi să căutaţi clasa de obiecte **person**, expandaţi meniul derulant şi căutaţi în jos până vedeţi **Page 14 of 16 nsLiServer** şi **Page 15 of 16 printerLPR**. Deoarece person se află alfabetic între nsLiServer şi printerLPR, selectaţi Page 14 şi apăsaţi **start**.

   Puteţi de asemenea afişa clasele de obiecte sortate după tip. Selectaţi **Tip** şi apăsaţi **Sortare**. Clasele de obiecte sunt sortate alfabetic în interiorul tipului lor, Abstract, Auxiliar sau Structural. Similar, puteţi inversa ordinea listei prin selectarea **Descendent** şi apăsarea pe **Sortare**.
2. După ce aţi localizat clasa de obiect pe care o vreţi, puteţi să îi vedeţi tipul, moştenirea, atributele necesare şi atributele opţionale. Expandaţi meniurile derulante pentru moştenire, atribute necesare şi atribute opţionale pentru a vedea listingurile complete pentru fiecare caracteristică. Puteţi alege operaţiile de clase de obiecte pe care vreţi să le efectuaţi din bara de unelte din partea dreaptă, precum:
   - Add - Adăugare
   - Editare
   - Copiere
   - Ştergere
3. Când aţi terminat, apăsaţi **Închidere** pentru a reveni la panoul IBM Directory Server **Bun venit**.

Pentru a vizualiza clasele de obiecte în schemă utilizând linia de comandă, introduceţi:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Adăugarea unei clase de obiecte

Folosiţi aceste informaţii pentru a adăuga o clasă de obiecte.

Dacă nu aţi făcut asta deja, expandaţi **Gestionare schemă** în zona de navigare, apoi apăsaţi pe **Gestionare clase obiect**. Pentru a crea o nouă clasă obiect:

1. Selectaţi **Adăugare**.

   Notă: De asemnea puteţi accesa acest panou prin expandara **Gestionare schemă** în zona de navigare, apoi apăsaţi pe **Adăugare clasă de obiecte**.
2. În fişa **Proprietăţi generale**:
   - Introduceţi **Nume clasă obiect**. Acesta este un câmp obligatoriu şi este descriptiv pentru funcţia clasei de obiecte. De exemplu, **tempEmployee** pentru o clasă de obiect folosită pentru urmări angajaţii temporari.
   - Introduceţi o **Descriere** a clasei de obiecte, de exemplu **Clasa de obiecte folosită pentru angajaţi temporari**.
   - Introduceţi **OID** pentru clasa de obiecte. Acesta este un câmp obligatoriu. Consultaţi “Identificatorul de obiect (OID)” la pagina 25. Dacă nu aveţi un OID, puteţi folosi **Nume clasă obiect** ataşat cu **-oid**. De exemplu, dacă numele clasei de obiect este **tempEmployee**, atunci OID este **tempEmployee-oid**. Puteţi schimba valoarea acestui câmp.
   - Selectaţi o **Clasă superioară de obiecte** din lista derulantă. Aceasta determină clasa de obiecte din care sunt moştenite atributele. În mod normal, **Clasa superioară de obiecte** este **top**, totuşi, ea poate fi altă clasă de obiecte. De exemplu, o clasă superioară de obiecte pentru **tempEmployee** ar putea fi **ePerson**.
   - Selectaţi un **Tip clasă de obiect**. Vedeţi “Clasele de obiecte” la pagina 17 pentru informaţii suplimentare despre tipurile de clase de obiecte.
   - Apăsaţi pe fişa Atribute pentru a specifica atributele obligatorii şi cele opţionale pentru clasa de obiecte şi pentru a vizualiza atributele moştenite sau apăsaţi **OK** pentru a adăuga noua clasă de obiecte sau apăsaţi **Anulare** pentru a reveni la **Gestionare clase de obiecte** fără a face vreo schimbare.
3. În fişa **Atribute**:
   - Selectaţi un atribut din lista alfabetică de **Atribute disponibile** şi apăsaţi **Adăugare la obligatorii** pentru a face atributul obligatoriu sau apăsaţi **Adăugare la opţionale** pentru a face atributul opţional pentru clasa de obiecte. Atributul este afişat în lista corespunzătoare de atribute selectate.
   - Repetaţi acest proces pentru toate atributele pe care vreţi să le selectaţi.
   - Puteţi muta un atribut de la o listă la alta sau să ştergeţi atributul din listele selectate prin selectarea lui şi apăsarea pe butonul corespunzător **Mutare la** sau **Ştergere**.
   - Puteţi vedea lista de atribute obligatorii şi opţionale moştenite. Atributele moştenite se bazează pe **Clasa superioară de obiecte** selectată în fişa **General**. Nu puteţi schimba atributele moştenite. Totuşi, dacă schimbaţi **Clasa superioară de obiecte** din fişa **General**, este afişat un alt set de atribute moştenite.
4. Apăsaţi **OK** pentru a adăuga noua clasă de obiecte sau apăsaţi **Anulare** pentru a reveni la **Gestionare clase de obiecte** fără a face vreo modificare.

Notă: Dacă aţi apăsat **OK** în fişa **General** fără a adăuga vreun atribut, puteţi adăuga atribute prin editarea noii clase de obiecte.

Pentru a adăuga o clasă de obiecte folosind linia de comandă, lansaţi comanda următoare:

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

unde <*filename*>conţine:

```
dn: cn=Schema
changetype: modify
add: objectclasses
objectclasses: ( <myobjectClass-oid> NAME '<myObjectClass>' DESC '<O clasă de obiecte
                Am definit pentru aplicaţia mea LDAP >' SUP '<objectclassinheritance>'
                <objectclasstype> MAY (<attribute1> $ <attribute2>))
```

Editarea unei clase de obiecte

Folosiţi aceste informaţii pentru a edita o clasă de obiecte.

Nu sunt permise toate modificările de schemă. Vedeţi “Modificări de schemă nepermise” la pagina 28 pentru restricţii de modificare.

Dacă nu aţi făcut asta deja, expandaţi **Gestionare schemă** în zona de navigare, apoi apăsaţi pe **Gestionare clase obiect**. Pentru a edita o clasă de obiecte:

1. Apăsaţi butonul radio de lângă clasa de obiecte pe care vreţi să o editaţi.
2. Faceţi clic pe **Editare**.
3. Selectaţi o fişă:
   - Folosiţi fişa **General** pentru:
     - Modificaţi **Descrierea**.
     - Modificaţi **Clasă superioară de obiecte**. Selectaţi o clasă superioară de obiecte din lista derulantă. Aceasta determină clasa de obiecte din care sunt moştenite atributele. În mod normal, **Clasa superioară de obiecte** este **top**, totuşi, ea poate fi altă clasă de obiecte. De exemplu, o clasă superioară de obiecte pentru **tempEmployee** ar putea fi **ePerson**.
     - Modificaţi **Tipul clasei de obiecte**. Selectaţi un tip de clasă de obiecte. Vedeţi “Clasele de obiecte” la pagina 17 pentru informaţii suplimentare despre tipurile de clase de obiecte.
     - Apăsaţi pe fişa Atribute pentru a modifica atributele obligatorii şi cele opţionale pentru clasa de obiecte şi pentru a vizualiza atributele moştenite sau apăsaţi **OK** pentru a aplica modificările sau apăsaţi **Anulare** pentru a reveni la **Gestionare clase de obiecte** fără a face vreo schimbare.
   - Folosiţi fişa **Atribute** pentru :

     Selectaţi un atribut din lista alfabetică de **Atribute disponibile** şi apăsaţi **Adăugare la obligatorii** pentru a face atributul obligatoriu sau apăsaţi **Adăugare la opţionale** pentru a face atributul opţional pentru clasa de obiecte. Atributul este afişat în lista corespunzătoare de atribute selectate.

     Repetaţi acest proces pentru toate atributele pe care vreţi să le selectaţi.

     Puteţi muta un atribut de la o listă la alta sau să ştergeţi atributul din listele selectate prin selectarea lui şi apăsarea pe butonul corespunzător **Mutare la** sau **Ştergere**.

     Puteţi vedea lista de atribute obligatorii şi opţionale moştenite. Atributele moştenite se bazează pe **Clasa superioară de obiecte** selectată în fişa **General**. Nu puteţi schimba atributele moştenite. Totuşi, dacă schimbaţi **Clasa superioară de obiecte** din fişa **General**, este afişat un alt set de atribute moştenite.
4. Apăsaţi **OK** pentru a aplica modificările sau apăsaţi **Anulare** pentru a reveni la **Gestionare clase de obiecte** fără a face vreo schimbare.

Pentru a vizualiza clasele de obiecte conţinute în schemă utilizând linia de comandă, emiteţi următoarea comandă:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Pentru a edita o clasă de obiecte folosind linia de comandă, lansaţi comanda următoare:

```
ldapmodify -D <adminDN> -w <adminPW> -i <nume fişier>
```

unde <*nume fişier* >conţine:

```
dn: cn=schema
changetype: modify
replace: objectclasses
objectclasses: ( <myobjectClass-oid> NUME '<myObjectClass>' DESC '<O clasă de obiecte
                 Pe care am definit-o pentru aplicaţia LDAP a mea>' SUP '<newsuperiorclassobject>'
                 <newobjectclasstype> MAY (atribut1> $ <atribut2>
                  $ <nouatribut3>) )
```

Copierea unei clase de obiecte

Folosiţi aceste informaţii pentru a copia o clasă de obiecte.

Dacă nu aţi făcut asta deja, expandaţi **Gestionare schemă** în zona de navigare, apoi apăsaţi pe **Gestionare clase obiect**. Pentru a copia o clasă de obiecte:

1. Apăsaţi butonul radio de lângă clasa de obiecte pe care vreţi să o copiaţi.
2. Faceţi clic pe **Copiere**.
3. Selectaţi o fişă:
   - Folosiţi fişa **General** pentru:
     - Modificaţi **numele clasei de obiecte**. Numele implicit este numele clasei de obiecte copiate ataşat cu cuvântul COPY. De exemplu, **tempPerson** este copiat ca **tempPersonCOPY**.
     - Modificaţi **Descrierea**.
     - Modificaţi **OID-ul**. OID-ul implicit este OID-ul clasei de obiecte copiate ataşat cu cuvântul COPY. De exemplu, **tempPerson-oid** este copiat ca **tempPerson-oidCOPY** .
     - Modificaţi **Clasă superioară de obiecte**. Selectaţi o clasă superioară de obiecte din lista derulantă. Aceasta determină clasa de obiecte din care sunt moştenite atributele. În mod normal, **Clasa superioară de obiecte** este **top**, totuşi, ea poate fi altă clasă de obiecte. De exemplu, o clasă superioară de obiecte pentru **tempEmployeeCOPY** ar putea fi **ePerson**.
     - Modificaţi **Tipul clasei de obiecte**. Selectaţi un tip de clasă de obiecte. Vedeţi “Clasele de obiecte” la pagina 17 pentru informaţii suplimentare despre tipurile de clase de obiecte.
     - Apăsaţi pe fişa **Atribute** pentru a modifica atributele obligatorii şi cele opţionale pentru clasa de obiecte şi pentru a vizualiza atributele moştenite sau apăsaţi **OK** pentru a aplica modificările sau apăsaţi **Anulare** pentru a reveni la **Gestionare clase de obiecte** fără a face vreo schimbare.
   - Folosiţi fişa **Atribute** pentru :

     Selectaţi un atribut din lista alfabetică de **Atribute disponibile** şi apăsaţi **Adăugare la obligatorii** pentru a face atributul obligatoriu sau apăsaţi **Adăugare la opţionale** pentru a face atributul opţional pentru clasa de obiecte. Atributul este afişat în lista corespunzătoare de atribute selectate.

     Repetaţi acest proces pentru toate atributele pe care vreţi să le selectaţi.

     Puteţi muta un atribut de la o listă la alta sau să ştergeţi atributul din listele selectate prin selectarea lui şi apăsarea pe butonul corespunzător **Mutare la** sau **Ştergere**.

     Puteţi vedea lista de atribute obligatorii şi opţionale moştenite. Atributele moştenite se bazează pe **Clasa superioară de obiecte** selectată în fişa **General**. Nu puteţi schimba atributele moştenite. Totuşi, dacă schimbaţi **Clasa superioară de obiecte** din fişa **General**, este afişat un alt set de atribute moştenite.
4. Apăsaţi **OK** pentru a aplica modificările sau apăsaţi **Anulare** pentru a reveni la **Gestionare clase de obiecte** fără a face vreo schimbare.

Pentru a vizualiza clasa de obiecte conţinută în schemă utilizând linia de comandă, lansaţi comanda:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Selectaţi clasa de obiecte pe care vreţi să o copiaţi. Folosiţi un editor pentru a modifica informaţiile corespunzătoare şi să salvaţi modificările la <*filename*>. Lansaţi următoarea comandă:

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

unde <*filename*>conţine:

```
dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: ( <mynewobjectClass-oid> NAME '<mynewObjectClass>'
                 DESC '<A new object class
                   Am copiat pentru aplicaţia mea LDAP >'
                SUP '<superiorclassobject>'<objectclasstype> MAY (attribute1>
                $ <attribute2> $ <attribute3>) )
```

Ştergerea unei clase de obiecte

Folosiţi aceste informaţii pentru a şterge o clasă de obiecte.

Nu sunt permise toate modificările de schemă. Vedeţi “Modificări de schemă nepermise” la pagina 28 pentru restricţii de modificare.

Dacă nu aţi făcut asta deja, expandaţi **Gestionare schemă** în zona de navigare, apoi apăsaţi pe **Gestionare clase obiect**. Pentru a şterge o clasă de obiecte:

1. Apăsaţi butonul radio de lângă clasa de obiecte pe care vreţi să o ştergeţi.
2. Faceţi clic pe **Ştergere**
3. Vi se va cere să confirmaţi ştergerea clasei de obiecte. Apăsaţi **OK** pentru a şterge clasa de obiecte sau apăsaţi **Anulare** pentru a reveni la **Gestionare clase de obiecte** fără a face vreo modificare.

Vizualizaţi clasele de obiecte conţinute în schemă lansând comanda:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Selectaţi clasa de obiecte pe care vreţi să o ştergeţi şi lansaţi următoarea comandă:

```
ldapmodify -D <adminDN> -w <adminPW> -i <nume fişier>
```

unde <*filename*>conţine:

```
dn: cn=schema
changetype: modify
delete: objectclasses
objectclasses: (<myobjectClass-oid>)
```

Vizualizarea atributelor

Folosiţi aceste informaţii pentru a vizualiza un atribut.

Puteţi vizualiza atributele din schemă folosind ori unealta de administrare web, metoda preferată sau folosind linia de comandă.

1. Expandaţi **Gestionare schemă** în zona de navigare şi apăsaţi pe **Gestionare atribute**.

   Este afişat un panou numai citire care vă permite să vedeţi atributele din schemă şi caracteristicile lor. Atributele sunt afişate în ordine alfabetică. Vă puteţi deplasa o pagină înapoi sau înainte apăsând pe Anterior sau Următor. Câmpul de lângă aceste butoane identifică pagina la care sunteţi. Puteţi de asemenea folosi meniul derulant al acestui câmp pentru a sări la o anumită pagină. Prima clasă de obiecte listată pe pagină este afişată cu numărul de pagină pentru a vă ajuta să localizaţi clasa de obiecte pe care vreţi să o vizualizaţi. De exemplu, dacă aţi căutat atributul **authenticationUserID**, expandaţi meniul derulant şi derulaţi în jos până când vedeţi **Pagina 3 din 62 applSystemHint** şi **Pagina 4 din 62 authorityRevocatonList**. Deoarece authenticationUserID se află alfabetic între applSystemHint şi authorityRevocatonList, selectaţi Page 3 şi apăsaţi **start**.

   Puteţi de asemenea afişa atributele sortate după sintaxă. Selectaţi **Sintaxă** şi apăsaţi **Sortare**. Atributele sunt sortate alfabetic în cadrul sintaxei lor. Vedeţi “Sintaxă atribut” la pagina 23 pentru o listă a tipurilor de sintaxă. Similar, puteţi inversa ordinea listei prin selectarea **Descendent** şi apăsarea pe **Sortare**.

   După ce aţi localizat atributul dorit, puteţi să îi vedeţi sintaxa, dacă este multi-valoare şi clasa de obiecte care îl conţine. Expandaţi meniul derulant pentru clasele de obiect pentru a vedea lista de clase de obiect pentru atribut.
2. Când aţi terminat, apăsaţi **Închidere** pentru a reveni la panoul IBM Directory Server **Bun venit**.

Pentru a vizualiza atributele conţinute în schemă, lansaţi comanda:

```
ldapsearch -b cn=schema -s base objectclass=* attributeTypes
IBMAttributeTypes
```

Adăugarea unui atribut

Folosiţi aceaste informaţii pentru a adăuga un atribut.

Folosiţi una din următoarele metode pentru a crea un atribut. Unealta de administrare web este metoda preferată.

Dacă nu aţi făcut asta deja, expandaţi **Gestionare schemă** în zona de navigare, apoi apăsaţi pe **Gestionare atribute**. Pentru a crea un nou atribut:

1. Selectaţi **Adăugare**.

   Notă: De asemnea puteţi accesa acest panou prin expandara **Gestionare schemă** în zona de navigare, apoi apăsaţi pe **Adăugare atribut**.
2. Introduceţi **Nume atribut**, spre exemplu, **tempId**. Acesta este un câmp obligatoriu şi trebuie să înceapă cu un caracter alfabetic.
3. Introduceţi o **Descriere** a atributului, de exemplu **Numărul ID asignat unui angajat temporar**.
4. Introduceţi **OID** pentru atribut. Acesta este un câmp obligatoriu. Consultaţi “Identificatorul de obiect (OID)” la pagina 25. Dacă nu aveţi un OID, puteţi folosi numele atributului ataşat cu -oid. De exemplu, dacă numele atributului este **tempID**, atunci OIDul implicit este **tempID-oid**. Puteţi schimba valoarea acestui câmp.
5. Selectaţi o **Atribut superior** din lista derulantă. Atributul superior determină atributul din care sunt moştenite proprietăţile.
6. Selectaţi o **Sintaxă** din lista derulantă. Vedeţi “Sintaxă atribut” la pagina 23 pentru informaţii suplimentare despre sintaxă.
7. Introduceţi **Lungime atribut** care specifică lungimea maximă a acestui atribut. Lungimea este exprimată ca numărul de octeţi.
8. Selectaţi căsuţa de bifare **Permite valori multiple** pentru a permite ca atributul să aibă valori multiple.
9. Selectaţi o regulă corespunzătoare din fiecare din meniurile derulante pentru regulile de egalitate, ordonare şi asemănare subşir. Vedeţi “Reguli de potrivire” la pagina 21 pentru o listă completă de reguli de potrivire.
10. Faceţi clic pe fişa **Extensii IBM** pentru a specifica extensii suplimentare pentru atribut sau apăsaţi **OK** pentru a adăuga noul atribut sau apăsaţi **Anulare** pentru a reveni la **Gestionare atribute** fără a face vreo modificare.
11. În fişa **Extensii IBM**:
    - Modificaţi **numele tabelei DB2**. Serverul generează numele tabelei DB2 dacă acest câmp este lăsat neînscris. Dacă introduceţi un nume de tabelă DB2, trebuie de asemenea să introduceţi un nume coloană DB2.
    - Modificaţi **numele coloanei DB2**. Serverul generează un nume de coloană DB2 dacă acest câmp este lăsat neînscris. Dacă introduceţi un nume de coloană DB2, trebuie să introduceţi de asemenea un nume de tabelă DB2.
    - Setaţi **Clasă de securitate** selectând **normal**, **sensibil** sau **critic** din lista derulantă.
    - Setaţi **Reguli de indexare** selectând una din următoarele reguli de indexare. Vedeţi “Reguli de indexare” la pagina 22 pentru informaţii suplimentare despre reguli de indexrare.

      Notă: Ca minim, este recomandabil să specificaţi Indexare de egalitate pe orice atribut care va fi folosit în filtrele de căutare.
12. Faceţi clic pe **OK** pentru a adăuga noul atribut sau faceţi clic pe **Anulare** pentru a vă întoarce la **Gestionare atribute** fără să faceţi modificări.

Notă: Dacă aţi apăsat OK în fişa General fără a adăuga vreo extensie, puteţi adăuga extensii editând noul atribut.

Pentru a adăuga un atribut utilizând linia de comandă, lansaţi următoarea comandă. Următorul exemplu adaugă o definiţie de tip de atribut pentru un atribut numit ″myAttribute″, cu sintaxa Directory String (vedeţi “Sintaxă atribut” la pagina 23) şi Case Ignore Equality matching (vedeţi “Reguli de potrivire” la pagina 21). Partea specifică IBM a definiţiei spune că datele atributului sunt stocate într-o coloană denumită ″myAttrColumn″ dintr-o tabelă denumită ″myAttrTable″. Dacă aceste nume nu erau specificate, numele coloanei şi tabelei ar fi avut valoarea implicită ″myAttribute″. Atributul este asignat clasei de acces ″normal″ şi valorile au o lungime maximă de 200 octeţi.

```
ldapmodify -D <admindn> -w <adminpw> -i myschema.ldif
```

unde fişierul **myschema.ldif** conţine:

```
dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: ( myAttribute-oid NAME ( 'myAttribute' )
                 DESC 'An attribute I defined for my LDAP application'
                 EQUALITY 2.5.13.2 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
```

```
                USAGE userApplications )
-
add: ibmattributetypes
ibmattributetypes: ( myAttribute-oid  DBNAME ( 'myAttrTable' 'myAttrColumn' )
                    ACCESS-CLASS normal LENGTH 200 )
```

Editarea unui atribut

Folosiţi aceste informaţii pentru a edita un atribut.

Nu sunt permise toate modificările de schemă. Vedeţi “Modificări de schemă nepermise” la pagina 28 pentru restricţii de modificare.

Orice parte a definiţiei poate fi modificată înainte să adăugaţi intrări care folosesc atributul. Folosiţi una din următoarele metode pentru a edita un atribut. Unealta de administrare web este metoda preferată.

Dacă nu aţi făcut asta deja, expandaţi **Gestionare schemă** în zona de navigare, apoi apăsaţi pe **Gestionare atribute**. Pentru a edita un atribut:

1. Apăsaţi butonul radio de lângă atributul pe care vreţi să o editaţi.
2. Faceţi clic pe **Editare**.
3. Selectaţi o fişă:
   - Folosiţi fişa **General** pentru:
     – Selectaţi o fişă:
       - **General** pentru a:
         - Modificaţi **Descriere**
         - Modificaţi **Sintaxa**
         - Setaţi **Lungime atribut**
         - Schimbaţi setările **Valori multiple**
         - Selectaţi o **Regulă de potrivire**
         - Modificaţi **Atribut superior**
       - Apăsaţi pe fişa **Extensii IBM** pentru a edita extensiile pentru atribut sau apăsaţi**OK** pentru a aplica modificările sau apăsaţi **Anulare** pentru a reveni la **Gestionare atribute** fără a face vreo modificare.
       - **Extensii IBM**, dacă folosiţi IBM Directory Server, pentru:
         - Modificaţi **Clasă securizată**
         - Modificaţi **Reguli indexare**
     – Faceţi clic pe **OK** pentru a aplica modificările dumneavoastă sau faceţi clic pe**Anulare** pentru a vă întoarce la **Gestionare atribute** fără să faceţi nici o modificare.
4. Faceţi clic pe **OK** pentru a aplica modificările dumneavoastă sau faceţi clic pe**Anulare** pentru a vă întoarce la **Gestionare atribute** fără să faceţi nici o modificare.

Pentru a edita un atribut utilizând linia de comandă, emiteţi următoarea comandă. Acest exemplu adaugă indexarea atributului, astfel încât căutarea este mai rapidă. Folosiţi comanda ldapmodify şi fişierul LDIF pentru a modifica definiţia:

```
ldapmodify -D <admindn> -w <adminpw> -i myschemachange.ldif
```

unde fişierul **myschemachange.ldif** conţine:

```
dn: cn=schema
changetype: modify
replace: attributetypes
attributetypes: ( myAttribute-oid NAME ( 'myAttribute' ) DESC 'An attribute
                I defined for my LDAP application' EQUALITY 2.5.13.2
                SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications )
-
```

```
replace: ibmattributetypes
ibmattributetypes: ( myAttribute-oid  DBNAME ( 'myAttrTable' 'myAttrColumn' )
                   ACCESS-CLASS normal LENGTH 200 EQUALITY SUBSTR )
```

Notă: Ambele porţiuni ale definiţiei (**attributetypes** şi **ibmattributetypes**) trebuie să fie incluse în operaţia de înlocuire, chiar dacă se modifică doar secţiunea **ibmattributetypes**. Singura modificare este adăugarea ″EQUALITY SUBSTR″ la sfârşitul definiţiei pentru a cere indexarea pentru potrivirea de egalitate şi de subşir.

Copierea unui atribut

Folosiţi aceste informaţii pentru a copia un atribut.

Folosiţi una din următoarele metode pentru a copia un atribut. Unealta de administrare web este metoda preferată.

Dacă nu aţi făcut asta deja, expandaţi **Gestionare schemă** în zona de navigare, apoi apăsaţi pe **Gestionare atribute**. Pentru a copia un atribut:

1. Apăsaţi butonul radio de lângă atributul pe care vreţi să îl copiaţi.
2. Faceţi clic pe **Copiere**.
3. Modificaţi **Numele atributului**. Numele implicit este numele atributului copiat ataşat cu cuvântul COPY. De exemplu, **tempID** este copiat ca **tempIDCOPY** .
4. Modificaţi o **Descriere** a atributului, de exemplu, **Numărul ID-ului asignat unui angajat temporar**.
5. Modificaţi **OID-ul**. OID-ul implicit este OID-ul atributului copiat ataşat cu cuvântul COPYOID. De exemplu, **tempID-oid** este copiat ca **tempID-oidCOPYOID** .
6. Selectaţi o **Atribut superior** din lista derulantă. Atributul superior determină atributul din care sunt moştenite proprietăţile.
7. Selectaţi o **Sintaxă** din lista derulantă. Vedeţi “Sintaxă atribut” la pagina 23 pentru informaţii suplimentare despre sintaxă.
8. Introduceţi **Lungime atribut** care specifică lungimea maximă a acestui atribut. Lungimea este exprimată ca numărul de octeţi.
9. Selectaţi căsuţa de bifare **Permite valori multiple** pentru a permite ca atributul să aibă valori multiple.
10. Selectaţi o regulă corespunzătoare din fiecare din meniurile derulante pentru regulile de egalitate, ordonare şi asemănare subşir. Vedeţi “Reguli de potrivire” la pagina 21 pentru o listă completă de reguli de potrivire.
11. Apăsaţi pe fişa **Extensii IBM** pentru a modifica extensii suplimentare pentru atribut sau apăsaţi **OK** pentru a aplica schimbările sau apăsaţi **Anulare** pentru a reveni la **Gestionare atribute** fără a face vreo modificare.
12. În fişa **Extensii IBM**:
    - Modificaţi **numele tabelei DB2**. Serverul generează numele tabelei DB2 dacă acest câmp este lăsat neînscris. Dacă introduceţi un nume de tabelă DB2, trebuie de asemenea să introduceţi un nume coloană DB2.
    - Modificaţi **numele coloanei DB2**. Serverul generează un nume de coloană DB2 dacă acest câmp este lăsat neînscris. Dacă introduceţi un nume de coloană DB2, trebuie să introduceţi de asemenea un nume de tabelă DB2.
    - Modificaţi **Clasa de securitate**, selectând **normală**, **sensibilă** sau **critică** din lista derulantă.
    - Modificaţi **Regulile de indexare**, selectând una sau mai multe reguli de indexare. Vedeţi “Reguli de indexare” la pagina 22 pentru informaţii suplimentare despre reguli de indexrare.

      Notă: Ca minim, este recomandabil să specificaţi Indexare egală pe orice atribut care va fi folosit în filtrele de căutare.
13. Faceţi clic pe **OK** pentru a vă aplica modificările sau faceţi clic pe **Anulare** pentru a vă întoarce la **Gestionare atribute** fără să faceţi vreo modificare.

Notă: Dacă aţi apăsat **OK** pe fişa **General** fără a adăuga vreo extensie, puteţi adăuga sau modifica extensii editând noul atribut.

Pentru a vizualiza atributele conţinute în schemă, emiteţi comanda:

```
ldapsearch -b cn=schema -s base objectclass=* attributeTypes
IBMAttributeTypes
```

Selectaţi atributul pe care vreţi să o copiaţi. Folosiţi un editor pentru a modifica informaţiile corespunzătoare şi salvaţi modificările la <*filename*>. Apoi lansaţi următoarea comandă:

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

unde <*filename*>conţine:

```
dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: ( <mynewAttribute-oid> NAME '<mynewAttribute>' DESC '<Un nou
                 atribut pe care l-am copiat pentru aplicaţia mea LDAP > EQUALITY 2.5.13.2
                 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications )
-
add: ibmattributetypes
ibmattributetypes: ( myAttribute-oid  DBNAME ( 'myAttrTable' 'myAttrColumn' )
                    ACCESS-CLASS normal LENGTH 200 )
```

Ştergerea unui atribut

Folosiţi aceste informaţii prentru a şterge un atribut fin arborele directorului.

Nu sunt permise toate modificările de schemă. Vedeţi “Modificări de schemă nepermise” la pagina 28 pentru restricţii de modificare.

Folosiţi una din următoarele metode pentru a şterge un atribut. Unealta de administrare web este metoda preferată.

Dacă nu aţi făcut asta deja, expandaţi **Gestionare schemă** în zona de navigare, apoi apăsaţi pe **Gestionare atribute**. Pentru a şterge un atribut:

1. Apăsaţi butonul radio de lângă atributul pe care vreţi să îl ştergeţi.
2. Faceţi clic pe **Ştergere**
3. Vi se va cere să confirmaţi ştergerea atributului. Apăsaţi **OK** pentru a şterge atributul sau apăsaţi **Anulare** pentru a reveni la **Gestionare atribute** fără a face vreo schimbare.

Pentru a şterge un atribut utilizând linia de comandă, emiteţi următoarea comandă:

```
ldapmodify -D <admindn> -w <adminpw> -i myschemadelete.ldif
```

unde fişierul **myschemadelete.ldif** include:

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

Copierea schemei la alte servere

Folosiţi aceste informaţii pentru a copia schema la alte servere.

Pentru a copia o schemă la alte servere faceţi următoarele:

1. Folosiţi utilitarul ldapsearch pentru a copia schema într-un fişier:

   ```
   ldapsearch -b cn=schema -L "(objectclass=*)" > schema.ldif
   ```

2. Fişierul schemă va include toate clasele de obiecte şi atributele Editaţi fişierul LDIF pentru a include doar elementele de schemă pe care le vreţi sau veţi putea filtra ieşirea ldapsearch folosind o comandă precum grep. Asiguraţi-vă că aţi pus atributele înainte de objectclasses care le referă. De exemplu, aţi putea ajunge cu următorul fişier (ţineţi cont că fiecare linie continuată are un singur spaţiu la sfârşit şi linia de continuare are cel puţin un spaţiu la început).

```
attributetypes: ( myattr1-oid NAME 'myattr1' DESC 'Some piece of
  information.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
  USAGE userApplications )
IBMAttributetypes: ( myattr1-oid DBNAME( 'myattr1'  'myattr1' )
  ACCESS-CLASS normal LENGTH 500 )
attributetypes: ( myattr2-oid NAME 'myattr2' DESC 'Some piece of
  information.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
  USAGE userApplications )
IBMAttributetypes: ( myattr2-oid DBNAME( 'myattr2'  'myattr2' )
  ACCESS-CLASS normal LENGTH 500 )
objectclasses: ( myobject-oid NAME 'myobject' DESC 'Represents
  something.' SUP 'top' STRUCTURAL MUST ( cn ) MAY ( myattr1 $ myattr2 ) )
```

3. Inseraţi linii înaintea fiecărei linii objectclasses sau attributetype pentru a construi directive LDIF pentru a adăuga aceste valori la intrarea cn=schema. Fiecare clasă de obiect şi atribut trebuie să fie adăugat ca o modificare individuală.

```
dn: cn=schema
changetype: modify
add: attributetypes ibmattributetypes
attributetypes: ( myattr1-oid NAME 'myattr1' DESC 'Some piece of
  information.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
  USAGE userApplications )
IBMAttributetypes: ( myattr1-oid DBNAME( 'myattr1'  'myattr1' )
  ACCESS-CLASS normal LENGTH 500 )

dn: cn=schema
changetype: modify
add: attributetypes ibmattributetypes
attributetypes: ( myattr2-oid NAME 'myattr2' DESC 'Some piece of
  information.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
  USAGE userApplications )
IBMAttributetypes: ( myattr2-oid DBNAME( 'myattr2'  'myattr2' )
  ACCESS-CLASS normal LENGTH 500 )

dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: ( myobject-oid NAME 'myobject' DESC 'Represents
  something.' SUP 'top' STRUCTURAL MUST ( cn ) MAY ( myattr1 $ myattr2 ) )
```

4. Încărcaţi acea schemă pe alte servere folosind utilitarul ldapmodify:

```
ldapmodify -D cn=administrator -w <password> -f schema.ldif
```

Taskuri de intrări de director

Folosiţi aceste informaţii pentru a gestiona intrările directorului.

Pentru a gestiona intrările director, expandaţi categoria **Gestionare director** din zona de navigare a uneltei de administrare web.

Concepte înrudite

“Sufixul (contextul de numire)” la pagina 12
Un sufix (numit şi context de numire) este un DN care identifică cea mai de sus intrare dintr-o ierarhie de director păstrată local.

“Schema” la pagina 14
O schemă este un set de reguli care controlează modalitatea prin care datele pot fi stocate în director. Schema defineşte tipul de intrări permise, structura atributelor lor şi sintaxa atributelor.

“Drept de proprietate asupra obiectelor direcorului LDAP” la pagina 75
Fiecare obiect din directorul dumneavoastră LDAP are el puţin un proprietar. Proprietarii de obiecte au puterea de a şterge obiectul. Proprietarii şi administratorii de server sunt singurii utilizatori care pot modifica proprietăţile dreptului de proprietate şi lista de control acces (ACL) atributele unui obiect. Dreptul de proprietate a obiectelor poate fi moştenit sau explicit.

Răsfoirea arborelui de director

Folosiţi aceste informaţii pentru a răsfoi arborele directorului.

Aveţi nevoie să faceţi aceasta mai întâi.

Etapa trebuie să fie setată întocmai.

1. Dacă nu aţi făcut asta deja, expandaţi categoria **Gestionare director** din zona de navigare.
2. Apăsaţi **Gestionare intrări**.

Puteţi expanda diverşi subarbori şi selecta intrarea cu care vreţi să lucraţi. Puteţi alege operaţia pe care vreţi să o efectuaţi din bara de unelte din ăartea dreaptă.

Adăugarea unei intrări

Folosiţi aceste informaţii pentru a adăuga o intrare în arborele directorului.

1. Dacă nu aţi făcut asta deja, expandaţi categoria **Gestionare director** din zona de navigare.
2. Apăsaţi **Adăugare intrare**.
3. Selectaţi o **Clasă structurală de obiecte** din lista derulantă.
4. Apăsaţi **Următorul**.
5. Selectaţi orice **Clase de obiecte auxiliare** pe care vreţi să le folosiţi din căsuţa Disponibile şi apăsaţi **Adăugare**. Repetaţi acest proces pentru fiecare clasă de obiecte auxiliare pe care vreţi să o adăugaţi. Puteţi de asemenea şterge o clasă de obiecte auxiliară din căsuţa Selectate prin selectarea ei şi apăsarea pe **Ştergere**.
6. Apăsaţi **Următorul**.
7. În câmpul **DN relativ**, introduceţi DN-ul relativ (RDN) al intrării pe care o adăugaţi, de exemplu, cn=John Doe.
8. În câmpul **DN părinte**, introduceţi numele distinctiv al intrării arbore pe care aţi selectat-o, de exemplu ou=Austin, o=IBM. Puteţi de asemenea să apăsaţi pe **Răsfoire** pentru a selecta DN-ul părinte din listă. Puteţi de asemenea expanda selecţia pentru a vedea alte alegeri de mai jos din subarbore. Specificaţi alegerea dvs. şi apăsaţi **Selectare** pentru a specifica DN-ul părinte pe care îl vreţi. **DN-ul părinte** are valoare implicită intrarea selectată în arbore.

   Notă: Dacă aţi pornit acest task din panoul **Gestionare intrări**, acest câmp este precompletat.
9. În fişa **Atribute obligatorii** introduceţi valorile pentru atributele obligatorii. Dacă vreţi să adăugaţi mai mult de o valoare pentru un anumit atribut, apăsaţi **Valori multiple** şi apoi adăugaţi valorile pe rând.
10. Apăsaţi **Atribute opţionale**.
11. În fişa **Atribute opţionale** introduceţi valorile corespunzătoare pentru atributele opţionale. Vedeţi “Modificarea atributelor binare” la pagina 191 pentru informaţii despre adăugarea valorilor binare. Dacă vreţi să adăugaţi mai mult de o valoare pentru un anumit atribut, apăsaţi **Valori multiple** şi apoi adăugaţi valorile pe rând.
12. Apăsaţi OK pentru a crea intrarea.
13. Apăsaţi butonul **ACL** pentru a modifica lista de control acces pentru această intrare. Vedeţi “Listele de control al accesului” la pagina 63 pentru informaţii despre ACL-uri.
14. După ce aţi completat cel puţin câmpurile obligatorii, apăsaţi **Adăugare** pentru a adăuga noua intrare sau apăsaţi **Anulare** pentru a reveni la **Răsfoire arbore** fără a face vreo modificare la director.

Adăugarea unei intrări ce conţine atribute cu taguri de limbaj

Folosiţi aceste informaţii pentru a crea o intrare ce conţine atribute cu taguri de limbaj.

Pentru a crea o intrare ce conţine atribute cu taguri de limbă:

1. Activare taguri de limbaj. Vedeţi“Activarea tagurilor de limbă” la pagina 121.
2. Din categoria **Gestionare director** din zona de navigare, apăsaţi**Gestionare intrări**.
3. Faceţi clic pe butonul **Editate atribute**.
4. Selectaţi atributul pentru care creaţi tagul de limbă.
5. Faceţi clic pe butonul **Valoare tag limbă** pentru a accesa panoul **Valori tag limbă**.

6. În câmpul **Tag limbă**, introduceţi numele tagului pe care îl creaţi. Tagul trebuie să înceapă cu sufixul lang-.
7. Introduceţi valoarea pentru tag în câmpul **Valoare**.
8. Selectaţi **Adăugare**. Tagul de limbă şi valoarea sa sunt afişate în lista meniu.
9. Creaţi taguri de limbaj adiţionale sau modificaţi tagurile de limbaj existente pentru atribute repetând aceşti paşi 4 la pagina 186, 5 la pagina 186 şi 6. După ce aţi creat tagurile de limbaj pe care le doriţi, faceţi clic pe **OK**.
10. Expandaţi meniul **Afişare cu tag de limbă** şi selectaţi tagul de limbă. Faceţi clic pe **Modificare vizualizare** şi sunt afişate valorile atribut pe care le-aţi introdus pentru tagul de limbă. Orice valori pe care le adăugaţi sau editaţi în această vizualizare se aplică doar tagului de limbă selectat.
11. Când aţi terminat, faceţi clic pe **OK**.

Referinţe înrudite

"Tagurile de limbă" la pagina 48
Termenul *taguri de limbă* defineşte un mecanism care permite ca Directory Server să asocieze codurile de limbă cu valori ţinute într-un director şi permite clienţilor să interogheze directorul pentru valorile care îndeplinesc anumite cerinţe de limbă.

Ştergerea unei intrări

Folosiţi aceste informaţii pentru a şterge o intrare din arborele directorului.

1. Dacă nu aţi făcut asta deja, expandaţi categoria **Gestionare director** din zona de navigare, apoi apăsaţi pe **Gestionare intrări**. Puteţi expanda diverşi subarbori şi selecta subarborele, sufixul sau intrarea cu care vreţi să lucraţi. Apăsaţi **Şterge** din bara de unelte din partea dreaptă.
2. Vi se va cere să confirmaţi ştergerea. Apăsaţi **OK**. Intrarea este ştearsă din director şi reveniţi la lista de intrări.

Editarea unei intrări

Folosiţi aceste informaţii pentru a edita o intrare în arborele directorului.

1. Dacă nu aţi făcut asta deja, expandaţi categoria **Gestionare director** din zona de navigare, apoi apăsaţi pe **Gestionare intrări**. Puteţi expanda diverşi subarbori şi selecta intrarea cu care vreţi să lucraţi. Apăsaţi **Editare atribute** din bara de unelte din partea dreaptă.
2. În fişa **Atribute obligatorii** introduceţi valorile pentru atributele obligatorii. Vedeţi "Modificarea atributelor binare" la pagina 191 pentru informaţii despre adăugarea valorilor binare. Dacă vreţi să adăugaţi mai mult de o valoare pentru un anumit atribut, apăsaţi **Valori multiple** şi apoi adăugaţi valorile pe rând.
3. Apăsaţi **Atribute opţionale**.
4. În fişa **Atribute opţionale** introduceţi valorile corespunzătoare pentru atributele opţionale. Dacă vreţi să adăugaţi mai mult de o valoare pentru un anumit atribut, apăsaţi **Valori multiple** şi apoi adăugaţi valorile pe rând.
5. Faceţi clic pe **Apartenenţă**.
6. Dacă aţi creat vreun grup, la fişa **Apartenenţă**:
   - Selectaţi un grup din **Grupuri disponibile** şi apăsaţi **Adăugare** pentru a face intrarea membru al **Apartenenţei la grupul static** selectate.
   - Selectaţi un grup din **Apartenenţe grup spatic** şi faceţi clic pe **Înlăturare** pentru a înlătura intrarea din grupul selectat.
7. Dacă intrarea este o intrare grup, o fişă **Membri** este disponibilă. Fişa **Membri** afişează membrii grupului selectat. Puteţi adăuga şi înlătura membrii din grup.
   - Pentru a adăuga un membru la grup:
     a. Fie faceţi clic pe **Valori multiple** din fişa **Membri** sau la fişa **Membri**, faceţi clic pe **Membri**.
     b. În câmpul Membru, introduceţi DN-ul intrării pe care doriţi să o adăugaţi.
     c. Selectaţi **Adăugare**.
     d. Apăsaţi **OK**.
   - Pentru a înlătura un membru din grup:
     a. Fie faceţi clic pe **Valori multiple** din fişa **Membri** sau la fişa **Membri**, faceţi clic pe **Membri**.
     b. Selectaţi intrarea pe care doriţi să o înlăturaţi:

c. Faceţi clic pe **Înlăturare**.
d. Apăsaţi **OK**.

- Pentru a reîmprospăta lista de membri, faceţi clic pe **Actualizare**.

8. Faceţi clic pe **OK** pentru a modifica intrarea.

Copierea unei intrări

Folosiţi aceste informaţii pentru a copia o intrare în arborele director.

Această funcţie este de ajutor în cazul în care creaţi intrări similare. Copia moşteneşte toate atributele originalului. Trebuie să faceţi unele modificări la numele noii intrări.

