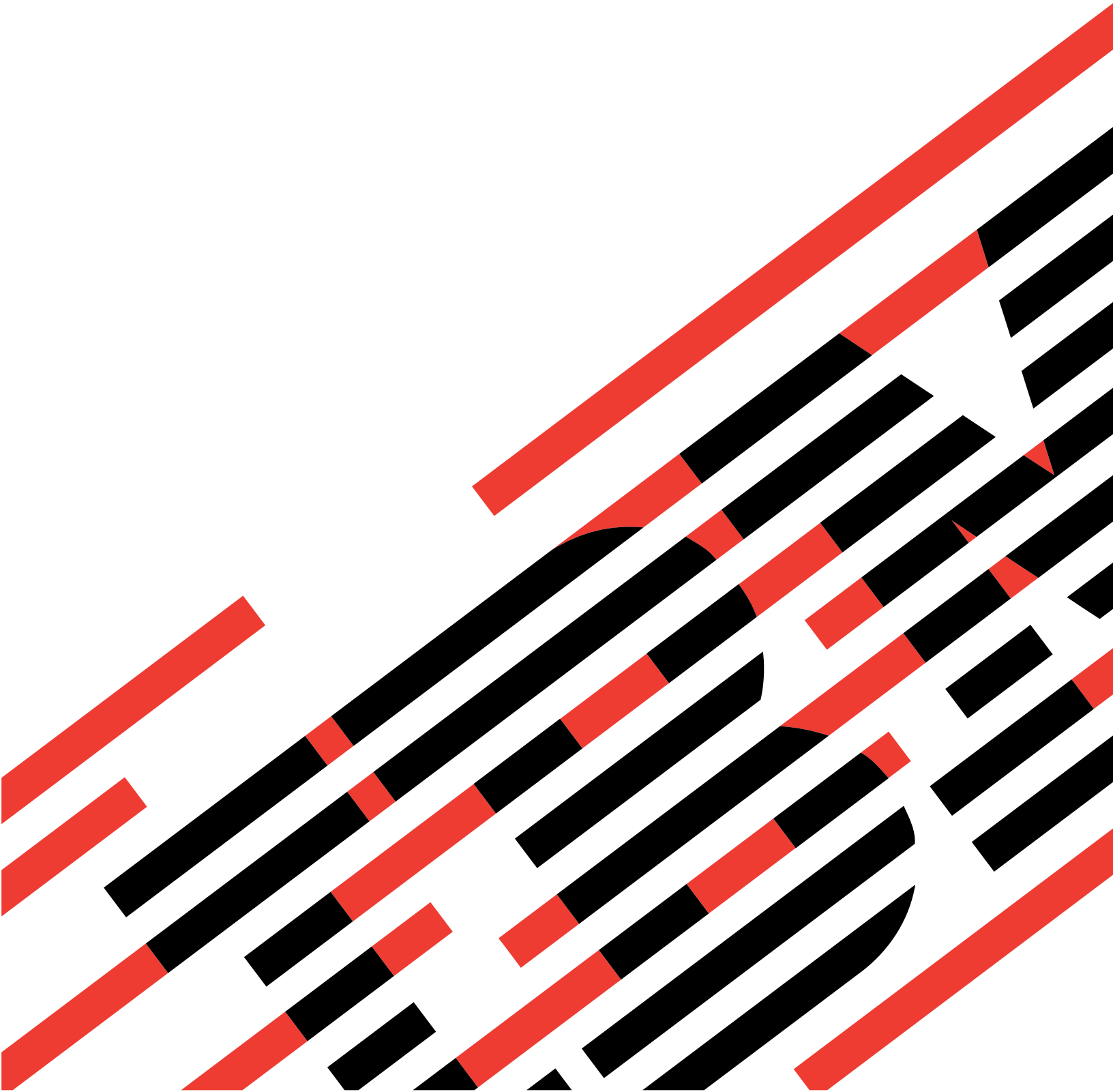
IBM

eserver

iSeries

Práca v sieti s adresárovými službami (LDAP)



IBM

@server

iSeries

Práca v sieti s adresárovými službami (LDAP)

Obsah

Časť 1. Adresárové služby (LDAP)

Directory Services poskytuje server LDAP (Lightweight Directory Access Protocol) na serveri iSeries. LDAP sa spúšťa cez TCP/IP (Transmission Control Protocol/Internet Protocol) a je obľúbený ako adresárová služba pre internetové, aj neinternetové aplikácie.

Ak poznáte Directory Services, možno budete chcieť začať tým, že si prečítate o novinkách v tomto vydaní. Ak chcete, môžete si vytlačiť alebo zobraziť PDF verziu informácií o Directory Services.

Nasledujúce témy predstavujú Directory Services a poskytujú informácie na pomoc pri správe servera LDAP na vašom serveri iSeries:

Ďalšie informácie o Directory Services nájdete na webovej stránke Directory Services  .

Server LDAP poskytovaný Directory Services je IBM SecureWay Directory  .

Kapitola 1. Čo je nové vo V5R2?