1. Dacă nu aţi făcut asta deja, expandaţi categoria **Gestionare director** din zona de navigare, apoi apăsaţi pe **Gestionare intrări**. Puteţi expanda diverşi subarbori şi selecta intrarea, precum John Doe, cu care vreţi să lucraţi. Apăsaţi **Copiere** din bara de unelte din partea dreaptă.
2. Modificaţi intrarea RDN din câmpul DN. De exemplu modificaţi cn=John Doe cu cn=Jim Smith.
3. În fişa de atribute necesară, modificaţi intrarea cn la noua RDN. În acest exemplu Jim Smith.
4. Modificaţi corespunzător celelalte atribute necesare. În acest exemplu modificaţi atributul sn de la Doe la Smith.
5. Când aţi terminat de modificat faceţi clic pe **OK** pentru a crea noua intrare. Noua intrare Jim Smith este adăugată în josul listei de intrare.

Notă: Această procedură copie doar atributele intrării. Apartenenţele grup ale intrării originale nu sunt copiate la intrarea nouă. Folosiţi funcţia de atribute Editare pentru a adăuga apartenenţă.

Editarea listelor de control al accesului

Folosiţi aceste informaţii pentru a gestiona liste de control acces (ACL-uri).

Pentru a vedea proprietăţile ACL folosind unealta de administrare Web şi să lucraţi cu ACL-uri, vedeţi “Listă control acces taskuri (ACL)” la pagina 203.

Concepte înrudite

“Listele de control al accesului” la pagina 63
Listele de control al accesului (Access control list - ACL) oferă un mijloc de a proteja informaţiile stocate într-un director LDAP. Administratorii folosesc ACL-urile pentru a restricţiona accesul la diverse porţiuni ale directorului sau la anumite intrări din director.

Adăugarea unei clase de obiecte auxiliare

Folosiţi aceaste informaţii pentru a adăuga o clasă de obiecte auxiliară.

Folosiţi butonul **Adăugare clasă auxiliară** din bara de unelte pentru a adăuga o clasă obiect auxiliar unei intrări existente din arborele director. O clasă obiect auxiliar furnizează atribute suplimentare intrării la care este adăugată.

Dacă nu aţi făcut asta deja, expandaţi categoria **Gestionare director** din zona de navigare, apoi apăsaţi pe **Gestionare intrări**. Puteţi expanda diverşi subarbori şi selecta intrarea, precum John Doe, cu care vreţi să lucraţi. Apăsaţi **Adăugare clasă auxiliară** din bara de unelte din partea dreaptă.

1. Selectaţi orice **Clase de obiecte auxiliare** pe care vreţi să le folosiţi din căsuţa Disponibile şi apăsaţi **Adăugare**. Repetaţi acest proces pentru fiecare clasă de obiecte auxiliare pe care vreţi să o adăugaţi. Puteţi de asemenea şterge o clasă de obiecte auxiliară din căsuţa Selectate prin selectarea ei şi apăsarea pe **Ştergere**.
2. În fişa **Atribute obligatorii** introduceţi valorile pentru atributele obligatorii. Dacă vreţi să adăugaţi mai mult de o valoare pentru un anumit atribut, apăsaţi **Valori multiple** şi apoi adăugaţi valorile pe rând.
3. Apăsaţi **Atribute opţionale**.
4. În fişa **Atribute opţionale** introduceţi valorile corespunzătoare pentru atributele opţionale. Dacă vreţi să adăugaţi mai mult de o valoare pentru un anumit atribut, apăsaţi **Valori multiple** şi apoi adăugaţi valorile pe rând.
5. Faceţi clic pe **Memberships**.
6. Dacă aţi creat vreun grup, la fişa **Apartenenţă**:

- Selectaţi un grup din **Grupuri disponibile** şi apăsaţi **Adăugare** pentru a face intrarea membru al **Apartenenţei la grupul static** selectate.
- Selectaţi un grup din **Apartenenţe grup spatic** şi faceţi clic pe **Înlăturare** pentru a înlătura intrarea din grupul selectat.

7. Faceţi clic pe **OK** pentru a modifica intrarea.

Ştergerea unei clase auxiliare

Folosiţi aceste informaţii pentru a şterge o clasă auxiliară.

Deşi puteţi şterge o clasă auxiliară în timpul procedurii de adăugare de clasă auxiliară, este mai uşor să folosiţi funcţia de şterge clasă auxiliară dacă doriţi să ştergeţi o singură clasă auxiliară dintr-o intrare. Oricum, poate fi mai convenabil să folosiţi procedusa de adăugare clasă auxiliară dacă doriţi să ştergeţi mai multe clase auxiliare din intrare.

1. Dacă nu aţi făcut asta deja, expandaţi categoria **Gestionare director** din zona de navigare, apoi apăsaţi pe **Gestionare intrări**. Puteţi expanda diverşi subarbori şi selecta intrarea, precum John Doe, cu care vreţi să lucraţi. Apăsaţi **Ştergere clasă auxiliară** din bara de unelte din partea dreaptă.
2. Din lista de clase auxiliare, selectaţi pe cea care doriţi să o ştergeţi şi apăsaţi **OK**.
3. Vi se cere să confirmaţi ştergerea, apăsaţi **OK**.
4. Clasa auxiliară este ştearsă din intrare şi dvs. sunteţi întors la lista de intrări.

Repetaţi aceşti paşi pentru fiecare clasă auxiliară pe care doriţi să o ştergeţi.

Modificarea apartenenţei la grup

Folosiţi aceste informaţii pentru a modifica apartenenţa la grup.

Dacă nu aţi făcut asta deja, expandaţi categoria **Gestionare director** din zona de navigare.

1. Apăsaţi **Gestionare intrări**.
2. Selectaţi un utilizator din arborele director şi apăsaţi pe pictograma **Editare atribute** din bara de unelte.
3. Faceţi clic pe fişa **Apartenenţe**.
4. Pentru a modifica apartenenţa pentru utilizator. Panoul **Modificare apartenenţe** afişează **Grupuri disponibile** în care pot fi adăugaţi utilizatori, la fel ca şi **Apartenenţele grup static** ale intrării.
   - Selectaţi un grup din **Grupuri disponibile** şi apăsaţi **Adăugare** pentru a face intrarea un membru al grupului selectat.
   - Selectaţi un grup din **Apartenenţe grup static** şi faceţi clic pe **Înlăturare** pentru a înlătura intrarea din grupul selectat.
5. Apăsaţi **OK** penru a salva modificările dvs sau apăsaţi **Anulare** pentru a vă întoarce în panoul anterior fără să salvaţi modificările.

Căutarea intrărilor directorului

Folosiţi aceste informaţii pentru a căuta intrările directorului.

Există 3 opţiuni pentru căutarea arborelui director:

- O căutare simplă folosind un set predefinit de criterii de căutare:
- O căutare avansată folosind un set definit de utilizator de criterii de căutare.
- O căutare manuală

Opţiunile de căutare sunt disponibile expandând categoria **Gestionare directoare** din zona de navigare, apăsaţi **Căutare intrări**. Selectaţi fie fişa **Căutare filtre**, fie **Opţiuni**.

Notă: Intrările binare, de exemplu parole, nu sunt căutabile.

O căutare simplă foloseşte un criteriu de căutare implicit:

- DN-ul de bază este **Toate sufixele**

- Scopul căutării este **Subarbore**
- Dimensiunea căutarii este **Unlimited**
- Timpul limită este **Nelimitat**
- Diferenţierea alias este **niciodată**
- Vânare referral-i este deselectată (off)

O căutare avansată vă permite să specificaţi restricţii de căutare şi să activaţi filtre de căutare. Folosiţi ccăutarea simplă pentru a folosi criterii de căutare implicite.

1. Pentru a executa o căutare simplă:
   a. În fişa **Filtru de căutare**, apăsaţi **Căutare simplă**.
   b. Selectaţi o clasă obiect din lista derulantă.
   c. Selectaţi un atribut specific pentru tipul de intrare selectat. Dacă alegeţi să căutaţi un atribut specific, selectaţi un atribut din lista derulantă şi intrpoduceţi valoarea atributului în caseta **Este egal cu**. Dacă nu specificaţi un atribut, căutarea întoarce toate intrările director ale tipului intrării selectate.
2. Pentru a executa o căutare avansată:
   a. În fişa **Filtru de căutare**, apăsaţi **Căutare avansată**.
   b. Selectaţi un **Atribut** din lista derulantă.
   c. Selectaţi un operator **Comparare**.
   d. Introduceţi **Valoare** pentru comparaţie.
   e. Folosiţi butoanele de operare căutare pentru interogări complexe.
      - Dacă aţi adăugat deja un filtru de căutare, specificaţi criteriile suplimentare şi apăsaţi **AND**. Comanda **AND** întoarce intrările care se potrivesc cu ambele seturi de criterii de căutare.
      - Dacă aţi adăugat deja un filtru de căutare, specificaţi criteriile suplimentare şi apăsaţi **OR**. Comanda **OR** întoarce intrările care se potrivesc cu unul din seturile de criterii de căutare.
      - Apăsaţi pe **Adăugare** pentru a adăuga criteriile de filtru de căutare la căutare avansată.
      - Apăsaţi pe **Ştergere** pentru a şterge criteriile de filtru de căutare la căutare avansată.
      - Faceţi clic pe **Reset** pentru a curăţa toate filtrele de căutare.
3. Pentru a reliza o căutare manuală, creaţi un filtru de căutare.

   De exemplu pentru a căuta nume de familie introduceţi sn=* în câmp. În cazul în care căutaţi atribute multiple, folosiţi sintaxa filtrului de căutare: De exemplu, pentru a căuta numele de familie al unui anumit departament, introduceţi:

   ```
   (&(sn=*)(dept=<departmentname>))
   ```

La **fişa Opţiuni**:

- **Căutare DN de bază** - Selectaţi sufixul din lista derulantă pentru a căuta doar în acel sufix.

  Notă: Dacă aţi pornit acest task din panoul **Gestionare intrări**, acest câmp este completat pentru dumneavoastră. Aţi selectat **DN părinte** înainte de a apăsa **Adăugare** pentru a porni procesul de adăugare intrare.

  Puteţi de asemenea **Toate sufixele** pentru a căuta întregul arbore.

  Notă: O căutare într-un subarbore cu **Toate sufixele** selectate nu va întoarce informaţii despre schemă, informaţii despre istoricul de modificări, sau ceva despre back-end-ul proiectat al sistemului.
- **Scopul căutării**
  - Selectaţi **Obiect** pentru a căuta doar în obiectul selectat.
  - Selectaţi **Nivel singular** pentru a căuta doar în copilul imediat al obiectului selectat.
  - Selectaţi **Subarbore** pentru a căuta toţi descendenţii intrării curente selectate.
- **Limită dimensiune căutare** - Introduceţi numărul maxim de intrări de căutare sau selectaţi **Nelimitat**.
- **Limită timp căutare** - Introduceţi numărul maxim de secunde pentru căutare sau selectaţi **Nelimitat**.

- Selectaţi un tip de **Dereferenţiere alias** din lista derulantă.
  - **Niciodată** - Dacă intrarea selectată este un alias, nu este dereferenţiată pentru căutare, adică căutarea ignoră referinţa la alias.
  - **Găsire** - Dacă intrarea selectată este un alias, căutarea dereferenţiază aliasul şi caută din locaţia aliasului.
  - **Căutare** - Intrarea selectată nu este dereferenţiată, dar orice intrare găsită în căutare este dereferenţiată.
  - **Mereu** - Toate aliasurile întâlnite în căutare sunt dereferenţiate.
- Selectaţi caseta de bifare **Vânare referral-i** pentru a urma referral-ii la un alt server, dacă este întors un referral la căutare. Când un referral directează căutarea la un alt server, conexiunea cu serverul foloseşte acreditările curente. Dacă sunteţi logat ca Anonymous aţi putea avea nevoie să vă înregistraţi pe server folosind un DN autentificat.

  Operaţii înrudite

  "Ajustarea setărilor de căutare" la pagina 123
  Folosiţi aceste informaţii pentru a controla capabilităţiile de căutare ale utilizatorului.

  Referinţe înrudite

  "Parametrii de căutare" la pagina 46
  Pentru a limita cantitatea de resurse folosite de server, un administrator poate configura parametrii de căutare pentru a restricţiona posibilităţile de căutare ale utilizatorilor. Posibilităţile de căutare pot fi şi extinse pentru utilizatori speciali.

Modificarea atributelor binare

Folosiţi aceste informaţii pentru a importa, exporta sau şterge date binare.

Dacă un atribut necesită date binare, un buton **Date binare** este afişat lângă câmpul atribut. Dacă atributul nu are date, câmpul este gol. Deoarece atributele binare nu pot fi afişate, dacă un atribut conţine date binare, câmpul afişează **Date binare - 1**. Dacă atributul conţine valori multiple, câmpul este afişat ca listă derulantă.

Faceţi clic pe butonul **Date binare** pentru a lucra cu atribute binare.

Puteţi importa, exporta sau şterge date binare.

1. Pentru a adăuga date binare la atribut:
   a. Faceţi clic pe butonul **Date binare**.
   b. Faceţi clic pe **Importare**.
   c. Puteţi fie să introduceţi numele cale pentru fişierul pe care doriţi fie să faceţi clic pe **Răsfoire** pentru a localiza şi selecta fişierul binar.
   d. Faceţi clic pe **Lansare fişier**. Este afişat un mesaj Fişier încărcat.
   e. Apăsaţi **Close**. **Date binare - 1** este acum afişat sunt **Intrări date binare**.
   f. Repetaţi procesul de importare pentru atâtea fişiere binare câte doriţi să adăugaţi. Intrările următoare sunt tipărite ca **Date binare - 2**, **Date binare -3** şamd.
   g. Când terminaţi adăugarea de date binare, apăsaţi **OK**.
2. Pentru a exporta date binare:
   a. Faceţi clic pe butonul **Date binare**.
   b. Faceţi clic pe **Export**.
   c. Apăsaţi pe **Date binare de descărcat**.
   d. Urmaţi direcţiile vrăjitorului dvs fie ca să afişaţi fişierul binar, fie să îl salvaţi într-o locaţie nouă.
   e. Apăsaţi **Close**.
   f. Repetaţi procesul de exportare pentru atâtea fişiere binare, câte doriţi să exportaţi.
   g. Când terminaţi exportarea de date binare, apăsaţi **OK**.
3. Pentru a şterge date binare:
   a. Faceţi clic pe butonul **Date binare**.
   b. Verificaţi fişierul de date binare pe care doriţi să îl ştergeţi. Pot fi selectate fişiere multiple.

c. Faceţi clic pe **Ştergere**
d. Când vi se cere să confirmaţi ştergerea, apăsaţi **OK**. Datele binare marcate pentru ştergere sunt înlăturare din listă.
e. Când terminaţi ştergerea datelor, apăsaţi **OK**.

Notă: Atributele binare sunt căutate numai pentru existenţă.

Taskuri de grup şi de utilizator

Folosiţi aceste informaţii pentru a gestiona grupuri şi utilizatori.

Pentru a gestiona utilizatori şi grupuri, expandaţi categoria **Utilizatori şi grupuri** din zona de navigare a uneltei de administrare web.

Concepte înrudite

"Grupurile şi rolurile" la pagina 55
Folosiţi grupurile şi rolurile pentru a organiza şi controla accesul sau permisiunile membrilor.

Taskuri utilizator

Folosiţi aceste informaţii pentru a gestiona utilizatori.

După ce aţi setat regiunile şi şabloanele dvs, le puteţi popula cu utilizatori.

Referinţe înrudite

"Autentificarea" la pagina 79
Folosiţi o metodă de autentificare pentru a controla accesul la Directory Server.

Adăugarea utilizatorilor:

Folosiţi aceste informaţii pentru a adăuga utilizatorii.

Expandaţi categoria **Utilizatori şi grupuri** din zona de navigare a uneltei de administrare web.

1. Faceţi clic pe **Adăugare utilizator** sau faceţi clic pe **Gestionare utilizatori** şi faceţi clic pe **Adăugare**.
2. Selectaţi regiunea în care doriţi să adăugaţi utilizatorul din meniul derulant.
3. Apăsaţi **Următorul**. Este afişat şablonul care este asociat cu regiunea. Completaţi câmpurile necesare, notate cu un asterisc (*) şi oricare alte câmpuri de pe fişe. Dacă aţi creat deja grupuri în regiune, puteţi de asemenea să adăugaţi utilizatorul în unul sau mai multe grupuri.
4. Când aţi terminat, faceţi clic pe **Sfârşit**.

Găsire utilizatori în regiune:

Folosiţi aceste informaţii pentru a găsi utilizatori în regiune.

Expandaţi categoria **Utilizatori şi grupuri** din zona de navigare a uneltei de administrare web.

1. Faceţi clic pe **Găsire utilizator** sau faceţi clic pe **Gestionare utilizatori** şi faceţi clic pe **Găsire**.
2. Selectaţi regiunea în care doriţi să căutaţi din câmpul **Selectare regiune**.
3. Introdceţi şirul de căutare în câmpul **Numire atribute**. Sunt suportate caractere de înlocuire, de exemplu, dacă aţi introdus ***smith** , rezultatul sunt toate căutările care au atributul de numire terminându-se cu smith.
4. Puteţi realiza următoarele operaţii pe un utilizator selectat:
   - **Editare** - Vedeţi "Editarea informaţiilor utilizatorului" la pagina 193.
   - **Copiere** - Vedeţi "Copiere utilizator" la pagina 193.
   - **Ştergere** - Vedeţi "Înlăturare utilizator" la pagina 193.
5. Când terminaţi faceţi clic pe **OK**.

Editarea informaţiilor utilizatorului:

Folosiţi aceste informaţii pentru a edita informaţiile unui utilizator.

Expandaţi categoria **Utilizatori şi grupuri** din zona de navigare a uneltei de administrare web.

1. Faceţi clic pe **Gestionare utilizatori**.
2. Selectaţi o regiune din meniul derulant. Faceţi clic pe **Vizualizare utilizatori**, dacă utilizatorii nu sunt afişaţi deja în caseta **Utilizatori**.
3. Selecatţi utilizatorul pe care doriţi să-l editaţi şi faceţi clic pe **Editare**.
4. Modificaţi informaţiile din fişe, modificaţi apartenenţa la grup.
5. Când terminaţi faceţi clic pe **OK**.

Copiere utilizator:

Folosiţi aceste informaţii pentru a copia un utilizator.

Daca trebuie să creaţi un număr de utilizatori care au informaţii aproape identice, puteţi crea utilizatori suplimentari prin copierea utilizatorului iniţial şi prin modificarea informaţiilor.

Expandaţi categoria **Utilizatori şi grupuri** din zona de navigare a uneltei de administrare web.

1. Faceţi clic pe **Gestionare utilizatori**.
2. Selectaţi o regiune din meniul derulant. Faceţi clic pe **Vizualizare utilizatori**, dacă utilizatorii nu sunt afişaţi deja în caseta **Utilizatori**.
3. Selectaţi utilizatorul pe care doriţi să-l copiaţi şi faceţi clic pe **Copiere**.
4. Modificaţi informaţiile corespunzătoare pentru noul utilizator, de exemplu informaţiile necesare care identifică un anumit utilizator, cum sunt sn sau cn. Nu trebuie modificate informaţiile care sunt comune ambilor utilizatori.
5. Când terminaţi faceţi clic pe **OK**.

Înlăturare utilizator:

Folosiţi aceste informaţii pentru a înlătura acest utilizator.

Expandaţi categoria **Utilizatori şi grupuri** din zona de navigare a uneltei de administrare web.

1. Faceţi clic pe **Gestionare utilizatori**.
2. Selectaţi o regiune din meniul derulant. Faceţi clic pe **Vizualizare utilizatori**, dacă utilizatorii nu sunt afişaţi deja în caseta **Utilizatori**.
3. Selecatţi utilizatorul pe care doriţi să-l înlăturaţi faceţi clic pe **Ştergere**.
4. Când vi se cere să confirmaţi ştergerea, apăsaţi **OK**.
5. Utilizatorul este înlăturat din lista de utilizatori.

Taskuri de grup

Folosiţi aceste informaţii pentru a gestiona grupuri.

După ce aţi setat regiunile şi şabloanele, puteţi crea grupuri.

Adăugarea grupurilor:

Folosiţi aceste informaţii pentru a adăuga grupuri.

Expandaţi categoria **Utilizatori şi grupuri** din zona de navigare a uneltei de administrare web.

1. Faceţi clic pe **Adăugare grup** sau faceţi clic pe **Gestionare grupuri** şi faceţi clic pe **Adăugare**.
2. Introduceţi numele grupului pe care doriţi să-l creaţi.

3. Selectaţi regiunea pe care doriţi să o adăugaţi la grup din meniul derulant.
4. Faceţi clic pe **Sfârşit** pentru a crea grupul. Dacă aveţi deja utilizatori în regiune puteţi apăsa clic pe **Următorul** şi selectaţi utilizatorii de adăugat la grup. Apoi faceţi clic pe **Sfârşit**.

Concepte înrudite

"Grupurile şi rolurile" la pagina 55
Folosiţi grupurile şi rolurile pentru a organiza şi controla accesul sau permisiunile membrilor.

Găsire grupuri în regiune:

Folosiţi aceste informaţii pentru a găsi grupuri în regiune.

Expandaţi categoria **Utilizatori şi grupuri** din zona de navigare a uneltei de administrare web.

1. Faceţi clic pe **Găsire grup** sau faceţi clic pe **Gestionare grupuri** şi faceţi clic pe **Găsire**.
2. Selectaţi regiunea în care doriţi să căutaţi din câmpul **Selectare regiune**.
3. Introdceţi şirul de căutare în câmpul **Numire atribute**. Sunt suportate wildcards, de exemplu, dacă aţi introdus ***club** , rezultatul sunt toate grupurile care au atributul de numire club, de exemplu, Club carte, club şah, club grădină şamd.
4. Puteţi realiza următoarele operaţii pe un utilizator selectat:
   - **Editare** - Vedeţi "Editarea informaţiilor grupului".
   - **Copiere** - Vedeţi "Copiere grup".
   - **Ştergere** - Vedeţi "Înlăturare grup" la pagina 195.
5. Când aţi terminat, faceţi clic pe **Sfârşit**.

Editarea informaţiilor grupului:

Folosiţi aceste informaţii pentru a edita informaţiile unui grup.

Expandaţi categoria **Utilizatori şi grupuri** din zona de navigare a uneltei de administrare web.

1. Apăsaţi **Gestionare grupuri**.
2. Selectaţi o regiune din meniul derulant. Faceţi clic pe **Vizualizare grupuri**, dacă utilizatorii nu sunt afişaţi deja în caseta **Grupuri**.
3. Selectaţi grupul pe care doriţi să-l editaţi şi faceţi clic pe **Editare**.
4. Puteţi apăsa clic pe **Filtru** pentru a limita numărul de **Utilizatori disponibili**. De exemplu, introducând *smith în ultimul câmp nume, limitaţi utilizatorii disponibili la cei a căror nume se termină cu smith precum Ann Smith, Bob Smith, Joe Goldsmith, şamd.
5. Puteţi adăuga şi înlătura membrii din grup.
6. Când terminaţi faceţi clic pe **OK**.

Copiere grup:

Folosiţi aceste informaţii pentru a copia un grup.

Daca trebuie să creaţi un număr de grupuri care au în general aceeaşi membri, puteţi crea grupuri suplimentari prin copierea grupului iniţial şi prin modificarea informaţiilor.

Expandaţi categoria **Utilizatori şi grupuri** din zona de navigare a uneltei de administrare web.

1. Apăsaţi **Gestionare grupuri**.
2. Selectaţi o regiune din meniul derulant. Faceţi clic pe **Vizualizare grupuri**, dacă grupurile nu sunt afişaţe deja în caseta **Grupuri**.
3. Selectaţi grupul pe care doriţi să-l copiaţi şi faceţi clic pe **Copiere**.
4. Modificaţi numele grupului din câmpul **Nume grup**. Noul grup are aceeaşi membri cu cel original.

5. Puteţi schimba membrii grupului.
6. Când terminaţi faceţi clic pe **OK**. Noul grup este creat şi conţine aceeaşi membri cu cel original împreună cu orice adăugare sau modificare pe care aţi făcut-o în timpul procedurii de copiere.

Înlăturare grup:

Folosiţi aceste informaţii pentru a înlătura un grup.

Expandaţi categoria **Utilizatori şi grupuri** din zona de navigare a uneltei de administrare web.

1. Apăsaţi **Gestionare grupuri**.
2. Selectaţi o regiune din meniul derulant. Faceţi clic pe **Vizualizare grupuri**, dacă utilizatorii nu sunt afişaţi deja în caseta **Grupuri**.
3. Selectaţi grupul pe care doriţi să-l înlăturaţi faceţi clic pe **Ştergere**.
4. Când vi se cere să confirmaţi ştergerea, apăsaţi **OK**.
5. Grupul este înlăturat din lista de utilizatori.

Taskuri ale şablonului utilizator şi ale regiunii

Folosiţi aceste informaţii pentru a gestiona şabloane ale utilizatorului şi regiunii.

Pentru a gestiona regiuni şi şabloane utilizator faceţi clic pe **Regiuni şi şabloane utilizator** din zone de navigare a uneltei de administrare Web. Folosiţi regiuni şi şabloane utilizator pentru a le uşura altora introducerea de date în director.

Concepte înrudite

"Regiuni şi şabloane utilizator" la pagina 46
Regiunea şi obiectele şablon ale utilizatorului găsite în unalta de administrare web sunt utilizate pentru a scăpa utiliza torul de nevoia de a învăţa unele din problemele LDAP subliniate.

Crearea unei regiuni

Folosiţi aceste informaţii pentru a crea o regiune.

Pentru a crea o regiune, faceţi următoarele:

1. Expandaţi categoria **Regiuni şi şabloane utilizator** din zona de navigare a uneltei de administrare web.
2. Faceţi clic pe **Adăugare regiune**.
   - Introduceţi numele pentru regiune. De exemplu **realm1**.
   - Introduceţi DN-ul părinte care identifică locaţia regiunii. Acesată intrare este forma sufixului, de exemplu o=ibm,c=us. Această intrare poate fi un sufix sau o intrare în altă parte a directorului. Puteţi de asemenea să apăsaţi pe **Răsfoire** pentru a selecta locaţia subarborelui pe care îl douiţi.
3. Faceţi clic pe **Următorul** pentru a continua sau faceţi clic pe **Sfârşit**.
4. Dacă aţi apăsat clic pe **Următorul**, revedeţi informaţiile. În acest moment nu aţi creat efectiv regiunea, deci **Şablon utilizator** şi **Filtru căutare utilizator** pot fi ignorate.
5. Faceţi clic pe **Sfârşit** pentru a crea regiunea.

Concepte înrudite

"Regiuni şi şabloane utilizator" la pagina 46
Regiunea şi obiectele şablon ale utilizatorului găsite în unalta de administrare web sunt utilizate pentru a scăpa utiliza torul de nevoia de a învăţa unele din problemele LDAP subliniate.

Crearea unui administrator de regiune

Folosiţi aceste informaţii pentru a crea un administrator de regiune.

Pentru a crea un administrator de regiune, trebuie mai întâi să creaţi un grup de administrare pentru regiune făcând următoarele:

1. Creaţi grupul de administrare regiune.
   a. Expandaţi categoria **Gestionare director** din zona de navigare a uneltei de administrare web.
   b. Apăsaţi **Gestionare intrări**.
   c. Expandaţi arborele şi selectaţi regiunea pe care tocmai aţi creat-o, **cn=realm1,o=ibm,c=us**.
   d. Faceţi clic pe **Editare ACL**.
   e. Faceţi clic pe fişa **Editare**.
   f. Asiguraţi-vă că este bifat **Propagare proprietar**.
   g. Introduceţi DN-ul pentru regiune, **cn=realm1,o=ibm,c=us**.
   h. Modificaţi **Tipul** la grup.
   i. Selectaţi **Adăugare**.
2. Creaţi intrarea administrator. Dacă nu aveţi deja o intrare utilizator pentru administrator, trebuie să creaţi una.
   a. Expandaţi categoria **Gestionare director** din zona de navigare a uneltei de administrare web.
   b. Apăsaţi **Gestionare intrări**.
   c. Expandaţi arborele la locaţia unde doriţo să se afle intrarea administrator.

      Notă: Localizarea intrării administrator în afara regiunii evită acordarea administratorului abilitatea de a se şterge accidental. În acest exemplu locaţia poate fi **o=ibm,c=us** .
   d. Selectaţi **Adăugare**.
   e. Selectaţi **Clasa obiect structurală**, de exemplu **inetOrgPerson**.
   f. Apăsaţi **Următorul**.
   g. Selectaţi price clasă obiect auxiliară pe care doriţi să o adăugaţi.
   h. Apăsaţi **Următorul**.
   i. Introduceţi atributele necesare pentru intrare. De exemplu,
      - **RDN** cn=JohnDoe
      - **DN** o=ibm,c=us
      - **cn** John Doe
      - **sn** Doe
   j. Pe fişa **Alte atribute** asiguraţi-vă că aţi alocat o parolă.
   k. Când aţi terminat, faceţi clic pe **Sfârşit**.
3. Adăugaţi administratorul în grupul de administrare.
   a. Expandaţi categoria **Gestionare director** din zona de navigare a uneltei de administrare web.
   b. Apăsaţi **Gestionare intrări**.
   c. Expandaţi arborele şi selectaţi regiunea pe care tocmai aţi creat-o, **cn=realm1,o=ibm,c=us**.
   d. Apăsaţi **Editare atribute**.
   e. Faceţi clic pe fişa **Membrii**.
   f. faceţi clic pe **Membrii**.
   g. În câmpul **Membri** introduceţi DN-ul administratorului, în acest exmplu **cn=John Doe,o=ibm,c=us**.
   h. Selectaţi **Adăugare**. DN-ul este afişat în lista **Membri**.
   i. Apăsaţi **OK**.
   j. Faceţi clic pe **Actualizare**. DN-ul este afişat în lista **Membri actuali**.
   k. Apăsaţi **OK**.
4. Aţi creat un administrator care poate gestiona intrări din regiune.

Crearea unui şablon

Folosiţi aceste informaţii pentru a crea un şablon.

După ce aţi creat o regiune, următorul pas este să creaţi un şablon utilizator. Un şablon vă ajută să organizaţi informaţiile pe care doriţi să le introduceţi. Expandaţi categoria **Regiuni şi şabloane utilizator** din zona de navigare a uneltei de administrare web.

1. Faceţi clic pe **Adăugare utilizator şablon**.
   - Introduceţi numele pentru şablon, de exemplu, **şablon1** .
   - Introduceţi locaţia unde se va afla şablonul. Pentru scopuri de replicare, localizaţi şablonul în subarborele regiunii care va folosi acest şablon. De exemplu, regiunea creată în operaţiile anterioare **cn=realm1,o=ibm,c=us**. De asemenea puteţi apăsa pe **Răsfoire** pentru a to selecta un alt subarbore pentru locaţia şablonului.
2. Apăsaţi **Următorul**. Puteţi apăsa pe **Sfârşit** pentru a crea un nou şablon gol. Puteţi să adăugaţi mai târziu informaţii la şablon, vedeţi “Editarea unui şablon” la pagina 202.
3. Dacă aţi apăsat pe **Continuare**, alegeţi clasa de obiecte structurală pentru şablon, de exemplu **inetOrgPerson**. Puteţi de asemenea să adăugaţi clase de obiecte auxiliare pe care le doriţi.
4. Apăsaţi **Următorul**.
5. A fost creată o fişă **Obligatorii** în acest şablon. Puteţi modifica informaţiile conţinute în această fişă.
   a. Selectaţi **Obligatorii** în meniul de fişe şi apăsaţi **Editare**. Este afişat panoul **Editare fişă**. Vedeţi numele fişei **Obligatorii** şi atributele seletate care sunt obligatorii pentru clasa de obiecte, **inetOrgPerson**:
      - *sn - surname
      - *cn - common name

      Notă: * indică informaţii obligatorii.
   b. Dacă vreţi să adăugaţi informaţii suplimentare la această fişă, selectaţi atributul din meniul **Atribute**. De exemplu, selectaţi **departmentNumber** şi apăsaţi **Adăugare**. Selectaţi **employeeNumber** şi faceţi clic pe **Adăugare**. Selectaţi **title** şi apăsaţi **Adăugare**. Meniul **Atribute selectate** arată acum:
      - title
      - employeeNumber
      - departmentNumber
      - *sn
      - *cn
   c. Puteţi rearanja ordinea în care apar aceste câmpuri în şablon prin evidenţierea atributului selectat şi apăsând pe **Mută în sus** sau **Mută în jos**. Aceasta schimbă poziţia atributului cu o poziţie. Repetaţi această procedură până când aţi aranjat atributele în ordinea în care le vreţi. De exemplu,
      - *sn
      - *cn
      - title
      - employeeNumber
      - departmentNumber
   d. Puteţi de asemenea modifica fiecare atribut selectat.
      1) Evidenţiaţi atributul în căsuţa **Atribute selectate** şi apăsaţi **Editare**.
      2) Puteţi schimba numele de afişare al câmpului folosit în şablon. De exemplu, dacă vreţi ca **departmentNumber** să fie afişat ca **Număr departament** introduceţi asta în câmpul **Nume afişat**.
      3) Puteţi de asemenea să furnizaţi o valoare implicită care să completeze câmpul atributului în şablon. De exemplu, dacă majoritatea utilizatorilor care vor fi introduşi sunt membri ai Departmentului 789, puteţi introduce 789 ca valoare implicită. Câmpul din şablon este precompletat cu 789. Valoarea poate fi schimbată când adăugaţi informaţiile efective despre utilizator.
      4) Apăsaţi **OK**.
   e. Apăsaţi **OK**.
6. Pentru a crea o altă categorie de fişă pentru informaţii suplimentare, apăsaţi **Adăugare**.
   - Introduceţi numele pentru noua fişă. De exemplu, Informaţii de adresă.

- Pentru această fişă, selectaţi atributele din meniul **Atribute** . De exemplu, selectaţi **homePostalAddress** şi apăsaţi **Adăugare**. Selectaţi **postOfficeBox** şi faceţi clic pe **Adăugare**. Selectaţi **telephoneNumber** şi faceţi clic pe **Adăugare**. Selectaţi **homePhone** şi faceţi clic pe **Adăugare**. Selectaţi **facsimileTelephoneNumber** şi faceţi clic pe **Adăugare**. Meniul **Atribute selectate** arată acum:
  - homePostalAddress
  - postOfficeBox
  - telephoneNumber
  - homePhone
  - facsimileTelephoneNumber
- Puteţi rearanja ordinea în care apar aceste câmpuri în şablon prin evidenţierea atributului selectat şi apăsând pe **Mută în sus** sau **Mută în jos**. Aceasta schimbă poziţia atributului cu o poziţie. Repetaţi această procedură până când aţi aranjat atributele în ordinea în care le vreţi. De exemplu,
  - homePostalAddress
  - postOfficeBox
  - telephoneNumber
  - facsimileTelephoneNumber
  - homePhone
- Apăsaţi **OK**.

7. Repetaţi acest proces pentru atâtea fişe câte vreţi să creaţi. Când aţi terminat apăsaţi **Sfârşit** pentru a crea şablonul.

Adăugarea şablonului la o regiune

Folosiţi aceste informaţii pentru a adăuga un şablon unei regiuni.

După ce aţi creat o regiune şi un şablon, trebuie să adăugaţi şablonul la regiune. Expandaţi categoria **Regiuni şi şabloane utilizator** din zona de navigare a uneltei de administrare web.

1. Apăsaţi pe **Gestionare regiuni**.
2. Selectaţi regiunea la care vreţi să adăugaţi şablonul, în acest exemplu, **cn=realm1,o=ibm,c=us** şi apăsaţi **Editare**.
3. Derulaţi în jos la **Şablon utilizator** şi expandaţi meniul derulant.
4. Selectaţi şablonul, în acest exemplu **cn=template1,cn=realm1,o=ibm,c=us**.
5. Apăsaţi **OK**.
6. Apăsaţi **Close**.

Creare grupuri

Folosiţi aceste informaţii pentru a crea grupuri.

Expandaţi categoria **Utilizatori şi grupuri** din zona de navigare a uneltei de administrare web.

1. Apăsaţi **Adăugare grup**.
2. Introduceţi numele grupului pe care doriţi să-l creaţi. De exemplu, **group1**.
3. Selectaţi regiunea în care doriţi să adăugaţi utilizatorul din meniul derulant. În acest caz **realm1**.
4. Faceţi clic pe **Sfârşit** pentru a crea grupul. Dacă aveţi deja utilizatori în regiune puteţi apăsa clic pe **Următorul** şi selectaţi utilizatorii de adăugat la group1. Apoi faceţi clic pe **Finalizare**.

Concepte înrudite

“Grupurile şi rolurile” la pagina 55
Folosiţi grupurile şi rolurile pentru a organiza şi controla accesul sau permisiunile membrilor.

Adăugarea unui utilizator la regiune

Folosiţi aceste informaţii pentru a adăuga un utilizator la regiune.

Expandaţi categoria **Utilizatori şi grupuri** din zona de navigare a uneltei de administrare web.

1. Faceţi clic pe **Adăugare utilizator**.

2. Selectaţi regiunea în care doriţi să adăugaţi utilizatorul din meniul derulant. În acest caz **realm1**.
3. Apăsaţi **Următorul**. Este afişat şablonul pe care tocmai l-aţi creat, template1. Completaţi câmpurile necesare, notate cu un asterisc (*) şi oricare alte câmpuri de pe fişe. Dacă aţi creat deja grupuri în regiune, puteţi de asemenea să adăugaţi utilizatorul în unul sau mai multe grupuri.
4. Când aţi terminat, faceţi clic pe **Sfârşit**.

Taskuri ale regiunii

Folosiţi aceste informaţii pentru a gestiona regiuni.

După ce aţi setat şi populat regiunea iniţială, puteţi adăuga mai multe regiuni sau să modificaţi regiuni existente.

Expandaţi categoria **Regiuni şi şabloane** din zona de navigare şi apăsaţi **Gestionare regiuni**. Este afişată o listă cu regiunile existente. Din acest panou puteţi adăuga o regiune, edita o regiune, şterge o regiune sau edita listele de control al accesului (ACL-uri) pentru regiune.

Adăugarea unei regiuni:

Folosiţi aceste informaţii pentru a adăuga o regiune.

Expandaţi categoria **Regiuni şi şabloane utilizator** din zona de navigare a uneltei de administrare web.

1. Faceţi clic pe **Adăugare regiune (la Kerberos)**.
   - Introduceţi numele pentru regiune. De exemplu **realm1**.
   - Dacă aveţi regiuni preexistente, de exemplu **realm1**, puteţi selecta o regiune pentru a avea setările copiate la regiunea pe care o creaţi.
   - Introduceţi DN-ul părinte care identifică locaţia regiunii. Acesată intrare este forma sufixului, de exemplu **o=ibm,c=us**. Puteţi de asemenea să apăsaţi pe **Răsfoire** pentru a selecta locaţia subarborelui pe care îl douiţi.
2. Faceţi clic pe **Următor** pentru a continua sau faceţi clic pe **Sfârşit**.
3. Dacă aţi apăsat clic pe **Următorul**, revedeţi informaţiile.
4. Selectaţi un **Şablon utilizator** din meniul derulant. Dacă aţi copiat setările dintr-o regiune preexistentă, şablonul ei este precompletat în acest câmp.
5. Introduceţi un **Filtru de căutare utilizator**.
6. Faceţi clic pe **Sfârşit** pentru a crea regiunea.

Editarea unei regiuni:

Folosiţi aceste informaţii pentru a edita o regiune.

Expandaţi categoria **Regiuni şi şabloane utilizator** din zona de navigare a uneltei de administrare web.

- Apăsaţi pe **Gestionare regiuni**.
- Selectaţi regiunea pe care vreţi să o editaţi din lista de regiuni.
- Faceţi clic pe **Editare**.
  - Puteţi folosi butoanele de **Răsfoire** pentru a schimba
    - Grupul de administrator
    - Containerul de grup
    - Containerul de utilizator
  - Puteţi selecta alt şablon din meniul derulant.
  - Apăsaţi **Editare** pentru a modifica **Filtrul de căutare utilizator**.
- Faceţi clic pe **OK** când aţi terminat.

Înlăturare regiune:

Folosiţi aceste informaţii pentru a înlătura o regiune.

Expandaţi categoria **Regiuni şi şabloane utilizator** din zona de navigare a uneltei de administrare web.

1. Apăsaţi pe **Gestionare regiuni**.
2. Selectaţi regiunea pe care doriţi să o înlăturaţi:
3. Faceţi clic pe **Ştergere**
4. Când vi se cere să confirmaţi ştergerea, apăsaţi **OK**.
5. Regiunea este înlăturată din lista de regiuni.

Editarea ACL-urilor pe regiune:

Folosiţi aceste informaţii pentru a edita ACL-urile pe regiune.

Pentru a vedea proprietăţile ACL folosind unealta de administrare Web şi să lucraţi cu ACL-uri, vedeţi “Listă control acces taskuri (ACL)” la pagina 203.

Concepte înrudite

“Listele de control al accesului” la pagina 63
Listele de control al accesului (Access control list - ACL) oferă un mijloc de a proteja informaţiile stocate într-un director LDAP. Administratorii folosesc ACL-urile pentru a restricţiona accesul la diverse porţiuni ale directorului sau la anumite intrări din director.

Taskuri de şablon

Folosiţi aceste informaţii pentru a gestiona şabloane.

După ce v-aţi creat şablonul iniţial, puteţi adăuga mai multe şabloane sau să modificaţi şabloane existente.

Expandaţi categoria **Regiuni şi şabloane** din zona de navigare şi apăsaţi **Gestionare şabloane utilizator**. Este afişată o listă cu şabloanele existente. Din acest panou puteţi adăuga un şablon, edita un şablon, şterge un şablon sau edita listele de control al accesului (ACL-uri) pentru şablon.

Adăugarea unui şablon de utilizator:

Folosiţi aceste informaţii pentru a adăuga un şablon de utilizator.

Expandaţi categoria **Regiuni şi şabloane utilizator** din zona de navigare a uneltei de administrare web.

1. Apăsaţi pe **Adăugare şablon utilizator** sau apăsaţi pe **Gestionare şabloane utilizator** şi apăsaţi **Adăugare**.
   - Introduceţi numele pentru noul şablon. De exemplu **template2** .
   - Dacă aveţi şabloane preexistente, de exemplu **template1**, puteţi selecta un şablon pentru a avea setările copiate la şablonul pe care îl creaţi.
   - Introduceţi DN-ul părinte care identifică locaţia şablonului. Acesată intrare este sub forma unui DN, de exemplu **cn=realm1,o=ibm,c=us**. Puteţi de asemenea să apăsaţi pe **Răsfoire** pentru a selecta locaţia subarborelui pe care îl douiţi.
2. Apăsaţi **Următorul**. Puteţi apăsa pe **Sfârşit** pentru a crea un nou şablon gol. Puteţi să adăugaţi mai târziu informaţii la şablon, vedeţi “Editarea unui şablon” la pagina 202.
3. Dacă aţi apăsat pe **Continuare**, alegeţi clasa de obiecte structurală pentru şablon, de exemplu **inetOrgPerson**. Puteţi de asemenea să adăugaţi clase de obiecte auxiliare pe care le doriţi.
4. Apăsaţi **Următorul**.
5. A fost creată o fişă **Obligatorii** în acest şablon. Puteţi modifica informaţiile conţinute în această fişă.
   a. Selectaţi **Obligatorii** în meniul de fişe şi apăsaţi **Editare**. Este afişat panoul **Editare fişă**. Vedeţi numele fişei **Obligatorii** şi atributele seletate care sunt obligatorii pentru clasa de obiecte, **inetOrgPerson**:
      - *sn - surname
      - *cn - common name

Notă: * indică informaţii obligatorii.

b. Dacă vreţi să adăugaţi informaţii suplimentare la această fişă, selectaţi atributul din meniul **Atribute**. De exemplu, selectaţi **departmentNumber** şi apăsaţi **Adăugare**. Selecta'i **Numărangajat** şi faceţi clic pe **Adăugare**. Selectaţi **title** şi apăsaţi **Adăugare**. Meniul **Atribute selectate** arată acum:
   - title
   - employeeNumber
   - departmentNumber
   - *sn
   - *cn

c. Puteţi rearanja ordinea în care apar aceste câmpuri în şablon prin evidenţierea atributului selectat şi apăsând pe **Mută în sus** sau **Mută în jos**. Aceasta schimbă poziţia atributului cu o poziţie. Repetaţi această procedură până când aţi aranjat atributele în ordinea în care le vreţi. De exemplu,
   - *sn
   - *cn
   - title
   - employeeNumber
   - departmentNumber

d. Puteţi de asemenea modifica fiecare atribut selectat.
   1) Evidenţiaţi atributul în căsuţa **Atribute selectate** şi apăsaţi **Editare**.
   2) Puteţi schimba numele de afişare al câmpului folosit în şablon. De exemplu, dacă vreţi ca **departmentNumber** să fie afişat ca **Număr departament** introduceţi asta în câmpul **Nume afişat**.
   3) Puteţi de asemenea să furnizaţi o valoare implicită care să completeze câmpul atributului în şablon. De exemplu, dacă majoritatea utilizatorilor care vor fi introduşi sunt membri ai Departmentului 789, puteţi introduce 789 ca valoare implicită. Câmpul din şablon este precompletat cu 789. Valoarea poate fi schimbată când adăugaţi informaţiile efective despre utilizator.
   4) Apăsaţi **OK**.

e. Apăsaţi **OK**.

6. Pentru a crea o altă categorie de fişă pentru informaţii suplimentare, apăsaţi **Adăugare**.
   - Introduceţi numele pentru noua fişă. De exemplu, Informaţii de adresă.
   - Pentru această fişă, selectaţi atributele din meniul **Atribute** . De exemplu, selectaţi **homePostalAddress** şi apăsaţi **Adăugare**. Selectaţi **postOfficeBox** şi apăsaţi **Adăugare**. Selectaţi **telephoneNumber** şi apăsaţi **Adăugare**. Selectaţi **Telefonacasă** şi faceţi clic pe **Adăugare**. Selectaţi **facsimileTelephoneNumber** şi faceţi clic pe **Adăugare**. Meniul **Atribute selectate** arată acum:
     – homePostalAddress
     – postOfficeBox
     – telephoneNumber
     – homePhone
     – facsimileTelephoneNumber
   - Puteţi rearanja ordinea în care apar aceste câmpuri în şablon prin evidenţierea atributului selectat şi apăsând pe **Mută în sus** sau **Mută în jos**. Aceasta schimbă poziţia atributului cu o poziţie. Repetaţi această procedură până când aţi aranjat atributele în ordinea în care le vreţi. De exemplu,
     – homePostalAddress
     – postOfficeBox
     – telephoneNumber
     – facsimileTelephoneNumber
     – homePhone
   - Apăsaţi **OK**.

7. Repetaţi acest proces pentru atâtea fişe câte vreţi să creaţi. Când aţi terminat apăsaţi **Sfârşit** pentru a crea şablonul.

Editarea unui şablon:

Folosiţi aceste informaţii pentru a edita un şablon.

Expandaţi categoria **Regiuni şi şabloane utilizator** din zona de navigare a uneltei de administrare web.

- Apăsaţi **Gestionare şabloane utilizator**.
- Selectaţi regiunea pe care vreţi să o editaţi din lista de regiuni.
- Faceţi clic pe **Editare**.
- Dacă aveţi şabloane preexistente, de exemplu template1, puteţi selecta un şablon pentru a avea setările copiate la şablonul pe care îl editaţi.
- Apăsaţi **Următorul**.
  - Puteţi utiliza meniul derulant pentru a modifica clasa de obiecte structurală a şablonului.
  - Puteţi adăuga şi înlătura clase de obiecte auxiliare.
- Apăsaţi **Următorul**.
- Puteţi modifica fişele şi atributele conţinute într-un şablon. Vedeţi 5 la pagina 200 pentru informaţii despre modificarea fişelor.
- Când aţi terminat, faceţi clic pe **Sfârşit**.

Înlăturare şablon:

Folosiţi aceste informaţii pentru a înlătura un şablon.

Expandaţi categoria **Regiuni şi şabloane utilizator** din zona de navigare a uneltei de administrare web.

1. Apăsaţi **Gestionare şabloane utilizator**.
2. Selectaţi şablonul pe care vreţi să îl ştergeţi.
3. Faceţi clic pe **Ştergere**
4. Când vi se cere să confirmaţi ştergerea, apăsaţi **OK**.
5. Şablonul este înlăturat din lista de utilizatori.

Editarea ACL-urilor pentru şablon:

Folosiţi aceste informaţii pentru a edita ACL-uri pentru şablon.

Expandaţi categoria **Regiuni şi şabloane utilizator** din zona de navigare a uneltei de administrare web.

1. Apăsaţi **Gestionare şabloane utilizator**.
2. Selectaţi şablonul pentru care vreţi să editaţi ACL-urile.
3. Faceţi clic pe **Editare ACL**.

Pentru a vedea proprietăţile ACL folosind unealta de administrare Web şi să lucraţi cu ACL-uri, vedeţi “Listă control acces taskuri (ACL)” la pagina 203.

Concepte înrudite

“Listele de control al accesului” la pagina 63
Listele de control al accesului (Access control list - ACL) oferă un mijloc de a proteja informaţiile stocate într-un director LDAP. Administratorii folosesc ACL-urile pentru a restricţiona accesul la diverse porţiuni ale directorului sau la anumite intrări din director.

Listă control acces taskuri (ACL)

utilizaţi aceste informaţii pentru a gestiona liste de control acces (ACL-uri).

Concepte înrudite

"Listele de control al accesului" la pagina 63
Listele de control al accesului (Access control list - ACL) oferă un mijloc de a proteja informaţiile stocate într-un director LDAP. Administratorii folosesc ACL-urile pentru a restricţiona accesul la diverse porţiuni ale directorului sau la anumite intrări din director.

Vizualizarea drepturilor de acces pentru un ACL efectiv specific

Folosiţi aceste informaţii pentru a vizualiza drepturi de acces pentru o listă de control acces efectivă specifică (ACL).

ACL-urile efective sunt ACL-urile explicite şi moştenite ale intrării selectate.

1. Selectaţi o intrare director. De exemplu, cn=John Doe,ou=Advertising,o=ibm,c=US.
2. Faceţi clic pe **Editare ACL**. Panoul Editare ACL este afişat cu fişa preselectată **ACL-uri efective**. Fişa **ACL-uri efective** conţine informaţii numai citire despre ACL-uri.
3. Selectând ACL-ul efectiv specific şi faceţi clic pe butonul **Vizualizare**. Se deschide panoul **Vizualizare drepturi de acces**.
4. Apăsaţi pe **OK** pentru a reveni la fişa ACL-uri efective.
5. Apăsaţi **Anulare** pentru a reveni la panoul Editare ACL.

Vizualizarea proprietarilor efectivi

Folosiţi aceste informaţii pentru a afişa proprietarii efectivi.

Proprietari efectivi sunt proprietarii expliciţi şi moşteniţi ai intrării selectate.

1. Selectaţi o intrare director. De exemplu, cn=John Doe,ou=Advertising,o=ibm,c=US.
2. Faceţi clic pe **Editare ACL**.
3. Faceţi clic pe fişa **Proprietari efectivi**. Fişa **Proprietari efectivi** conţine informaţii numai citire despre ACL-uri.
4. Apăsaţi **Anulare** pentru a reveni la panoul Editare ACL.

Adăugarea, editarea şi înlăturarea ACL-urilor nefiltrate

Folosiţi aceste informaţii pentru a gestiona liste de control acces nefiltrate (ACL-uri).

Puteţi adăuga ACL-uri nefiltrate într-o intrare sau să editaţi ACL-urile nefiltrate existente.

ACL-urile nefiltrate pot fi propagate. Aceasta înseamnă că informaţiile de cotrol acces definite pentru o intrare pot fi aplicate la toate intrările subordonate. Sursa ACL este sursa ACL-ului curent pentru intrarea selectată. Dacă intrarea nu are un ACL, el moşteneşte un ACL de la obiectele părinte pe baza setărilor ACL ale obiectelor părinte.

Introduceţi următoarele infos în fişa de ACL-uri **Nefiltrate**:

- Propagaţi ACL-uri - Selectaţi caseta de bifare **Propagare** pentru a permite descendenţilor fără un ACL definit explicit pentru a moşteni această intrare. Dacă caseta de bifare este selectată descendentul moştenesc ACL-urile din această intrare şi dacă ACL-ul este4 explicit definit pentru intrarea copil, atunci ACL-ul care a fost moştenit de la părinte cu noul ACL care a fsot adăugat. Dacă caseta de bifare nu este selectată, intrările descendent fără un ACL definit explicit va moşteni ACL-uri de la un părinte al intrării care are această opţiune activată.
- DN (NUme distinctiv) - Introduceţi **numele distinctiv (DN)** al entităţii care cere acces pentru a executa operaţii pe intrarea selectată, de exemplu, cn=Marketing Group.
- Tip - Introduceţi **Tipul** DN-ului. De exemplu, selectaţi ID-ul de acces dacă DN-ul este un utilizator.

Faceţi clic fie pe butonul **Adăugare** pentru a adăuga DN-ul în câmpul DN (Nume distinctiv) în lista ACL, fie butonul Editare pentru a modifica ACL-urile unui DN existent.

Panourile **Adăugare drepturi de acces** şi **Editare drepturi de acces** vă permit să setaţi drepturile de acces pentru un ACL (listă de control acces) nou sau existent. Câmpul **Tip** revine la valoarea implicită a tipului pe care l-aţi selectat în panoul **Editare ACL**. Dacă adăugaţi un ACL, toate celelalte câmpuri sunt implicit goale. Dacă editaţi un ACL, câmpurile conţin valorile setate ultima oară când a fost modificat ACL-ul.

Puteţi:

- Modifica tipul ACL-ului
- Seta drepturi de adăugare şi ştergere
- Seta permisiuni pentru clase de securitate

Pentru a seta drepturi de acces:

1. Selectaţi **Tip** al intrării pentru ACL. De exemplu, selectaţi ID-ul de acces dacă DN-ul este un utilizator.
2. Secţiunea **Drepturi** afişează adăugarea şi ştergerea drepturilor pentru subiect.
   - **Adăugare copil** acordă sau respinge subiectului dreptul de a adăuga o intrare director sub intrarea selectată.
   - **Ştergere intrare** acordă sau respinge subiectului dreptul de a şterge intrarea selectată.
3. Secţiunea **Clasă de securitate** defineşte permisiunile pentru clasele de atribute. Atributele sunt grupate în clase de securitate:
   - **Normal** - Clasele de atribute normale necesită cea mai mică securitate, de exemplu, atributul commonName.
   - **Sensibil** - Clasele de atribute sensibile necesită o securitate moderată, de exemplu homePhone.
   - **Critic** - Clasele de atribute critice necesită cea mai mare securitate, de exemplu, atributul userpassword.
   - **Sistem** - Atributele sistem sunt atribute doar citire care sunt menţinute de server.
   - **Restricţionat** - Atributele restricţionate sunt folosite pentru a defini controlul accesului.

   Fiecare clasă de securitate are permisiuni asociate cu ea.
   - Citire - subiectul poate citi atribute.
   - Scriere - subiectul poate modifica atributele.
   - Căutare - subiectul poate căuta atribute.
   - Comparare - subiectul poate compara atribute.

   Suplimentar, puteţi spcifica permisiuni bazete pe atribut în locul clasei de securitate de care atributul aparţine. Secţiunea de atribute este listată sub **Clasa de securitate critică**.
   - Selectaţi un atribut din lista derulantă **Definire atribut**.
   - Faceţi clic pe **Definire**. Atributul este afişat cu tabela de permisiuni.
   - Specificaţi dacă să acordaţi sau să refuzaţi fiecare din cele 4 permisiuni de clase de securitate asociate cu atributul.
   - Puteţi repeta această procedură pentru atribute multiple.
   - Pentru a înlătura un atribut, selectaţi doar atributul şi apăsaţi pe **Ştergere**.
   - Când terminaţi, apăsaţi **OK**.

Puteţi înlătura ACL-urile în fiecare din următoarele 2 modalităţi:

- Selectaţi butonul radio de lângă ACL-ul pe care doriţi să îl ştergeţi. Faceţi clic pe **Înlăturare**.
- Apăsaţi **Înlăturare toate** pentru a şterge toate DN-urile din listă.

Adăugarea, editarea şi înlăturarea ACL-urilor filtrate

Folosiţi aceste informaţii pentru a vizualiza drepturile de acces pentru listă de control acces filtrată (ACL).

Puteţi adăuga noi ACL-uri noi filtrate la o intrare sau să editaţi ACL-uri la o intrare sau să editaţi ACL-uri filtrate existente.

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

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

Introduceţi următoarele infos în fişa ACL-uri filtrate.

- Acumulaţi ACL-uri filtrate -
  - Selectaţi butonul radio în **Nespecificat** pentru a înlătura atributul ibm-filterACLInherit din intrarea selectată.
  - Selectaţi butonul radio **Adevărat** pentru a permite ACL-urilor pentru intrarea selectată să se acumuleze din acea intrare în sus de-a lungul lanţului de intrare următor, la cel mai înalt filtru ACL conţinând intrarea în DIT.
  - Selectaţi butonul radio **Fals** pentru a opri acumularea de ACL-uri de filtrare la intrarea selectată.
- DN (NUme distinctiv) - Introduceţi **numele distinctiv (DN)** al entităţii care cere acces pentru a executa operaţii pe intrarea selectată, de exemplu, cn=Marketing Group.
- Tip - Introduceţi **Tipul** DN-ului. De exemplu, selectaţi ID-ul de acces dacă DN-ul este un utilizator.

Faceţi clic fie pe butonul **Adăugare** pentru a adăuga DN-ul în câmpul DN (Nume distinctiv) în lista ACL, fie butonul Editare pentru a modifica ACL-urile unui DN existent.

Panourile **Adăugare drepturi de acces** şi **Editare drepturi de acces** vă permit să setaţi drepturile de acces pentru un ACL (listă de control acces) nou sau existent. Câmpul Tip revine la valoarea implicită pe care aţi selectat-o în panoul Editare ACL. Dacă adăugaţi un ACL, toate celelalte câmpuri sunt implicit goale. Dacă editaţi un ACL, câmpurile conţin valorile setate ultima oară când a fost modificat ACL-ul.

Puteţi:

- Modifica tipul ACL-ului
- Seta drepturi de adăugare şi ştergere
- Seta filtrul obiect pentru ACL-uri filtrate
- Seta permisiuni pentru clase de securitate

Pentru a seta drepturi de acces:

1. Selectaţi **Tip** al intrării pentru ACL. De exemplu, selectaţi ID-ul de acces dacă DN-ul este un utilizator.
2. Secţiunea **Drepturi** afişează adăugarea şi ştergerea drepturilor pentru subiect.
   - **Adăugare copil** acordă sau respinge subiectului dreptul de a adăuga o intrare director sub intrarea selectată.
   - **Ştergere intrare** acordă sau respinge subiectului dreptul de a şterge intrarea selectată.
3. Seta filtrul obiect pentru o comparaţie bazată pe filtru. În câmpul **Filtru obiect**, introduceţi filtrul de obiect dorit pentru ACL-ul selectat. Faceţi clic pe butonul **Editare filtru** pentru ajutor în compunerea şirul filtrului de căutare. ACL-ul filtrat curent se propagă în fiecare obiect descendent din subarborele asociat care se potriveşte cu filtrul din acel câmp.
4. Secţiunea **Clasă de securitate** defineşte permisiunile pentru clasele de atribute. Atributele sunt grupate în clase de securitate:
   - **Normal** - Clasele de atribute normale necesită cea mai mică securitate, de exemplu, atributul commonName.
   - **Sensibil** - Clasele de atribute sensibile necesită o securitate moderată, de exemplu homePhone.
   - **Critic** - Clasele de atribute critice necesită cea mai mare securitate, de exemplu, atributul userpassword.
   - **Sistem** - Atributele sistem sunt atribute doar citire care sunt menţinute de server.
   - **Restricţionat** - Atributele restricţionate sunt folosite pentru a defini controlul accesului.

   Fiecare clasă de securitate are permisiuni asociate cu ea.
   - Citire - subiectul poate citi atribute.
   - Scriere - subiectul poate modifica atributele.

- Căutare - subiectul poate căuta atribute.
- Comparare - subiectul poate compara atribute.

Suplimentar, puteţi spcifica permisiuni bazete pe atribut în locul clasei de securitate de care atributul aparţine. Secţiunea de atribute este listată sub **Clasa de securitate critică**.

- Selectaţi un atribut din lista derulantă **Definire atribut**.
- Faceţi clic pe **Definire**. Atributul este afişat cu tabela de permisiuni.
- Specificaţi dacă să acordaţi sau să refuzaţi fiecare din cele 4 permisiuni de clase de securitate asociate cu atributul.
- Puteţi repeta această procedură pentru atribute multiple.
- Pentru a înlătura un atribut, selectaţi doar atributul şi apăsaţi pe **Ştergere**.
- Când terminaţi, apăsaţi **OK**.

Puteţi înlătura ACL-urile în fiecare din următoarele 2 modalităţi:

- Selectaţi butonul radio de lângă ACL-ul pe care doriţi să îl ştergeţi. Faceţi clic pe **Înlăturare**.
- Apăsaţi **Înlăturare toate** pentru a şterge toate DN-urile din listă.

Adăugarea sau înlăturarea proprietarilor

Folosiţi aceste informaţii pentru a adăuga sau înlătura proprietari.

Proprietarii de intrare au permisiuni complete pentru a efectua orice operaţie asupra obiectului. Proprietarii de intrare pot fi expliciţi sau propagaţi (moşteniţi).

Introduceţi următoarele informaţii în fişa de **Proprietari**:

1. Selectaţi caseta de bifare **Propagare proprietari** pentru a permite desccendenţilor fără un proprietar definit explicit să moştenească din această intrare. Dacă caseta de bifare nu este selectată, intrările descendent fără un proprietar definit explicit vor moşteni proprietari de la un părinte al intrării care are această opţiune activată.
2. DN (NUme distinctiv) - Introduceţi **numele distinctiv (DN)** al entităţii care cere acces pentru a executa operaţii pe intrarea selectată, de exemplu, cn=Marketing Group. Folosirea cn=this cu obiecte care îşi propagă dreptul de proprietate la alte obiecte face mai uşoară crearea unui subarbore de creare în care fiecare obiect este deţinut de el însuşi.
3. Tip - Introduceţi **Tipul** DN-ului. De exemplu, selectaţi ID-ul de acces dacă DN-ul este un utilizator.

Pentru a adăuga un proprietar, faceţi clic pe **Adăugare** pentru a adăuga DN-ul în câmpul **DN (Nume distinctiv)** la listă.

Puteţi înlătura un proprietar în fiecare din următoarele 2 modalităţi:

- Selectaţi butonul radio de lângă DN-ul proprietarului pe care vreţi să îl ştergeţi. Faceţi clic pe **Înlăturare**.
- Apăsaţi **Înlăturare toate** pentru a şterge toate DN-urile din listă.

Referinţe

Material de referinţă referitor la Directory Server, cum ar fi informaţiile despre utilitarele pentru linia de comandă şi LDIF.

Vedeţi următoarele informaţii de referinţe adiţionale.

Utilitare pentru linie de comandă server de director

Această secţiune descrie utilitarele Directory Server ce pot fi rulate din mediul comandă Qshell.

Reţineţi că unele şiruri trebuie să fie încadrate de ghilimele pentru a fi procesate corect în mediul de comandă Qshell. Aceasta este în general valabil pentru şirurile care sunt DN-uri, filtre de căutare şi lista de atribute întoarsă de ldapsearch. Vedeţi următoarea listă pentru următoarele exemple.

- Şirurile care conţin spaţii: "cn=John Smith,cn=users"
- Şirurile care conţin caractere wildcard "*"
- Şirurile care conţin paranteze "(objectclass=person)"

Pentru informaţii suplimentare despre mediul de comandă Qshell, vedeţi subiectul “Qshell”.

Vedeţi următoarele comenzi pentru informaţii:

ldapmodify şi ldapadd

Utilitarele de linie de comandă modificare-intrare LDAP şi adăugare-intrare LDAP.

Sinopsis

```
ldapmodify [-a] [-b] [-c] [-C charset] [-d debuglevel][-D binddn] [-e errorfile]
[-g] [-f file][-F][-g][-G realm] [-h ldaphost] [-i file] [-k] [-K keyfile]
[-m mechanism] [-M][-n][-N certificatename] [-O maxhops] [-p ldapport]
[-P keyfilepw] [-r] [-R][-U username] [-v] [-V] [-w passwd | ?] [-y proxydn]
[-Y] [-Z]
```

```
ldapadd [-a] [-b] [-c] [-C charset] [-d debuglevel] [-D binddn] [-e errorfile]
[-g] [-f file][-F][-g][-G realm] [-h ldaphost] [-i file] [-k] [-K keyfile]
[-m mechanism] [-M][-n][-N certificatename] [-O maxhops] [-p ldapport]
[-P keyfilepw] [-r] [-R][-U username] [-v] [-V] [-w passwd | ?] [-y proxydn]
[-Y] [-Z]
```

Descriere

ldapmodify este o interfaţă în linie de comandă la API-urile (application programming iterfaces) ldap_modify, ldap_add, ldap_delete şi ldap_rename. **ldapadd** este implementat ca o versiune redenumită a ldapmodify. Când este invocat ca ldapadd, steguleţul **-a** (adăugare intrare nouă) este activat automat.

ldapmodify deschide o conexiune la serverul LDAP şi face legătura la server. Puteţi folosi **ldapmodify** pentru a modifica sau adăuga intrări. Informaţiile de intrare sunt citite de la intrarea standard sau din fişier prin folosirea opţiunii **-i**.

Pentru a afişa ajutorul de sintaxă pentru **ldapmodify** sau pentru **ldapadd**, introduceţi

```
ldapmodify -?
```

sau

```
ldapadd -?
```

Opţiuni

-a Adăugaţi intrări noi. Acţiunea implicită pentru **ldapmodify** este de a modifica intrările existente. Dacă este invocat ca**ldapadd**, acest steguleţ este mereu setat.

-b Presupuneţi că orice valori care încep cu un `/’ sunt valori binare şi că valoarea reală se află într-un fişier a cărui cale este specificată în locul valorii.

-c Modul de operare continuu. Erorile sunt raportate, dar **ldapmodify** continuă modificările. Altfel acţiunea implicită este de a ieşi după raportarea unei erori.

-C *charset*
Specifică faptul că şirurile raportate ca intrare utilitarelor **ldapmodify** şi **ldapadd** sunt reprezentate într-un set de caractere local după cum se specifică în setul de caractere şi trebuie să fie convertit la UTF-8. Folosiţi **-C** *charset* ption dacă intrarea şir pagină de cod este diferită faţă de valoarea jobului pagină de cod. Referiţi-vă la API-ul ldap_set_iconv_local_charset() pentru a vedea valorile set de caractere suportate.

-d *debuglevel*
Setaţi nivelul de depanare LDAP la debuglevel.

-D *binddn*
Folosiţi ***binddn*** pentru a lega la directorul LDAP. ***binddn*** este un DN reprezentat pe şiruri. Când se foloseşte cu -m DIGEST-MD5, acesta este utilizat pentru a specifica ID-ul de autorizaţie. Poate fi ori un DN, ori un şir authzId care începe cu ″u:″ sau ″dn:″.

-e *errorfile*
Specifică fişierul în care sunt scrise intrări respinse. Această opţiune necesită opţiunea de operaţii continue -c. Dacă procesarea unei intrări eşuează, intrarea este scrisă în fişierul respins şi numărarea intrărilor respinse avansează. Dacă intrarea comenzii ldapmodify sau ldapadd este de la un fişier, când fişierul este procesat, se dă numărul de intrări totale scrise în fişierul respins.

-f *fişier* Citiţi informaţiile de intrare de modificare de la un fişier LDIF în locul intrării standard. Dacă nu este specificat un fişier LDIF, trebuie să folosiţi intrarea standard pentru a specifica înregistrările de actualizare în format LDIF. Fie opţiunea -i sau -f pot fi folosite pentru a specifica un fişier; comportamentul este identic.

-F Forţaţi aplicarea tuturor modificărilor, indiferent de conţinutul liniilor de intrare care încep cu replică: (implicit, replică: liniile sunt comparate cu portul şi gazda serverului LDAP utilizate pentru a decide dacă o înregistrare a istoricului de replicare ar trebui să fie efectiv aplicată).

-g Nu eliminaţi spaţiile coadă din valorile atribut.

–G Specificaţi regiunea. Acest parametru este opţional. Când este utilizat cu -m DIGEST-MD5, valoarea este transmisă la server în timpul legării.

-h *ldaphost*
Specificaţi o gazdă alternativă în care rulează serverul ldap.

-i *fişier* Citiţi informaţiile de intrare de modificare de la un fişier LDIF în locul intrării standard. Dacă nu este specificat un fişier LDIF, trebuie să folosiţi intrarea standard pentru a specifica înregistrările de actualizare în format LDIF. Fie opţiunea -i sau -f pot fi folosite pentru a specifica un fişier; comportamentul este identic.

-k Specificaţi controlul de administrare server.

-K *keyfile*
Specificaţi numele fişierului bază de date de chei SSL cu extensia implicită **kdb**. Dacă fişierul bază de date de chei nu este în directorul curent, specificaţi numele fişierului bazei de date de chei complet calificat. Dacă numele de fişier bază de date de chei nu este specificat, acest utilitar va căuta prima dată prezenţa unei variabile de mediu SSL_KEYRING cu un nume de fişier asociat. Dacă variabila de mediu SSL_KEYRING nu este definită, fişierul inel de chei sistem va fi folosit, dacă este prezent.

Acest parametru activează efectiv comutatorul **-Z**. Pentru Serverul de director de pe i5/OS dacă utilizaţi -Z şi nu utilizaţi -K sau -N, va fi utilizat certificatul asociat cu ID-ul aplicaţiei Client server de director.

-l Nu copiază modificarea. Elementul de control Nu copiază este utilizat pentru a cere ca o modificare dată să nu fie replicată. Aceasta este intenţionată să fie utilizată de către Topologia de replicare pentru a preveni ca serverul vizat să copieze modificările făcute pentru a primi topologia de replicare în sincronizare, astfel încât să nu provoace modificări altor servere. Acest element de control poate fi utilizat, de asemenea, de către un client administrativ.

-m *mecanism*
Folosiţi ***mechanism*** pentru a specifica mecanismul SASL de folosit pentru legarea la server. Este folosit API-ul ldap_sasl_bind_s() . Parametrul **-m** este ignorat dacă este setat **-V 2**. Dacă **-m** nu este specificat, este folosită autentificarea simplă. Mecanismele valide sunt:

- CRAM-MD5 - protejează parola trimisă serverului.
- EXTERNAL - foloseşte certificatul SSL. Necesită -Z.
- GSSAPI - foloseşte acreditările Kerberos ale utilizatorului.

- DIGEST-MD5 - necesită ca valoarea username să fie trimisă la server de către client. Necesită -U. Parametrul -D (de obicei DN-ul de legare) este folosit pentru a specifica ID-ul de autorizare. Poate fi un DN sau un şir authzId care începe cu u: sau dn:
- OS400_PRFTKN - se autentifică către severul local LDAP ca fiind utilizatorul curent i5/OS ce foloseşte DN-ul utilizatorului în back-end-ul priectat al sistemului. Parametrii -D (DN legare) şi -w (parolă) nu ar trebui specificaţi.

-M Gestionează obiecte referral ca intrări obişnuite.

-n Specifică opţiunea operaţie nu pentru a vă permite să vizualizaţi rezultatul comenzii pe care o lansaţi fără ca să realizaţi de fapt acţiunea pe director. Modificările ce vor fi făcute sunt precedate de către un semn de exclamare şi tipărite la ieşiri standard. Orice erori de sintaxă ce vor fi găsite în procesarea fişierului de intrare, înaintea apelării funcţiilor ce realizează modificările directorului, sunt afişate la erori standard. Această opţiune este în mod special utilă cu opţiunea -v pentru depanarea operaţiilor dacă sunt întâlnite erori.

-N *numecertificat*
Specifică eticheta asociată cu certificatul client din fişierul bază de date chei. Dacă serverul LDAP este configurat pentru a executa doar autentificare server, un certificat client nu este necesar. Dacă serverul LDAP este configurat pentru a executa autentificare client şi server, un certificat client poate fi necesar. ***certificatename*** nu este necesar dacă o pereche de chei certificat/privat a fost desemnată ca implicită pentru fişierul bază de date de chei. Similar, ***certificatename*** nu este necesar dacă este o pereche singură cheie privată/certificat în fişierul bază de date chei desemnat. Acest parametru este ignorat dacă nu este specificat nici **-Z**, nici **-K**. Pentru Serverul de director de pe i5/OS dacă utilizaţi -Z şi nu utilizaţi -K sau -N, va fi utilizat certificatul asociat cu ID-ul aplicaţiei Client server de director.

-O *maxhops*
Specificaţi ***maxhops*** pentru a seta numărul maxim de hop-uri pe care le obţine biblioteca client când se urmăresc acreditările. Numărul de hopuri implicit este 10.

-p *ldapport*
Specificaţi un port TCP alternativ pe care ascultă serverul ldap. Portul LDAP implicit este 389. Dacă **-p** nu este specifcat şi **-Z** este specificat, este folosit portul implicit SSL LDAP.

-P *keyfilepw*
Specifică parola bazei de date chei. Această parolă este necesară pentru a accesa informaţiile cifrate din fişierul bazei de date, care poate include una sau mai multe chei private. Dacă un fişier stivă de parole este asociat cu fişierul bază de date de chei, parola este obţinută din fişierul stivă de parole, iar parametrul **-P** nu este necesar. Acest parametru este ignorat dacă nu este specificat nici **-Z**, nici **-K**.

-r Înlocuieşte valorile existente cu cele implicite.

-R Specifică faptul că referral-ii nu vor fi urmaţi automat.

–U Specificaţi username-ul. Necesar cu -m DIGEST-MD5 şi ignorat cu orice alt mecanism.

-v Foloseşte modul comunicativ, cu multe diagnostice scrise la ieşirea standard.

-V *versiune*
Specifică versiunea LDAP de folosit de către **ldapmodify** când se leagă la serverul LDAP. Implicit, o conexiune V3 LDAP este stabilită. Pentru a selecta explicit LDAP V3, specificaţi **-V 3**. Specificaţi **-V 2** pentru a rula ca aplicaţie LDAP V2.

-w *passwd* **| ?**
Folosiţi ***passwd*** ca parolă pentru autentificare. Folosiţi ? pentru a genera un prompt de parolă.

-y *proxydn*
Setaţi ID proxy pentru opţiunea de autorizare cu proxy.

-Y Folosiţi o conexiune sigură LDAP (TLS).

-Z Foloseşte o conexiune SSL pentru a comunica cu serverul LDAP. Pentru Serverul de director de pe i5/OS dacă utilizaţi -Z şi nu utilizaţi -K sau -N, va fi utilizat certificatul asociat cu ID-ul aplicaţiei Client server de director.

Format intrare

Conţinutul fişierului (sau intrării standard dacă nici un steguleţ **-i** nu este dat la linia de comandă) ar trebui să se conformeze formatului LDIF.

Exemple

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

```
dn: cn=Modify Me, o=University of Higher Learning, c=US
changetype: modify
replace: mail
mail: modme@student.of.life.edu
-
add: title
title: Grand Poobah
-
add: jpegPhoto
jpegPhoto: /tmp/modme.jpeg
-
delete: description
-
```

comanda:

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

va înlocui conţinutul atributului de mail a intrării Modify Me cu valoarea modme@student.of.life.edu, adăugaţi un titlu de Grand Poobah şi conţinutul fişierului /tmp/modme.jpeg ca un jpegPhoto şi va înlătura complet atributul de descriere. Aceleaşi modificări pot fi efectuate folosind vechiul format de intrare ldapmodify:

```
cn=Modify Me, o=University of Higher Learning, c=US
mail=modme@student.of.life.edu
+title=Grand Poobah
+jpegPhoto=/tmp/modme.jpeg
-description
```

şi comanda:

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

Presupunând că există fişierul /tmp/newentry şi are următorul conţinut:

```
dn: cn=John Doe, o=University of Higher Learning, c=US
objectClass: person
cn: John Doe
cn: Johnny
sn: Doe
titlu: cea mai cunoscută persoană mitică din lume
mail: johndoe@student.of.life.edu
uid: jdoe
```

comanda:

```
ldapadd -i /tmp/entrymods
```

adaugă o nouă intrare pentru John Doe, folosind valorile pentru fişierul /tmp/newentry.

Observaţii

Dacă informaţiile de intrare nu sunt furnizate din fişier prin folosirea opţiunii **-i**, comanda **ldapmodify** va aştepta să citească intrări pentru introducerea standard.

Diagnoze

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

Concepte înrudite

"Sufixul (contextul de numire)" la pagina 12
Un sufix (numit şi context de numire) este un DN care identifică cea mai de sus intrare dintr-o ierarhie de director păstrată local.

API-urile LDAP (Lightweight Directory Access Protocol)
Vedeţi API-urile LDAP (Lightweight Directory Access Protocol) pentru informaţii suplimentare despre API Directory Server

"Schemă de configurare Directory Server" la pagina 244
Aceste informaţii descriu Directory Information Tree (DIT) şi atributele care sunt folosite pentru a configura fişierul ibmslapd.conf.

Referinţe înrudite

"Formatul pentru schimbul de date LDAP (LDIF)" la pagina 238
Formatul interschimbare date LDAP este un format text standard pentru reprezentarea obiectelor LDAP şi actualizărilor LDAP (adăugare, modificare, ştergere, modificare DN) într-un formular textual. Fişierele ce conţin înregistrări LDIF pot fi utilizate pentru trasferul datelor între serverele de director sau utilizate ca intrări de către unelte LDAP precum **ldapadd** şi **ldapmodify**.

ldapdelete

Utilitarul pentru linie de comandă de ştergere intrare LDAP.

Sinopsis

```
ldapdelete [-c] [-C charset] [-d debuglevel][-D binddn] [-f file]
[-G realm] [-h ldaphost] [-i file] [-k] [-K keyfile] [-m mechanism]
[-M] [-n] [-N certificatename] [-O maxops] [-p ldapport]
[-P keyfilepw] [-R] [-s][-U username} [-v] [-V version]
[-w passwd | ?] [-y proxydn][-Y] [-Z] [dn]......
```

Descriere

ldapdelete este o interfaţă de linie de comandă pentru API-ul ldap_delete.

ldapdelete deschide o conexiune la serverul LDAP, face legătura şi şterge una sau mai multe intrări. Dacă sunt furnizate unul sau mai multe argumente nume distinctive (DN), intrările cu acele DN-uri sunt şterse. Fiecare DN este un DN reprezentat prin şir. Dacă nu sunt furnizate argumente DN, o listă de DN-uri este citită din intrarea standard sau dintr-un fişier daca steguleţul **-i** este folosit.

Pentru a afişa sintaxa ajutor pentru **ldapdelete**, introduceţi:

```
ldapdelete -?
```

Opţiuni

-c Modul de operare continuu. Erorile sunt raportate, dar **ldapdelete** continuă ştergerile. Altfel acţiunea implicită este de a ieşi după raportarea unei erori.

-C *setdecaractere*
Specifică faptul că DN-urile furnizate ca intrare la utilitarul **ldapdelete** sunt reprezentate într-un set de caractere local, precum este specificat în setul de caractere. Folosiţi opţiunea **-C** *charset* dacă pagina de cod a şirului de intrare este diferită de valoarea de pagină de cod job. Referiţi-vă la API-ul ldap_set_iconv_local_charset() pentru a vedea valorile set de caractere suportate.

-d *niveldepanare*
Setaţi nivelul de depanare LDAP la debuglevel.

-D *binddn*

Folosiţi ***binddn*** pentru a lega la directorul LDAP. ***binddn*** este un DN reprezentat pe şiruri. Când se foloseşte cu -m DIGEST-MD5, acesta este utilizat pentru a specifica ID-ul de autorizaţie. Poate fi ori un DN, ori un şir authzId care începe cu ″u:″ sau ″dn:″.

-f *fişier* Citiţi o serie de linii din fişier, executând o ştergere LDAP pentru fiecare linie de fişier. Fiecare linie din fişier ar trebui să conţină un singur DN (nume distinctiv).

-G *regiune*

Specificaţi regiunea. Acest parametru este opţional. Când este utilizat cu -m DIGEST-MD5, valoarea este transmisă la server în timpul legării.

-h *gazdăldap*

Specifică o gazdă alternativă pe care rulează serverul LDAP.

-i *fişier* Citiţi o serie de linii din fişier, executând o ştergere LDAP pentru fiecare linie de fişier. Fiecare linie din fişier ar trebui să conţină un singur nume distinctiv.

-k Specificaţi să folosiţi controlul de administrare server.

-K *fişiercheie*

Specifică nuumele fişierului bază de date de chei SSL. Dacă fişierul bază de date de chei nu este în directorul curent, specificaţi numele fişierului bazei de date de chei complet calificat.

Dacă utilitarul nu poate localiza baza de date de chei, va folosi un set hard-coded de rădăcina Autorităţii implicită de certificare de înredere. Fişierul bază de date chei conţine tipic unul au mai multe certificate de autorităţi de certificare (CA) care sunt crezute de client. Aceste tipuri de certificate X.509 sunt de asemenea cunoscute ca rădăcini de încredere.

Acest parametru activează efectiv comutatorul **-Z**. Pentru Serverul de director pe i5/OS dacă utilizaţi -Z şi nu utilizaţi -K sau -N, certificatul asociat cu ID-ul aplicaţiei Director servicii clienţi va fi utilizat.

-m *mecanism*

Folosiţi ***mechanism*** pentru a specifica mecanismul SASL de folosit pentru legarea la server. Este folosit API-ul ldap_sasl_bind_s() . Parametrul **-m** este ignorat dacă este setat **-V 2**. Dacă **-m** nu este specificat, este folosită autentificarea simplă. Mecanismele valide sunt:

- CRAM-MD5 - protejează parola trimisă serverului.
- EXTERNAL - foloseşte certificatul SSL. Necesită -Z.
- GSSAPI - utilizează acreditările Kerberos ale utilizatorului.
- DIGEST-MD5 - necesită ca valoarea username să fie trimisă la server de către client. Necesită -U. Parametrul -D (de obicei DN-ul de legare) este folosit pentru a specifica ID-ul de autorizare. Poate fi un DN sau un şir authzId care începe cu u: sau dn:
- OS400_PRFTKN - se autentifică la serverul local LDAP ca utilizatorul i5/OS cur ent utilizând DN-ul utilizatorului backend-ul proiectat al utilizatorului. Parametrii -D (DN legare) şi -w (parolă) nu ar trebui specificaţi.

-M Gestionează obiecte referral ca intrări obişnuite.

-n Arată ce s-ar efectua, însă în realitate nu modifică intrările. Folositoare pentru depanare în conjuncţie cu **-v**.

-N *numecertificat*

Specifică eticheta asociată cu certificatul client din fişierul bază de date chei. Dacă serverul LDAP este configurat pentru a executa doar autentificare server, un certificat client nu este necesar. Dacă serverul LDAP este configurat pentru a executa autentificare client şi server, un certificat client poate fi necesar. ***certificatename*** nu este necesar, dacă o pereche cheie privată/certificat a fost desemnată ca implicită. Similar, ***certificatename*** nu este necesar dacă este o pereche singură cheie privată/certificat în fişierul bază de date chei desemnat. Acest parametru este ignorat dacă nu este specificat nici **-Z**, nici **-K**. Pentru serverul de director i5/OS dacă utilizaţi -Z şi nu utilizaţi -K sau -N, c ertificatul asociat cu ID-ul aplicaţiei Director servicii client va fi utilizat.

-O *maxhops*
Specificaţi ***maxhops*** pentru a seta numărul maxim de hop-uri pe care le obţine biblioteca client când se urmăresc acreditările. Numărul de hopuri implicit este 10.

-p *portldap*
Specificaţi un port TCP alternativ pe care ascultă serverul LDAP. Portul LDAP implicit este 389. Dacă **-p** nu este specifcat şi **-Z** este specificat, este folosit portul implicit SSL LDAP.

-P *keyfilepw*
Specifică parola bazei de date chei. Această parolă este necesară pentru a accesa informaţiile cifrate din fişierul cheie al bazei de date, care poate include una sau mai multe chei private. Dacă un fişier stivă de parole este asociat cu fişierul bază de date de chei, parola este obţinută din fişierul stivă de parole, iar parametrul **-P** nu este necesar. Acest parametru este ignorat dacă nu este specificat nici **-Z**, nici **-K**.

-R Specifică faptul că referral-ii nu vor fi urmaţi automat.

-s Folosiţi această opţiune pentru a şterge subarborele din rădăcina intrării specificate.

–U *numeutilizator*
Specificaţi username-ul. Necesar cu -m DIGEST-MD5 şi ignorat cu orice alt mecanism.

-v Foloseşte modul comunicativ, cu multe diagnostice scrise la ieşirea standard.

-V *versiune*
Specifică versiunea LDAP de folosit de către **ldapdelete** când se leagă la serverul LDAP. Implicit, o conexiune V3 LDAP este stabilită. Pentru a selecta explicit LDAP V3, specificaţi **-V 3**. Specificaţi **-V 2** pentru a rula ca aplicaţie LDAP V2.

-w *passwd* **| ?**
Folosiţi ***passwd*** ca parolă pentru autentificare. Folosiţi ? pentru a genera un prompt de parolă.

-y proxydn
Setaţi ID proxy pentru operaţia de autorizare cu proxy.

–Y Folosiţi o conexiune sigură LDAP (TLS).

-Z Foloseşte o conexiune SSL pentru a comunica cu serverul LDAP. Pentru serverul de director i5/OS dacă utilizaţi -Z şi nu utilizaţi -K sau -N, c ertificatul asociat cu ID-ul aplicaţiei Director servicii client va fi utilizat.

dn Specifică unul sau mai multe argumente DN. Fiecare DN ar trebui să fie un DN reprezentat de şir.

Exemple

Următoarea comandă,

```
ldapdelete -D cn=administrator -w secret "cn=Delete Me, o=University of Life, c=US"
```

încearcă să şteargă intrarea cu numele de commonName ″Delete Me″ direct sub intrarea Universitatea organizaţională a vieţii.

Observaţii

Dacă nu sunt furnizate argumente DN, comanda **ldapdelete** aşteaptă să citească o listă de DN-uri din intrarea standard.

Diagnoze

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

Concepte înrudite

API-urile Directory Server

ldapexop

Utilitarul pentru linie de comandă de operaţie extinsă LDAP.

Sinopsis

```
ldapexop [-C charset] [-d debuglevel][-D binddn][-e] [-G realm]
[-h ldaphost][-help][-K keyfile] [-m mechanism] [-N certificatename]
[-p ldapport] [-P keyfilepw] [-?] [-U] [-v] [-w passwd | ?] [-Y] [-Z]
-op {cascrepl | controlqueue | controlrepl | getAttributes |
getusertype | quiesce | readconfig | uniqueattr}
```

Descriere

Utilitarul **ldapexop** este o interfaţă linie de comandă care furnizează capacitatea de a se lega la serverul de director şi de a emite o singură operaţie extinsă împreună cu orice date care alcătuiesc valoarea operaţiei extinse.