Adresárové služby majú nasledujúce rozšírenia a nové vlastnosti.

- Adresárové služby sú súčasťou základného operačného systému začínajúceho sa vo V5R1. Počnúc V5R2 už voľba 32 nie je dostupná.
- S cieľom ďalej chrániť všetky údaje uložené na adresárovom serveri boli vykonané nové bezpečnostné rozšírenia.
- Adresárový server LDAP možno teraz použiť ako radič domény pre doménu EIM (Enterprise Identity Mapping).
- Pre správcov je k dispozícii nová voľba, pomocou ktorej možno udeliť prístup správcu na adresárový server pre užívateľov, ktorým bol udelený prístup na identifikátor (ID) funkcie správcu adresárových služieb (QIBM_DIRSRV_ADMIN) operačného systému cez aplikačnú podporu iSeries Navigator.
- Môžete si zvoliť, aby váš adresárový server používal špecifickú adresu IP alebo si môžete zvoliť použitie všetkých nakonfigurovaných adries IP na serveri. Ďalšie informácie nájdete v téme “Zmena portu alebo adresy IP” na strane 21.
- API **ldap_set_option** má novú vlastnosť sledovania ladenia pre V5R2. Voľbu LDAP_OPT_DEBUG možno použiť na pomoc pri diagnostike problémov s klientmi, ktorí používajú API LDAP C. Ďalšie informácie obsahuje “Použitie voľby LDAP_OPT_DEBUG na sledovanie chýb” na strane 63 alebo API adresárových služieb v iSeriesinformačnom centre  .

Ako možno vidieť, čo je nové alebo zmenené:

Na to, aby ste mohli vidieť, kde boli spravené technické zmeny, používa táto informácia:

- Obrázok  na vyznačenie začiatku nových alebo zmenených informácií.
- Obrázok  na vyznačenie ukončenia nových alebo zmenených informácií.

Kapitola 2. Tlač tejto témy

Ak si chcete prezerať alebo stiahnuť dokument typu PDF, zvoľte si Adresárové služby (LDAP) (približne 323 kB alebo 66 strán).

Ostatné informácie

Môžete si tiež prezrieť alebo vytlačiť ktorýkoľvek z nasledujúcich PDF dokumentov:

- *Príručka implementácie LDAP* .
- *Pochopenie LDAP* .
- *Použitie LDAP na integráciu adresára: pohľad naIBM SecureWay Directory, Active Directory a Domino*
- *Implementácia a praktické použitie LDAP na serveri iSeries* .

Ak chcete uložiť dokument typu PDF na svojej pracovnej stanici s cieľom prezerania alebo tlače:
1. Vo svojom prehliadači otvorte PDF (kliknite na predchádzajúci odkaz).
2. V ponuke svojho prehliadača kliknite na **Súbor**.
3. Kliknite na **Uložiť ako...**
4. Prejdite do adresára, do ktorého chcete uložiť dokument PDF.
5. Kliknite na **Uložiť**.

Stiahnutie Adobe Acrobat Reader

Ak potrebujete na prezeranie alebo tlač týchto PDF dokumentov Adobe Acrobat Reader, môžete si ho stiahnuť zo stránky Adobe Web (www.adobe.com/products/acrobat/readstep.html) .

Kapitola 3. Začíname s Directory Services

Directory Services poskytuje server LDAP (Lightweight Directory Access Protocol) na serveri iSeries. LDAP spúšťa TCP/IP (Transmission Control Protocol/Internet Protocol) a získava si popularitu ako adresárová služba pre internetové, aj neinternetové aplikácie. Väčšinu nastavovania a správcovských úloh adresárového LDAP servera, založeného na OS/400 vykonávate cez grafické užívateľské prostredie (GUI) iSeries Navigator. Ak chcete riadiť Directory Services, musíte mať nainštalovaný iSeries Navigator na PC, ktoré je pripojené k vášmu serveru iSeries. Directory Services môžete použiť s aplikáciami, ktoré majú povolené LDAP, ako napríklad poštové aplikácie, ktoré vyhľadávajú e-mailové adresy z LDAP serverov.

Okrem LDAP servera Directory Services tiež obsahuje:

- Klient LDAP založený na OS/400. Tento klient obsahuje sadu aplikačných programových rozhraní (API), ktoré môžete použiť v OS/400 programoch na vytvorenie svojich vlastných klientskych aplikácií. Informácie o týchto API nájdete v téme Adresárové služby pod Programovaním v iSeries Information Center.
- Verzia 3.2 IBM SecureWay Directory Client Software Development Kit (SDK). SDK zahŕňa klienta LDAP Windows a nasledujúce nástroje:
  - IBM SecureWay Directory Management Tool, ktorý vám poskytuje grafické užívateľské rozhranie na riadenie obsahu adresárov.
  - programy príkazového riadka (ldapsearch, ldapadd, atď.)
  - C LDAP API (súbory knižníc, súbory hlavičiek a príklady zdrojového textu)
  - poskytovateľ služieb IBM JNDI LDAP (ibmjndi.jar)
  - online dokumentácia pre všetky vyššie spomenuté nástroje. Prečítajte si súbor readme pre umiestnenie a názvy týchto HTML súborov.