Utilitarul **ldapexop** suportă gazda standard, portul, SSL-ul şi opţiunile de autentificare de toate utilitarele client LDAP. În plus, un set de opţiuni este definit pentru a specifica operaţia ce urmează să fie realizată şi argumentele pentru fiecare operaţie extinsă.

Pentru a afişa ajutorul de sintaxă pentru **ldapexop**, introduceţi:

```
ldapexop -?
```

sau

```
ldapexop -help
```

Opţiuni

Opţiunile pentru comanda ldapexop sunt împărţite în 2 categorii:

1. Opţiunile generale care specifică modul de conectare la serverul de director. Aceste opţiuni trebuie specificat înaintea opţiunilor specifice operaţiei.
2. Opţiunea de operaţie extinsă care identifică operaţia extinsă de realizat.

Opţiuni generale

Aceste opţiuni specifică metodele de conectare la server şi trebuie să fie specificate înaintea opţiunii **-op**.

-C *charset*
: Specifică faptul că DN-urile furnizate ca intrare la utilitarul **ldapexop** sunt reprezentate într-un set de caractere local, precum este specificat în setul de caractere. Folosiţi **-C** *charset* ption dacă intrarea şir pagină de cod este diferită faţă de valoarea jobului pagină de cod. Referiţi-vă la API-ul ldap_set_iconv_local_charset() pentru a vedea valorile set de caractere suportate.

-d *debuglevel*
: Setaţi nivelul de depanare LDAP la debuglevel.

-D *binddn*
: Folosiţi ***binddn*** pentru a lega la directorul LDAP. ***binddn*** este un DN reprezentat pe şiruri. Când se foloseşte cu -m DIGEST-MD5, acesta este utilizat pentru a specifica ID-ul de autorizaţie. Poate fi ori un DN, ori un şir authzId care începe cu ″u:″ sau ″dn:″.

-e Afişează informaţiile versiunii bibliotecii LDAP şi apoi iese.

-G Specificaţi regiunea. Acest parametru este opţional. Când este utilizat cu -m DIGEST-MD5, valoarea este transmisă la server în timpul legării.

-h *ldaphost*
: Specifică o gazdă alternativă pe care rulează serverul LDAP.

-help Afişează sintaxa comenzii şi informaţiile de folosire.

-K *keyfile*

Specifică nuumele fişierului bază de date de chei SSL. Dacă fişierul bază de date de chei nu este în directorul curent, specificaţi numele fişierului bazei de date de chei complet calificat.

Dacă utilitarul nu poate localiza o bază de date de chei, este folosită baza de date de chei sistem. Fişierul bază de date chei conţine tipic unul au mai multe certificate de autorităţi de certificare (CA) care sunt crezute de client. Aceste tipuri de certificate X.509 sunt de asemenea cunoscute ca rădăcini de încredere.

Acest parametru activează efectiv comutatorul **-Z**. Pentru Serverul de director de pe i5/OS dacă utilizaţi -Z şi nu utilizaţi -K sau -N, va fi utilizat certificatul asociat cu ID-ul aplicaţiei Client server de director.

-m *mecanism*

Folosiţi ***mechanism*** pentru a specifica mecanismul SASL de folosit pentru legarea la server. Este folosit API-ul ldap_sasl_bind_s() . Parametrul **-m** este ignorat dacă este setat **-V 2**. Dacă **-m** nu este specificat, este folosită autentificarea simplă. Mecanismele valide sunt:

- CRAM-MD5 - protejează parola trimisă serverului.
- EXTERNAL - foloseşte certificatul SSL. Necesită -Z.
- GSSAPI - foloseşte acreditările Kerberos ale utilizatorului.
- DIGEST-MD5 - necesită ca valoarea username să fie trimisă la server de către client. Necesită -U. Parametrul -D (de obicei DN-ul de legare) este folosit pentru a specifica ID-ul de autorizare. Poate fi un DN sau un şir authzId care începe cu u: sau dn:
- OS400_PRFTKN - se autentifică către severul local LDAP ca fiind utilizatorul curent i5/OS ce foloseşte DN-ul utilizatorului în back-end-ul priectat al sistemului. Parametrii -D (DN legare) şi -w (parolă) nu ar trebui specificaţi.

-N *numecertificat*

Specifică eticheta asociată cu certificatul client din fişierul bază de date chei. Dacă serverul LDAP este configurat pentru a executa doar autentificare server, un certificat client nu este necesar. Dacă serverul LDAP este configurat pentru a executa autentificare client şi server, un certificat client poate fi necesar. ***certificatename*** nu este necesar, dacă o pereche cheie privată/certificat a fost desemnată ca implicită. Similar, ***certificatename*** nu este necesar dacă este o pereche singură cheie privată/certificat în fişierul bază de date chei desemnat. Acest parametru este ignorat dacă nu este specificat nici **-Z**, nici **-K**. Pentru Serverul de director de pe i5/OS dacă utilizaţi -Z şi nu utilizaţi -K sau -N, va fi utilizat certificatul asociat cu ID-ul aplicaţiei Client server de director.

-p *ldapport*

Specificaţi un port TCP alternativ pe care ascultă serverul LDAP. Portul LDAP implicit este 389. Dacă **-p** nu este specifcat şi **-Z** este specificat, este folosit portul implicit SSL LDAP.

-P *keyfilepw*

Specifică parola bazei de date chei. Această parolă este necesară pentru a accesa informaţiile cifrate din fişierul cheie al bazei de date, care poate include una sau mai multe chei private. Dacă un fişier stivă de parole este asociat cu fişierul bază de date de chei, parola este obţinută din fişierul stivă de parole, iar parametrul **-P** nu este necesar. Acest parametru este ignorat dacă nu este specificat nici **-Z**, nici **-K**.

-? Afişează sintaxa comenzii şi informaţiile de folosire.

–U Specificaţi username-ul. Necesar cu -m DIGEST-MD5 şi ignorat cu orice alt mecanism.

-v Foloseşte modul comunicativ, cu multe diagnostice scrise la ieşirea standard.

-w *passwd* **| ?**

Folosiţi ***passwd*** ca parolă pentru autentificare. Folosiţi ? pentru a genera un prompt de parolă.

–Y Folosiţi o conexiune sigură LDAP (TLS).

-Z Foloseşte o conexiune SSL pentru a comunica cu serverul LDAP. Pentru Serverul de director de pe i5/OS dacă utilizaţi -Z şi nu utilizaţi -K sau -N, va fi utilizat certificatul asociat cu ID-ul aplicaţiei Client server de director.

Opţiune operaţii extinse

Opţiunea **-op** operaţie extinsă identifică operaţia extinsă de realizat. Operaţia extinsă poate fi una din următoarele valori:

- **acctstatus**: Stare cont operaţii extinse. Afişează starea contului specificat.

```
ldapexop –op acctstatus –d <DN>
```

-d DN

Identifică DN-ul intrării pentru care trebuie extrasă starea contului.

Starea contului poate fi deschisă, blocată sau expirată.

- **cascrepl**: operaţie extinsă de replicare control de cascadare. Acţiunea cerută este aplicată serverul specificat şi de asemenea transmisă tuturor replicilor subarborelui dat. Dacă oricare dintre acestea sunt înaintate ca replici, ele trec operaţia extinsă împreună cu replicile ei. Operaţia se cascadează în întreaga topologie de replicare.

  -action quiesce | unquiesce | replnow | wait
  Acesta este un atribut necesar care specifică acţiunea de realizat.

  quiesce
  Nu sunt permise actualizări viitoare, cu excepţia replicării.

  unquiesce
  Se reia operaţia normală, sunt acceptate actualizările client.

  replnow
  Face replica tuturor modificărilor din coadă la toate serverele replică cât mai curând posibil indiferent de planificare.

  wait Aşteaptă ca toate actualizările să fie replicate la toate replicile.

  -rc *contextDn*
  Acesta este un atribut necesar care specifică rădăcina subarborelui.

  -timeout *secs*
  Acesta este un atribut opţional care, dacă este prezent, specifică perioada de timeout în secunde. Dacă nu este prezent sau este 0, operaţia aşteaptă nedefinit.

  Exemplu:

```
ldapexop -op cascrepl -action -quiesce -rc "o=acme,c=us" -timeout 60
```

- **clearlog | getlogsize | readlog -log ...**

Aceste trei operaţii suportă un nou fişier istoric:

LostAndFound

Aceste operaţii pot fi utilizate cu serverul de director i5/OS (V6R1 şi mai târziu), dar doar anumite fişiere istoric sunt suportate:

LostAndFound – conflictul de replicare fişier istoric

- **controlqueue**: operaţia extinsă de replicare coadă de control. Această operaţie vă permite să ştergeţi sau să înlăturaţi modificările în aşteptare din lista de modificări de replicare care a fost pusă în coadă şi unde nu sunt rulate din cauza erorilor de replicare. Această operaţie este folositoare când datele replică sunt fixate manual. Veţi folosi atunci această operaţie pentru a evita realizarea unpr eşuări din coadă.

  -skip all | change-id
  Acesta este un atribut necesar.
  - **-skip all** indică să evitaţi toate modificările în curs pentru acest acord.
  - **change-id** identifică singura modificare de evitat. Dacă serverul nu face replicarea aceste modificări acum, cererea eşuează.

  -ra *agreementDn*
  Acesta este un atribut necesar care specifică DN-ul acordului de replicare.

  Exemple:

```
ldapexop -op controlqueue -skip all -ra "cn=server3,
            ibm-replicaSubentry=master1-id,ibm-replicaGroup=default,
            o=acme,c=us"

ldapexop -op controlqueue -skip 2185 -ra "cn=server3,
            ibm-replicaSubentry=master1-id,ibm-replicaGroup=default,
            o=acme,c=us"
```

- **controlrepl**: control replication extended operation

  -action suspend | resume | replnow
  Acesta este un atribut necesar care specifică acţiunea de realizat.

  -rc *contextDn* **| -ra** *agreementDn*
  -rc *contextDn* este DN-ul contextului de replicare. Acţiunea este realizată pentru toate acordurile pentru acest context. **-ra** *agreementDn* este DN-ul acordului de replicare. Acţiunea este realizată pentru acordul de replicare specificat.

  Exemplu:

```
ldapexop -op controlrepl -action suspend -ra "cn=server3,
            ibm-replicaSubentry=master1-id,ibm-replicaGroup=default,
            o=acme,c=us"
```

- **controlreplerr**

Operaţia extinsă controlreplerr vă permite să gestionaţi tabela de erori de replicare de pe un server i5/OS V6R1 (sau IBM Tivoli Directory Server v6.0) sau un server ulterior. Opţiunile sunt:

```
ldapexop -op controlreplerr –show <failure_ID> -ra <agreementDN>
```

Vă permite să vizualizaţi intrările în tabela de erori de replicare

<eşuare_ID>
ID-ul eşuării. Specificaţi 0 pentru a afişa toate intrările.

<agreementDN>
Acordul de replicare cu care este asociat intrarea.

```
ldapexop -op controlreplerr –delete <failure_ID> -ra <agreementDN>
```

Vă permite să ştergeţi intrările din tabela de erori de replicare

<eşuare_ID>
ID-ul eşuării. Specificaţi 0 pentru a afişa toate intrările.

<agreementDN>
Acordul de replicare cu care este asociată intrarea.

```
ldapexop -op controlreplerr –retry <failure_ID> -ra <agreementDN>
```

Vă permite să reîncercaţi o intrare în tabela de erori de replicare

<eşuare_ID>
ID-ul eşuării. Specificaţi 0 pentru a afişa toate intrările.

<agreementDN>
Acordul de replicare cu care este asociată intrarea.

- **evaluateGroups**

Utilitarul ldapexop suportă o operaţie evaluateGroups nouă:

```
ldapexop –op evaluateGroups –d userDN –a <listă de atribute şi fiecare pereche de valori
separate de un space>
```

Afişează o listă de de grupuri de care aparţine utilizatorulDN specificat.

Opţiunea ″–a″ este utilizată pentru a specifica valori de atribute pentru intrare şi să extragă grupuri dinamice ce se potrivesc cu această intrare. Dacă opţiunea ″–a″ nu este specificată cererea va fi trimisă la server doar pentru grupurile statice. Operaţia extinsă este utilizată pentru a extrage informaţii despre aparteneţa la grup pentru un utilizatorDN ce nu există pe server (Spre exemplu, utilizatorulDN reprezintă un membru de grup la distanţă). Atributul opţional ibm-allGroups ar trebui să fie utilizat pentru a lista apartenenţele la grup pentru serverul ce conţine utilizatorDN.

Exemplu:

Pentru a evalua apartenenţa la grup pentru fiecare intrarea uid=sample,cn=users,o=ibm bazată pe valorile atributelor *departmentnumber* şi *objectclass* ale intrării:

```
ldapexop -op evaluateGroups -d uid=sample,cn=users,o=ibm -a objectclass=person
departmentnumber=abc
```

Notă: În mod tipic acestei operaţii extinse îi vor fi date toate valorile atributelor pentru intrarea de interes.

- **getattributes -attrType<*tip*> -matches bool<*valoare*>**

  -attrType {operational | language_tag | attribute_cache | unique | configuration}
  Acesta este un atribut necesar care specifică tipul atributului care este cerut.

  -matches bool {true | false}
  Specifică dacă lista de atribute întoarse se potriveşte cu tipul de atribute specificat de opţiunea -attrType<.

  Exemplu:

  ```
  ldapexop -op getattributes -attrType unique -matches bool true
  ```

  Întoarce o listă cu toate atributele care au fost desemnate ca atribute unice.

  ```
  ldapexop -op getattributes -attrType unique -matches bool false
  ```

  Întoarce o listă cu toate atributele care nu au fost desemnate ca atribute unice.

- **getusertype:** cerere operaţie extinsă tip utilizator

  Această operaţie extinsă întoarce tipul utilizator bazat pe DN-ul legat.

  Exemplu:

  ```
  ldapexop - D <AdminDN> -w <Adminpw> -op getusertype
  ```

  întoarce:

  ```
  Utilizator : root_administrator
  Rol(uri) : server_config_administrator directory_administrator
  Utilizator : global_admin_group_member
  Rol(uri) : directory_administrator
  ```

- **quiesce**: activare sau dezactivare operaţie extinsă de replicare subarbore

  -rc *contextDn*
  Acesta este un atribut necesar care specifică DN-ul contextului (subarbore) replicare pentru a fi activat sau dezactivat.

  -end Acesta este un atribut opţional care, dacă este prezent, specifică dezactivarea subarborelui. Dacă nu este specificat, valoarea implicită este de activare a subarborelui.

  Exemple:

  ```
  ldapexop -op quiesce -rc "o=acme,c=us"

  ldapexop -op quiesce -end -rc "o=ibm,c=us"
  ```

- **readconfig**: operaţia extinsă recitire fişier de configurare

  -domeniu întreg | singur<*intrare DN***><***atribut***>**
  Acesta este un atribut necesar.
  - **entire** indică recitirea întregului fişier de configurare.
  - **single** înseamnă să citiţi singura intrare şi atributul specificat.

  Exemple:

  ```
  ldapexop -op readconfig -scope entire

  ldapexop -op readconfig -scope single "cn=configuration" ibm-slapdAdminPW
  ```

  Notă: Următoarele intrări marcate cu:
  - [1] are efect imediat după o readconfig
  - [2] au efect în noile operaţii

– [3] au efect imediat ce parola este modificată (nu este necesară readconfig)

– [4] sunt suportate de utilitarul liniei de comandă din i5/OS, dar nu sunt suportate de Directory Server i5/OS

```
cn=Configuraţie
ibm-slapdadmindn[2]
ibm-slapdadminpw[2, 3]
ibm-slapderrorlog[1, 4]
ibm-slapdpwencryption[1]
ibm-slapdsizelimit[1]
ibm-slapdsysloglevel[1, 4]
ibm-slapdtimelimit[1]

cn=Front End, cn=Configuration
ibm-slapdaclcache[1]
ibm-slapdaclcachesize[1]
ibm-slapdentrycachesize[1]
ibm-slapdfiltercachebypasslimit[1]
ibm-slapdfiltercachesize[1]
ibm-slapdidletimeout[1]

cn=Event Notification, cn=Configuration
ibm-slapdmaxeventsperconnection[2]
ibm-slapdmaxeventstotal[2]

cn=Transaction, cn=Configuration
ibm-slapdmaxnumoftransactions[2]
ibm-slapdmaxoppertransaction[2]
ibm-slapdmaxtimelimitoftransactions[2]


cn=ConfigDB, cn=Config Backends, cn=IBM SecureWay, cn=Schemas, cn=Configuration
ibm-slapdreadonly[2]

cn=Directory, cn=RDBM Backends, cn=IBM SecureWay, cn=Schemas, cn=Configuration
ibm-slapdbulkloaderrors[1, 4]
ibm-slapdclierrors[1, 4]
ibm-slapdpagedresallownonadmin[2]
ibm-slapdpagedreslmt[2]
ibm-slapdpagesizelmt[2]
ibm-slapdreadonly[2]
ibm-slapdsortkeylimit[2]
ibm-slapdsortsrchallownonadmin[2]
ibm-slapdsuffix[2]
```

- **repltopology -rc [opţiuni]**:

  Operaţia extinsă repltopology este utilizată pentru a face informaţia de replicare topologie de pe un server consumator să se potrivească cu topologia de pe serverul furnizor.

  ```
  ldapexop –op repltopology –rc  [-timeout secs] [-ra agreementDn]
  ```

  unde

  -rc contextDn
  Acesta este un atribut necesar care specifică rădăcina subarborelui.

  -timeout secs
  Acesta este un atribut opţional care, dacă este prezent, specifică perioada de timeout în secunde. Dacă nu este prezent sau este 0, operaţia aşteaptă nedefinit.

  -ra agreementDn
  AcordulDN **-ra** este DN-ul acordului de replicare. Acţiunea este realizată pentru acordul de replicare specificat. Dacă opţiunea -ra nu este specificată, acţiunea este realizată pentru toate acordurile de replicare definite sub context.

  Exemplu:

  ```
  ldapexop -op repltopology -rc "o=acme,c=us" -ra "cn=server3,
            ibm-replicaSubentry=master1-id,ibm-replicaGroup=default,
            o=acme,c=us"-timeout 60
  ```

Serverul furnizor se leagă de serverul consumator utilizând acreditările de replicare configurate. DN-rile furnizoare au autorizarea de a adăuga sufixe la furnizorul configuraţiei unui server consumator. Aceasta este utilizată de către un server furnizor ca fiind parte a operaţiei extinse de Replicare topologie de a adăuga sufixe lipsă la serverul consumator. Pentru sufixe pentru care intrarea contextDN nu există, DN-urile furnizoare au autorizarea de a crea un nou subarbore replicat. Dacă intrarea contextDN există deja, trebuie să fie deja definită ca rădăcina subarborelui replicat; i.e. trebuie să aibe clasa de obiecte ibm-replicationcontext.

- **nelegat** {**-dn**<*specificDN*>| **-ip**<*sourceIP*> | **-dn**<*specificDN*> **-ip**<*sourceIP*> | **tot**}:

  deconectare conexiuni bazată pe DN, IP, DN/IP sau deconectare toate conexiunile. Toate conexiunile fără operaţii şi toate conexiunile cu operaţii din coada de lucru sun terminate imediat. Dacă un lucrător lucrează în prezent la o conexiune, aceasta este terminată imediat ce lucrătorul termină acea singură operaţie.

  -dn<*specificDN*>
  Emite o cerere pentru a termina o conexiune doar prin DN. Această cerere duce la eliminarea tuturor conexiunilor legate la DN-ul specificat.

  -ip<*sourceIP*>
  Emite o cerere pentru a termina o conexiune doar prin IP. Această cerere duce la eliminarea tuturor conexiunilor la sursa IP specificată.

  -dn<*specificDN*> **-ip**<*sourceIP*>
  Emite o cerere pentru a termina o conexiune determinată de o pereche DN/IP. Această cerere duce la eliminarea tuturor conexiunilor legate la DN-ul specificat şi de la o sursă IP specificată.

  -all Emite o cerere pentru a termina toate conexiunile. Această cerere duce la eliminarea tuturor conexiunilor, cu excepţia conexiuniii de la care a plecat această cerere. Acest atribut nu poate fi folosit cu atributele -D sau -IP .

  Exemple:

  ```
  ldapexop -op unbind -dn cn=john
  ldapexop -op unbind -ip 9.182.173.43
  ldapexop -op unbind -dn cn=john -ip 9.182.173.43
  ldapexop -op unbind -all
  ```

- **uniqueattr -a <*attributeType*>:** identifică toate velorile care nu sunt unice pentru un atribut specific.

  -a <*atribut*>
  Specificaţi atributul pentru care sunt afişate toate valorile conflictuale.

  Notă: Nu sunt afişate valorile duplicate pentru atributele binare, operaţionale, de configurare şi atributul objectclass. Aceste atribute nu sunt operaţii extinse suportate pentru atributele unice.

  Exemplu:

  ```
  ldapexop -op uniqueattr -a "uid"
  ```

  Următoarea linie este adăugată în fişierul de configurare sub intrarea ″cn=Directory,cn=RDBM Backends,cn=IBM Directory,cn=schema,cn=Configuration″ pentru această operaţie extinsă:

  ```
  ibm-slapdPlugin: extendedop /QSYS.LIB/QGLDRDBM.SRVPGM initUniqueAttr
  ```

Diagnoze

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

Concepte înrudite

API-urile Directory Server

“Tabela cu erori de replicare” la pagina 43
Tabela cu erori de replicare înregistrează actualizările eşuate, pentru recuperarea ulterioară. Când începe replicarea, este contorizat numărul de eşuări înregistrate pentru fiecare acord de replicare. Acest număr creşte dacă o eşuează o actualizare, fiind adăugată o nouă intrare în tabelă.

Operaţii înrudite

"Vizualizarea fişierului istoric pierdute şi găsite" la pagina 158
Fişierul istoric pierdute şi găsite de replicare poate fi vizualizat utilizând unealta de administrare Web IBM Tivoli Directory Server, folosind opţiunile fişierului istoric al utilitarului ldapexop sau vizualizând fişierul direct.

ldapmodrdn

Utilitarul pentru linie de comandă de modificare intrare LDAP RDN.

Sinopsis

```
ldapmodrdn [-c] [-C charset] [-d debuglevel][-D binddn]
[-f file][-G realm] [-h ldaphost] [-i file] [-k] [-K keyfile]
[-m mechanism] [-M] [-n] [-N certificatename] [-O hopcount]
[-p ldapport] [-P keyfilepw] [-r] [-R] [-U username] [-v] [-V version]
[-w passwd | ?] [-y proxydn] [-Y] [-Z] [dn newrdn | [-i file]]
```

Descriere

ldapmodrdn este o interfaţă în linie de comandă la API-ul ldap_rename.

ldapmodrdn deschide o conexiune la un server LDAP, leagă şi mută sau redenumeşte intrările. Informaţiile de intrare sunt citite de la intrarea standard sau din fişier prin folosirea opţiunii **-f** sau a perechii linie de comandă DN şi RDN. Când se utilizează opţiunea -s pentru a muta intrările, opţiunea -s se aplică la toate intrările acţionate de către comandă.

Pentru a afişa ajutorul de sintaxă pentru **ldapmodrdn**, introduceţi:

```
ldapmodrdn -?
```

Opţiuni

-c Modul de operare continuu. Erorile sunt raportate, dar **ldapmodrdn** continuă modificările. Altfel acţiunea implicită este de a ieşi după raportarea unei erori.

-C *charset*
Specifică faptul că şirurile furnizate ca intrare la utilitarul **ldapmodrdn** sunt reprezentate într-un set de caractere local, precum este specificat în setul de caractere. Folosiţi opţiunea **-C** *charset* dacă pagina de cod a şirului de intrare este diferită de valoarea de pagină de cod job. Referiţi-vă la API-ul ldap_set_iconv_local_charset() pentru a vedea valorile setului de caractere suportate. Notaţi că valorile suportate pentru setul de caractere sunt aceleaşi valori suportate pentru fişa setului de caractere care este definită opţional în Versiunea 1 a fişierelor LDIF.

-d *debuglevel*
Setaţi nivelul de depanare LDAP la debuglevel.

-D *binddn*
Folosiţi ***binddn*** pentru a lega la directorul LDAP. ***binddn*** ar trebui să fie un DN reprezentat pe şiruri. Când se foloseşte cu -m DIGEST-MD5, acesta este utilizat pentru a specifica ID-ul de autorizaţie. Poate fi ori un DN, ori un şir authzId care începe cu ″u:″ sau ″dn:″.

-f *fişier* Citiţi informaţiile de modificare intrare de la un fişier LDIF în locul intrării standard sau al liniei de comandă (specificând dn şi noul rdn). Intrarea standard mai poate fi furnizată de la un fişier (< file).

-G *realm*
Specificaţi regiunea. Acest parametru este opţional. Când este utilizat cu -m DIGEST-MD5, valoarea este transmisă la server în timpul legării.

-h *ldaphost*
Specificaţi o gazdă alternativă în care rulează serverul ldap.

-i *fişier* Citiţi informaţiile de modificare intrare de un fişier în locul intrării standard sau a liniei de comandă (specificând rdn şi newrdn). Intrarea standard poate fi furnizată dintr-un fişier la fel ca şi (″< file″).

-k Specificaţi controlul de administrare server.

-K *keyfile*

Specifică nuumele fişierului bază de date de chei SSL. Dacă fişierul bază de date de chei nu este în directorul curent, specificaţi numele fişierului bazei de date de chei complet calificat.

Dacă utilitarul nu poate localiza baza de date de chei, va folosi un set hard-coded de rădăcina Autorităţii implicită de certificare de înredere. Fişierul bază de date chei conţine tipic unul au mai multe certificate de autorităţi de certificare (CA) care sunt crezute de client. Aceste tipuri de certificate X.509 sunt de asemenea cunoscute ca rădăcini de încredere.

Acest parametru activează efectiv comutatorul **-Z**. Pentru Serverul de director de pe i5/OS dacă utilizaţi -Z şi nu utilizaţi -K sau -N, va fi utilizat certificatul asociat cu ID-ul aplicaţiei Client server de director.

-m *mecanism*

Folosiţi ***mechanism*** pentru a specifica mecanismul SASL de folosit pentru legarea la server. Este folosit API-ul ldap_sasl_bind_s() . Parametrul **-m** este ignorat dacă este setat **-V 2**. Dacă **-m** nu este specificat, este folosită autentificarea simplă. Mecanismele valide sunt:

- CRAM-MD5 - protejează parola trimisă serverului.
- EXTERNAL - foloseşte certificatul SSL. Necesită -Z.
- GSSAPI - foloseşte acreditările Kerberos ale utilizatorului.
- DIGEST-MD5 - necesită ca valoarea username să fie trimisă la server de către client. Necesită -U. Parametrul -D (de obicei DN-ul de legare) este folosit pentru a specifica ID-ul de autorizare. Poate fi un DN sau un şir authzId care începe cu u: sau dn:
- OS400_PRFTKN - se autentifică către severul local LDAP ca fiind utilizatorul curent i5/OS ce foloseşte DN-ul utilizatorului în back-end-ul priectat al sistemului. Parametrii -D (DN legare) şi -w (parolă) nu ar trebui specificaţi.

-M Gestionează obiecte referral ca intrări obişnuite.

-n Arată ce s-ar efectua, însă în realitate nu modifică intrările. Folositoare pentru depanare în conjuncţie cu **-v**.

-N *numecertificat*

Specifică eticheta asociată cu certificatul client din fişierul bază de date chei. Notaţi că dacă serverul LDAP este configurat pentru a executa doar autentificare server, un certificat client nu este necesar. Dacă serverul LDAP este configurat pentru a executa autentificare client şi server, un certificat client poate fi necesar. ***certificatename*** nu este necesar, dacă o pereche cheie privată/certificat a fost desemnată ca implicită. Similar, ***certificatename*** nu este necesar dacă este o pereche singură cheie privată/certificat în fişierul bază de date chei desemnat. Acest parametru este ignorat dacă nu este specificat nici **-Z**, nici **-K**. Pentru Serverul de director de pe i5/OS dacă utilizaţi -Z şi nu utilizaţi -K sau -N, va fi utilizat certificatul asociat cu ID-ul aplicaţiei Client server de director.

-O *numărul de hop-uri*

Specificaţi ***hopcount*** pentru a seta numărul maxim de hopuri pe care le obţine biblioteca client când se urmăresc acreditările. Numărul de hopuri implicit este 10.

-p *ldapport*

Specificaţi un port TCP alternativ pe care ascultă serverul ldap. Portul LDAP implicit este 389. Dacă nu este specificat şi este specificat -Z, este folosit portul SSL LDAP implicit 636.

-P *keyfilepw*

Specifică parola bazei de date chei. Această parolă este necesară pentru a accesa informaţiile criptate din fişierul bazei de date de chei (care poate include una sau mai multe chei private). Dacă un fişier stivă de parole este asociat cu fişierul bază de date de chei, parola este obţinută din fişierul stivă de parole, iar parametrul **-P** nu este necesar. Acest parametru este ignorat dacă nu este specificat nici **-Z**, nici **-K**.

-r Înlăturare valori vechi RDN de la intrare. Acţiunea implicită este de a păstra valorile vechi.

-R Specifică faptul că referral-ii nu vor fi urmaţi automat.

-s newSuperior

Specifică DN-ul noii intrări superioare sub care intrarea redenumită este relocată. Argumentul newSuperior poate fi şirul de lungime zero (-s ″″).

Notă: Opţiunea superior nou nu este suportată la conexiunea cu un server la o ediţie anterioară la V6R1 (ITDS v6.0). Această opţiune este permisă doar pe o intrare frunză.

–U *username*
Specificaţi username-ul. Necesar cu -m DIGEST-MD5 şi ignorat cu orice alt mecanism.

-v Foloseşte modul comunicativ, cu multe diagnostice scrise la ieşirea standard.

-V *versiune*
Specifică versiunea LDAP de folosit de către **ldapmodrdn** când se leagă la serverul LDAP. Implicit, o conexiune V3 LDAP este stabilită. Pentru a selecta explicit LDAP V3, specificaţi **-V 3**. Specificaţi **-V 2** pentru a rula ca aplicaţie LDAP V2. O aplicaţie, ca **ldapmodrdn**, selectează LDAP V3 ca protocol preferat folosind ldap_init în loc de ldap_open.

-w *passwd* **| ?**
Folosiţi ***passwd*** ca parolă pentru autentificare. Folosiţi ? pentru a genera un prompt de parolă.

-y proxydn
Setaţi ID proxy pentru operaţia de autorizare cu proxy.

–Y Folosiţi o conexiune sigură LDAP (TLS).

-Z Foloseşte o conexiune SSL pentru a comunica cu serverul LDAP. Pentru Serverul de director de pe i5/OS dacă utilizaţi -Z şi nu utilizaţi -K sau -N, va fi utilizat certificatul asociat cu ID-ul aplicaţiei Client server de director.

dn newrdn
Vedeţi următoarea secţiune, “Format de intrare pentru dn newrdn” pentru informaţii suplimentare.

Format intrare pentru dn newrdn

Dacă argumentele liniei de comandă *dn* şi *newrdn* sunt date, *newrdn* înlocuieşte RDN-ul intrării specificate de DN, *dn*. Altfel, conţinutul fişierului (sau intrarea standard, dacă nu este dat nici un steguleţ **- i**) conţine una sau mai multe intrări:

```
Nume distinctiv (DN)

Nume distinctiv relativ (RDN)
```

Unul sau mai multe linii blanc pot fi utilizate să separe fiecare DN şi fiecare pereche RDN.

Exemple

Se presupune că fişierul /tmp/entrymods există şi are conţinutul:

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

comanda:

```
ldapmodrdn -r -i /tmp/entrymods
```

modifică RDN-ul intrării Modify Me de la Modify Me către The New Me şi cn-ul vechi, Modify Me este înlăturat.

Observaţii

Dacă informaţiile de intrare nu sunt furnizate din fişier prin folosirea opţiunii **-i** (sa u din perechea din linia de comandă *dn* şi *rdn*), comanda **ldapmodrdn** va aştepta să citească intrările din intrarea standard.

Diagnoze

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

Concepte înrudite

API-urile Directory Server

“Nume distinctive (DN-uri)” la pagina 9
Fiecare intrare din director are un nume distinctiv (DN). DN-ul este numele care identifică în mod unic o intrare din director. Prima componentă a DN-ului se numeşte nume distinctiv relativ (RDN - Relative Distinguished Name).

ldapsearch

Utilitarul pentru linie de comandă de căutare LDAP.

Sinopsis

```
ldapsearch [-a deref] [-A] [-b searchbase] [-B] [-C charset] [-d debuglevel]
[-D binddn] [-e] [-f file] [-F sep] [-G realm] [-h ldaphost] [-i file] [-K keyfile]
[-l timelimit] [-L] [-m mechanism] [-M] [-n] [-N certificatename]
[-o attr_type] [-O maxhops] [-p ldapport] [-P keyfilepw] [-q pagesize]
[-R] [-s scope ] [-t] [-T seconds] [-U username] [-v] [-V version]
[-w passwd | ?] [-z sizelimit] [-y proxydn] [-Y] [-Z]
filter [-9 p] [-9 s] [attrs...]
```

Descriere

ldapsearch este o interfaţă linie de comandă la API-ul ldap_search.

ldapsearch deschide o conexiune la serverul LDAP, face legătura şi execută o căutare folosind filtru. Filtrul ar trebui să se conformeze la reprezentarea şirului pentru filtrele LDAP (vedeţi ldap_search din API-uri Directory Server pentru informaţii suplimentare despre filtre).

Dacă **ldapsearch** găseşte una sau mai multe intrări, atributele specificate de attrs sunt retrase, iar intrările şi valorile sunt tipărite la ieşirea standard. Dacă nu este listat nici un attrs, toate atributele sunt întoarse.

Pentru a afişa sintaxa ajutor pentru **ldapsearch**, introduceţi ldapsearch -?.

Opţiuni

-a deref
: Specifică cum diferenţierea alias-urilor. deref ar trebui să fie unul dintre niciodată, întotdeauna, căutare sau găsire pentru a specifica faptul că aliasurile nu sunt niciodată dereferenţiate, întotdeauna dereferenţiate, dereferenţiate la căutare sau dereferenţiate doar când se localizează obiectul de bază pentru căutare. Implicit este ca niciodată să nu se diferenţieze alias-urile.

-A
: Extrage doar atributele (fără valori). Aceasta este folositoare când doar vreţi să vedeţi dacă un atribut este prezent într-o intrare şi nu sunteţi interesat de valorile specifice.

-b searchbase
: Folosiţi searchbase ca punct de pornire pentru căutare în locul valorii implicite. Dacă nu este specificat **-b**, acest utilitar va examina variabila de mediu LDAP_BASEDN pentru o definiţie searchbase. Dacă nu este specificat nimic, baza implicită este setată la ″″.

-B
: Nu suprimaţi afişarea valorilor non-ASCII. Aceasta este utilă atunci când lucraţi cu valori care apar în seturi de caractere alternative precum ISO-8859.1. Această opţiune este impusă de opţiunea **-L**.

-C charset
: Specifică faptul că şirurile furnizate ca intrare pentru utilitarul ldapsearch sunt reprezentate într-un set de caractere local (după cum este specificat de charset). Intrarea şir include filtrul, DN-ul de legare şi DN-ul de bază. Similar, când afişaţi date, **ldapsearch** converteşte datele primite de la serverul LDAP la setul de caractere specificat. Folosiţi opţiunea **-C charset** dacă pagina de cod şir de intrare este diferită de valoarea paginii de cod a jobului. Referiţi-vă la API-ul ldap_set_iconv_local_charset() pentru a vedea valorile set de caractere suportate. De asemenea, dacă opţiunile **-C** şi **-L** sunt ambele specificate, intrarea se presupune că este specificată în setul de caractere specificat, dar ieşirea de la **ldapsearch** este mereu păstrată în reprezentarea sa UTF-8 sau o reprezentare codată base-64 a datelor când sunt detectate caractere netipăribile.

Aceasta este situaţia dacă fişierele standard LDIF conţin doar reprezentări UTF-8 (sau UTF-8 codat base-64) a datelor şir. Notaţi că valorile suportate pentru charset sunt aceleaşi valori suportate pentru fişa charset care este definită opţional în fişierele LDIF cu Versiunea 1.

-d debuglevel
Setaţi nivelul de depanare LDAP la debuglevel.

-D binddn
Folosiţi binddn pentru legarea la directorul LDAP. ***binddn*** ar trebui să fie un DN reprezentat pe şiruri (vedeţi Nume distinctiv LDAP). Când se foloseşte cu -m DIGEST-MD5, acesta este utilizat pentru a specifica ID-ul de autorizaţie. Poate fi ori un DN, ori un şir authzId care începe cu ″u:″ sau ″dn:″.

-e Afişaţi informaţiile versiunii bibliotecii LDAP şi apoi ieşiţi.

-F sep Folosiţi sep ca separator de câmp între numele atribut şi valori. Separatorul implicit este `=', doar dacă steguleţul **-L** nu a fost specificat, caz în care această opţiune este ignorată.

-G *regiune*
Specificaţi regiunea. Acest parametru este opţional. Când este utilizat cu -m DIGEST-MD5, valoarea este transmisă la server în timpul legării.

-h ldaphost
Specificaţi o gazdă alternativă în care rulează serverul ldap.

-i file Citiţi o serie de linii din fişier, executând o căutare LDAP pentru fiecare linie. În acest caz, filtrul dat în linia de comandă este tratat ca un model unde prima apariţie a %s este înlocuită cu o linie de fişier. Dacă fişierul este un singur caracter ″-″, atunci liniile sunt citite din intrarea standard.

-K keyfile
Specifică nuumele fişierului bază de date de chei SSL. Dacă fişierul bază de date de chei nu este în directorul curent, specificaţi numele fişierului bazei de date de chei complet calificat.

Dacă utilitarul nu poate localiza baza de date de chei, va folosi un set hard-coded de rădăcina Autorităţii implicită de certificare de înredere. Fişierul bază de date chei conţine tipic unul au mai multe certificate de autorităţi de certificare (CA) care sunt crezute de client. Aceste tipuri de certificate X.509 sunt de asemenea cunoscute ca rădăcini de încredere.

Acest parametru activează efectiv comutatorul **-Z**. Pentru serverul de director i5/OS dacă utilizaţi -Z şi nu utilizaţi -K sau -N, c ertificatul asociat cu ID-ul aplicaţiei Director servicii client va fi utilizat.

-l timelimit
Aşteptaţi cel mult secundele specificate în limita de timp pentru terminarea unei căutări.

-L Afişează rezultatele căutării în format LDIF. Această opţiune activează de asemenea opţiunea **-B** şi cauzează opţiunea **-F** să fie ignorată.

-m *mecanism*
Folosiţi ***mechanism*** pentru a specifica mecanismul SASL de folosit pentru legarea la server. Este folosit API-ul ldap_sasl_bind_s() . Parametrul **-m** este ignorat dacă este setat **-V 2**. Dacă **-m** nu este specificat, este folosită autentificarea simplă. Mecanismele valide sunt:

- CRAM-MD5 - protejează parola trimisă serverului.
- EXTERNAL - foloseşte certificatul SSL. Necesită -Z.
- GSSAPI - utilizează acreditările Kerberos ale utilizatorului.
- DIGEST-MD5 - necesită ca valoarea username să fie trimisă la server de către client. Necesită -U. Parametrul -D (de obicei DN-ul de legare) este folosit pentru a specifica ID-ul de autorizare. Poate fi un DN sau un şir authzId care începe cu u: sau dn:
- OS400_PRFTKN - se autentifică la serverul local LDAP ca utilizatorul i5/OS cur ent utilizând DN-ul utilizatorului backend-ul proiectat al utilizatorului. Parametrii -D (DN legare) şi -w (parolă) nu ar trebui specificaţi.

-M Gestionează obiecte referral ca intrări obişnuite.

-n Arată ce s-ar efectua, însă în realitate nu modifică intrările. Folositoare pentru depanare în conjuncţie cu **-v**.

-N certificatename
Specifică eticheta asociată cu certificatul client din fişierul bază de date chei.

Notă: Dacă serverul LDAP este configurat pentru a executa doar autentificare server, un certificat client nu este necesar. Dacă serverul LDAP este configurat pentru a executa autentificare client şi server, un certificat client poate fi necesar. *certificatename* nu este necesar, dacă o pereche cheie privată/certificat a fost desemnată ca implicită. Similar, *certificatename* nu este necesar dacă este o pereche singură de chei certificate/private în fişierul bază de date chei. Acest parametru este ignorat dacă nu este specificat nici **-Z**, nici **-K**.

Pentru serverul de director i5/OS dacă utilizaţi -Z şi nu utilizaţi -K sau -N, c ertificatul asociat cu ID-ul aplicaţiei Director servicii client va fi utilizat.

-o *attr_type*
Pentru a sepcifica un atribut de folosit pentru criteriile de sortare a rezultatelor căutării, puteţi folosi parametrul -o (order). Puteţi folosi mai mulţi parametri -o pentru a defini în viitor ordinea de sortare. În exemplul următor, rezultatele de căutare sunt sortate mai întâi după numele de familie (sn), apoi după numele de naştere, cu numele dat (givename) fiind sortat în ordine inversă (descrescătoare) precum a fost specificat de semnul minus predefinit (-):

```
-o sn -o -givenname
```

Astfel, sintaxa parametrului de sortare este după cum urmează:

```
[-]<nume atribut>[:<regulă de potrivire OID>]
```

unde

- nume atribut este numele atributului după doriţi să sortaţi.
- OID regulă de potrivire este OID-ul opţional al unei reguli de potrivire pe care doriţi să îl folosiţi pentru sortare. Atributul OID al regulii de potrivire nu este suportat de Directory Server, totuşi alte servere LDAP ar putea suporta acest atribut.
- Semnul minus (-) indică faptul că rezultate trebuie sortate în ordine inversă.
- Starea critică este mereu importantă.

Operaţia implicită ldapsearch nu este de a sorta rezultatele întoarse.

-O maxhops
Specificaţi maxhops pentru a seta numărul maxim de hopuri pe care biblioteca client le foloseşte când vânează referral-ii. Numărul de hopuri implicit este 10.

-p ldapport
Specificaţi un port TCP alternativ pe care ascultă serverul ldap. Portul LDAP implicit este 389. Dacă nu este specificat şi este specificat -Z, este folosit portul SSL LDAP implicit 636.

-P keyfilepw
Specifică parola bazei de date chei. Această parolă este necesară pentru a accesa informaţiile criptate din fişierul bazei de date de chei (care poate include una sau mai multe chei private). Dacă un fişier stivă de parole este asociat cu fişierul bază de date de chei, parola este obţinută din fişierul stivă de parole, iar parametrul **-P** nu este necesar. Acest parametru este ignorat dacă nu este specificat nici **-Z**, nici **-K**.

-q *dimensiunepagină*
Pentru a specifica paginarea rezultatelor de căutare, pot fi folosiţi 2 parametri: -q (dimensiune pagină de interogare) şi -T (timp între căutări în secunde). În următorul exemplu, rezultatele căutării întoarce o pagină (25 de intrări) la un moment dat, la fiecare 15 secunde, până când toate rezultatele pentru acea căutare sunt întoarse. Clientul ldapsearch tratează toată continuarea de conexiune pentru fiecare cerere de rezultate paginate pentru viaţa operaţiei de căutare.

Aceşti parametri pot fi folositori când clientul are resurse limitate sau când este conectat printr-o conexiune de bandă joasă. În general, vă permite să controlaţi rata la care datele sunt întoarse de o cerere de căutare. În loc

să primiţi toate rezultatele o dată, puteţi să obţineţi câteva intrări (o pagină) la un moment dat. În plus, puteţi controla durata întârzierii între fiecare pagină de cerere, dând clientului timp pentru a procesa rezultatele.

```
-q 25  -T 15
```

Dacă parametrul -v (verbose) este specificat, ldapsearch listează câte intrări au fost întoarse până acum, după fiecare pagină de intrări întoarse de la server, de exemplu, **au fost întoarse 30 de intrări.**

Parametrii multipli -q sunt activaţi pentru a putea specifica diferite dimensiuni de pagină de-a lungul vieţii unei singure operaţii de căutare. În următorul exemplu, prima pagină are 15 intrări, a 2-a are 20 de intrări şi a al 3-lea parametrul termină operaţia paginată de căutare/rezultate.

```
-q 15 -q 20 -q 0
```

În exemplul următor, prima pa gină sunt 15 intrări şi tot restul paginilor sunt 20 de intrări, continuând cu ultimul specificat **-q** valoare până când operaţea de căutare s-a terminat:

```
-q 15 -q 20
```

Operaţia implicită ldapsearch este de a întoarce toate intrările într-o singură cerere. Nici o paginare nu este realizată pentru operaţia implicită ldapsearch.

-R Specifică faptul că referral-ii nu vor fi urmaţi automat.

-s scope
Specifică domeniul căutării. Valoarea scope trebuie să fie base, one sau sub pentru a specifica un obiect de bază, un nivel 1 sau o căutare de subarbore. Valoare implicită este sub.

-t Scrie valorile extrase într-un set de fişiere temporare. Aceasta este utilă pentru lucrul cu valori non-ASCII cum ar fi jpegPhoto sau audio.

-T *secunde*
Timpul între căutări (în secunde). Opţiunea **-T** este suportată doar când este specificată opţiunea **-q**.

–U *numeutilizator*
Specificaţi username-ul. Necesar cu -m DIGEST-MD5 şi ignorat cu orice alt mecanism.

-v Foloseşte modul comunicativ, cu multe diagnostice scrise la ieşirea standard.

-V Specifică versiunea LDAP de folosit de către ldapmodify când se leagă la serverul LDAP. Implicit, o conexiune V3 LDAP este stabilită. Pentru a selecta explicit LDAP V3, specificaţi ″-V 3″. Specificaţi ″-V 2″ pentru a rula ca o aplicaţie LDAP V2. O aplicaţie, precum ldapmodify, selectează LDAP V3 ca protocol preferat prin folosirea ldap_init în locul ldap_open.

-w *passwd* **| ?**
Folosiţi ***passwd*** ca parolă pentru autentificare. Folosiţi ? pentru a genera un prompt de parolă.

-y proxydn
Setaţi ID proxy pentru operaţia de autorizare cu proxy.

–Y Folosiţi o conexiune sigură LDAP (TLS).

-z sizelimit
Limitaţi rezultatele căutării la intrările care au cel puţin limita de dimensiune. Aceasta face posibil plasarea unei graniţe superioare la numărul de intrări care sunt întoarse pentru o operaţie de căutare.

-Z Foloseşte o conexiune SSL pentru a comunica cu serverul LDAP. Pentru serverul de director i5/OS dacă utilizaţi -Z şi nu utilizaţi -K sau -N, c ertificatul asociat cu ID-ul aplicaţiei Director servicii client va fi utilizat.

filtrare Specifică o reprezentare pe şir a filtrului de aplicare în căutare. Filtrele simple pot fi specificate ca attributetype=attributevalue. Mai multe filtre complexe sunt specificate folosind o notaţie prefix în concordanţă cu următorul Backus Naur Form (BNF):

```
<filtru> ::='('<filtercomp>')'
<filtercomp> ::= <şi>|<or>|<nu>|<simplu>
<şi> ::= '&' <filterlist>
<sau> ::= '|' <filterlist>
```

```
<nu> ::= '!' <filtru>
<filterlist> ::= <filtru>|<filtru><filterlist>
<simplu> ::= <attributetype><filtertype>
<attributevalue>
<filtertype> ::= '='|'~='|'<='|'>='
```

Construcţia '~=' este utilizată la specificarea potrivirii aproximative. Reprezentarea pentru <*attributetype*> şi <*attributevalue*> sunt descrise în Definiţiile de sintaxă atribut RFC 2252, LDAP V3. Suplimentar, dacă tipul filtrului este '=' atunci <*attributevalue*> poate fi o * simplă pentru a realiza un test de existenţă atribut sau poate conţine text sau asteriscuri (*) împrăştiate pentru a realiza potrivirea de substring.

De exemplu, filtrul ″mail=*″ găseşte orice intrare care are un atribut mail. Filtrul ″mail=*@student.of.life.edu″ găseşte orice intrare care are un atribut mail care se termină cu şirul specificat. Pentru a pune paranteze într-un filtru, însoţiţi-le cu un caracter backslash (\).

Notă: Un filtru ca "cn=Bob *", unde este un spaţiu între Bob şi asterisc(*), se potriveşte cu ″Bob Carter″ dar nu cu ″Bobby Carter″ în directorul IBM. Spaţiul dintre ″Bob″ şi caracterul wildcard (*) afectează rezultatul unei căutări folosind filtre.

Vedeţi RFC 2254, O reprezentare şir a filtrelor de căutare LDAP pentru o descriere mai completă a filtrelor disponibile.

Format ieşire

Dacă una sau mai multe intrări sunt găsite, fiecare intrare este scrisă la rezultatul standard în formatul:

```
Nume distinctiv (DN)

attributename=value

attributename=value

attributename=value

...
```

Intrările multiple sunt separate cu o singură linie goală. Dacă opţiunea **-F** este folosită pentru a specifica un caracter separator, va fi folosită în locul caracterului `='. Dacă este folosită opţiunea **-t**, numele fişierului temporar este folosit în locul valorii actuale. Dacă este dată opţiunea **-A**, este scrisă doar partea ″attributename″.

Exemple

Următoarea comandă:

```
ldapsearch "cn=john doe" cn telephoneNumber
```

execută o căutare de subarbore (folosind baza de căutare implicită) pentru intrările cu un commonName de ″john doe″. Valorile commonName şi telephoneNumber sunt extrase şi tipărite în ieşirea standard. Ieşirea ar putea arăta astfel dacă sunt găsite 2 intrări:

```
  cn=John E Doe, ou="College of Literature, Science, and the Arts",
ou=Students, ou=People, o=University of Higher Learning, c=US

  cn=John Doe

  cn=John Edward Doe

  cn=John E Doe 1

  cn=John E Doe

  telephoneNumber=+1 313 555-5432
```

```
  cn=John B Doe, ou=Information Technology Division,
ou=Faculty and Staff, ou=People, o=University of Higher Learning, c=US

  cn=John Doe

  cn=John B Doe 1

  cn=John B Doe

  telephoneNumber=+1 313 555-1111
```

Comanda:

```
ldapsearch -t "uid=jed" jpegPhoto audio
```

execută o căutare de subarbore (folosind baza de căutare implicită) pentru intrările cu un id de ″jed″. Valorile jpegPhoto şi audio sunt extrase şi scrise în fişiere temporare. Ieşirea poate arăta astfel dacă se găsesşte una dintre intrări a fi o valoare pentru fiecare dintre atributele cerute:

```
cn=John E Doe, ou=Information Technology Division,

  ou=Faculty and Staff,

  ou=People, o=University of Higher Learning, c=US

  audio=/tmp/ldapsearch-audio-a19924

  jpegPhoto=/tmp/ldapsearch-jpegPhoto-a19924
```

Comanda:

```
ldapsearch -L -s one -b "c=US" "o=university*" o descriere
```

execută o căutare de un nivel la nivelul c=US pentru toate organizaţiile a căror organizationName începe cu University. Rezultatele de căutare vor fi afişate în formatul LDIF (vedeţi Format de interschimbare date LDAP). Valorile atribut organizationName şi descriere vor fi extrase şi tipărite la ieşirea standard, rezultând în ieşire similară cu aceasta:

```
dn: o=University of Alaska Fairbanks, c=US

  o: University of Alaska Fairbanks

  description: Preparing Alaska for a brave new tomorrow

  description: leaf node only


  dn: o=University of Colorado at Boulder, c=US

  o: University of Colorado at Boulder

  description: No personnel information

  description: Institution of education and research


  dn: o=University of Colorado at Denver, c=US

  o: University of Colorado at Denver

  o: UCD

  o: CU/Denver

  o: CU-Denver
```

```
description: Institute for Higher Learning and Research


dn: o=University of Florida, c=US

o: University of Florida

o: UFl

description: Shaper of young minds


...
```

Comanda:

```
ldapsearch -b "c=US" -o ibm-slapdDN "objectclass=person" ibm-slapdDN
```

execută o căutare de un nivel subarbore la nivelul c=US pentru toate persoanele. Acest atribut special (ibm-slapdDN), când este folosit pentru căutări sortate, sortează rezultatele căutării după reprezentarea şir a numelui distinctiv (DN). Ieşirea poate arăta astfel:

```
cn=Al Edwards,ou=Widget Division,ou=Austin,o=IBM,c=US

cn=Al Garcia,ou=Home Entertainment,ou=Austin,o=IBM,c=US

cn=Amy Nguyen,ou=In Flight Systems,ou=Austin,o=IBM,c=US

cn=Arthur Edwards,ou=Widget Division,ou=Austin,o=IBM,c=US

cn=Becky Garcia,ou=In Flight Systems,ou=Austin,o=IBM,c=US

cn=Ben Catu,ou=In Flight Systems,ou=Austin,o=IBM,c=US

cn=Ben Garcia Jr,ou=Home Entertainment,ou=Austin,o=IBM,c=US

cn=Bill Keller Jr.,ou=In Flight Systems,ou=Austin,o=IBM,c=US

cn=Bob Campbell,ou=In Flight Systems,ou=Austin,o=IBM,c=US
```

Comanda:

```
ldapsearch –h numegazdă –o sn –b "o=ibm,c=us" "title=engineer"
```

întoarce to ate intrările într-un director al angajatuluiIBM a cărui titlu este ″inginer″, cu rezultatele sortate după numele de familie.

Comanda:

```
ldapsearch –h hostname –o -sn –o cn –b "o=ibm,c=us" "title=engineer"
```

întoarce to ate intrările într-un director al angajatuluiIBM a cărui titlu este ″inginer″, cu rezultatele sortate după numele de familie (în ordine descrescătoare) şi apoi după numele obişnuit(în ordine crescătoare).

Comanda:

```
ldapsearch –h hostname –q 5 –T 3 –b o=ibm,c=us "title=engineer"
```

întoarce cinci intrări pe pagină, cu o întârziere de 3 secunde între pagini pentru toate intrările directorului angajatuluiIBM a cărui titlu este ″inginer″.

Acest exemplu demonstrează căutările unde un obiect referinţă este implicat. D irectoarele serverului de director LDAP poate obţine obiecte referral, furnizate cu condiţia de a conţine numai:

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

Se presupune că 'System_A' deţine intrarea de 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 existe pe 'System_B'.

System_B conţine o intrare:

```
dn: cn=Barb Jensen, ou=Rochester, o=Big Company, c=US
cn: Barb Jensen
objectclass: organizationalPerson
sn: Jensen
telephonenumber: (800) 555 1212
```

Când un client emite o cerere la 'System_A', serverul LDAP de pe System_A răspunde clientului cu URL:

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

Clientul foloseşte aceste informaţii pentru a emite o cerere la System_B. Dacă intrarea de pe System_A conţine atribute suplimentare la dn, objectclass şi ref, serverul ignoră acele atribute (doar dacă specificaţi steguleţul **-R** pentru a indica să nu se urmărească referinţele).

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. Noua cerere are acelaşi domeniu ca cererea originală. Rezultatele acestei căutări variază depinzând de valoarea pe care o specificaţi pentru domeniul căutării (**-b**).

Dacă specificaţi -s base, după cum este arătat aici:

```
ldapsearch -h System_A -b 'ou=Rochester, o=Big Company, c=US'
     -s base 'sn=Jensen'
```

căutarea întoarce toate atributele pentru toate intrările cu 'sn=Jensen' care există în 'ou=Rochester, o=Big Company, c=US' pe ambele sisteme System_A şi System_B.

Dacă specificaţi -s sub, cum se arată aici:

```
ldapsearch -s sub "cn=John"
```

serverul va căuta toate sufixele şi va întoarce toate intrările cu ″cn=John″. Aceasta este cunoscută ca o căutare în subarbore pe o bază nulă. Se caută în întregul director cu o singură operaţie de căutare, în locul efectuării mai multor căutări, fiecare cu un sufix diferit ca bază de căutare. Acest tip de operaţie de căutare durează mai mult şi consumă mai multe resurse de sistem deoarece caută în întregul director (toate sufixele).

Notă: O căutare într-un subarbore cu o bază nulă nu întoarce informaţii despre schemă, informaţii despre istoricul de modificări, sau ceva despre back-end-ul proiectat al sistemului.

Dacă specificaţi -s sub, cum se arată aici:

```
ldapsearch -h System_A -b 'ou=Rochester, o=Big Company, c=US'
     -s sub 'sn=Jensen'
```

căutarea întoarce toate atributele pentru toate intrările cu 'sn=Jensen' care există în sau mai jos de 'ou=Rochester, o=Big Company, c=US' pe ambele sisteme System_A şi System_B.

Dacă specificaţi -s one, cum se arată aici:

```
ldapsearch -h System_A -b 'ou=Rochester, o=Big Company, c=US'
     -s one 'sn=Jensen'
```

căutarea nu întoarce vreo valoare pe acel sistem. În schimb, serverul întoarce clientului URL-ul referral:

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

Clientul în schimb lansează o cerere:

```
 ldapsearch -h System_B -b 'ou=Rochester, o=Big Company, c=US'
     -s one 'sn=Jensen'
```

Aceasta nu dă nici un rezultat, pentru că intrarea

```
dn: cn=Barb Jensen, ou=Rochester, o=Big Company, c=US
```

se află la

```
ou=Rochester, o=Big Company, c=US
```

O căutare cu -s one încearcă să găsească intrări în nivelul imediat de jos.

```
ou=Rochester, o=Big Company, c=US
```

Diagnoze

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

Concepte înrudite

API-urile Directory Server

"Referral-ii directorului LDAP" la pagina 50
Referral-ii permit mai multor servere de director să lucreze în echipe. Dacă DN-ul pe care un client îl cere nu este într-un director, serverul poate trimite automat cererea la orice alt server LDAP.

Referinţe înrudite

"Formatul pentru schimbul de date LDAP (LDIF)" la pagina 238
Formatul interschimbare date LDAP este un format text standard pentru reprezentarea obiectelor LDAP şi actualizărilor LDAP (adăugare, modificare, ştergere, modificare DN) într-un formular textual. Fişierele ce conţin înregistrări LDIF pot fi utilizate pentru trasferul datelor între serverele de director sau utilizate ca intrări de către unelte LDAP precum **ldapadd** şi **ldapmodify**.

Informaţii înrudite

RFC 2252, LDAP V3 Attribute Syntax Definitions

RFC 2254, A String Representation of LDAP Search Filters

ldapchangepwd

Utilitarul pentru linie de comandă de modificare a parolei LDAP.

Sinopsis

```
ldapchangepwd -D binddn -w passwd | ? -n newpassword | ?
[-C charset] [-d debuglevel][-G realm][-h ldaphost]
[-K keyfile] [-m mechanism] [-M] [-N certificatename]
[-O maxhops] [-p ldapport] [-P keyfilepw] [-R]
[-U username] [-v] [-V version] [-y proxydn] [-Y] [-Z] [-?]
```

Descriere

Trimite cereri de modificare parolă unui server LDAP. Permite parolei pentru o intrare director să fie modificată.

Opţiuni

-C *charset*
Specifică faptul că DN-urile furnizate ca intrare la utilitarul ldapdelete sunt reprezentate într-un set de caractere local, precum este specificat în setul de caractere. Folosiţi opţiunea -C charset dacă pagina de cod şir de intrare este diferită de valoarea paginii de cod a jobului. Referiţi-vă la API-ul ldap_set_iconv_local_charset() pentru a vedea valorile set de caractere suportate.

-d *debuglevel*
Setaţi nivelul de depanare LDAP la debuglevel.

-D *binddn*
Folosiţi ***binddn*** pentru a lega la directorul LDAP. ***binddn*** este un DN reprezentat pe şiruri. Când se foloseşte cu -m DIGEST-MD5, acesta este utilizat pentru a specifica ID-ul de autorizaţie. Poate fi ori un DN, ori un şir authzId care începe cu ″u:″ sau ″dn:″.

–G *regiune*
Specificaţi regiunea. Acest parametru este opţional. Când este utilizat cu -m DIGEST-MD5, valoarea este transmisă la server în timpul legării.

-h *ldaphost*
Specificaţi o gazdă alternativă în care rulează serverul ldap.

-K *keyfile*
Specifică nuumele fişierului bază de date de chei SSL. Dacă fişierul bază de date de chei nu este în directorul curent, specificaţi numele fişierului bazei de date de chei complet calificat.

Dacă utilitarul nu poate localiza baza de date de chei, va folosi un set hard-coded de rădăcina Autorităţii implicită de certificare de înredere. Fişierul bază de date chei conţine tipic unul au mai multe certificate de autorităţi de certificare (CA) care sunt crezute de client. Aceste tipuri de certificate X.509 sunt de asemenea cunoscute ca rădăcini de încredere.

Acest parametru activează efectiv comutatorul -Z. Pentru serverul de director i5/OS dacă utilizaţi -Z şi nu utilizaţi -K sau -N, c ertificatul asociat cu ID-ul aplicaţiei Director servicii client va fi utilizat.

-m *mecanism*
Folosiţi ***mechanism*** pentru a specifica mecanismul SASL de folosit pentru legarea la server. Este folosit API-ul ldap_sasl_bind_s() . Parametrul **-m** este ignorat dacă este setat **-V 2**. Dacă **-m** nu este specificat, este folosită autentificarea simplă. Mecanismele valide sunt:

- CRAM-MD5 - protejează parola trimisă serverului.
- EXTERNAL - foloseşte certificatul SSL. Necesită -Z.
- GSSAPI - utilizează acreditările Kerberos ale utilizatorului.
- DIGEST-MD5 - necesită ca valoarea username să fie trimisă la server de către client. Necesită -U. Parametrul -D (de obicei DN-ul de legare) este folosit pentru a specifica ID-ul de autorizare. Poate fi un DN sau un şir authzId care începe cu u: sau dn:

-M Gestionează obiecte referral ca intrări obişnuite.

-n *newpassword* **| ?**
Specifică noua parolă. Folosiţi ? pentru a genera un prompt de parolă.

-N *numecertificat*
Specifică eticheta asociată cu certificatul client din fişierul bază de date chei. Dacă serverul LDAP este configurat pentru a executa doar autentificare server, un certificat client nu este necesar. Dacă serverul LDAP este configurat pentru a executa autentificare client şi server, un certificat client poate fi necesar. ***certificatename*** nu este necesar, dacă o pereche cheie privată/certificat a fost desemnată ca implicită. Similar, ***certificatename*** nu este necesar dacă este o pereche singură cheie privată/certificat în fişierul bază de date chei

desemnat. Acest parametru este ignorat dacă nu este specificat nici **-Z**, nici **-K**. Pentru serverul de director i5/OS dacă utilizaţi -Z şi nu utilizaţi -K sau -N, c ertificatul asociat cu ID-ul aplicaţiei Director servicii client va fi utilizat.

-O *maxhops*
Specificaţi ***maxhops*** pentru a seta numărul maxim de hop-uri pe care le obţine biblioteca client când se urmăresc acreditările. Numărul de hopuri implicit este 10.

-p *ldapport*
Specificaţi un port TCP alternativ pe care ascultă serverul ldap. Portul LDAP implicit este 389. Dacă **-p** nu este specifcat şi **-Z** este specificat, este folosit portul implicit SSL LDAP.

-P *keyfilepw*
Specifică parola bazei de date chei. Această parolă este necesară pentru a accesa informaţiile cifrate din fişierul cheie al bazei de date, care poate include una sau mai multe chei private. Dacă un fişier stivă de parole este asociat cu fişierul bază de date de chei, parola este obţinută din fişierul stivă de parole, iar parametrul **-P** nu este necesar. Acest parametru este ignorat dacă nu este specificat nici **-Z**, nici **-K**.

-R Specifică faptul că referral-ii nu vor fi urmaţi automat.

-U *numeutilizator*
Specificaţi username-ul. Necesar cu -m DIGEST-MD5 şi ignorat cu orice alt mecanism.

-v Foloseşte modul comunicativ, cu multe diagnostice scrise la ieşirea standard.

-V *versiune*
Specifică versiunea LDAP de folosit de către **ldapdchangepwd** când se leagă la serverul LDAP. Implicit, o conexiune V3 LDAP este stabilită. Pentru a selecta explicit LDAP V3, specificaţi **-V 3**. Specificaţi **-V 2** pentru a rula ca aplicaţie LDAP V2. O aplicaţie, ca **ldapdchangepwd**, selectează LDAP V3 ca protocol preferat folosind ldap_init în loc de ldap_open.

-w *passwd* **| ?**
Folosiţi ***passwd*** ca parolă pentru autentificare. Folosiţi ? pentru a genera un prompt de parolă.

-y proxydn
Setaţi ID proxy pentru operaţia de autorizare cu proxy.

–Y Folosiţi o conexiune sigură LDAP (TLS).

-Z Foloseşte o conexiune SSL pentru a comunica cu serverul LDAP. Pentru serverul de director i5/OS dacă utilizaţi -Z şi nu utilizaţi -K sau -N, c ertificatul asociat cu ID-ul aplicaţiei Director servicii client va fi utilizat.

-? Afişează ajutorul sintaxei pentru ldapchangepwd.

Exemple

Următoarea comandă,

```
ldapchangepwd -D cn=John Doe -w a1b2c3d4 -n wxyz9876
```

modifică parola pentru intrarea cu numele commonName ″John Doe″ din a1b2c3d4 la wxyz9876

Diagnoze

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

Concepte înrudite

API-urile LDAP (Lightweight Directory Access Protocol)
Vedeţi API-urile LDAP (Lightweight Directory Access Protocol) pentru informaţii suplimentare despre API Directory Server

ldapdiff

Utilitarul pentru linie de comandă de sincronizare a replicii LDAP.

Notă: Această comandă poate rula pentru o perioadă îndelungată în funcţie de numărul de intrări (şi atributele pentru acele intrări) care sunt replicate.

Sinopsis

(Compară şi sincronizează intrările de date între 2 servere dintr-un mediu de replicare).

```
ldapdiff -b baseDN -sh host -ch host [-a] [-C countnumber]
 [-cD dn] [-cK keyStore] [-cw password] -[cN keyLabel]
 [-cp port] [-cP keyStorePwd]  [-cZ] [-F] [-L filename] [-sD dn] [-sK keyStore]
 [-sw password] -[sN keyLabel] [-sp port] [-sP keyStorePwd]
 [-sZ] [-v]
```

sau

(Compară schema între 2 servere).

```
 ldapdiff -S -sh host -ch host [-a] [-C countnumber][-cD dn]
 [-cK keyStore] [-cw password] -[cN keyLabel] [-cp port]
 [-cP keyStorePwd] [-cZ] [-L filename] [-sD dn]
 [-sK keyStore] [-sw password] [-sN keyLabel] [-sp port]
 [-sP keyStorePwd] [-sZ] [-v]
```

Descriere

Această unealtă sincronizează un server replică cu masterul său. Pentru a afişa ajutorul de sintaxă pentru **ldapdiff**, introduceţi:

```
ldapdiff -?
```

Opţiuni

Următoarele opţiuni se aplică la comanda **ldapdiff**. Există 2 subgrupuri care se aplică specific fie la serverul furnizor fie la cel consumator.

-a Specifică să folosiţi controlul administrare server pentru scrieri la o replică numai citire.

-b *baseDN*
Folosiţi searchbase ca punct de pornire pentru căutare în locul valorii implicite. Dacă nu este specificat **-b**, acest utilitar examinează variabila de mediu LDAP_BASEDN pentru o definiţie searchbase.

-C *numărănumăr*
Numără numărul de intrări de corectat. Dacă sunt găsite mai multe nepotriviri decât numărul specificat, unealta există.

-F Aceasta este opţiunea de corectare. Dacă este specificată, conţinutul din replica consumator este modificat pentru a se potrivi cu cel al serverului furnizor. Aceasta nu poate fi folosită dacă este specificată de asemenea **-S**.

-L Dacă opţiunea **-F** nu este specificată, folosiţi această opţiune pentru a genera un fişier LDIF pentru ieşire. Fişierul LDIF poate fi folosit pentru a actualiza consumatorul să elimine diferenţele.

-S Specifică să se compare schema pe ambele servere.

-v Foloseşte modul comunicativ, cu multe diagnostice scrise la ieşirea standard.

Opţiuni pentru un furnizor de replicare

Următoarele opţiuni se aplică serverului consumator şi denotă dintr-un ’s’ iniţial în numele opţiunii.

-sD *dn* Folosiţi ***dn*** pentru legarea la directorul LDAP. ***dn*** este un DN reprezentat pe şiruri.

-sh *gazdă*
Specifică numele gazdă.

-sK *memorarecheie*
Specificaţi numele fişierului bază de date de chei SSL cu extensia implicită **kdb**. Dacă acest parametru nu este specificat sau valoarea este un şir gol, sistemul este un şir gol. Dacă fişierul bază de date de chei nu este în directorul curent, specificaţi numele fişierului bazei de date de chei complet calificat.

-sN *etichetăcheie*
Specifică eticheta asociată cu certificatul client din fişierul bază de date chei. Dacă este specificată o etichetă fără specificarea unui depozit de chei (keystore), eticheta este un identificator de aplicaţie din DCM (Digital Certificate Manager). Eticheta implicită (id aplicaţie) este QIBM_GLD_DIRSRV_CLIENT. Dacă serverul LDAP este configurat pentru a executa doar autentificare server, un certificat client nu este necesar. Dacă serverul LDAP este configurat pentru a executa autentificare client şi server, un certificat client este necesară. ***keyLabel*** nu este necesar dacă a fost desemnată o pereche implicită certificat/cheie privată. Similar, ***keyLabel*** nu este necesar dacă există o singură pereche certificat/cheie privată în fişierul bază de date cheie desemnat. Acest parametru este ignorat dacă nu sunt specificate **-sZ** sau **-sK**.

-sp *portldap*
Specificaţi un port TCP alternativ pe care ascultă serverul ldap. Portul LDAP implicit este 389. Dacă **-sp** nu este specifcat şi **-sZ** este specificat, este folosit portul implicit SSL LDAP.

-sP *keyStorePwd*
Specifică parola bazei de date chei. Această parolă este necesară pentru a accesa informaţiile cifrate din fişierul cheie al bazei de date, care poate include una sau mai multe chei private. Dacă un fişier stivă de parole este asociat cu fişierul bază de date de chei, parola este obţinută din fişierul stivă de parole, iar parametrul **-sP** nu este necesar. Acest parametru este ignorat dacă nu sunt specificate **-sZ** sau **-sK**. Parola nu este folosită dacă există un fişier stash pentru depozitul de chei folosit.

-st *trustStoreType*
Specificaţi eticheta asociată cu certificatul client din fişierul bază de date de încredere. Dacă serverul LDAP este configurat pentru a executa doar autentificare server, un certificat client nu este necesar. Dacă serverul LDAP este configurat pentru a executa autentificare client şi server, un certificat client poate fi necesar. ***trustStoreType*** nu este necesar dacă a fost desemnată o pereche implicită certificat/cheie privată. Similar, ***trustStoreType*** nu este necesar dacă există o singură pereche certificat/cheie privată în fişierul bază de date cheie desemnat. Acest parametru este ignorat dacă nu sunt specificate **-sZ** sau **-sT**.

-sZ Foloseşte o conexiune SSL pentru a comunica cu serverul LDAP.

Opţiuni pentru un consumator de replicare

Următoarele opţiuni se aplică serverului consumator şi denotă dintr-un ’c’ iniţial în numele opţiunii. Pentru uşurinţă, dacă este specificat -cZ fără a specifica valori pentru -cK, -cN sau -cP, aceste opţiuni folosesc aceeaşi valoare specificată pentru opţiunile SSL ale furnizorului. Pentru suprascrie opţiunile furnizorului şi pentru a folosi setările implicite, specificaţi -cK ″″ -cN ″″ -cP ″″.

-cD *dn* Folosiţi ***dn*** pentru legarea la directorul LDAP. ***dn*** este un DN reprezentat pe şiruri.

-ch *gazdă*
Specifică numele gazdă.

-cK *memorarecheie*
Specificaţi numele fişierului bază de date de chei SSL cu extensia implicită kdb. Dacă valoarea este un şir gol, sistemul este un şir gol. Dacă fişierul bază de date de chei nu este în directorul curent, specificaţi numele fişierului bazei de date de chei complet calificat.

-cN *etichetă cheie*
Specifică eticheta asociată cu certificatul client din fişierul bază de date chei. Dacă serverul LDAP este configurat pentru a executa doar autentificare server, un certificat client nu este necesar. Dacă este specificată o etichetă fără specificarea unui depozit de chei (keystore), eticheta este un identificator de aplicaţie din DCM (Digital Certificate Manager). Eticheta implicită (id aplicaţie) este QIBM_GLD_DIRSRV_CLIENT. Dacă

serverul LDAP este configurat pentru a executa autentificare client şi server, un certificat client este necesară. ***keyLabel*** nu este necesar dacă a fost desemnată o pereche implicită certificat/cheie privată. Similar, ***keyLabel*** nu este necesar dacă există o singură pereche certificat/cheie privată în fişierul bază de date cheie desemnat. Acest parametru este ignorat dacă nu este specificat nici **-cZ**, nici **-cK**.

-cp *portldap*
Specificaţi un port TCP alternativ pe care ascultă serverul ldap. Portul LDAP implicit este 389. Dacă **-cp** nu este specifcat şi **-cZ** este specificat, este folosit portul implicit SSL LDAP.

-cP *keyStorePwd*
Specifică parola bazei de date chei. Această parolă este necesară pentru a accesa informaţiile cifrate din fişierul cheie al bazei de date, care poate include una sau mai multe chei private. Dacă un fişier stivă de parole este asociat cu fişierul bază de date de chei, parola este obţinută din fişierul stivă de parole, iar parametrul **-cP** nu este necesar. Acest parametru este ignorat dacă nu este specificat nici **-cZ**, nici **-cK**.

-cw *parolă* **| ?**
Folosiţi ***password*** ca parolă pentru autentificare. Folosiţi ? pentru a genera un prompt de parolă.

-cZ Foloseşte o conexiune SSL pentru a comunica cu serverul LDAP.

Exemple

```
ldapdiff -b <baseDN> -sh <numefurnizorgazdă> -ch <numegazdăconsumator> [opţiuni]
```

sau

```
ldapdiff -S  -sh <numegazdăfurnizor> -ch <numegazdăconsumator> [opţiuni]
```

Diagnoze

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

Operaţii înrudite

“Gestionarea cozilor de replicare” la pagina 156
Folosiţi aceste informaţii pentru a monitoriza starea replicării pentru fiecare acord de replicare (coadă) utilizat de acest server.

Referinţe înrudite

“Privire generală asupra replicării” la pagina 37
Prin replicare, o modificare făcută la un director este propagată la unul sau mai multe directoare suplimentare. Ca efect, o modificare la un director apare pe diferite directoare multiple.

Folosirea SSL cu utilitarele liniei de comandă LDAP

Folosiţi aceste informaţii pentru a înţelege cum să utilizaţi SSL împreună cu utilitarele de linie de comandă LDAP.

“SSL (Secure Sockets Layer) şi TLS (Transport Layer Security) cu Directory Server” la pagina 52 discută utilizarea SSL cu serverul LDAP Directory Server. Aceste informaţii includ gestionarea şi crearea Autorităţilor de certificare (CA) de încredere cu Digital Certificate Manager.

Unele din serverele LDAP accesate de client folosesc doar autentificarea server. Pentru aceste servere, aveţi nevoie doar să definiţi unul sau mai multe certificate rădăcină de încredere în memoria de certificate. Cu autentificarea server, clientul poate fi asigurat că serverul LDAP destinaţie a emis un certificat de de către unul din Autorităţi de certificare de încredere (CA-uri). În plus, toate tranzacţiile LDAP care trec prin conexiunea SSL cu serverul sunt cifrate. Aceasta include acreditări LDAP care sunt livrate pe API-uri care sunt folosite pentru a lega la serverul de director. De exemplu, dacă serverul LDAP foloseşte un certificat de mare siguranţă Verisign, ar trebui să faceţi una din următoarele:

1. Obţineţi un certificat CA de la Verisign.
2. Folosiţi DCM pentru a-l importa în memoria de certificate.
3. Folosiţi DCM pentru marcarea ca fiind de încredere.

Dacă serverul LDAP foloseşte un certificat server emis privat, administratorul serverelor vă poate livra o copie a fişierului cerut de certificatele serverului. Importaţi fişierul cerut de certificat în memoria de certificat şi marcaţi-o ca de încredere.

Dacă folosiţi utilitarele shell pentru a accesa serverele LDAP care folosesc şi autentificarea client şi server trebuie să faci următoarele:

- Definiţi unul sau mai multe certificate rădăcină de încredere în memoria sistem de certificate. Aceasta permite clientului să fie asigurat că serverul LDAP destinaţie a fost asigurat cu un certificat de unul din CA-urile de încredere. În plus, toate tranzacţiile LDAP care trec prin conexiunea SSL cu serverul sunt cifrate. Aceasta include acreditări LDAP care sunt livrate pe API-uri care sunt folosite pentru a lega la serverul de director.
- 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.

Concepte înrudite

"SSL (Secure Sockets Layer) şi TLS (Transport Layer Security) cu Directory Server" la pagina 52
Pentru comunicarea mai sigură cu Directory Server, se poate folosi securitatea SSL şi TLS.

Formatul pentru schimbul de date LDAP (LDIF)

Formatul interschimbare date LDAP este un format text standard pentru reprezentarea obiectelor LDAP şi actualizărilor LDAP (adăugare, modificare, ştergere, modificare DN) într-un formular textual. Fişierele ce conţin înregistrări LDIF pot fi utilizate pentru trasferul datelor între serverele de director sau utilizate ca intrări de către unelte LDAP precum **ldapadd** şi **ldapmodify**.

Înregistrările conţinutului LDIF sunt utilizate pentru a reprezenta conţinutul directorului LDAP şi conţin o linie ce identifică obiectele, urmată de linii conţinând perechi de valori-atribut pentru obiect. Acest tip de fişier este folosit de utilitarul Qshell **ldapadd**, precum şi de uneltele de import şi export ale directorului în Navigator System i şi comenzile CL CPYFRMLDIF (LDIF2DB) şi CPYTOLDIF (DB2LDIF).

Notă: Se recomandă folosirea comenzii DB2LDIF într-un job independent.

Modificarea înregistrărilor LDIF este utilizată pentru a reprezenta actualizările directorului. Aceste înregistrări conţin o linie ce indentifică obiectul de director, urmată de linii ce descriu modificările aduse obiectului. Modificările includ adăugarea, ştergerea, redenumirea sau mutarea obiectelor, precum şi modificarea obiectelor existente.

Există două stiluri de intrări pentru ambele înregistrări: Un stil standard, LDIF definit de RFC 2849: The LDAP Data Interchange Format (LDIF) - Technical Specification, şi un stil mai vechi, de modificare nestandard. Se recomandă utilizarea stilului standard LDIF; stilul mai vechi este documentat aici pentru a fi folosit cu uneltele mai vechi ce produc sau utilizează acel stil.

Stilurile de intrare

Utilitarele Qshell **ldapmodify** şi **ldapadd** acceptă două forme de intrări. Tipul de intrare este determinat de formatul primei linii de intrare livrate la **ldapmodify** sau **ldapadd**.

Prima linie de intrare pentru comanda ldapmodify sau ldapadd trebuie să desemneze numele distinctiv al intrării din director care urmează să fie adăugată sau modificată. Această linie de intrare trebuie să fie de forma:

```
dn: distinguished_name
```

sau

```
distinguished_name
```

unde dn: este un şir literal şi distinguished_name este numele distinctiv al intrării directorului care urmează să fie modificată (sau adăugată). Dacă dn: este găsit, stilul de intrare este setat la stilul RFC 2849 LDIF. Dacă nu este găsit, stilul de intrare este setat la stilul de modificare.

Notă:

1. Comanda **ldapadd** este echivalentă cu invocarea comenzii **ldapmodify -a**.
2. Utilitarele **ldapmodify** şi **ldapadd** nu suportă nume distinctive codate base64.

Referinţe înrudite

“ldapmodify şi ldapadd” la pagina 207
Utilitarele de linie de comandă modificare-intrare LDAP şi adăugare-intrare LDAP.

“ldapsearch” la pagina 224
Utilitarul pentru linie de comandă de căutare LDAP.

Intrare RFC 2849 LDIF

Un stil LDIF standard definit de RFC 2849: LDIF-ul (Data Interchange Format) LDAP este recomandat. Un fişier LDIF poate porni cu versiune opţionslă şi directive charset: versiune: 1 şi charset: ISO-8859-1.

Directiva charset este utilă când se foloseşte sistemul de fişiere pe alte platforme ce nu suportă punerea între taguri a unui fişier cu un CCSID. Pe i5/OS, comportamentul standard este de a deschide fişiere LDIF în UTF-8 (CCSID 1208) şi de a permite sistemului de fişiere să convertească datele de la and CCSID-ul fişierului la UTF-8 iar directiva charset este de obicei nefolositoare.

Urmărirea versiunii opţionale şi liniilor charset este o serie de modificări înregistrări precum este descris mai jos.

Când se utilizează intrarea RFC 2849 LDIF, tipurile atributelor şi valorile sunt delimitate de două puncte (:) sau două puncte duble (::). Mai mult, modificările individuale aduse valorilor atributelor sunt delimitate cu o linie de intrare changetype:. Formularul general al liniilor de intrare pentru RFC 2849 LDIF este:

```
modificare_înregistrare
<linie blanc>
modificare_înregistrare
<linie blanc>
.
.
.
```

Un fişier de intrare în stil RFC 2849 LDIF conţine una sau mai multe setări de linii modificare_înregistrare ce sunt separate de o singură linie blanc. Fiecare modificare_înregistrare are următorul formular:

```
dn: <nume distinctiv>
[modificaretip: {modificare|adăugare|modrdn|moddn|ştergere}]
modificare_clauză
modificare_clauză
.
.
.
```

Deci, o modificare_înregistrare conţine o linie ce indică numele distinctiv al intrării directorului ce urmează a fi modificat, o linie opţională ce indică tipul de modificare ce trebuie realizată pentru intrarea directorului şi încă o modificare_clauză setări de linii. Dacă linia modificaretip: este omisă, tipul de modificare este presupus că este modificare doar dacă invocaţia comenzii a fost -a sau ldapadd, în care caz modificaretip este presupus să fie adăugare.

Când tipul de modificare este modificare, fiecare modificare_clauză este definită ca fiind un set de linii ale formularului:

```
adăugare:  {tipadăugare}
{attrtype}{sep}{valoare}
.
.
.
-
```

sau

```
înlocuire: {attrtype}
{attrtype}{sep}{valoare}
.
.
.
-
```

sau

```
ştergere: {attrtype}
[{attrtype}{sep}{valoare}]
.
.
.
-
```

sau

```
{attrtype}{sep}{valoare}
.
.
.
```

Specificare înlocuire înlocuieşte toate valorile existente pentru atribut cu setul specificat de atribute. Specificare adăugare adaugă la setul existent de valori ale atributelor. Specificare ştergere fără nici o înregistrare de pereche atribute-valoare înlătură toate valorile pentru atributul specificat. Specificare ştergere urmată de una sau mai multe înregistrări de pereche atribut-valoare înlătură doar acele valori specificate în înregistrările pereche atribut-valoare.

Dacă oricare dintre liniile (modificare indicator) adăugare: *attrtype*, înlocuire: *attrtype*, sau ştergere: *attrtype* este specificată, o linie ce conţine o liniuţă de despărţire (-) este aşteptată ca un delimitator de încidere pentru modificările pentru acel *attrtype*. Perechile atribut-valoare sunt aşteptate pe liniile de intrare ce se găsesc între indicatorul de modificare şi liniuţa de despărţire. Dacă linia modificaretip este omisă, modificaretip este presupus a fi adăugare pentru ldapadd şi înlocuire pentru ldapmodify.

Valoarea atributului poate fi specificată ca un şir text, o valoare codată base-64 sau URL-ul unui fişier conform separatorului utilizat, *sep*.

attrtype: valoare
: două puncte (:) specifică faptul că valoarea este *valoarea* şirului.

attrtype:: base64string
: Două puncte duble (: :) specifică faptul că *base64string* este reprezentarea codată a şirului în bază 64 a unei valori binare a unui şir UTF-8 ce conţine caractere multibiţi.

attrtype:< URLfişier
: două puncte şi colţar de unghi stâng (:<) specifică faptul că valoarea va fi citită de la fişierul identificat de către URLfişier. Un exemplu de o linie URL fişier specificând că valoarea pentru atributul jpegPhoto este în fişierul /tmp/photo.jpg este

  jpegphoto:< fişier:///tmp/photo.jpg

Orice caracter spaţiu gol dintre separator şi valoarea atributului este ignorat. Valorile atributelor pot fi continuate de-a lungul liniilor multiple utilizând un caracter spaţiu singular ca fiind primul caracter al următoarei linii de intrări. Dacă două puncte duble sunt utilizate ca un separator, intrarea este aşteptată să fie în format base64. Acest format este o codare ce reprezintă fiecare trei biţi binari cu patru caractere text.

Valorile atributelor multiple sunt specificate utilizând specificaţii multiple {attrtype}{sep}{value}.

Când tipul modificării este adăugare, fiecare modificare_clauză este defintă ca fiind un set de linii pentru formular:

```
{attrtype}{sep}{valoare}
```

Ca şi cu tipul de modificare al modificării, separatorul, sep şi valoare pot fi fie două puncte (:), două puncte duble (: :) sau două puncte şi colţar de unghi stâng (:<). Orice caracter spaţiu gol dintre separator şi valoarea atributului este ignorat. Valorile atributelor pot fi continuate de-a lungul liniilor multiple utilizând un caracter spaţiu singular ca fiind primul caracter al următoarei linii de intrări. Dacă două puncte duble sunt utilizate ca un separator, intrarea este aşteptată să fie în format base64.

Când tipul de modificare este modrdn sau moddn, fiecare modificare_clauză este definită ca un set de linii a formularului:

```
newrdn: valoare
deleteoldrdn:{0|1}
[newsuperior: newSuperiorDn]
```

Aceştia sunt parametrii pe care îi puteţi specifica pe un RDN modificare (redenumire) sau operaţie LDAP modificareDN (mutare). Valoarea pentru setarea newrdn este noul RDN ce urmează a fi folosit când se realizează operaţia de modificare RDN. Specificaţi 0 pentru valoarea setării deleteoldrdn cu scopul de a salva atributul în vechiul RDN şi specificaţi 1 pentru a înlătura valorile atributului în vechiul RDN. Valoarea pentru setarea superiornou este DN-ul noului superior (părinte) când se mută o intrare.

Când tipul de modificare este ştergere, nu modificare_clauză este specificat.

Exemple stil LDIF:

Acest subiect furnizează unele exemple de intrare validă pentru comanda **ldapmodify** utilizând stilul LDIF RFC 1849.

Adăugarea unei noi intrări

Următorul exemplu adaudă o nouă intrare în director utilizând numele cn=Tim Doe, ou=Your Department, o=Your Company, c=US, presupunând că **ldapadd** sau **ldapmodify -a** invocate:

```
dn:cn=Tim Doe, ou=Departamentul dumneavoastră, o=Compania dumneavoastră, c=US
changetype:adăugare
cn: Tim Doe
sn: Doe
objectclass: organizationalperson
objectclass: person
objectclass: top
```

Următorul exemplu adaugă o nouă intrare în director folosind numele cn=Tim Doe, ou=Departamentul dumneavoastră, o=Compania dumneavoastră, c=US, presupunând că **ldapadd** sau **ldapmodify -a** este invocată. Luaţi la cunoştinţă că atributul jpegphoto este în cărcat din fişierul /tmp/timdoe.jpg.

```
dn:cn=Tim Doe, ou=Departamentul dumneavoastră, o=Compania dumneavoastră, c=US
changetype:adăugare
cn: Tim Doe
sn: Doe
jpegphoto:< file:///tmp/timdoe.jpg
objectclass: inetorgperson
objectclass: organizationalperson
objectclass: person
objectclass: top
```

Adăugarea tipurilor de atribut

Următorul exemplu adaugă două noi tipuri de atribute la intrarea existentă. Luaţi la cunoştiinţă că atributului registeredaddress îi sunt alocate două valori:

```
dn:cn=Tim Doe, ou=Departamentul dumneavoastră, o=Compania dumneavoastră, c=US
changetype: modify
adăugare:telephonenumber
telephonenumber: 888 555 1234
```

```
-
adăugare: registeredaddress
registeredaddress: td@yourcompany.com
registeredaddress: ttd@yourcompany.com
```

Modificarea numelui de intrare

Următorul exemplu modifică numele intrării existente cn=Tim Tom Doe, ou=Departamentul dumneavoastră, o=Compania dumneavoastră, c=US. Vechiul RDN, cn=Tim Doe, este reţinut ca o valoare de atribut suplimentară a atributului cn. Noul RDN, cn=Tim Tom Doe, este adăugat automat de serverul LDAP la valorile atributului cn în intrarea:

```
dn:cn=Tim Doe, ou=Departamentul dumneavoastră, o=Compania dumneavoastră, c=US
changetype:modrdn
newrdn: cn=Tim Tom Doe
deleteoldrdn: 0
```

Următorul exemplu mută cn=Tim Doe la ou=Nou departament; RDN-ul (cn=Tim Doe) nu este modificat.

```
dn: cn=Tim Doe, ou=Departamentul dumneavoastră, o=Compania dumneavoastră, c=US
changetype:moddn
newrdn: cn=Tim Doe
deleteoldrdn: 0
newsuperior: ou=Nou departament, o=Compania dumneavoastră, c=US
```

Înlocuirea valorilor atributului

Următorul exemplu înlocuieşte valorile atribu tului pentru atributeletelephonenumber şi registeredaddress cu valorile atributului specificate.

```
dn: cn=Tim Tom Doe, ou=Your Department, o=Your Company, c=US
changetype: modify
înlocuiţi: telephonenumber
telephonenumber: 888 555 4321
-
înlocuiţi: registeredaddress
registeredaddress: tim@yourcompany.com
registeredaddress: timtd@yourcompany.com
```

Ştergerea şi adăugarea atributelor

Următorul exemplu şterge atributul telephonenumber, şt erge o singură valoare a atributului registeredaddress şi adaugă o descriere atribut:

```
dn: cn=Tim Tom Doe, ou=Your Department, o=Your Company, c=US
changetype: modify
adăugaţi: descriere
descriere: Acesta este o valoare atribut foarte lungă
 care este continuată pe o a doua linie.
 Vedeţi spaţierea de la începutul liniilor
 continuate, care indică faptul că
 linia este continuată.
-
ştergere: telephonenumber
-
ştergere: registeredaddress
registeredaddress: tim@yourcompany.com
```

Ştergerea unei intrări

Următorul exemplu şterge intrarea directorului cu numele cn=Tim Tom Doe, ou=Departamentul dumneavoastră, o=Compania dumneavoastră, c=US:

```
dn: cn=Tim Tom Doe, ou=Your Department, o=Your Company, c=US
changetype:ştergere
```

Intrarea LDIF cu stil modificare

Stilul de modificare vechi, non-standard al intrării pentru comenzile **ldapmodify** sau **ldapadd** nu este aşa de flexibil ca stilul RFC 2849 LDIF. Totuşi, este uneori mai uşor de utilizat decât stilul LDIF.

Când se utilizează intrarea cu stil modificare, tipurile atributelor şi valorile sunt delimitate de un semn egal (=). Forma generală a liniilor de intrare pentru stilul mofificare este:

```
change_record
<linie blanc>
change_record
<linie blanc>
.
.
.
```

Un fişier de intrare în stilul modificare conţine unul sau mai multe setări *change_record* de linii separate de către o singură linie blanc. Fiecare *change_record* are formularul următor:

```
distinguished_name
[+|-]{attrtype} = {value_line1[\
value_line2[\
...value_lineN]]}
.
.
.
```

Deci, *change_record* conţine o linie ce indică numele distinctiv al intrării directorului ce trebuie să fie modificat împreună cu unul sau mai multe linii de modificare atribut. Fiecare linie de modificare de atribut conţine un identificator opţional de adăugare sau ştergere (+ or -), un tip de atribut şi o valoarea de atribut. Dacă semnul plus (+) este specificat, tipul modificare este setat la **adăugare**. Dacă un hyphen (-) este specificat, tipul modificare este setat la ştergere. Pentru o modificare de ştergere, semnul egal (=) şi *valoare* ar trebui omise pentru a înlătura un atribut întreg. Dacă indicatorul adăugare sau ştergere nu este specificat, tipul modificare este setat la adăuga re doar dacă opţiunea -r este utilizată, în care tipul modificare este setat la înlocuire. Orice caracter spaţiu gol de conducere sau de coadă este înlăturat de la valorile atributului. Dacă caracterul spaţiu gol de coadă este cerut pentru valoarile atributelor, stilul de intrare RFC 2849 LDIF trebuie să fie utilizat. Liniile sunt continuate utilizând un backslash (\) ca fiind ultimul caracter al linii. Dacă o linie este continuată, caracterul backslash este înlăturat şi linia reuşită este adăugată la afârşit imediat după caracterul ce precedează caracterul backslash. Caracterul linie-nouă la sfărşitul liniei intrare nu este reţinut ca fiind parte a valorii atributului.

Valorile multiple ale atributelor sunt specificate utilizând specificaţii multiple *attrtype=value*.

Dacă suportul pentru valori binare de la opţiunile fişiere (-b) este specificat, o *valoare* ce începe cu '/' indică faptul că valoarea este un nume de fişier. Spre exemplu, linia următoare indică faptul că atributul jpegphoto va fi citit de la fişierul /tmp/photo.jpg:

```
jpegphoto=/tmp/photo.jpg
```

Modificarea exemplelor de stil:

Acest subiect furnizează unele exemple de intrare validă pentru comanda **ldapmodify** utilizând modificare stil.

Adăugarea unei noi intrări

Următorul exemplu adaugă o nouă intrare în director utilizând numele cn=Tim Doe, ou=Departamentul dumneavoastră, o=Compania dumneavoastră, c=US:

```
cn=Tim Doe, ou=Departamentul dumneavoastră, o=Compania dumneavoastră, c=US
cn=Tim Doe
sn=Doe
objectclass=organizationalperson
objectclass=person
objectclass=top
```

Adăugarea unui nou tip de atribut

Următorul exemplu adaugă două noi tipuri de atribute la intrarea existentă. L uaţi la cunoştiinţă că atributului registeredaddress îi sunt alocate două valori:

```
cn=Tim Doe, ou=Departamentul dumneavoastră, o=Compania dumneavoastră, c=US
+telephonenumber=888 555 1234
+registeredaddress=td@yourcompany.com
+registeredaddress=ttd@yourcompany.com
```

Înlocuirea valorilor atributului

Presupunând că invocarea comenzii a fost:

```
ldapmodify -r ...
```

U rmătorul exemplu înlocuieşte valorile atributului pentru atributele telephonenumber şi registeredaddress cu valorile atributului specificate. Dacă **-r** opţiunea linia de comandă nu a fost specificată, valorile atributului sunt adăugate la setul existent de valori ale atributului.

```
cn=Tim Doe, ou=Departamentul dumneavoastră, o=Compania dumneavoastră, c=US
telephonenumber=888 555 4321
registeredaddress: tim@yourcompany.com
registeredaddress: timtd@yourcompany.com
```

Ştergerea unui tip de atribut

Următorul exemplu şterge o singură valoare a atributuluiregisteredaddress de la intrarea existentă.

```
cn=Tim Doe, ou=Departamentul dumneavoastră, o=Compania dumneavoastră, c=US
-registeredaddress=tim@yourcompany.com
```

Adăugarea unui atribut

Următorul exemplu adaugă un atribut de descriere. Valoarea atributului de descriere extinde liniile multiple:

```
cn=Tim Doe, ou=Departamentul dumneavoastră, o=Compania dumneavoastră, c=US
+descriere=Acesta este un atribut foarte lung \
valoare care este continuată pe o a doua linie.  \
Luaţi la cunoştiinţă backslashul la sfârşit de linie pentru \
a fi continuat în ordine pentru a însemna că \
linia este continuată.
```

Schemă de configurare Directory Server

Aceste informaţii descriu Directory Information Tree (DIT) şi atributele care sunt folosite pentru a configura fişierul ibmslapd.conf.

În ediţiile anterioare, setările de configurare ale directorului au fost memorate într-un format patentat din fişierul de configurare. Setările director sunt stocate acum folosind formatul LDIF în fişierul de configurare.

Fişierul de configurare este denumit ibmslapd.conf. Schema folosită de fişierul de configurare este de asemenea disponibilă acum. Tipurile de atribute pot fi găsite în fişierul v3.config.at şi clasele de obiecte sunt în fişierul v3.config.oc. Atributele pot fi modificate folosind comanda ldapmodify.

Concepte înrudite

“Verificare schemă” la pagina 30
Când serverul este iniţializat, fişierele schemei sunt citite şi verificate pentru consistenţă şi corectitudine.

Referinţe înrudite

“ldapmodify şi ldapadd” la pagina 207
Utilitarele de linie de comandă modificare-intrare LDAP şi adăugare-intrare LDAP.

Arborele cu informaţii de director

Aceste informaţii prezintă DIT-ul (Directory Server directory information tree).

cn=Configuration

- cn=Admin
- cn=Event Notification
- cn=Front End
- cn=Kerberos
- cn=Master Server
- cn=Referral
- cn=Schema
  - cn=IBM Directory
    - cn=Config Backends
      - cn=ConfigDB
    - cn=RDBM Backends
      - cn=Directory
      - cn=ChangeLog
    - cn=LDCF Backends
      - cn=SchemaDB
- cn=SSL
  - cn=CRL
- cn=Transaction

cn=Configuration

DN cn=Configuration

Descriere

Aceasta este intrarea de pe nivelul de sus din DIT-ul de configurare. Ea păstrează date de interes global pentru server, deşi în practică ea conţine de asemenea diverse elemente. Fiecare atribut din această intrare vine prima secţiune (global stanza) a ibmslapd.conf.

Număr

1 (necesar)

Clasă Obiect

ibm-slapdTop

Atribute obligatorii

- cn
- ibm-slapdAdminDN
- ibm-slapdAdminPW
- ibm-slapdErrorLog
- ibm-slapdPort
- ibm-slapdPwEncryption
- ibm-slapdSizeLimit

- ibm-slapdSysLogLevel
- ibm-slapdTimeLimit
- objectClass

Atribute opţionale

- ibm-slapdACLAccess
- ibm-slapdACIMechanism
- ibm-slapdConcurrentRW (Deprecated)
- ibm-slapdMaxPendingChangesDisplayed
- ibm-slapdServerId
- ibm-slapdSupportedWebAdmVersion
- ibm-slapdVersion

cn=Admin

DN cn=Admin, cn=Configuration

Descriere
Setări de configuraţie globale pentru IBM Admin Daemon

Număr
1 (necesar)

Clasă Obiect
ibm-slapdAdmin

Atribute obligatorii

- cn
- ibm-slapdErrorLog
- ibm-slapdPort

Atribute opţionale

- ibm-slapdSecurePort

cn=Event Notification

DN cn=Event Notification, cn=Configuration

Descriere
Setările globale de notificare evenimente pentru Directory Server

Număr
0 sau 1 (opţional; necesar doar dacă vreţi să activaţi notificarea evenimentelor)

Clasă Obiect
ibm-slapdEventNotification

Atribute obligatorii

- cn
- ibm-slapdEnableEventNotification
- objectClass

Atribute opţionale

- ibm-slapdMaxEventsPerConnection
- ibm-slapdMaxEventsTotal

cn=Front End

DN cn=Front End, cn=Configuration

Descriere
Setările globale de mediu pe care serverul le aplică la pornire.

Număr
0 sa 1 (opţional)

Clasă Obiect
ibm-slapdFrontEnd

Atribute obligatorii

- cn
- objectClass

Atribute opţionale

- ibm-slapdACLCache
- ibm-slapdACLCacheSize
- ibm-slapdDB2CP
- ibm-slapdEntryCacheSize
- ibm-slapdFilterCacheBypassLimit
- ibm-slapdFilterCacheSize
- ibm-slapdPlugin
- ibm-slapdSetenv
- ibm-slapdIdleTimeOut

cn=Kerberos

DN cn=Kerberos, cn=Configuration

Descriere
Setările globale de autentificare Kerberos pentru Directory Server.

Număr
0 sa 1 (opţional)

Clasă Obiect
ibm-slapdKerberos

Atribute obligatorii

- cn
- ibm-slapdKrbEnable
- ibm-slapdKrbRealm
- ibm-slapdKrbKeyTab
- ibm-slapdKrbIdentityMap
- ibm-slapdKrbAdminDN
- objectClass

Atribute opţionale

- Fără

cn=Master Server

DN cn=Master Server, cn=Configuration

Descriere

Când configuraţi o replică, această intrare păstrează acreditările de legare şi URL-ul referral al serverului master.

Număr

0 sa 1 (opţional)

Clasă Obiect

ibm-slapdReplication

Atribute obligatorii

- cn
- ibm-slapdMasterPW (Obligatoriu dacă nu folosiţi autentificare Kerberos.)

Atribute opţionale

- ibm-slapdMasterDN
- ibm-slapdMasterPW (Opţional dacă folosiţi autentificare Kerberos.)
- ibm-slapdMasterReferral
- objectClass

cn=Referral

DN cn=Referral, cn=Configuration

Descriere

Această intrare conţine toate intrările referral din prima secţiune (global stanza) a ibmslapd.conf. Dacă nu există referral-i (nu există nici unul în mod implicit), această intrare este opţională.

Număr

0 sa 1 (opţional)

Clasă Obiect

ibm-slapdReferral

Atribute obligatorii

- cn
- ibm-slapdReferral
- objectClass

Atribute opţionale

- Fără

cn=Schemas

DN cn=Schemas, cn=Configuration

Descriere

Această intrare serveşte drept container pentru scheme. Acestă intrare nu este cu adevărat necesară deoarece schemele pot fi distinse după clasa de obiecte ibm-slapdSchema. Este inclusă pentru a îmbunătăţi lizibilitatea DIT.

Doar o intrare schemă este permisă în prezent: cn=IBM Directory.

Număr

1 (necesar)

Clasă Obiect

Container

Atribute obligatorii

- cn

- objectClass

Atribute opţionale

- Fără

cn=IBM Directory

DN cn=IBM Directory, cn=Schemas, cn=Configuration

Descriere

Această intrare conţine toate datele de configurare schemă din prima secţiune (global stanza) a ibmslapd.conf. Ea serveşte de asemenea drept container pentru toate backend-urile care folosesc schema. Schemele multiple nu sunt suportate în prezent, dar dacă ar fi fost, atunci ar fi fost câte o intrare ibm-slapdSchema per schemă. Notaţi că schemele multiple se presupune că sunt incompatibile. Aşadar, un backend poate fi asociat doar cu o singură schemă.

Număr

1 (necesar)

Clasă Obiect

ibm-slapdSchema

Atribute obligatorii

- cn
- ibm-slapdSchemaCheck
- ibm-slapdIncludeSchema
- objectClass

Atribute opţionale

- ibm-slapdSchemaAdditions

cn=Config Backends

DN cn=Config Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Descriere

Această intrare serveşte drept container pentru backend-urile Config.

Număr

1 (necesar)

Clasă Obiect

Container

Atribute obligatorii

- cn
- objectClass

Atribute opţionale

Fără

cn=ConfigDB

DN cn=ConfigDB, cn=Config Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Descriere

Backend configuraţie pentru configuraţia IBM Directory

Număr

0 - n (opţional)

Clasă Obiect
ibm-slapdConfigBackend

Atribute obligatorii

- ibm-slapdSuffix
- ibm-slapdPlugin

Atribute opţionale

- ibm-slapdReadOnly

cn=RDBM Backends

DN cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Descriere
Această intrare serveşte drept container pentru backend-urile RDBM. Acesta înlocuieşte efectiv linia rdbm din baza de date de la ibmslapd.conf prin identificarea tuturor subintrărilor ca backend-uri DB2. Acestă intrare nu este cu adevărat necesară deoarece backend-urile RDBM pot fi distinse după clasa de obiecte ibm-slapdRdbmBackend. Este inclusă pentru a îmbunătăţi lizibilitatea DIT.

Număr
0 sa 1 (opţional)

Clasă Obiect
Container

Atribute obligatorii

- cn
- objectClass

Atribute opţionale

- Fără

cn=Directory

DN cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Descriere
Această intrare conţine toate setările de configurare baze de date pentru backend-ul implicit baze de date RDBM.

Deşi pot fi create mai multe backend-uri cu nume arbitrare, Administrare server presupune că ″cn=Directory″ este principalul backend director şi că ″cn=ChangeLog Log″ este backend-ul istoricului de modificări opţional. Doar sufixele afişate în ″cn=Directory″ sunt configurabile prin Administrare server (cu excepţia sufixului de modificare istoric, care este setat transparent prin activarea istoricului de modificări).

Număr
0 - n (opţional)

Clasă Obiect
ibm-slapdRdbmBackend

Atribute obligatorii

- cn
- ibm-slapdDbInstance
- ibm-slapdDbName
- ibm-slapdDbUserID
- objectClass

Atribute opţionale

- ibm-slapdBulkloadErrors
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdDBAlias
- ibm-slapdDB2CP
- ibm-slapdDbConnections
- ibm-slapdDbLocation
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPageSizeLmt
- ibm-slapdPlugin
- ibm-slapdReadOnly
- ibm-slapdReplDbConns
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSuffix
- ibm-slapdUseProcessIdPw

Notă: Dacă folosiţi **ibm-slapdUseProcessIdPw**, trebuie să modificaţi schema pentru a face **ibm-slapdDbUserPW** opţional.

cn=Change Log

DN cn=Change Log, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Descriere
Această intrare conţine toate setările de configurare baze de date pentru backend-ul de istoric de modificări.

Număr
0 - n (opţional)

Clasă Obiect
ibm-slapdRdbmBackend

Atribute obligatorii
- cn
- ibm-slapdDbInstance
- ibm-slapdDbName
- ibm-slapdDbUserID
- objectClass

Atribute opţionale
- ibm-slapdBulkloadErrors
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdDBAlias
- ibm-slapdDB2CP
- ibm-slapdDbConnections
- ibm-slapdDbLocation
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt

- ibm-slapdPageSizeLmt
- ibm-slapdPlugin
- ibm-slapdReadOnly
- ibm-slapdReplDbConns
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSuffix
- ibm-slapdUseProcessIdPw

Notă: Dacă folosiţi **ibm-slapdUseProcessIdPw**, trebuie să modificaţi schema pentru a face **ibm-slapdDbUserPW** opţional.

cn=LDCF Backends

DN cn=LDCF Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Descriere
Această intrare serveşte drept container pentru backend-urile LDCF. Ea înlocuieşte efectiv linia ldcf bază de date din ibmslapd.conf prin identificarea tuturor subintrărilor drept backend-uri LDCF. Acestă intrare nu este cu adevărat necesară deoarece backend-urile LDCF pot fi distinse după clasa de obiecte ibm-slapdLdcfBackend. Este inclusă pentru a îmbunătăţi lizibilitatea DIT.

Număr
1 (necesar)

Clasă Obiect
Container

Atribute obligatorii
- cn
- objectClass

Atribute opţionale
- ibm-slapdPlugin

cn=SchemaDB

DN cn=SchemaDB, cn=LDCF Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Descriere
Această intrare conţine toate datele de configurare bază de date din prima secţiune a ibmslapd.conf.

Număr
1 (necesar)

Clasă Obiect
ibm-slapdLdcfBackend

Atribute obligatorii
- cn
- objectClass

Atribute opţionale
- ibm-slapdPlugin
- ibm-slapdSuffix

cn=SSL

DN cn=SSL, cn=Configuration

Descriere
Setări globale de conexiune SSL pentru Directory Server.

Număr
0 sau 1 (opţional)

Clasă Obiect
ibm-slapdSSL

Atribute obligatorii

- cn
- ibm-slapdSecurity
- ibm-slapdSecurePort
- ibm-slapdSslAuth
- objectClass

Atribute opţionale

- ibm-slapdSslCertificate
- ibm-slapdSslCipherSpec

  Notă: **ibm-slapdSslCipherSpecs** este acum depreciat. Folosiţi în schimb **ibm-slapdSslCipherSpec** . Dacă folosiţi **ibm-slapdSslCipherSpecs**, serverul va converti la atributul suportat.
- ibm-slapdSslKeyDatabase
- ibm-slapdSslKeyDatabasePW

cn=CRL

DN cn=CRL, cn=SSL, cn=Configuration

Descriere
Această intrare conţine datele de listă revocare certificat din prima secţiune (global stanza) a ibmslapd.conf. Este necesar doar dacă ″ibm-slapdSslAuth = serverclientauth″ din intrarea cn=SSL şi certificatele client au fost emise pentru validarea CRL.

Număr
0 sa 1 (opţional)

Clasă Obiect
ibm-slapdCRL

Atribute obligatorii

- cn
- ibm-slapdLdapCrlHost
- ibm-slapdLdapCrlPort
- objectClass

Atribute opţionale

- ibm-slapdLdapCrlUser
- ibm-slapdLdapCrlPassword

cn=Transaction

DN cn = Transaction, cn = Configuration

Descriere
Specifică setările globale de suport tranzacţie. Suportul de tranzacţie este oferit folosind plug-in-ul:

```
extendedop /QSYS.LIB/QGLDTRANEX.SRVPGM tranExtOpInit 1.3.18.0.2.12.5
1.3.18.0.2.12.6
```

Serverul (**slapd**) încarcă acest plugin automat la pornire dacă **ibm-slapdTransactionEnable = TRUE**. Pluginul nu necesită să fie adăugat explicit la **ibmslapd.conf**.

Număr

0 sau 1 (opţional; necesar doar dacă vreţi să folosiţi tranzacţii.)

Clasă Obiect

ibm-slapdTransaction

Atribute obligatorii

- cn
- ibm-slapdMaxNumOfTransactions
- ibm-slapdMaxOpPerTransaction
- ibm-slapdMaxTimeLimitOfTransactions
- ibm-slapdTransactionEnable
- objectClass

Atribute opţionale

- Fără

Atributele

Aceste informaţii prezintă atributele Directory Server utilizate pentru a configura fişierul ibmslapd.conf.

- cn
- ibm-slapdACIMechanism
- ibm-slapdACLAccess
- ibm-slapdACLCache
- ibm-slapdACLCacheSize
- ibm-slapdAdminDN
- ibm-slapdAdminGroupEnabled
- ibm-slapdAdminPW
- ibm-slapdAllowAnon
- ibm-slapdAllReapingThreshold
- ibm-slapdAnonReapingThreshold
- ibm-slapdBoundReapingThreshold
- ibm-slapdBulkloadErrors
- ibm-slapdCachedAttribute
- ibm-slapdCachedAttributeAutoAdjust
- ibm-slapdCachedAttributeAutoAdjustTime
- ibm-slapdCachedAttributeAutoAdjustTimeInterval
- ibm-slapdCachedAttributeSize
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdConcurrentRW
- ibm-slapdDB2CP
- ibm-slapdDBAlias
- ibm-slapdDbConnections
- ibm-slapdDbInstance
- ibm-slapdDbLocation
- ibm-slapdDbName

- ibm-slapdDbUserID
- ibm-slapdDbUserPW
- ibm-slapdDerefAliases
- ibm-slapdDigestAdminUser
- ibm-slapdDigestAttr
- ibm-slapdDigestRealm
- ibm-slapdEnableEventNotification
- ibm-slapdEntryCacheSize
- ibm-slapdErrorLog
- ibm-slapdESizeThreshold
- ibm-slapdEThreadActivate
- ibm-slapdEThreadEnable
- ibm-slapdETimeThreshold
- ibm-slapdFilterCacheBypassLimit
- ibm-slapdFilterCacheSize
- ibm-slapdIdleTimeOut
- ibm-slapdIncludeSchema
- ibm-slapdKrbAdminDN
- ibm-slapdKrbEnable
- ibm-slapdKrbIdentityMap
- ibm-slapdKrbKeyTab
- ibm-slapdKrbRealm
- ibm-slapdLanguageTagsEnabled
- ibm-slapdLdapCrlHost
- ibm-slapdLdapCrlPassword
- ibm-slapdLdapCrlPort
- ibm-slapdLdapCrlUser
- ibm-slapdMasterDN
- ibm-slapdMasterPW
- ibm-slapdMasterReferral
- ibm-slapdMaxEventsPerConnection
- ibm-slapdMaxEventsTotal
- ibm-slapdMaxNumOfTransactions
- ibm-slapdMaxOpPerTransaction
- ibm-slapdMaxPendingChangesDisplayed
- ibm-slapdMaxTimeLimitOfTransactions
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPageSizeLmt
- ibm-slapdPlugin
- ibm-slapdPort
- ibm-slapdPwEncryption
- ibm-slapdReadOnly
- ibm-slapdReferral
- ibm-slapdReplDbConns

- ibm-slapdReplicaSubtree
- ibm-slapdSchemaAdditions
- ibm-slapdSchemaCheck
- ibm-slapdSecurePort
- ibm-slapdSecurity
- ibm-slapdServerId
- ibm-slapdSetenv
- ibm-slapdSizeLimit
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSslAuth
- ibm-slapdSslCertificate
- ibm-slapdSslCipherSpec
- ibm-slapdSslKeyDatabase
- ibm-slapdSslKeyDatabasePW
- ibm-slapdSslKeyRingFile
- ibm-slapdSuffix
- ibm-slapdSupportedWebAdmVersion
- ibm-slapdSysLogLevel
- ibm-slapdTimeLimit
- ibm-slapdTransactionEnable
- ibm-slapdUseProcessIdPw
- ibm-slapdVersion
- ibm-slapdWriteTimeout
- objectClass

cn

Descriere
Acesta este atributul X.500 common Name, care conţine un nume de obiect.

Sintaxa
Şir director

Lungime maximă
256

Valoarea
Multi-valoric

ibm-slapdACIMechanism

Descriere
Determină ce model ACL foloseşte serverul. (Suportat doar pe i5/OS şi OS/400 de la v3.2, ignorat pe alte platforme.)

- 1.3.18.0.2.26.1 = Modelul IBM SecureWay v3.1 ACL
- 1.3.18.0.2.26.2 = Modelul IBM SecureWay v3.2 ACL

Default
1.3.18.0.2.26.2 = Modelul IBM SecureWay v3.2 ACL

Sintaxa
Şir director

Lungime maximă
256

Valoarea
Multi-valoric

ibm-slapdACLAccess

Descriere
Controlează dacă este activat accesul la ACL-uri. Dacă este setat pe TRUE, accesul la ACL-uri este activat. Dacă este setat pe FALSE, accesul la ACL-uri este dezactivat.

Default
TRUE

Sintaxa
Boolean

Lungime maximă
5

Valoarea
Valoare singulară

ibm-slapdACLCache

Descriere
Controlează dacă serverul stochează sau nu în cache informaţiile ACL.

- Dacă este setat pe TRUE, serverul memorează în cache informaţiile ACL.
- Dacă este setat pe FALSE, serverul nu memorează în cache informaţiile ACL.

Default
TRUE

Sintaxa
Boolean

Lungime maximă
5

Valoarea
Valoare singulară

ibm-slapdACLCacheSize

Descriere
Numărul maxim de intrări de păstrat în cache-ul ACL.

Default
25000

Sintaxa
Întreg

Lungime maximă
11

Valoarea
Valoare singulară

ibm-slapdAdminDN

Descriere
DN-ul de legare administrator pentru Directory Server.

Default
cn=root

Sintaxa
DN

Lungime maximă
Nelimitat

Valoarea
Valoare singulară

ibm-slapdAdminGroupEnabled

Descriere
Specifică dacă Grupul administrativ este în prezent activat. Dacă este setat la TRUE, serverul va permite utilizatorilor din grupul administrativ să se logheze.

Default
FALSE

Sintaxa
Boolean

Lungime maximă
128

Valoarea
Valoare singulară

ibm-slapdAdminPW

Descriere
Parola de legare administrator pentru Directory Server.

Default
secret

Sintaxa
Binar

Lungime maximă
128

Valoarea
Valoare singulară

ibm-slapdAllowAnon

Descriere
Specifică dacă sunt permise legări anonime.

Default
Adevărat

Sintaxa
Boolean

Lungime maximă
128

Valoarea
Valoare singulară

ibm-slapdAllReapingThreshold

Descriere
Specifică un număr de conexiuni de menţinut în server înainte ca gestiunea conexiunilor să fie activată.

Default
1200

Sintaxa
Şir director cu potrivire exactă la majuscule.

Lungime maximă
1024

Valoarea
Valoare singulară

ibm-slapdAnonReapingThreshold

Descriere
Specifică un număr de conexiuni de menţinut în server înainte ca gestiunea conexiunilor pentru conexiuni anonime să fie activată.

Default
0

Sintaxa
Şir director cu potrivire exactă la majuscule.

Lungime maximă
1024

Valoarea
Valoare singulară

ibm-slapdBoundReapingThreshold

Descriere
Specifică un număr de conexiuni de menţinut în server înainte ca gestiunea conexiunilor pentru conexiuni anonime şi legate să fie activată.

Default
1100

Sintaxa
Şir director cu potrivire exactă la majuscule.

Lungime maximă
1024

Valoarea
Valoare singulară

ibm-slapdBulkloadErrors

Descriere
Calea fişierului sau dispozitivul de pe maşina gazdă ibmslapd la care vor fi scrise mesajele de eroare bulkload.

Default
/var/bulkload.log

Sintaxa
Şir director cu potrivire exactă de majusculă

Lungime maximă
1024

Valoarea
Valoare singulară

ibm-slapdCachedAttribute

Descriere
Conţine numele atributelor de pus în cache în cache-ul de atribute, un nume atribut la o valoare.

Default
Fără

Sintaxa
Şir director

Lungime maximă
256

Valoarea
Multi-valoric

ibm-slapdCachedAttributeAutoAdjust

Descriere
Controlează dacă serverul va ajusta automat cache-urile de atribute la intervalele de timp configurate definite în ibm-slapdCachedAttributeAutoAdjustTime şi ibm-slapdCachedAttributeAutoAdjustTimeInterval.

Default
FALSE

Sintaxa
Boolean

Lungime maximă
5

Valoarea
Valoare singulară

ibm-slapdCachedAttributeAutoAdjustTime

Descriere
Când ibm-slapdCachedAttributeAutoAdjust este setat la TRUE, controlează ora la care serverul începe să ajusteze automat cache-urile de atribute.

```
Minim = T000000
Maxim = T235959
```

Default
T000000

Sintaxa
Oră militară

Lungime maximă
7

Valoarea
Valoare singulară

ibm-slapdCachedAttributeAutoAdjustTimeInterval

Descriere

Când ibm-slapdCachedAttributeAutoAdjust este setat la TRUE, controlează intervalul de timp dintre ajustările automate ala cache-ului de atribute.

```
Minim = 1
Maxim = 24
```

Default

2

Sintaxa

Întreg

Lungime maximă

2

Valoarea

Valoare singulară

ibm-slapdCachedAttributeSize

Descriere

Cantitatea de memorie, în octeţi, care poate fi folosită de cache-ul de atribute. O valoare 0 indică neutilizarea unui cache de atribute.

Default

0

Sintaxa

Întreg

Lungime maximă

11

Valoarea

Valoare singulară

ibm-slapdChangeLogMaxEntries

Descriere

Acest atribut este folosit de un plug-in istoric de modificări pentru a specifica numărul maxim de intrări din istoricul de modificări permise în baza de date RDBM. Fiecare istoric de modificări are propriul atribut changeLogMaxEntries.

```
Minim = 0 (nelimitat)
Maxim = 2,147,483,647 (32-biţi, întreg înregistrat)
```

Default

0

Sintaxa

Întreg

Lungime maximă

11

Valoarea

Valoare singulară

ibm-slapdCLIErrors

Descriere

Calea fişierului sau dispozitivul de pe maşina gazdă ibmslapd la care vor fi scrise mesajele de eroare CLI.

Default
/var/db2cli.log

Sintaxa
Şir director cu potrivire exactă de majusculă

Lungime maximă
1024

Valoarea
Valoare singulară

ibm-slapdConcurrentRW

Descriere
Setând aceasta pe TRUE permite efectuarea căutărilor simultan cu actualizările. Aceasta permite 'citiri murdare' ('dirty reads'), adică rezultate care ar putea să nu fie consistente cu starea comisă a bazei de date.

Atenţie: Acest atribut este învechit.

Default
FALSE

Sintaxa
Boolean

Lungime maximă
5

Valoarea
Valoare singulară

ibm-slapdDB2CP

Descriere
Specifică pagina de cod a bazei de date director. 1208 este pagina de cod pentru bazele de date UTF-8.

Sintaxa
Şir director cu potrivire exactă de majusculă

Lungime maximă
11

Valoarea
Valoare singulară

ibm-slapdDBAlias

Descriere
Aliasul bazei de date DB2.

Sintaxa
Şir director cu potrivire exactă de majusculă

Lungime maximă
8

Valoarea
Valoare singulară

ibm-slapdDbConnections

Descriere

Specificaţi numărul de conexiuni la DB2 pe care serverul le va dedica back-endu-ului DB2. Valoarea trebuie să fie între 5 & 50 (inclusiv).

Notă: Variabila de mediu ODBCCONS înlocuieşte valoarea acestei directive.
Dacă ibm-slapdDbConnections (sau ODBCCONS) este mai mic decât 5 sau mai mare decât 50, atunci serverul va folosi 5 sau 50, respectiv. Va fi creată 1 conexiune adiţională pentru replicare (chiar dacă nu este definită nici o replicare). Vor fi create 2 conexiuni adiţionale pentru istoricul de modificări (dacă acesta este activat).

Default

15

Sintaxa

Întreg

Lungime maximă

50

Valoarea

Valoare singulară

ibm-slapdDbInstance

Descriere

Specifică instanţa bazei de date DB2 pentru acest back-end.

Default

ldapdb2

Sintaxa

Şir director cu potrivire exactă de majusculă

Lungime maximă

8

Valoarea

Valoare singulară

Notă: Toate obiectele ibm-slapdRdbmBackend trebuie să folosească acelaşi set de caractere ibm-slapdDbInstance, ibm-slapdDbUserID, ibm-slapdDbUserPW şi DB2.

ibm-slapdDbLocation

Descriere

Calea în sistemul de fişiere unde se află baza de date backend.

Sintaxa

Şir director cu potrivire exactă de majusculă

Lungime maximă

1024

Valoarea

Valoare singulară

ibm-slapdDbName

Descriere

Specifică numele bazei de date DB2 pentru acest back-end.

Default
ldapdb2

Sintaxa
Şir director cu potrivire exactă de majusculă

Lungime maximă
8

Valoarea
Valoare singulară

ibm-slapdDbUserID

Descriere
Specifică numele utilizator cu care să vă legaţi la baza de date DB2 pentru acest back-end.

Default
ldapdb2

Sintaxa
Şir director cu potrivire exactă de majusculă

Lungime maximă
8

Valoarea
Valoare singulară

Notă: Toate obiectele ibm-slapdRdbmBackend trebuie să folosească acelaşi set de caractere ibm-slapdDbInstance ibm-slapdDbUserID, ibm-slapdDbUserPW şi DB2.

ibm-slapdDerefAliases

Descriere
Nivelul de dereferenţiere alias maxim la cererile de căutare, în ciuda oricăror derefAliases care ar fi putut să fie specificate la cererea clientului. Valorile permise sunt **niciodată**, **găsire**, **căutare** şi **întotdeauna**.

Default
întotdeauna

Sintaxa
Şir director

Lungime maximă
6

Valoarea
Valoare singulară

ibm-slapdDbUserPW

Descriere
Specifică parola utilizator cu care să vă legaţi la baza de date DB2 pentru acest back-end. Parola poate fi text întreg sau mască cifrată.

Default
ldapdb2

Sintaxa
Binar

Lungime maximă
128

Valoarea
Valoare singulară

Notă: Toate obiectele ibm-slapdRdbmBackend trebuie să folosească acelaşi set de caractere ibm-slapdDbInstance, ibm-slapdDbUserID, ibm-slapdDbUserPW şi DB2.

ibm-slapdDigestAdminUser

Descriere
Specifică Numele utilizator Digest MD5 al administratorului sau membrilor grupului administrattiv LDAP. Folosit când autentificarea MD5 Digest este folosită pentru a autentifica un administrator.

Default
Fără

Sintaxa
Şir director

Lungime maximă
512

Valoarea
Valoare singulară

ibm-slapdDigestAttr

Descriere
Înlocuieşte atributul username DIGEST-MD5 implicit. Numele atributului de utilizat pentru căutare username legare SASL DIGEST-MD5. Dacă valoarea nu este specificată, serverul foloseşte uid.

Default
Dacă nu este specificat, serverul foloseşte uid.

Sintaxa
Şir director.

Lungime maximă
64

Valoarea
Valoare singulară

ibm-slapdDigestRealm

Descriere
Înlocuieşte regiunea DIGEST-MD5 implicită. Un şir care poate permite utilizatorilor să afle ce username şi parolă să folosească, în cazul în care acestea ar fi diferite pentru servere diferite. Conceptual, acesta este numele unei colecţii de conturi care ar putea include contul utilizatorilor. Acest şir ar trebui să conţină ce puţin numele gazdei care realizează autentificarea şi ar putea indica în plus colecţia de utilizatori care ar putea avea acces. Un exemplu ar putea fi registered_users@gotham.news.example.com. Dacă atributul nu este specificat, serverul foloseşte hostname-ul complet calificat al serverului.

Default
Hostname-ul (numele gazdă) complet calificat al serverului

Sintaxa
Şir director.

Lungime maximă
1024

Valoarea
Valoare singulară

ibm-slapdEnableEventNotification

Descriere
Specifică dacă se activează Event Notification. Trebuie să fie setat ori pe TRUE ori pe FALSE.

Dacă este setat pe FALSE, serverul rejectază toate cererile client de înregistrare notificări evenimente cu rezultatul extins LDAP_UNWILLING_TO_PERFORM.

Default
TRUE

Sintaxa
Boolean

Lungime maximă
5

Valoarea
Valoare singulară

ibm-slapdEntryCacheSize

Descriere
Numărul maxim de intrări de păstrat în cache-ul de intrări.

Default
25000

Sintaxa
Întreg

Lungime maximă
11

Valoarea
Valoare singulară

ibm-slapdErrorLog

Descriere
Specifică calea fişierului sau dispozitivul de pe maşina Directory Server către care sunt scrise mesajele de eroare.

Default
/var/ibmslapd.log

Sintaxa
Şir director cu potrivire exactă de majusculă

Lungime maximă
1024

Valoarea
Valoare singulară

ibm-slapdESizeThreshold

Descriere
Specifică numărul de elemente în lucru în coada de lucru înainte de activarea firului de execuţie de urgenţă.

Default
50

Sintaxa
Întreg

Lungime maximă
1024

Valoarea
Valoare singulară

ibm-slapdEThreadActivate

Descriere
Specifică ce condiţii vor activa Firul de execuţie de urgenţă. Trebuie setat la una din următoarele valori:

S Numai dimensiune

T Numai ora

SOT Dimensiune sau oră

SAT Dimensiune şi oră

Default
SAT

Sintaxa
Şir

Lungime maximă
1024

Valoarea
Valoare singulară

ibm-slapdEThreadEnable

Descriere
Specifică dacă Firul de execuţie de urgenţă este activ.

Default
Adevărat

Sintaxa
Boolean

Lungime maximă
1024

Valoarea
Valoare singulară

ibm-slapdETimeThreshold

Descriere
Specifică durata de timp în minute între elementele înlăturate din coada de lucru înainte ca Firul de execuţie de urgenţă să fie activat.

Default
5

Sintaxa
Întreg

Lungime maximă
1024

Valoarea
Valoare singulară

ibm-slapdFilterCacheBypassLimit

Descriere
Filtrele de căutare care se potrivesc cu mai mult de acest număr de intrări nu vor fi adăugate în cache-ul de filtru de căutare. Deoarece lista de Id-uri intrări care s-au potrivit cu filtrul este inclusă în acest cache, această setare ajută la limitarea utilizării memoriei. O valoare 0 indică nici o limită.

Default
100

Sintaxa
Întreg

Lungime maximă
11

Valoarea
Valoare singulară

ibm-slapdFilterCacheSize

Descriere
Specifică numărul maxim de intrări de ţinut în Search Filter Cache.

Default
25000

Sintaxa
Întreg

Lungime maximă
11

Valoarea
Valoare singulară

ibm-slapdIdleTimeOut

Descriere
Timpul maxim cât se menţine deschisă o conexiune LDAP când nu este activitate pe conexiune. Timpul de inactivitate pentru o conexiune LDAP este timpul scurs (în secunde) de la ultima activitate de pe conexiune până în momentul curent. Dacă conexiunea a expirat, adică dacă perioada de inactivitate este mai mare decât valoarea acestui atribut, atunci serverul LDAP va curăţa şi va termina conexiunea LDAP, făcând-o astfel disponibilă pentru cereri de intrare.

Default
300

Sintaxa
Întreg

Lungime
11

Numărare
Singular

Folosire
Operaţie director

Modificare utilizator
Da

Clasă acces
Critică

Necesar
Nu

ibm-slapdIncludeSchema

Descriere
Specifică o cale de fişier de pe maşina Directory Server care conţine definiţiile schemei.

Default

- /etc/V3.system.at
- /etc/V3.system.oc
- /etc/V3.config.at
- /etc/V3.config.oc
- /etc/V3.ibm.at
- /etc/V3.ibm.oc
- /etc/V3.user.at
- /etc/V3.user.oc
- /etc/V3.ldapsyntaxes
- /etc/V3.matchingrules

Sintaxa
Şir director cu potrivire exactă de majusculă

Lungime maximă
1024

Valoarea
Multi-valoric

ibm-slapdKrbAdminDN

Descriere
Specifică ID-ul Kerberos al administratorului LDAP (de exemplu, ibm-kn=admin1@realm1). Folosit când este folosită autentificarea Kerberos pentru a autentifica administratorul când este înregistrat la interfaţa de administrare server. Aceasta ar putea fi specificată în loc de sau în plus faţă de adminDN şi adminPW.

Default
Nu este definită nici o valoare implicită.

Sintaxa
Şir director cu potrivire exactă de majusculă

Lungime maximă
128

Valoarea
Valoare singulară

ibm-slapdKrbEnable

Descriere
Specifică dacă serverul suportă Kerberos. Trebuie să fie TRUE sau FALSE.

Default
TRUE

Sintaxa
Boolean

Lungime maximă
5

Valoarea
Valoare singulară

ibm-slapdKrbIdentityMap

Descriere
Specifică dacă să folosiţi maparea de identităţi Kerberos. Trebuie să fie setat ori pe TRUE ori pe FALSE. Dacă este setat pe TRUE, când un client este autentificat cu un ID Kerberos, serverul caută toţi utilizatorii locali cu acreditări Kerberos corespunzătoare şi adaugă DNurile acelor utilizatori la acreditările de legare ale conexiunii. Aceasta permite ca ACL-urile bazate pe DNuri utilizator LDAP să fie încă utilizabile cu Kerberos.

Default
FALSE

Sintaxa
Boolean

Lungime maximă
5

Valoarea
Valoare singulară

ibm-slapdKrbKeyTab

Descriere
Specifică fişierul keytab Kerberos de pe serverul LDAP. Acest fişier conţine cheia privată a serverului LDAP, care este asociată cu contul său Kerberos. Acest fişier trebuie să fie protejat (precum fişierul de bază de date chei SSL al serverului).

Default
Nu este definită nici o valoare implicită.

Sintaxa
Şir director cu potrivire exactă de majusculă

Lungime maximă
1024

Valoarea
Valoare singulară

ibm-slapdKrbRealm

Descriere
Specifică regiunea Kerberos a serverului LDAP. Este folosit pentru a publica atributul ldapservicename din rădăcina DSE. Luaţi la cunoştinţă că un server LDAP poate servi ca depozitul de informaţii cont pentru multiple KDCs (şi regiuni), dar serverul LDAP, ca un server kerberized, poate fi membru al unei singure regiuni.

Default
Nu este definită nici o valoare implicită.

Sintaxa
Şir director cu potrivire inexactă de majusculă

Lungime maximă
256

Valoarea
Valoare singulară

ibm-slapdLanguageTagsEnabled

Descriere

Dacă serverul ar trebui sau nu să permită taguri de limbă. Valoarea citită din fişierul ibmslapd.conf file pentru acest atribut este FALSE, dar poate fi setată la TRUE.

Default

FALSE

Sintaxa

Boolean

Lungime maximă

5

Valoarea

Valoare singulară

ibm-slapdLdapCrlHost

Descriere

Specifică numele gazdă al serverului LDAP care conţine lista de revocare certificate (Certificate Revocation Lists - CRLuri) pentru validarea certificatelor client x.509v3. Acest parametru este necesar când ibm-slapdSslAuth=serverclientauth şi certificatele client au fost emise pentru validarea CRL.

Default

Nu este definită nici o valoare implicită.

Sintaxa

Şir director cu potrivire inexactă de majusculă

Lungime maximă

256

Valoarea

Valoare singulară

ibm-slapdLdapCrlPassword

Descriere

Specifică parola serverului LDAP care conţine lista de revocare certificate (Certificate Revocation Lists - CRLuri) pentru validarea certificatelor client x.509v3. Acest parametru ar putea fi necesar când ibm-slapdSslAuth=serverclientauth şi certificatele client au fost emise pentru validarea CRL.

Notă: Dacă serverul LDAP care păstrează CRLurile permite accesul neautentificat la CRLuri (adica acces anonim), atunci ibm-slapdLdapCrlPassword nu este necesar.

Default

Nu este definită nici o valoare implicită.

Sintaxa

Binar

Lungime maximă

128

Valoarea

Valoare singulară

ibm-slapdLdapCrlPort

Descriere

Specifică portul folosit pentru conectarea la serverul LDAP care conţine lista de revocare certificate (Certificate Revocation Lists - CRLuri) pentru validarea certificatelor client x.509v3. Acest parametru este

necesar când ibm-slapdSslAuth=serverclientauth şi certificatele client au fost emise pentru validarea CRL. (porturile IP nu sunt marcate, întregi de 16-biţi din intervalul 1 - 65535.)

Default
Nu este definită nici o valoare implicită.

Sintaxa
Întreg

Lungime maximă
11

Valoarea
Valoare singulară

ibm-slapdLdapCrlUser

Descriere
Specifică binDN-ul pe care SSL server-side îl foloseşte pentru a se lega la serverul LDAP care conţine lista de revocare certificate (Certificate Revocation Lists - CRLuri) pentru validarea certificatelor client x.509v3. Acest parametru ar putea fi necesar când ibm-slapdSslAuth=serverclientauth şi certificatele client au fost emise pentru validarea CRL.

Notă: Dacă serverul LDAP care păstrează CRLurile permite accesul neautentificat la CRLuri (adica acces anonim), atunci ibm-slapdLdapCrlUser nu este necesar.

Default
Nu este definită nici o valoare implicită.

Sintaxa
DN

Lungime maximă
1000

Valoarea
Valoare singulară

ibm-slapdMasterDN

Descriere
Specifică legarea DN a serverului master. Valoarea trebuie să se potrivească cu replicaBindDN din replicaObject definit pentru un server master. Când este folosit Kerberos pentru a autentifica la replică, ibm-slapdMasterDN trebuie să specifice reprezentarea DN a ID-ului Kerberos (de exemplu, ibm-kn=freddy@realm1). Când este folosit Kerberos, MasterServerPW este ignorat.

Default
Nu este definită nici o valoare implicită.

Sintaxa
DN

Lungime maximă
1000

Valoarea
Valoare singulară

ibm-slapdMasterPW

Descriere
Specifică parola de legare a serverului replică master. Valoarea trebuie să se potrivească cu replicaBindDN din replicaObject definit pentru un server master. Când este folosit Kerberos pentru a autentifica la replică,

ibm-slapdMasterDN trebuie să specifice reprezentarea DN a ID-ului Kerberos (de exemplu, ibm-kn=freddy@realm1). Când este folosit Kerberos, MasterServerPW este ignorat.

Default
Nu este definită nici o valoare implicită.

Sintaxa
Binar

Lungime maximă
128

Valoarea
Valoare singulară

ibm-slapdMasterReferral

Descriere
Specifică URL-ul serverului replică master. De exemplu:

```
ldap://master.us.ibm.com
```

Pentru securitate setaţi doar pe SSL:

```
ldaps://master.us.ibm.com:636
```

Pentru securitate setaţi pe nimic şi folosiţi un port nonstandard:

```
ldap://master.us.ibm.com:1389
```

Default
fără

Sintaxa
Şir director cu potrivire inexactă de majusculă

Lungime maximă
256

Valoarea
Valoare singulară

ibm-slapdMaxEventsPerConnection

Descriere
Specifică numărul maxim de notificări de evenimente care pot fi înregistrate pentru o conexiune.

```
Minim = 0 (nelimitat)
Maxim = 2,147,483,647
```

Default
100

Sintaxa
Întreg

Lungime maximă
11

Valoarea
Valoare singulară

ibm-slapdMaxEventsTotal

Descriere
Specifică numărul maxim de notificări de evenimente care pot fi înregistrate pentru toate conexiunile.

```
Minim = 0 (nelimitat)
Maxim = 2,147,483,647
```

Default
0

Sintaxa
Întreg

Lungime maximă
11

Valoarea
Valoare singulară

ibm-slapdMaxNumOfTransactions

Descriere
Specifică numărul maxim de tranzacţii pentru un server.

```
Minim = 0 (nelimitat)
Maxim = 2,147,483,647
```

Default
20

Sintaxa
Întreg

Lungime maximă
11

Valoarea
Valoare singulară

ibm-slapdMaxOpPerTransaction

Descriere
Specifică numărul maxim de operaţii pentru o tranzacţie.

```
Minim = 0 (nelimitat)
Maxim = 2,147,483,647
```

Default
5

Sintaxa
Întreg

Lungime maximă
11

Valoarea
Valoare singulară

ibm-slapdMaxPendingChangesDisplayed

Descriere
Numărul maxim de modificări în aşteptare de afişat.

Default
200

Sintaxa
Întreg

Lungime maximă
11

Valoarea
Valoare singulară

ibm-slapdMaxTimeLimitOfTransactions

Descriere
Specifică, în secunde, valoarea timeout maximă a unei tranzacţii în aşteptare.

```
Minim = 0 (nelimitat)
Maxim = 2,147,483,647
```

Default
300

Sintaxa
Întreg

Lungime maximă
11

Valoarea
Valoare singulară

ibm-slapdPagedResAllowNonAdmin

Descriere
Indiferent dacă serverul ar trebui să permită sau nu legarea non-administrator pentru cererile rezultate paginate dintr-o cerere de căutare. Dacă valoarea citită din fişierul ibmslapd.conf este FALSE, serverul va procesa doar acele cereri client emise de un utilizator cu autorizarea de administrator. Dacă un client cere rezultate paginate pentru o operaţie de căutare, nu are autorizare de administrator şi valoarea citită din fişierul ibmslapd.conf pentru acest atribut este FALSE, serverul va returna la client codul retur insufficientAccessRights; nu va fi efectuată nici o căutare sau paginare.

Default
FALSE

Sintaxa
Boolean

Lungime
5

Numărare
Singular

Folosire
directoryOperation

Modificare utilizator
Da

Clasă acces
critic

Objectclass
ibm-slapdRdbmBackend

Necesar
Nu

ibm-slapdPagedResLmt

Descriere

Numărul maxim de cereri de căutare rezultate paginate remarcabile permise active simultan. Range = 0.... Dacă un client cere o operaţie cu rezultate paginate şi numărul maxim de rezultate paginate remarcabile sunt active, serverul va returna la client codul retur ocupat (busy); nu va fi efectuată nici o căutare sau paginare.

Default

3

Sintaxa

Întreg

Lungime

11

Numărare

Singular

Folosire

directoryOperation

Modificare utilizator

Da

Clasă acces

critic

Necesar

Nu

Objectclass

ibm-slapdRdbmBackend

ibm-slapdPageSizeLmt

Descriere

Numărul maxim de intrări de returnat de la o căutare a unei pagini individuale când este specificat controlul rezultatelor paginate, indiferent de orice dimensiune de pagină care ar fi putut fi specificată în cererea de căutare de la client. Range = 0.... Dacă un client a pasat o dimensiune de pagină, atunci va fi folosită valoarea cea mai mică dintre valoarea client şi valoarea citită din ibmslapd.conf.

Default

50

Sintaxa

Întreg

Lungime

11

Numărare

Singular

Folosire

directoryOperation

Modificare utilizator

Da

Clasă acces

critic

Necesar

Nu

Objectclass
ibm-slapdRdbmBackend

ibm-slapdPlugin

Descriere
Un plugin este o bibliotecă încărcată dinamic care extinde capabilităţile serverului. Un atribut ibm-slapdPlugin specifică serverului cum să încarce şi să iniţializeze o bibliotecă plug-in. Sintaxa este:

cuvânt cheie nume fişier `init_function [`*`args`*`...]`

Sintaxa este uşor diferită pentru fiecare platformă datorită convenţiilor de numire ale bibliotecii.

Majoritatea plug-in-urilor sunt opţionale, dar pluginul backend RDBM este necesar pentru toate backend-urile RDBM.

Default
database /bin/libback-rdbm.dll rdbm_backend_init

Sintaxa
Şir director cu potrivire exactă de majusculă

Lungime maximă
2000

Valoarea
Multi-valoric

ibm-slapdPort

Descriere
Specifică portul TCP/IP dolosit pentru conexiuni non-SSL. Nu poate avea aceeaşi valoare ca şi ibm-slapdSecurePort. (porturile IP nu sunt marcate, întregi de 16-biţi din intervalul 1 - 65535.)

Default
389

Sintaxa
Întreg

Lungime maximă
5

Valoarea
Valoare singulară

ibm-slapdPWEncryption

Descriere
Specifică mecanismul de codificare pentru parolele utilizator înainte de a fi stocate în director. Trebuie să fie specificat ca none, imask, crypt sau sha (trebuie să folosiţi cuvântul cheie **sha** pentru a obţine codificarea SHA-1). Valoarea trebuie să fie setată la none pentru ca legarea SASL cram-md5 să aibă succes.

Default
fără

Sintaxa
Şir director cu potrivire inexactă de majusculă

Lungime maximă
5

Valoarea
Valoare singulară

ibm-slapdReadOnly

Descriere

Acest atribut este aplicat în mod normal doar la backend-ul director. El specifică dacă se poate scrie în backend. Trebuie să fie specificat ori pe TRUE ori pe FALSE. Are valoarea implicită FALSE dacă nu este specificat. Dacă este setat pe TRUE, serverul întoarce LDAP_UNWILLING_TO_PERFORM (0x35) ca răspuns la orice cerere client care modifică datele din baza de date readOnly.

Default

FALSE

Sintaxa

Boolean

Lungime maximă

5

Valoarea

Valoare singulară

ibm-slapdReferral

Descriere

Specifică URL-ul LDAP referral de trimis înapoi când sufixele locale nu corespund cererii. Este folosit pentru referral superior (adică sufixul nu este în cadrul contextului de nume al serverului).

Default

Nu este definită nici o valoare implicită.

Sintaxa

Şir director cu potrivire exactă de majusculă

Lungime maximă

32700

Valoarea

Multi-valoric

ibm-slapdReplDbConns

Descriere

Numărul maxim de conexiuni ale bazei de date pentru folosul de către replicare.

Default

4

Sintaxa

Întreg

Lungime maximă

11

Valoarea

Valoare singulară

ibm-slapdReplicaSubtree

Descriere

Identifică DN-ul unui subarbore replicat

Sintaxa

DN

Lungime maximă

1000

Valoarea
Valoare singulară

ibm-slapdSchemaAdditions

Descriere
Atributul ibm-slapdSchemaAdditions este folosit pentru a identifica explicit ce fişier păstrează noile intrări de schemă. Acesta este setat implicit pe /etc/V3.modifiedschema. Dacă acest atribut nu este definit, serverul revine la folosirea ultimului fişier ibm-slapdIncludeSchema ca în ediţiile anterioare.

Înainte de Version 3.2, ultima intrare includeSchema din **slapd.conf** era fişierul în care erau adăugate de către server orice noi intrări de schemă dacă primea o cerere de adăugare de la un client. În mod normal ultima includeSchema este fişierul V3.modifiedschema, care este un fişier gol instalat doar pentru acest scop.

Notă: Numele modified este înşelător, deoarece stochează doar intrări noi. Schimbările la intrările de schemă existente sunt făcute în fişierele lor originale.

Default
/etc/V3.modifiedschema

Sintaxa
Şir director cu potrivire exactă de majusculă

Lungime maximă
1024

Valoarea
Valoare singulară

ibm-slapdSchemaCheck

Descriere
Specifică mecanismul de verificare schemă pentru operaţia de adăugare/modificare/ştergere. Trebuie specificat ca V2, V3 sau V3_lenient.

- V2 - Reţine verificarea v2 şi v2.1. Recomandat pentru migrare.
- V3 - Realizează verificare v3.
- V3_lenient - Nu toate clasele de obiecte părinte sunt necesare. Doar clasa de obiecte imediată este necesară când se adaugă intrări.

Default
V3_permisiv

Sintaxa
Şir director cu potrivire inexactă de majusculă

Lungime maximă
10

Valoarea
Valoare singulară

ibm-slapdSecurePort

Descriere
Specifică portul TCP/IP folosit de conexiuni SSL. Nu poate avea aceeaşi valoare ca ibm-slapdPort. (porturile IP nu sunt marcate, întregi de 16-biţi din intervalul 1 - 65535.)

Default
636

Sintaxa
Întreg

Lungime maximă
5

Valoarea
Valoare singulară

ibm-slapdSecurity

Descriere
Activează conexiunile SSL şi TLS. Trebuei să fie nici una, SSL, SSLOnly, TLS sau SSLTLS.

- nici una - Serverul ascultă numai pe porul nesecurizat.
- SSL - Serverul ascultă pe ambele porturi SSL şi non-SSL. Portul securizat este singurul mod de a folosi o conexiune sigură.
- SSLOnly - Serverul ascultă doar pe portul SSL.
- TLS - Serverul ascultă numai pe portul nesecurizat. Operaţia extinsă StartTLS este singura modalitate de a folosi o conexiune sigură.
- SSLTLS - Serverul ascultă atât pe portul implicit, cât şi pe cel securizat. Operaţia extinsă StartTLS poate fi folosită pentru a obţine o conexiune sigură peste portul implicit sau clientul poate folosi direct portul securizat. Trimiterea unei StartTLS peste portul secutizat va întoarce mesajul LDAP_OPERATIONS_ERROR.

Default
fără

Sintaxa
Şir director cu potrivire inexactă de majusculă

Lungime maximă
7

Valoarea
Valoare singulară

ibm-slapdServerId

Descriere
Identifică serverul de folosit în replicare.

Sintaxa
Şir IA5 cu potrivire sensibilă la majusculă

Lungime maximă
240

Valoarea
Valoare singulară

ibm-slapdSetenv

Descriere
Serverul rulează **putenv()** pentru toate valorile ibm-slapdSetenv la pornire pentru a modifica mediul runtime al serverului. Variabilele shell (precum %PATH% sau $LANG) nu sunt expandate.

Default
Nu este definită nici o valoare implicită.

Sintaxa
Şir director cu potrivire exactă de majusculă

Lungime maximă
2000

Valoarea
Multi-valoric

ibm-slapdSizeLimit

Descriere
Specifică numărul maxim de intrări de returnat de la o căutare, indiferent de orice dimensiune limită care ar fi putut fi specificată în cererea de căutare de la client (Range = 0...). Dacă un client a pasat o limită, atunci va fi folosită cea mai mică valoare dintre valorile client şi valoarea citită din **ibmslapd.conf**. Dacă un client nu a pasat o limită şi s-a legat ca DN admin, limita este considerată nelimitată. Dacă clientul nu a pasat o limită şi nu s-a legat ca DN admin, atunci limita este cea care a fost citită din fişierul **ibmslapd.conf**. 0 = nelimitat.

Default
500

Sintaxa
Întreg

Lungime maximă
12

Valoarea
Valoare singulară

ibm-slapdSortKeyLimit

Descriere
Numărul maxim de condiţii (chei) de sortare care pot fi specificate la o singură cerere de căutare. Range = 0.... Dacă un client a pasat o cerere de căutare cu mai multe chei de sortare decât permite limita şi caracterul critic al controlului de căutare sortată este FALSE, atunci serverul va onora valoarea citită din fişierul ibmslapd.conf şi va ignora orice chei de sortare întâlnite după ce a fost atinsă limita - căutarea şi sortarea vor fi efectuate. Dacă un client a pasat o cerere de căutare cu mai multe chei de sortare decât permite limita şi caracterul critic al controlului de căutare sortată este TRUE, atunci serverul va reveni la client cu un cod de întoarcere **adminLimitExceeded** - nu va fi realizată nici o căutare sau sortare.

Default
3

Sintaxa
cis

Lungime
11

Numărare
Singular

Folosire
directoryOperation

Modificare utilizator
Da

Clasă acces
critic

Objectclass
ibm-slapdRdbmBackend

Necesar
Nu

ibm-slapdSortSrchAllowNonAdmin

Descriere

Dacă serverul ar trebui să permită sau nu legarea non-administrator pentru sortare într-o cerere de căutare. Dacă valoarea citită din fişierul ibmslapd.conf este FALSE, serverul va procesa doar acele cereri client emise de un utilizator cu autorizarea de administrator. Dacă un client cere sortare pentru o operaţie de căutare, nu are autorizare de administrator şi valoarea citită din fişierul ibmslapd.conf pentru acest atribut este FALSE, serverul va returna la client codul retur insufficientAccessRights; nu va fi efectuată nici o căutare sau paginare.

Default

FALSE

Sintaxa

Boolean

Lungime

5

Numărare

Singular

Folosire

directoryOperation

Modificare utilizator

Da

Clasă acces

critic

Objectclass

ibm-slapdRdbmBackend

Necesar

Nu

ibm-slapdSslAuth

Descriere

Specifică tipul de autentificare pentru conexiunea SSL, ori serverauth ori serverclientauth.

- serverauth - suportă autentificarea server la client. Aceasta este situaţia implicită.
- serverclientauth - suportă atât autentificarea server cât şi client.

Default

serverauth

Sintaxa

Şir director cu potrivire inexactă de majusculă

Lungime maximă

16

Valoarea

Valoare singulară

ibm-slapdSslCertificate

Descriere

Specifică eticheta care identifică Certificatul personal al serverului în fişierul bază de date chei. Această etichetă este specificată când cheia privată a serverului şi certificatul sunt create cu aplicaţia **gsk4ikm**. Dacă nu este definit ibm-slapdSslCertificate, atunci cheia privată implicită, aşa cum este definită în fişierul bază de date chei, este folosită de către serverul LDAP pentru conexiuni SSL.

Default
Nu este definită nici o valoare implicită.

Sintaxa
Şir director cu potrivire exactă de majusculă

Lungime maximă
128

Valoarea
Valoare singulară

ibm-slapdSslCipherSpec

Specifică metoda de criptare SSL pentru clienţii care accesează serverul. Trebuie setată la una din următoarele:

Tabela 6. Metode de criptare SSL

Atribut	Nivel criptare
TripleDES-168	Criptare Triple DES cu o cheie de 168-biţi şi SHA-1 MAC
DES-56	Criptare DES cu o cheie de 56-biţi şi SHA-1 MAC
RC4-128-SHA	Criptare RC4 cu o cheie de 128-biţi şi SHA-1 MAC
RC4-128-MD5	Criptare RC4 cu o cheie de 128-biţi şi MD5 MAC
RC2-40-MD5	Criptare RC4 cu o cheie de 40-biţi şi MD5 MAC
RC4-40-MD5	Criptare RC4 cu o cheie de 40-biţi şi MD5 MAC
AES	Criptare AES

Sintaxa
Şir IA5

Lungime maximă
30

ibm-slapdSslKeyDatabase

Descriere
Specifică calea fişierului către fişierul bază de date chei SSL ale serverului LDAP. Acest fişier bază de date chei este folosit pentru tratarea conexiunilor SSL de la clienţii LDAP precum şi pentru crearea conexiunilor securizate SSL cu serverele LDAP replică.

Default
/etc/key.kdb

Sintaxa
Şir director cu potrivire exactă de majusculă

Lungime maximă
1024

Valoarea
Valoare singulară

ibm-slapdSslKeyDatabasePW

Descriere
Specifică parola asociată cu fişierul bază de date chei SSL ale serverului LDAP, aşa cum este specificată în parametrul ibm-slapdSslKeyDatabase. Dacă fişierul bază de date chei server LDAP are asociat un fişier stash parole, atunci parametrul ibm-slapdSslKeyDatabasePW poate fi omis sau setat pe none.

Notă: Fişierul stash parole trebuie să se afle în acelaşi director ca şi fişierul baze de date chei şi trebuie să aibă acelaşi nume ca şi fişierul baze de date chei, dar cu extensia .sth în loc de .kdb.

Default
fără

Sintaxa
Binar

Lungime maximă
128

Valoarea
Valoare singulară

ibm-slapdSslKeyRingFile

Descriere
Calea către fişierul baze de date chei SSL ale serverului LDAP. Acest fişier bază de date chei este folosit pentru tratarea conexiunilor SSL de la clienţii LDAP precum şi pentru crearea conexiunilor securizate SSL cu serverele LDAP replică.

Default
key.kdb

Sintaxa
Şir director cu potrivire sensibilă la majusculă

Lungime maximă
1024

Valoarea
Valoare singulară

ibm-slapdSuffix

Descriere
Specifică un context de numire de memorat în acest back-end.

Notă: Acesta are acelaşi nume cu clasa obiectului.

Default
Nu este definită nici o valoare implicită.

Sintaxa
DN

Lungime maximă
1000

Valoarea
Multi-valoric

ibm-slapdSupportedWebAdmVersion

Descriere
Acest atribut defineşte cea mai veche versiune a uneltei de administrare care suportă acest server de cn=configuration.

Default

Sintaxa
Şir director

Lungime maximă

Valoarea
Valoare singulară

ibm-slapdSysLogLevel

Descriere
Specifică nivelul la care statisticele de depanare şi de operaţii sunt înregistrate în istoricul fişierului slapd.errors. Trebuie specificat ca l, m sau h.

- h - înalt (high)(furnizează cele mai multe informaţii)
- m - mediu (medium)(valoarea implicită)
- l - jos (low) (furnizează cele mai puţine informaţii)

Default
m

Sintaxa
Şir director cu potrivire inexactă de majusculă

Lungime maximă
1

Valoarea
Valoare singulară

ibm-slapdTimeLimit

Descriere
Specifică numărul maxim de secunde pentru o cerere de căutare, indiferent de orice limită de timp care ar fi putut fi specificată în cererea de la client. Dacă un client a pasat o limită, atunci va fi folosită cea mai mică valoare dintre valorile client şi valoarea citită din **ibmslapd.conf**. Dacă un client nu a pasat o limită şi s-a legat ca DN admin, limita este considerată nelimitată. Dacă clientul nu a pasat o limită şi nu s-a legat ca DN admin, atunci limita este cea care a fost citită din fişierul **ibmslapd.conf**. 0 = nelimitat.

Default
900

Sintaxa
Întreg

Lungime maximă

Valoarea
Valoare singulară

ibm-slapdTransactionEnable

Descriere
Dacă plug-in-ul de tranzacţii este încărcat, dar ibm-slapdTransactionEnable este setat pe FALSE, serverul rejectează toate cererile StartTransaction cu răspunsul LDAP_UNWILLING_TO_PERFORM.

Default
TRUE

Sintaxa
Boolean

Lungime maximă
5

Valoarea
Valoare singulară

ibm-slapdUseProcessIdPw

Descriere
Dacă este setat la TRUE, serverul ignoră atributele ibm-slapdDbUserID şi ibm-slapdDbUserPW şi foloseşte propriile acreditări de proces pentru a se autentifica la DB2.

Default
FALSE

Sintaxa
Boolean

Lungime maximă
5

Valoarea
Valoare singulară

ibm-slapdVersion

Descriere
Număr versiune IBM Slapd

Default

Sintaxa
Şir director cu potrivire sensibilă la majusculă

Lungime maximă

Valoarea
Valoare singulară

ibm-slapdWriteTimeout

Descriere
Specifică o valoare de timeout în secunde pentru scrierile blocate. Când limita de timp este atinsă, conexiunea va fi abandonată.

Default
120

Sintaxa
Întreg

Lungime maximă
1024

Valoarea
Valoare singulară

objectClass

Descriere
Valorile atributului objectClass descriu tipul de obiect pe care îl reprezintă o intrare.

Sintaxa
Şir director

Lungime maximă
128

Valoarea
Multi-valoric

Identificatorii de obiecte (OID)

Aceste informaţii conţin identificatorii de obiect (OID) utilizaţi în Directory Server.

OID-urile afişate în următoarele tabele sunt folosite în Directory Server. Aceste OID-uri sunt în DSE-ul rădăcină. Intrarea DSE rădăcină conţine informaţii despre însuşi serverul. În Centrul de informare Tivoli software, aflaţi mai multe despre identificatoarele de obiecte (OID-uri) pentru operaţii extinse şi elemente de control, inclusiv codarea cererii şi datele răspuns asociate cu următoarele elemente de control şi operaţii extinse.

Controale

Tabela 7. Controale suportate de Directory Server

Nume	OID	Cele mai vechi sau ediţia i5/OS sau OS/400	Cea mai veche versiune de IBM Tivoli Directory Server	Descriere
Manage DSA IT	2.16.840.1.1137.30.3.4.2	V4R5	V3.2	Tratează intrările trimitere ca intrări obişnuite.
“Tranzacţiile” la pagina 50	1.3.18.0.2.10.5	V4R5	V3.2	Marchează o operaţie ca parte a tranzacţiei.
os400-dltusrprf-ownobjopt	1.3.18.0.2.10.8	V5R2		Ştergeţi opţiunea profil utilizator pentru proprietarul obiectului. Consultaţi “Back-end proiectat de sistem de operare” la pagina 83 pentru detalii.
os400-dltusrprf-pgpopt	1.3.18.0.2.10.9	V5R2		Ştergeţi opţiunea profil utilizator pentru grupul primar. Consultaţi “Back-end proiectat de sistem de operare” la pagina 83 pentru detalii.
Căutare sortată	1.2.840.113556.1.4.473 (cerere) şi 1.2.840.113556.1.4.474 (răspuns)	V5R2 cu PTF	V4.1	Sortare rezultate căutare înainte de a întoarce intrările către client. Vedeţi“Parametrii de căutare” la pagina 46.
Căutare paginată	1.2.840.113556.1.4.319	V5R2 cu PTF	V4.1	Întoarce către client rezultatele căutării în pagini în loc de a le întoarce pe toate deodată. Vedeţi“Parametrii de căutare” la pagina 46.

Tabela 7. Controale suportate de Directory Server (continuare)

Nume	OID	Cele mai vechi sau ediţia i5/OS sau OS/400	Cea mai veche versiune de IBM Tivoli Directory Server	Descriere
Control ştergere arbore	1.2.840.113556.1.4.805	V5R3	V5.1	Acest control este ataşat unei cereri de Ştergere pentru a indica faptul că intrarea specificată şi toate intrările descendente vor fi şterse. Utilizatorul trebuie să fie un administrator al directorului. Intrarea care va fi ştearsă nu poate fi un context de replicare.
"Politica de parolă" la pagina 75	1.3.6.1.4.1.42.2.27.8.5.1	V5R3	V5.1	Întoarce către client informaţiile suplimentare de eroare de politică parolă.
Administrare server	1.3.18.0.2.10.15	V5R3	V5.1	Permite administratorului să efectueze operaţii de reparare care ar fi în mod normal refuzate (de exemplu: actualizarea unei replici numai-citire, actualizarea unui server liniştit sau setarea anumitor atribute operaţionale).
"Autorizarea proxy" la pagina 62	2.16.840.1.113730.3.4.18	V5R4	V5.2	Aplicaţia client se poate lega la director folosind propria identitate, dar îi este permis să realizeze operaţii din partea altui utilizator.
Control legare furnizor replicare	1.3.18.0.2.10.18	V5R3	V5.2	Acest control este adăugat de furnizor, dacă furnizorul este un server gateway.
Reîmprospătare control intrare	1.3.18.0.2.10.24	V6R1	V6.0	Acest control este utilizat în totalitate de către server pentru a suporta replicare conflict rezoluţie.
Nici o replicare conflict rezoluţie	1.3.19.0.2.10.27	V6R1	V6.0	Acest control este utilizat în totalitate de către server pentru a suporta replicare conflict rezoluţie.

Tabela 7. Controale suportate de Directory Server (continuare)

Nume	OID	Cele mai vechi sau ediţia i5/OS sau OS/400	Cea mai veche versiune de IBM Tivoli Directory Server	Descriere
Nu copiaţi controlul	1.3.19.0.2.10.23	V6R1	V6.0	Acest control poate fi specificat de către un administrator pentru a cere ca operaţia asociată să nu fie copiată la alte servere. Controlul nu are o valoare de control.
Auditare control	1.3.18.0.2.10.22	V6R1	V6.0	Acest control este utilizat de către clienţi autorizaţi, incluzând serverul proxy, pentru a identifica clientul ce a iniţiat cererea ce poate fi rutată prin mai multe servere.
Control autorizaţie grup	1.3.18.0.2.10.21	V6R1	V6.0	Acest control este utilizat pentru a presupune apartenenţa la grup a identităţii autorizate a clientului, decât apartenenţa grup server. Este utilizat în conjunctură cu controlul de autorizare proxy.
Modificare grupuri doar element de control	1.3.18.0.2.10.25	V6R1	V6.0	Operaţia cu acest element de control (fie ştergere sau modrdn/dn) va fi recunoscută de către serverele back-end ca un tip special de operaţie unde dn-ul nu este şters sau redenumit; mai degrabă, grupurile în care se află sunt modificate fie la ştergere sau redenumire de referinţă la dn-ul destinaţie în apartenenţa sa.
Omitere control integritate referenţial grup	1.3.18.0.2.10.26	V6R1	V6.0	Omiterea procesării integrităţii referenţial grup pe o cerere de ştergere sau modrdn. ACI şi apartenenţă grup nu sunt actualizate pentru a reflecta modificarea.

Tabela 7. Controale suportate de Directory Server (continuare)

Nume	OID	Cele mai vechi sau ediţia i5/OS sau OS/400	Cea mai veche versiune de IBM Tivoli Directory Server	Descriere
AES control legătură	1.3.18.0.2.10.28	V6R1	V6.0	Acest control permite ca IBM Tivoli Directory Server să trimită actualizări către serverul consumator cu parole deja criptate utilizând AES.

Operaţii extinse

Tabela 8. OID-uri pentru operaţiile extinse

Nume	OID	Cea mai veche ediţie i5/OS sau OS/400	Cea mai veche versiune de IBM Tivoli Directory Server	Descriere
Înregistrare pentru evenimente	1.3.18.0.2.12.1	V4R5	V3.2	Cerere înregistrare pentru evenimente în Suport evenimente Tivoli Directory Server
Anulare înregistrare pentru evenimente	1.3.18.0.2.12.3	V4R5	V3.2	Anularea înregistrării evenimentelor ce au fost înregsitrate pentru utilizare Cerere înregistrare evenimet.
Începere tranzacţie	1.3.18.0.2.12.5	V4R5	V3.2	Începerea unui context tranzacţional
Terminare tranzacţie	1.3.18.0.2.12.6	V4R5	V3.2	Oprire context tranzacţional (commit/rollback)
Cerere normalizare DN	1.3.18.0.2.12.30	V5R3	V5.1	Cerere de normalizare a unui DN sau a unei secvenţe de DN-uri.
StartTLS	1.3.6.1.4.1.1466.20037	V5R4	V5.2	Cerere de pornire Transport Layer Security.

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

Tabela 9. Operaţii extinse suplimentare

Nume	OID	Cea mai veche ediţie i5/OS	Cea mai veche versiune de IBM Tivoli Directory Server	Descriere
Replicare control	1.3.18.0.2.12.16	V5R3	V5.1	Această operaţie efectuează acţiunea cerută pe server şi este emisă către şi cascadează apelul către toţi consumatorii de sub el din topologia de replicare. Clientul trebuie să fie administratorul directorului sau să aibă autorizare de scriere pentru obiectul ibm-replicagroup=default pentru contextul de replicare asociat.
Coada de replicare control	1.3.18.0.2.12.17	V5R3	V5.1	Această operaţie marchează elementele ca deja replicate pentru o înţelegere specificată. Această operaţie este permisă doar când clientul are autoritate de scriere pentru acordul (agreement) de replicare.
Liniştire (quiesce) sau trezire (unquiesce)	1.3.18.0.2.12.19	V5R3	V5.1	Această operaţie pune subarborele într-o stare în care el nu acceptă actualizări client (sau termină această stare), cu excepţia acelora de la clienţi autentificaţi ca administrator al directorului în care este prezent controlul de Administrare server. Clientul trebuie să fie autentificat ca administratorul directorului sau să aibă autoritate de scriere pentru obiectul ibm-replicagroup=default pentru contextul de replicare asociat.
Cascadarea replicării controlului	1.3.18.0.2.12.15	V5R3	V5.1	Această operaţie efectuează acţiunea cerută pe server şi este emisă către şi cascadează apelul către toţi consumatorii de sub el din topologia de replicare. Clientul trebuie să fie administratorul directorului sau să aibă autorizare de scriere pentru obiectul ibm-replicagroup=default pentru contextul de replicare asociat.
Actualizare configuraţie	1.3.18.0.2.12.28	V5R3	V5.1	Această operaţie este folosită pentru a face ca serverul să recitească setările specificate din configuraţia lui. Operaţia este permisă doar când clientul este administratorul directorului.
Oprire cerere de conexiune	1.3.18.0.2.12.35	V5R4	V5.2	Cerere de oprire a conexiunilor de pe server. Cel care apelează trebuie să fie un administrator de director.
Cerere de atribut unic	1.3.18.0.2.12.44	V5R4	V5.2	Cere serverului să întoarcă o listă de valori care nu sunt unice pentru un nume de atribut dat. Vedeţi “ldapexop” la pagina 214 -op uniqueattr. Cel care apelează trebuie să fie un administrator de director.

Tabela 9. Operaţii extinse suplimentare (continuare)

Nume	OID	Cea mai veche ediţie i5/OS	Cea mai veche versiune de IBM Tivoli Directory Server	Descriere
Cerere tip de atribut	1.3.18.0.2.12.46	V5R4	V5.2	Cere serverului să întoarcă o listă de nume de atribute care au o anumită caracteristică. Vedeţi“ldapexop” la pagina 214 -op getattributes
Cerere tip utilizator	1.3.18.0.2.12.37	V5R3	V5.2	Cerere pentru a obţine Tipul utilzator al utilizatorului legat.
Operaţie extinsă istoric eroare replicare	1.3.18.0.2.12.56	V6R1	V6.0	Cererea extinsă IBM Replication Error Control este utilizată pentru a vizualiza istoricul cu erori de replicare, reîncercare intrări de la istoric sau ştergere intrări istoric. Cel care apelează trebuie să fie un administrator de director sau să aibe autorizarea de scris la obiectul ibm-replicagroup=default pentru contextul de replicare asociat.
Operaţie extinsă evaluare grup	1.3.18.0.2.12.50	V6R1	V6.0	Cere toate grupurile de care aparţine un utilizator dat. Cel care apelează trebuie să fie un administrator de director.
Operaţie extinsă topologie replicare	1.3.18.0.2.12.54	V6R1	V6.0	Declanşarea unei replicări de replicare intrări înrudite-topologie sub un context de replicare dat. Cel care apelează trebuie să fie un administrator de director sau să aibe autorizarea de scris la obiectul ibm-replicagroup=default pentru contextul de replicare asociat.
Operaţie extinsă stare cont	1.3.18.0.2.12.58	V6R1	V6.0	Această operaţie extinsă trimite serverului un DN al unei intrări ce conţine un atribut userPassword şi serverul trimite înapoi starea contului utilizatorului ce este interogată: dechis, blocat sau expirat. Cel care apelează trebuie să fie un administrator de director.
Operaţie extinsă obţinere fişier	1.3.18.0.2.12.73	V6R1	V6.0	Returnează conţinutul unui fişier dat din server. Cel care apelează trebuie să fie un administrator de director.Suportă istoricul LostAndFound şi istoricul de auditare Tivoli Directory Server. Istoricul de auditare nu este înrudit cu capabilităţile de auditare securitate i5/OS ale serverului de director.
Operaţie extinsă obţinere linii	1.3.18.0.2.12.22	V6R1	V6.0	Cerere de obţinere linii de la istoricul unui fişier. Cel care apelează trebuie să fie un administrator de director. Suportă istoricul LostAndFound şi istoricul de auditare Tivoli Directory Server. Istoricul de auditare nu este înrudit cu capabilităţile de auditare securitate i5/OS ale serverului de director.

Tabela 9. Operaţii extinse suplimentare (continuare)

Nume	OID	Cea mai veche ediţie i5/OS	Cea mai veche versiune de IBM Tivoli Directory Server	Descriere
Operaţie extinsă obţinere număr de linii	1.3.18.0.2.12.24	V6R1	V6.0	Cerere număr de linii într-un fişier istoric. Cel care apelează trebuie să fie un administrator de director. Suportă istoricul LostAndFound şi istoricul de auditare Tivoli Directory Server. Istoricul de auditare nu este înrudit cu capabilităţile de auditare securitate i5/OS ale serverului de director.

Capabilităţi activate şi suportate

Următoarea tabelă arată OID-uri pentru capabilităţile suportate şi activate. Puteţi folosi aceste OID-uri pentru a vedea dacă un anumit server suportă aceste caracteristici.

Tabela 10. OID-uri pentru capabilităţile suportate şi activate

Nume	OID	Descriere
Model de replicare îmbunătăţit	1.3.18.0.2.32.1	Identifică modelul de replicare introdus în IBM Directory Server v5.1, inclusiv replicarea subarborelui şi în cascadă.
Sumă de control a intrării	1.3.18.0.2.32.2	Indică faptul că acest server suportă caracteristicile ibm-entrychecksum şi ibm-entrychecksumop.
UUID intrare	1.3.18.0.2.32.3	Identifică faptul că acest server suportă atributul operaţional ibm-entryuuid.
ACL-uri cu filtru	1.3.18.0.2.32.4	Identifică faptul că acest server suportă modelul ACL cu filtru al IBM.
Politică de parolă	1.3.18.0.2.32.5	Identifică faptul că acest server suportă politicile de parolă.
Sortare după DN	1.3.18.0.2.32.6	Indică faptul că acest server suportă folosirea atributului ibm-slapdDn pentru a sorta după DN.
Delegaţie grup administrativ	1.3.18.0.2.32.8	Serverul suportă delegaţia de administrare a serverului pentru un grup de administratori care sunt specificaţi în back-end-ul configuraţiei.
Prevenire refuzare serviciu	1.3.18.0.2.32.9	Serverul suportă caracteristica de refuzare a serviciului. Sunt incluse timeout-urile de citire/scriere şi firele de execuţie de urgenţă.
Actualizări dinamice ale intrării şi subarborelui	1.3.18.0.2.32.15	Serverul suportă actualizări dinamice de configuraţie ale intrărilor şi subarborilor
Opţiune de dereferenţiere alias	1.3.18.0.2.32.10	Serverul suportă o opţiune de a nu dereferenţia alias-urile implicit
Limitele de căutare specifice grupului	1.3.18.0.2.32.17	Limitele de căutare specifice grupului suportă limite de căutare extinse pentru un grup de persoane
Urmărire dinamică	1.3.18.0.2.32.14	Serverul suportă o urmărire activă pentru server cu o operaţie extinsă LDAP
Capabilităţi TLS	1.3.18.0.2.32.28	Specifică faptul că serverul este într-adevăr capabil să efectueze TLS.
Auditare Demon Admin	1.3.18.0.2.32.11	Serverul suportă auditarea demonului admin.

Tabela 10. OID-uri pentru capabilităţile suportate şi activate (continuare)

Nume	OID	Descriere
Capabilităţi Kerberos	1.3.18.0.2.32.30	Specifică faptul că serverul este într-adevăr capabil să efectueze Kerberos.
Replicare fără blocare	1.3.18.0.2.32.29	Furnizorul nu reîncearcă întotdeauna să trimită o actualizare dacă consumatorul întoarce o eroare
Atribute operaţionale ibm-allMembers şi ibm-allGroups	1.3.18.0.2.32.31	Back-end-ul suportă căutare de grup statică, dinamică şi imbricată prin atributele operaţionale ibm-allMembers şi ibm-allGroups. Memmbrii unui grup static, dinamic şi/sau imbricat pot fi obţinuţi prin efectuarea unei căutări în atributul operaţional ibm-allMembers. Grupurile statice, dinamice şi/sau imbricate la care aparţine un membru DN pot fi obţinute printr-o căutare în atributul operaţional ibm-allGroups.
Atribute unice globale	1.3.18.0.2.32.16	Opţiunea serverului de a impune valori de atribut unice globale.
Monitorizare numărători operaţii	1.3.18.0.2.32.24	Serverul oferă o monitorizare a numărătorilor de operaţii pentru tipuri de operaţii începute şi terminate.
Monitorizare numărători de înregistrări	1.3.18.0.2.32.20	Serverul oferă monitorizarea numărătorilor de înregistrări pentru mesaje adăugate la server, CLI şi fişiere înregistrare de auditare.
Monitorizare numărători tipuri de conexiune	1.3.18.0.2.32.22	Serverul oferă monitorizarea numărătorilor tipurilor de conexiune pentru conexiunile SSL şi TLS.
Monitorizare informaţii lucrători activi	1.3.18.0.2.32.21	Serverul oferă monitorizarea informaţiilor pentru lucrătorii activi (cn=workers,cn=monitor).
Monitorizare informaţii conexiuni	1.3.18.0.2.32.23	Serverul oferă monitorizarea informaţiilor pentru conexiuni după adresa IP în loc de ID-ul conexiunii (cn=connections, cn=monitor).
Monitorizare informaţii urmărire	1.3.18.0.2.32.25	Serverul oferă monitorizarea informaţiilor pentru opţiunile de urmărire folosite în prezent.
Rezoluţia filtrului de căutare al memoriei cache a atributului	1.3.18.0.2.32.13	Serverul suportă punerea în cache a atributelor pentru rezoluţia filtrului de căutare.
Autorizare proxy	1.3.18.0.2.32.27	Serverul suportă Autorizarea proxy pentru un grup de utilizatori.
Suport opţiuni tag de limbă	1.3.6.1.4.1.4203.1.5.4	Indică faptul că serverul suportă taguri de limbă aşa cum sunt definite în RFC 2596.
Vârstă maximă intrări ChangeLog	1.3.18.0.2.32.19	Specifică faptul că serverul este capabil să reţină intrări changelog bazate pe vârstă.
Subarbore de replicare IBMpolicies	1.3.18.0.2.32.18	Serverul suportă replicarea subarborelui cn=IBMpolicies.
Căutare în subarbore pe bază nulă	1.3.18.0.2.32.26	Serverul permite căutarea în subarbore pe bază nulă, căutând în întregul DIT definit în server.
Cache de atribute autonom	1.3.18.0.2.32.50	Suportă punerea în cache autonomă
ibm-entrychecksumop	1.3.18.0.2.32.56	Funcţionalitatea 6.0 IDS ibm-entrychecksumop
Capabilitate server referrale filtrate	1.3.18.0.2.32.36	Utilizat pentru a indica suport pentru referrale filtrate îmbunătăţite. Aceasta înseamnă că valoarea filtrată va fi combinată cu filtrul original pe o cerere de căutare.
Capabilitate server grup admin global	1.3.18.0.2.32.38	Utilizat pentru a indica suportul pentru un grup admin global.
Auditarea capabilităţii de comparare	1.3.18.0.2.32.40	Utilizat pentru a indica suport pentru auditarea operaţiei de comparare.
Criptare parolă AES	1.3.18.0.2.32.39	Indică suport pentru criptare parolă AES.

Tabela 10. OID-uri pentru capabilităţile suportate şi activate (continuare)

Nume	OID	Descriere
Dimensiune intrare maximă	1.3.18.0.2.32.51	Utilizat pentru a rezolva conflictul de replicare. Bazat pe acest număr, un furnizor poate decide dacă o intrare ar trebui să fie adăugată la un server vizat din nou cu scopul de a rezolva un conflict de replicare.
Fişier istoric LostAndFound	1.3.18.0.2.32.52	Un fişier ce arhivează intrările înlocuite ca un rezultat al rezoluţiei de conflict de replicare.
Istoric gestiune	1.3.18.0.2.32.41	Indică suportul pentru operaţiile extinse de acces la fişierul istoric şi istoricului de auditare Tivoli Directory Server.
Replicare cu mai multe fire de execuţie	1.3.18.0.2.32.42	
Configuraţie server furnizori pentru replicare	1.3.18.0.2.32.43	
Subarbore replicare IBMPolicies	1.3.18.0.2.32.18	Suportă configuraţa replicării pentru cn=ibmpolicies şi cn=schema utilizând subarborele cn=ibmpolicies.

OID-uri pentru mecanismele ACL

Următoarea tabelă arată OID-urile pentru pentru mecanismele ACL.

Tabela 11. OID-uri pentru mecanismele ACL

Nume	OID	Descriere
Model ACL IBM SecureWay V3.2	1.3.18.0.2.26.2	Indică faptul că serverul LDAP suportă modelul ACL IBM SecureWay V3.2
Mecanismul ACL baza pe filtru al IBM	1.3.18.0.2.26.3	Indică faptul că serverul LDAP suportă filtrul IBM Directory Server v5.1 bazat pe ACL-uri
Suport ACL restricţionat de sistem	1.3.18.0.2.26.4	Indică faptul că serverul suportă sistemul şi clasa de acces restricţionat în intrările ACL.

Concepte înrudite

“Controalele şi operaţiile extinse” la pagina 91
Controalele şi operaţiile extinse permit extinderea protocolului LDAP fără a-l modifica.

Echivalenţa IBM Tivoli Directory Server

Directory Server este compatibil cu produsul IBM Tivoli Directory Server disponibil pe alte platforme. Următoarea tabelă listează versiunea echivalentă a produsului IBM Tivoli Directory Server corepunzător versiunilor particulare de Directory Server i5/OS. Tabela poate fi de ajutor când determinaţi dacă Directory Server i5/OS satisface cerinţele preliminare ale serverului de director pentru un produs particular.

Tabela 12. Echivalenţa IBM Tivoli Directory Server

Directory Server i5/OS	IBM Tivoli Directory Server
Versiunea 6 ediţia 1	IBM Tivoli Directory Server versiunea 6.0
Versiunea 5 ediţia 4	IBM Tivoli Directory Server versiunea 5.2
Versiunea 5 ediţia 3	IBM Directory Server versiunea 5.1
Versiunea 5 ediţia 2 (cu PTF SI08487)	IBM Directory Server versiunea 4.1
Versiunea 5 ediţia 2 (GA)	IBM SecureWay Directory Server versiunea 3.2.2

Configurarea implicită pentru Directory Server

Directory Server este instalat automat când instalaţi i5/OS. Această instalare include o configuraţie implicită.

Directory Server foloseşte configuraţia implicită când următoarele sunt toate adevărate:

- Administratorii nu au rulat vrăjitorul de configurare Directory Server sau nu au modificat setările de director cu paginile proprietăţi.
- Publicarea Directory Server nu este configurată.
- Directory Server nu poate găsi nici o informaţie LDAP DNS.

Dacă Directory Server foloseşte configuraţia implicită, atunci se întâmplă următoarele:

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

Operaţii înrudite

“Configurarea Directory Server” la pagina 99
Rulaţi vrăjitorul Configurare Directory Server pentru a personaliza setările Directory Server.

Depanarea Directory Server

Informaţii pentru a vă ajuta să rezolvaţi probleme. Includ sugestii pentru colectarea datelor de service şi rezolvarea problemelor specifice.

Din păcate, chiar şi serverele de încredere ca Serverul de director uneori au probleme. Când Directory Server are probleme, următoarele informaţii vă pot ajuta să găsiţi problema şi să o rezolvaţi.

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

Pentru informaţii suplimentare despre probleme obişnuite Server de director, vedeţi pagina de bază Server de director(www.iseries.ibm.com/ldap).

Serverul de director utilizează mai multe servere Limbaj interogare structurat (SQL)care sunt joburi QSQSRVR. Când apare o eroare SQL istoricul jobului QDIRSRV va conţine uzual, următorul mesaj:

```
SQL error -1 occurred
```

În aceste situaţii istoricul jobului QDIRSRV vă va referi la istoricele joburilor server SQL. Totuşi, în unele cazuri QDIRSRV ar putea să nu conţină acest mesaj şi această referinţă, chiar dacă un server SQL este cauza problemei. În aceste instanţe, vă va ajuta să ştiţi ce joburi server SQL a pornit serverul, astfel încât să ştiţi în ce istorice job QSQSRVR să căutaţi pentru erori suplimentare.

Când Directory Server porneşte normal, el generează mesaje similare cu următoarele:

```
                                                    Sistem:   SISTEMULMEU
 Job..:   QDIRSRV       Utilizator..:   QDIRSRV       Număr...:   174440

  >> APELAŢI PGM(QSYS/QGLDSVR)
     Jobul 057448/QUSER/QSQSRVR folosit pentru procesarea mod server SQL.
```

```
  Jobul 057340/QUSER/QSQSRVR folosit pentru procesarea mod server SQL.
  Jobul 057448/QUSER/QSQSRVR folosit pentru procesarea mod server SQL.
  Jobul 057166/QUSER/QSQSRVR folosit pentru procesarea mod server SQL.
  Jobul 057279/QUSER/QSQSRVR folosit pentru procesarea mod server SQL.
Jobul 057288/QUSER/QSQSRVR folosit pentru procesarea mod server SQL.
  Directory Server a pornit cu succes.
```

Mesajele se referă la joburile QSQSRVR care au fost pornite pentru pentru server. Numărul de mesaje ar putea fi diferit pe serverul dumneavoastră, în funcţie de configuraţia şi de numărul de job-uri QSQSRVR necesare pentru a realiza pornirea serverului.

Pe pagina de proprietăţi servere dde director **Bază de date/Sufixe** înNavigator System i specificaţi numărul total de servere SQL pe care Serverele de director le utilizează pentru operaţiile de director după pornirea serverului. Sunt pornite pentru replicare servere SQL adiţionale.

Informaţii înrudite

Pagina acasă Directory Server

Monitorizarea erorilor şi a accesului cu istoricul de job Directory Server

Când apare o eroare în Directory Server şi doriţi detalii suplimentare, o altă acţiune de luat este vizualizarea istoricului de job QDIRSRV.

Vizualizarea istoricului de job pentru Directory Server vă poate alerta la erori şi vă poate ajuta să monitorizaţi accesul serverului. Istoricul jobului conţine:

- Mesajele despre operaţia de server şi orice problemă din interiorul serverului precum jobul serverului SQL sau eşuările de replicare.
- Mesajele înrudite cu securitatea care reflectă operaţiile după clienţi precum parole greşite.
- Mesajele care redau detalii despre erorile client precum atribute necesare lipsă.

Aţi putea dori să nu înregistraţi erorile client, doar dacă nu depanaţi problemele client. Puteţi controla logarea erorile clientului pe fişa de proprietăţi **General** a Serverului de director Navigator System i.

Vizualizarea istoricului de joburi QDIRSRV dacă serverul este pornit

Dacă serverul dumneavoastră este pornit, urmaţi aceşti paşi pentru a vizualiza istoricul job-ului QDIRSRV:

1. În Navigator System i, expandaţi **Reţea**.
2. Expandaţi **Servere**.
3. faceţi clic pe **TCP/IP**.
4. Faceţi clic dreapta pe **IBM Directory Server** şi selectaţi **Joburi server**.
5. Din meniul **Fişier**, alegeţi **Istoric job**.

Vizualizarea istoricului de joburi QDIRSRV dacă serverul este oprit

Dacă serverul dumneavoastră este oprit, urmaţi aceşti paşi pentru a vizualiza juranul job QDIRSRV:

1. În Navigator System i, expandaţi **Operaţii de bază**.
2. Faceţi clic pe **Ieşire imprimantă**.
3. QDIRSRV apare în coloana **Utilizator** a panoului din dreapta Navigator System i. Pentru a vedea istoricul job-ului, faceţi clic dreapta pe **Qpjoblog** în stânga QDIRSRV din aceeaşi linie.

   Notă: Navigator System ipoate fi configurat pentru a afişa foar fişierele 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: Serverul de director utilizează alte resurse de sistem pentru a realiza unele taskuri. Dacă apare vreo eroare cu una din aceste resurse, istoricul jobului va indica unde să se meargă pentru informaţii. În unele cazuri Serverul

de director ar putea să nu fie capabil să determine unde să caute. În aceste cazuri, căutaţi în jurnalele 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

Pentru erori ce pot fi reproduse, puteţi folosi comanda TRCTCPAPP APP(*DIRSRV) (Trace TCP/IP Application - Urmărire aplicaţie TCP/IP) pentru a rula o urmărire de erori.

Serverul dumneavoastră furnizează o urmă de comunicaţie pentru a colecta date p o linie de comunicaţii cum ar fi reţeaua locală (LAN) sau o interfaţă largă de reţea (WAN). Utilizatorul obişnuit s-ar putea să nu înţeleagă tot conţinutul datelor de urmărire. Totuşi, puteţi folosi intrările de urmărire pentru a determina dacă într-adevăr a avut loc un schimb de date între două puncte.

Comanda Urmărire aplicaţie TCP/IP (TRCTCPAPP) poate fi utilizată pe Serverul de director pentru a ajuta în găsirea problemelor cu clienţii sau cu aplicaţiile.

Puteţi utiliza comanda TRCTCPAPP pentru a urmări o instanţă server activă. De exemplu:

TRCTCPAPP APP(*DIRSRV) INSTANŢĂ(QUSRDIR)

Puteţi de asemenea porni urmărirea utilizând comanda STRTCPSVR şi adăugând '-h dft' instance startup values. Aceasta va porni urmărirea în instanţa serverului şi va porni instanţa serverului. De exemplu:

STRTCPSVR SERVER(*DIRSRV) INSTANŢĂ(QUSRDIR '-h dft')

Pentru a opri urmărirea utilizaţi următoarea comandă:

TRCTCPAPP APP(*DIRSRV) SET(*OFF)

Concepte înrudite

Urmărirea comunicaţiilor

Informaţii înrudite

TRCTCPAPP (Trace TCP/IP Application - Urmărire aplicaţie TCP/IP)

Utilizarea opţiunii LDAP_OPT_DEBUG pentru a depista erori

Urmărirea problemelor cu clienţii care folosesc API-uri C LDAP.

Puteţi folosi opţiunea LDAP_OPT_DEBUG din API-ul **ldap_set_option()** pentru a urmări probleme cu clienţii care folosesc API-uri C LDAP. Opţiunea de depanare are multe setări nivele de depanare care le puteţi folosi penru a vă ajuta în probleme de depanare cu aceste aplicaţii.

Următorul este un exemplu de activare a opţiunii de depanare urmă client.

```
int debugvalue= LDAP_DEBUG_TRACE | LDAP_DEBUG_PACKETS;
ldap_set_option(  1d, LDAP_OPT_DEBUG, &debugvalue);
```

O cale alternativă de setare a nivelului de depanare este de a configura valoarea numerică a variabilei mediu LDAP_DEBUG, pentru job-ul în care aplicaţia client rulează, la aceeaşi valoare numerică la care debugvalue ar fi dacă este folosit API-ul **ldap_set_option()** .

Un exemplu de activare a urmăririi client folosind variabila mediu LDAP_DEBUG este următorul:

```
ADDENVVAR ENVVAR(LDAP_DEBUG) VALUE(0x0003)
```

După rularea clientului ce produce problema pe care o aveţi, tastaţi următoarele pe linia de comandă:

```
DMPUSRTRC  ClientJobNumber
```

unde ClientJobNumber este numărul jobului client.

Pentru a afişa această informaţie interactiv, tastaţi următoarele la linia de comandă:

```
DSPPFM QAP0ZDMP QP0Znnnnnn
```

unde QAP0ZDMP conţine un zero şi nnnnnn este un număr de job.

Pentru a salva aceste informaţii pentru a le trimite la service, urmaţi aceşti paşi:

1. Creaţi un fişier SAVF folosind comanda de creare SAVF (CRTSAVF).
2. Tastaţi următoarele la linia de comandă.

   ```
   SAVOBJ OBJ(QAP0ZDMP) LIB(QTEMP) DEV(*SAVF) SAVF(xxx)
   ```

   unde QAP0ZDMP conţine un zero şi *xxx* este numel pe care l-aţi specificat pentru fişierul SAVF.

Concepte înrudite

API-urile LDAP (Lightweight Directory Access Protocol)
Vedeţi API-urile LDAP (Lightweight Directory Access Protocol) pentru informaţii suplimentare despre API Directory Server

Informaţii înrudite

ADDENVVAR (Add Environment Variable - Adăugare variabilă mediu)

DMPUSRTRC (Dump User Trace - Dump urmărire utilizator)

DSPPFM (Display Physical File Member - Afişare membru fişier fizic)

CRTSAVF (Create Save File - Creare fişier de salvare)

SAVOBJ (Save Object - Salvare obiect)

Identificatorii de mesaje GLEnnnn

Aceste informaşii listează identificatorii de mesaj GLE şi descrierile lor.

Identificatorii de mesaje iau forma GLEnnnn, unde nnnn este numărul de eroare zecimal. De exemplu, o descriere pentru codul retur 50 (0x32) poate fi vizualizată introducând următoarea comandă:

```
| DSPMSGD RANGE(GLE0050) MSGF(QGLDMSG)
```

Acesta v-ar oferi descrierea pentru LDAP_INSUFFICIENT_ACCESS.

Următoarea tabelă afişează identificatorii de mesaje GLE şi descrierile lor.

Identificator de mesaj	Descriere
GLE0000	Cererea a fost reuşită (LDAP_SUCCESS)
GLE0001	Eroare operaţii (LDAP_OPERATIONS_ERROR)
GLE0002	Eroare protocol (LDAP_PROTOCOL_ERROR)
GLE0003	Limită de timp depăşită (LDAP_TIMELIMIT_EXCEEDED)
GLE0004	Limită de dimensiune depăşită (LDAP_SIZELIMIT_EXCEEDED)
GLE0005	Un tip şi o valoare comparate nu există în intrare (LDAP_COMPARE_FALSE)
GLE0006	Un tip şi o valoare comparate există în intrare (LDAP_COMPARE_TRUE)
GLE0007	Metoda de autentificare nu este suportată (LDAP_AUTH_METHOD_NOT_SUPPORTED)
GLE0008	Este necesară o autentificare solidă (LDAP_STRONG_AUTH_REQUIRED)

Identificator de mesaj	Descriere
GLE0009	Rezultatele parţiale şi referinţa primite (LDAP_PARTIAL_RESULTS)
GLE0010	Referral întors (LDAP_REFERRAL)
GLE0011	Limită administrativă depăşită (LDAP_ADMIN_LIMIT_EXCEEDED)
GLE0012	Extensia critică nu este suportată (LDAP_UNAVAILABLE_CRITICAL_EXTENSION)
GLE0013	Confidenţialitatea este necesară (LDAP_CONFIDENTIALITY_REQUIRED)
GLE0014	Legare SASL în curs (LDAP_SASLBIND_IN_PROGRESS)
GLE0016	Nu există un asemenea atribut (LDAP_NO_SUCH_ATTRIBUTE)
GLE0017	Tip de atribut nedefinit (LDAP_UNDEFINED_TYPE)
GLE0018	Potrivire necorespunzătoare (LDAP_INAPPROPRIATE_MATCHING)
GLE0019	Violare constrângere (LDAP_CONSTRAINT_VIOLATION)
GLE0020	Tipul de valoare există (LDAP_TYPE_OR_VALUE_EXISTS)
GLE0021	Sintaxă nevalidă (LDAP_INVALID_SYNTAX)
GLE0032	Nu există un asemenea obiect (LDAP_NO_SUCH_OBJECT)
GLE0033	Problemă de alias (LDAP_ALIAS_PROBLEM)
GLE0034	Sintaxă DN nevalidă (LDAP_INVALID_DN_SYNTAX)
GLE0035	Obiectul este o frunză (LDAP_IS_LEAF)
GLE0036	Problemă de dereferenţiere alias (LDAP_ALIAS_DEREF_PROBLEM)
GLE0048	Autentificare necorespunzătoare (LDAP_INAPPROPRIATE_AUTH)
GLE0049	Acreditări nevalide (LDAP_INVALID_CREDENTIALS)
GLE0050	Acces insuficient (LDAP_INSUFFICIENT_ACCESS)
GLE0051	Serverul de director este ocupat (LDAP_BUSY)
GLE0052	Agentul service de director nu este disponibil (LDAP_UNAVAILABLE)
GLE0053	Serverul de director nu este dispus să realizeze operaţia cerută (LDAP_UNWILLING_TO_PERFORM)
GLE0054	Buclă detectată (LDAP_LOOP_DETECT)
LE0064	Violare numire (LDAP_NAMING_VIOLATION)
LE0065	Violare clasă obiect (LDAP_OBJECT_CLASS_VIOLATION)
GLE0066	Operaţia nu este permisă decât pe o frunză (LDAP_NOT_ALLOWED_ON_NONLEAF)
GLE0067	Operaţai nu este permisă pe un nume distinctiv relativ (LDAP_NOT_ALLOWED_ON_RDN)
GLE0068	Deja există (LDAP_ALREADY_EXISTS)
GLE0069	Clasa obiect nu se poate modifica (LDAP_NO_OBJECT_CLASS_MODS)
GLE0070	Rezultatele sunt prea mari (LDAP_RESULTS_TOO_LARGE)

Identificator de mesaj	Descriere
GLE0071	Afectează mai multe servere. (LDAP_AFFECTS_MULTIPLE_DSAS)
GLE0080	Eroare necunoscută (LDAP_OTHER)
GLE0081	Nu se poate contacta serverul LDAP (LDAP_SERVER_DOWN)
GLE0082	Eroare locală (LDAP_LOCAL_ERROR)
GLE0083	Eroare de codare (LDAP_ENCODING_ERROR)
GLE0084	Eroare de decodare (LDAP_DECODING_ERROR)
GLE0085	Expirare timp cerere (LDAP_TIMEOUT)
GLE0086	Metodă de autentificare necunoscută (LDAP_AUTH_UNKNOWN)
GLE0087	Filtru de căutare necorespunzător (LDAP_FILTER_ERROR)
GLE0088	Operaţie anulată de utilizator (LDAP_USER_CANCELLED)
GLE0089	Parametru necorespunzător pentru o rutină LDAP (LDAP_PARAM_ERROR)
GLE0090	Memorie insuficientă (LDAP_NO_MEMORY)
GLE0091	Eroare conexiune (LDAP_CONNECT_ERROR)
GLE0092	Caracteristica nu este suportată (LDAP_NOT_SUPPORTED)
GLE0093	Controlul nu a fost găsit (LDAP_CONTROL_NOT_FOUND)
GLE0094	Nu au fost întoarse rezultate (LDAP_NO_RESULTS_RETURNED)
GLE0095	Mai multe rezultate de întors (LDAP_MORE_RESULTS_TO_RETURN)
GLE0096	Nu este un URL LDAP (LDAP_URL_ERR_NOTLDAP)
GLE0097	URL-ul nu are un DN (LDAP_URL_ERR_NODN)
GLE0098	Valoarea scop a URL-ului nu este validă (LDAP_URL_ERR_BADSCOPE)
GLE0099	Eroare de alocare memorie (LDAP_URL_ERR_MEM)
GLE0100	Buclă client (LDAP_CLIENT_LOOP)
GLE0101	Limită referral depăşită (LDAP_REFERRAL_LIMIT_EXCEEDED)
GLE0112	Mediu SSL deja iniţializat (LDAP_SSL_ALREADY_INITIALIZED)
GLE0113	Apelul de iniţializare eşuat (LDAP_SSL_INITIALIZE_FAILED)
GLE0114	Mediu SSL neiniţializat (LDAP_SSL_CLIENT_INIT_NOT_CALLED)
GLE0115	Valoare ilegală specificată pentru parametrul SSL (LDAP_SSL_PARAM_ERROR)
GLE0116	Eşuare negociere conexiune sigură (LDAP_SSL_HANDSHAKE_FAILED)
GLE0118	Biblioteca SSL nu poate fi localizată (LDAP_SSL_NOT_AVAILABLE)
GLE0128	Nu a fost găsit nici un proprietar explicit (LDAP_NO_EXPLICIT_OWNER)

Identificator de mesaj	Descriere
GLE0129	Nu s-a putut obţine blocarea asupra resursei necesare (LDAP_NO_LOCK)
GLE0133	Nu s-au găsit servere LDAP în DNS (LDAP_DNS_NO_SERVERS)
GLE0134	Rezultate DNS trunchiate (LDAP_DNS_TRUNCATED)
GLE0135	Datele DNS nu au putut fi analizate (LDAP_DNS_INVALID_DATA)
GLE0136	Domeniul sistemului sau numeserver nu pot fi rezolvate (LDAP_DNS_RESOLVE_ERROR)
GLE0137	Eroare în fişierul de configurare al DNS (LDAP_DNS_CONF_FILE_ERROR)
GLE0160	Depăşire buffer ieşire (LDAP_XLATE_E2BIG)
GLE0161	Buffer de intrare trunchiat (LDAP_XLATE_EINVAL)
GLE0162	Caracter de intrare neutilizabil (LDAP_XLATE_EILSEQ)
GLE0163	Caracterul nu este asociat cu un punct setarecod (LDAP_XLATE_NO_ENTRY)

Informaţii înrudite

DSPMSGD (Display Message Description - Afişare descriere mesaj)

Erori comune de client LDAP

Aceste informaţii descriu erorile clienţi LDAP obişnuite.

Cunoaşterea cauzelor erorile clientului LDAP vă poate ajuta să rezolvaţi problemele serverului dumneavoastră. Pentru o listă completă a condiţiilor de eroare LDAP, vedeţi “API-uri Server de director” în colecţia de subiectProgramare.

Mesajele de eroare client au următorul format:

```
[Operaţie LDAP eşuată ]:[Condiţii de eroare API client LDAP ]
```

Notă: Explicarea acestor erori presupune că clientul comunică cu un server LDAP pe i5/OS. Un client ce comunică cu un server pe o platformă diferită poate avea erori similare, dar cauzele şi rezolvările vor fi diferite.

Concepte înrudite

API-urile LDAP (Lightweight Directory Access Protocol)
Vedeţi API-urile LDAP (Lightweight Directory Access Protocol) pentru informaţii suplimentare despre API Directory Server

ldap_search: Depăşirea limitei de timp

Această eroare survine atunci când comanda ldapsearch se realizează în mod lent.

Pentru a corecta această eroare, puteţi face una din următoarele:

- Creşteţi limita de timp de căutare pentru Directory Server.
- Reduceţi activitatea pe sistemul dumneavoastră. Puteţi de asemenea reduce numărul de joburi client LDAP active care rulează.

Operaţii înrudite

“Ajustarea setărilor de căutare” la pagina 123
Folosiţi aceste informaţii pentru a controla capabilităţiile de căutare ale utilizatorului.

[Operaţie LDAP eşuată]: Eroare operaţii

Mai multe lucruri pot genera această eroare.

Pentru a obţine informaţii despre cauza acestei erori pentru o instanţă particulară, priviţi la înregistrările în istoric a jobului QDIRSRV şi la înregistrările în istoric a joburilor serverului SQL (Structured Query Language).

Concepte înrudite

"Depanarea Directory Server" la pagina 296
Informaţii pentru a vă ajuta să rezolvaţi probleme. Includ sugestii pentru colectarea datelor de service şi rezolvarea problemelor specifice.

Operaţii înrudite

"Monitorizarea erorilor şi a accesului cu istoricul de job Directory Server" la pagina 297
Când apare o eroare în Directory Server şi doriţi detalii suplimentare, o altă acţiune de luat este vizualizarea istoricului de job QDIRSRV.

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 de fapt DN-ul administratorului ar putea fi asemănător cu cn=Administrator.

Pentru detalii despre eroare, priviţi la istoricul jobului QDIRSRV.

Operaţii înrudite

"Monitorizarea erorilor şi a accesului cu istoricul de job Directory Server" la pagina 297
Când apare o eroare în Directory Server şi doriţi detalii suplimentare, o altă acţiune de luat este vizualizarea istoricului de job QDIRSRV.

ldap_bind: Autentificare necorespunzătoare

Serverul întoarce acreditări invalide când parola sau legătura DN sunt incorecte.

Server întoarce Autentificare necorespunzătoare când clientul încearcă să asocieze în unul din felurile următoare:

- O intrare ce nu are un atribut de parolă utilizator.
- O intrare ce reprezintă un utilizator i5/OS, ce are un atribut UID şi nu un atribut de parolă utilizator. Aceasta cauzează efectuarea unei comparaţii între parola specificată şi parola utilizatorului i5/OS, ce nu se potrivesc.
- O intrare reprezintă un utilizator proiectat şi o metodă de legare alta decât simplă a fost cerută.

Această eroare eset de obicei generată când clientul încearcă să asocieze cu o parolă care nu este validă. Pentru a obţine detalii despre eroare, priviţi la istoricul jobului QDIRSRV.

Operaţii înrudite

"Monitorizarea erorilor şi a accesului cu istoricul de job Directory Server" la pagina 297
Când apare o eroare în Directory Server şi doriţi detalii suplimentare, o altă acţiune de luat este vizualizarea istoricului de job QDIRSRV.

[Failing LDAP operation]: Acces insuficient

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 informaţii despre eroare, priviţi la istoricul jobului QDIRSRV.

Operaţii înrudite

"Monitorizarea erorilor şi a accesului cu istoricul de job Directory Server" la pagina 297
Când apare o eroare în Directory Server şi doriţi detalii suplimentare, o altă acţiune de luat este vizualizarea istoricului de job QDIRSRV.

[Failing LDAP operation]: Nu poate fi contactat serverul LDAP

Cele mai obişnuite cauze ale acestei erori includ o cerere înainte ca serverul să fie pregătit sau un număr de port invalid.

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 informaţii despre eroare, priviţi la istoricul jobului QDIRSRV. Dacă Directory Server porneşte cu succes, mesajul că Directory Server a pornit cu succes va fi în istoricul de joburi QDIRSRV.

Operaţii înrudite

"Monitorizarea erorilor şi a accesului cu istoricul de job Directory Server" la pagina 297
Când apare o eroare în Directory Server şi doriţi detalii suplimentare, o altă acţiune de luat este vizualizarea istoricului de job QDIRSRV.

[Operaţie LDAP eşuată]: Nu s-a putut realiza conexiunea 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 Gestionarea certificatelor respinge încercările clienţilor de a se conecta la server. Folosiţi Managerul de certificate digitale pentru a vă asigura că ceritficatele dvs sunt setate corespunzător şi apoi reporniţi serverul şi reîncercaţi conectarea.
- Utilizatorul ar putea să nu aibă acces de citire la memorarea certificatului *SYSTEM (implicit /QIBM/userdata/ICSS/Cert/Server/default.kdb).

Pentru i5/OS aplicaţii C, informaţii de eroare SSL adiţionale sunt disponibile. Vedeţi "API-urile serverului de director" în subiectul Programare pentru detalii.

Concepte înrudite

API-urile LDAP (Lightweight Directory Access Protocol)
Vedeţi API-urile LDAP (Lightweight Directory Access Protocol) pentru informaţii suplimentare despre API Directory Server

Erorile privind poltica de parolă

Activarea unei politici de parolă poate căteodată să determine erori neaşteptate.

Când anumite politici de parolă sunt activate, ele pot cauza eşăuri care pot să nu fie evidente. Revedeţi următoarele pentru ajutor în depanarea erorilor legate politica de parolă.

Legarea cu parola corespunzătoare eşuează cu ″acreditări nevalide″: Parola ar putea să fi expirat sau contul ar putea fi blocat. Uitaţi-vă la atributele pwdchangedtime şi pwdaccountlockedtime ale intrării.

Cererile eşuează cu ″nedispus să realizeze″ după o legare reuşită: Parola s-ar putea să fi fost resetată, caz în care o legare va fi reuşită, dar singura operaţie permisă de server este ca utilizatorul să îşi poată schimba parola. Alte cereri eşuează cu ″nedispus să realizeze″ până la schimbarea parolei.

Autentificarea folosind o parolă care a fost resetată se comportă neaşteptat: Când parola a fost resetată, cererea de legare va reuşi, aşa cum a fost descris mai sus. Aceasta înseamnă că un utilizator ar putea să se autentifice pe timp nedefinit folosind o parolă de resetare.

Referinţe înrudite

"Sugestii privind politica de parolă" la pagina 79
Politica de parolă nu se potcomporta întotdeauna cum se aşteaptă.

Depanarea API-ului QGLDCPYVL

Utilizarea facilităţii Urmărire utilizator poate explica eroarea sau poate determina dacă service-ul este necesar.

Acest API foloseşte facilitatea Urmărire utilizator pentru a-şi înregistra operaţia. Dacă apar erori sau sunt suspectate, o urmărire ar putea explica eroarea aparentă sau dacă este necesar service-ul. O urmărire ar putea fi obţinută după cum urmează:

```
STRTRC SSNID(COPYVLDL) JOBTRCTYPE(*TRCTYPE) TRCTYPE((*DIRSRV *INFO))
CALL QGLDCPYVL PARM(...)
ENDTRC SSNID(COPYVLDL) DTALIB(QTEMP) PRTTRC(*YES)
```

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 următoarea la promptul de comandă.

   ```
   SAVOBJ OBJ(QAP0ZDMP) LIB(QTEMP) DEV(*SAVF) SAVF(xxx)
   ```

   unde QAP0ZDMP conţine un zero şi *xxx* este numel pe care l-aţi specificat pentru fişierul SAVF.

   Concepte înrudite

   API-urile LDAP (Lightweight Directory Access Protocol)
   Vedeţi API-urile LDAP (Lightweight Directory Access Protocol) pentru informaţii suplimentare despre API Directory Server

   Informaţii înrudite

   STRTRC (Start Trace - Începere urmărire)

   CRTSAVF (Create Save File - Creare fişier de salvare)

   SAVOBJ (Save Object - Salvare obiect)

Informaţii înrudite

Listate mai jos sunt publicaţiile IBM Cărţi roşii (în format PDF), site-uri web şi subiecte Centrul de informare care se înrudesc cu subiectul Server de director. Puteţi vizualiza sau tipări oricare PDF.

Publicaţiile IBM Cărţi roşii (www.redbooks.ibm.com)

- Understanding LDAP, SG24-4986 .
- Utilizarea LDAP Integrarea directorului: O privire la IBM SecureWay Director, Director activ şi Domino, SG24-6163 .
- Implementarea şi utilizarea practică a LDAP pe iSeries Server, SG24-6193 .

Situri web

- Serverul de director IBM pentru iSeries site-ul Web (www.ibm.com/servers/eserver/iseries/ldap)
- Site-ul tutorial web al JNDI-ului (Naming and Directory Interface) Java (java.sun.com/products/jndi/tutorial/)

Alte informaţii

“API-uri LDAP (Lightweight Directory Access Protocol) ” în categoria Programare.

Anexa. Observaţii

Aceste informaţii au fost elaborate pentru produse şi servicii oferite în S.U.A.

Este posibil ca IBM să nu ofere în alte ţări produsele, serviciile sau caracteristicile discutate în acest document. Luaţi legătura cu reprezentantul IBM local pentru informaţii despre produsele şi serviciile disponibile în zona dumneavoastră. Referirea la un produs, program sau serviciu IBM nu înseamnă că se afirmă sau că se sugerează faptul că poate fi folosit numai acel produs, program sau serviciu IBM. Poate fi folosit în loc orice produs, program sau serviciu care este echivalent din punct de vedere funcţional şi care nu încalcă dreptul de proprietate intelectuală al IBM. Însă evaluarea şi verificarea modului în care funcţionează un produs, program sau serviciu non-IBM ţine de responsabilitatea utilizatorului.

IBM poate avea brevete sau aplicaţii în curs de brevetare care să acopere subiectele descrise în acest document. Oferirea acestui document nu vă conferă nici o licenţă cu privire la aceste brevete. Puteţi trimite întrebări cu privire la licenţe, în scris, la:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Pentru întrebări privind licenţa pentru informaţiile DBCS (double-byte character set), contactaţi departamentul IBM de Proprietate intelectuală din ţara dumneavoastră sau trimiteţi întrebările în scris la:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

Următorul paragraf nu se aplică în cazul Marii Britanii sau al altor ţări unde asemenea prevederi nu sunt în concordanţă cu legile locale: INTERNATIONAL BUSINESS MACHINES CORPORATION OFERĂ ACEASTĂ PUBLICAŢIE “CA ATARE”, FĂRĂ NICI UN FEL DE GARANŢIE, EXPRESĂ SAU IMPLICITĂ, INCLUSIV, DAR NELIMITÂNDU-SE LA ELE, GARANŢIILE IMPLICITE DE NEÎNCĂLCARE A UNOR DREPTURI SAU NORME, DE VANDABILITATE SAU DE POTRIVIRE PENTRU UN ANUMIT SCOP. Unele state nu permit declinarea responsabilităţii pentru garanţiile exprese sau implicite în anumite tranzacţii şi de aceea este posibil ca aceste clauze să nu fie valabile în cazul dumneavoastră.

Aceste informaţii pot include inexactităţi tehnice sau erori tipografice. Se efectuează modificări periodice la informaţiile incluse aici; aceste modificări vor fi încorporate în noi ediţii ale publicaţiei. IBM poate aduce îmbunătăţiri şi/sau modificări produsului (produselor) şi/sau programului (programelor) descrise în această publicaţie în orice moment, fără notificare.

Referirile din aceste informaţii la adrese de situri Web non-IBM sunt făcute numai pentru a vă ajuta, fără ca prezenţa lor să însemne un gir acordat acestor situri Web. Materialele de pe siturile Web respective nu fac parte din materialele pentru acest produs IBM, iar utilizarea acestor situri Web se face pe propriul risc.

IBM poate utiliza sau distribui oricare dintre informaţiile pe care le furnizaţi, în orice mod considerat adecvat, fără ca aceasta să implice vreo obligaţie pentru dumneavoastră.

Posesorii de licenţe pentru acest program care doresc să aibă informaţii despre el în scopul de a permite: (I) schimbul de informaţii între programe create independent şi alte programe (inclusiv acesta) şi (II) utilizarea mutuală a informaţiilor care au fost schimbate, vor contacta:

IBM Corporation

© Copyright IBM Corp. 1998, 2008

Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Aceste informaţii pot fi disponibile cu respectarea termenilor şi condiţiilor corespunzătoare, iar în unele cazuri cu plata unei taxe.

Programul licenţiat la care se referă aceste informaţii şi toate materialele licenţiate disponibile pentru el sunt furnizate de IBM în conformitate cu termenii din IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code sau din alt acord echivalent încheiat între noi.

Toate datele de performanţă din acest document au fost determinate într-un mediu controlat. De aceea, rezultatele obţinute în alte medii de funcţionare pot fi diferite. Unele măsurători s-ar putea să fi fost făcute pe sisteme la nivel de dezvoltare şi nu există nici o garanţie că aceste măsurători vor fi identice pe sistemele disponibile pe piaţă. Mai mult de atât, unele măsurători s-ar putea să fi fost estimate prin extrapolare. Rezultatele reale pot fi diferite. Utilizatorii acestui document trebuie să verifice datele aplicabile pentru mediul lor specific.

Informaţiile privind produsele non-IBM au fost obţinute de la furnizorii acestor produse, din anunţurile lor publicate sau din alte surse disponibile publicului. IBM nu a testat produsele respective şi nu poate confirma acurateţea performanţei, compatibilitatea sau orice alte pretenţii legate de produsele non-IBM. Întrebări legate de capacităţile produselor non-IBM le veţi adresa furnizorilor acestor produse.

Toate declaraţiile privind direcţiile de viitor şi intenţiile IBM pot fi schimbate sau retractate fără notificare prealabilă şi reprezintă doar scopuri şi obiective.

Toate preţurile IBM prezentate sunt preţurile cu amănuntul sugerate de IBM, sunt actuale şi pot fi modificate fără notificare. Preţurile dealer-ului pot fi diferite.

Aceste informaţii sunt doar pentru planificare. Informaţiile prezentate aici se pot modifica înainte ca produsele descrise să devină disponibile pe piaţă.

Aceste informaţii conţin exemple de date şi rapoarte folosite în operaţiile comerciale de zi cu zi. Pentru a fi cât mai complete, exemplele includ nume de persoane, de companii, de mărci şi de produse. Toate aceste nume sunt fictive şi orice asemănare cu nume sau adrese folosite de o întreprindere reală este pură coincidenţă.

LICENŢĂ COPYRIGHT:

Aceste informaţii conţin exemple de programe de aplicaţii în limbaje sursă, care ilustrează tehnici de programare pe diferite platforme de operare. Puteţi copia, modifica şi distribui aceste exemple de programe sub orice formă fără ca IBM să pretindă vreo plată, când o faceţi în scopul dezvoltării, folosirii, promovării şi distribuirii programelor de aplicaţii conform cu interfaţa de programare a aplicaţiilor pentru platforma de operare pentru care au fost scrise exemplele de program. Aceste exemple nu au fost testate amănunţit în toate condiţiile. De aceea, IBM nu poate garanta sau sugera fiabilitatea, suportul pentru service sau funcţionarea acestor programe.

Dacă vizualizaţi aceste informaţii în format electronic, este posibil să nu apară fotografiile şi ilustraţiile color.

Mărci comerciale

Următorii termeni sunt mărci comerciale deţinute de International Business Machines Corporation în Statele Unite, în alte ţări sau ambele:

Application System/400
AS/400
DB2
Domino

e(logo)server
eServer
i5/OS
IBM
iSeries
Java
Lotus
Lotus Notes
Operating System/400
OS/400
Redbooks
RDN
SecureWay
System i
Tivoli
UNIX
WebSphere
XT
400

Adobe, logo-ul Adobe, PostScript şi logo-ul PostScript sunt mărci comerciale înregistrate sau mărci comerciale deţinute de Adobe Systems Incorporated în Statele Unite şi/sau alte ţări.

Microsoft, Windows, Windows NT şi logo-ul Windows sunt mărci comerciale deţinute de Microsoft Corporation în Statele Unite, în alte ţări sau ambele.

Java şi toate mărcile comerciale bazate pe Java sunt mărci comerciale deţinute de Sun Microsystems, Inc. în Statele Unite, în alte ţări sau ambele.

UNIX este o marcă comercială înregistrată deţinută de Open Group în Statele Unite şi în alte ţări.

Alte nume de companii, produse sau servicii pot fi mărci comerciale sau mărci de serviciu ale altora.

Termenii şi condiţiile

Permisiunile pentru utilizarea acestor publicaţii sunt acordate în conformitate cu următorii termeni şi condiţii.

Utilizare personală: Puteţi reproduce aceste publicaţii pentru utilizarea personală, necomercială, cu condiţia ca toate anunţurile de proprietate să fie păstrate. Nu puteţi distribui, afişa sau realiza obiecte derivate din aceste publicaţii sau dintr-o porţiune a lor fără consimţământul explicit al IBM.

Utilizare comercială: Puteţi reproduce, distribui şi afişa aceste publicaţii doar în cadrul întreprinderii dumneavoastră, cu condiţia ca toate anunţurile de proprietate să fie păstrate. Nu puteţi să realizaţi lucrări derivate din aceste informaţii, nici să reproduceţi, să distribuiţi sau să afişaţi aceste informaţii sau o porţiune a lor în afara întreprinderii dumneavoastră fără consimţământul explicit al IBM.

Cu excepţia a ceea ce este acordat explicit prin această permisiune, nu sunt acordate alte permisiuni, licenţe sau drepturi, explicit sau implicit, pentru Publicaţii sau alte informaţii, date, software sau altă proprietate intelectuală conţină în acestea.

IBM îşi rezervă dreptul de a retrage permisiunile acordate aici oricând consideră că folosirea publicaţiilor este în detrimentul intereselor sale sau când personalul IBM constată că instrucţiunile de mai sus nu sunt urmate corespunzător.

Nu puteţi descărca, exporta sau reexporta aceste informaţii decât în deplină conformitate cu legile şi regulamentele aplicabile, inclusiv toate legile şi regulamentele de export ale Statelor Unite.

IBM NU ACORDĂ NICI O GARANŢIE PENTRU CONŢINUTUL ACESTOR PUBLICAŢII. ACESTE PUBLICAŢII SUNT FURNIZATE ″CA ATARE″, FĂRĂ NICI UN FEL DE GARANŢIE, EXPLICITĂ SAU IMPLICITĂ, INCLUZÂND, DAR FĂRĂ A SE LIMITA LA ELE, GARANŢIILE IMPLICITE DE VANDABILITATE, DE NEÎNCĂLCARE A UNOR DREPTURI SAU NORME ŞI DE POTRIVIRE PENTRU UN ANUMIT SCOP.

Tipărit în S.U.A.