Ak ste použili Directory Services so starším vydaním OS/400, pozrite si “Migrácia na V5R2 zo staršieho vydania Directory Services” na strane 11.

Na zoznámenie s LDAP si pozrite “Základy LDAP” na strane 8. Ak ste použili servery LDAP na iných platformách, mali by ste venovať zopár minút a prečítať si túto tému, ktorá obsahuje niektoré informácie špecifické pre OS/400.

Po oboznámení sa so základnými informáciami, pokračujte na “Plánovanie vášho adresárového servera LDAP” na strane 11.

Informácie o inštalovaní a konfigurácii svojho adresárového servera nájdete v “Inštalácia a konfigurácia Directory Services” na strane 14.

Dokumentácia

Téma Directory Services Information Center poskytuje prehľad o LDAP a sústreďuje sa hlavne na riadenie adresárového servera LDAP na OS/400. Táto dokumentácia poskytuje tiež úplnú dokumentáciu pre SecureWay Directory Client SDK. Ďalšie informácie o LDAP obsahujú odkazy na LDAP, ako napríklad:

- *LDAP Implementation Cookbook* .
- *Understanding LDAP* .
- *Using LDAP for Directory Integration: A Look at IBM SecureWay Directory, Active Directory, and Domino*
- *Implementation and Practical Use of LDAP on the iSeries server* .

- *LDAP: Programming Directory-enabled Applications with Lightweight Directory Access Protocol*, ktorú napísali Tim Howes a Mark Smith.
- *Understanding and Deploying LDAP Directory Services* ktorú napísali Mark C. Smith, Gordon S. Good a Tim Howes.

Ďalšie informácie o Directory Services na serveri iSeries sú dostupné na iSeriesdomovskej stránke servera adresárových služieb .

Poznámka: Časť materiálov tohto dokumentu je derivátom dokumentácie LDAP, ktorú poskytla Michiganská univerzita. Copyright © 1992-1996, Regents of the University of Michigan, All Rights Reserved.

Základy LDAP

Lightweight Directory Access Protocol (LDAP) je protokolom adresárovej služby, ktorý beží nad protokolom Transmission Control Protocol/Internet (TCP/IP). LDAP verzia 2 je formálne definovaná v Internet Engineering Task Force (IETF) Request for Comments (RFC) 1777, *Lightweight Directory Access Protocol*. Verzia 3 LDAP je formálne definovaná v IETF RFC 2251, *Lightweight Directory Access Protocol (v3)*. Tieto RFC si môžete prezrieť na internete na nasledujúcej adrese URL:

http://www.ietf.org

Adresárová služba LDAP vychádza z modelu klient/server. Jeden alebo viac LDAP serverov obsahuje adresárové údaje. LDAP klient sa pripája k LDAP serveru a dáva požiadavku. Server odpovedá odpoveďou alebo ukazovateľom (odvolávka) iný LDAP server.

Použitie LDAP:

Keďže LDAP je adresárová služba, a nie databáza, informácie v adresári LDAP sú zvyčajne opisné a založené na atribúte. Používatelia LDAP obyčajne informáciu v adresári čítajú a nemenia. Aktualizácie sú zvyčajne jednoduchými celkovými zmenami. Adresáre LDAP sa bežne používajú na on-line telefónne zoznamy a adresáre e-mailových adries.

Štruktúra adresárov LDAP:

Model adresárovej služby LDAP je založený na **záznamoch** (ktoré sa tiež označujú ako **objekty**). Každý záznam sa skladá z jedného alebo viacerých **atribútov**, ako napríklad meno alebo adresa a **typ**. Typy sa zvyčajne skladajú z mnemonických reťazcov, ako napríklad cn pre bežný názov alebo mail pre e-mailovú adresu.

Príklad adresára v Obrázok 1 na strane 10 ukazuje záznam Tima Jonesa, ktorý obsahuje atribúty *mail* a *telefónne číslo*. Ďalšie možné atribúty sú *fax*, *titul*, *sn* (pre priezvisko) a *jpegPhoto*.

Každý adresár má **schému**, ktorá je súborom pravidiel, ktoré určujú štruktúru a obsah adresára. Na editovanie súborov schém pre váš LDAP server by ste mali používať IBM SecureWay Directory Management Tool (DMT). Po inštalácii Directory Services sa súbory nachádzajú na vašom systéme v /QIBM/UserData/OS400/DirSrv.

Poznámka: Pôvodné kópie štandardných súborov schém sú uložené v /QIBM/ProdData/OS400/DirSrv. Ak chcete vymeniť súbory v adresári UserData, môžete ich skopírovať do adresára /QIBM/ProdData/OS400/DirSrv.

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

Každá adresárová položka musí mať nasledujúce **operačné atribúty**, ktoré automaticky udržiava LDAP server:

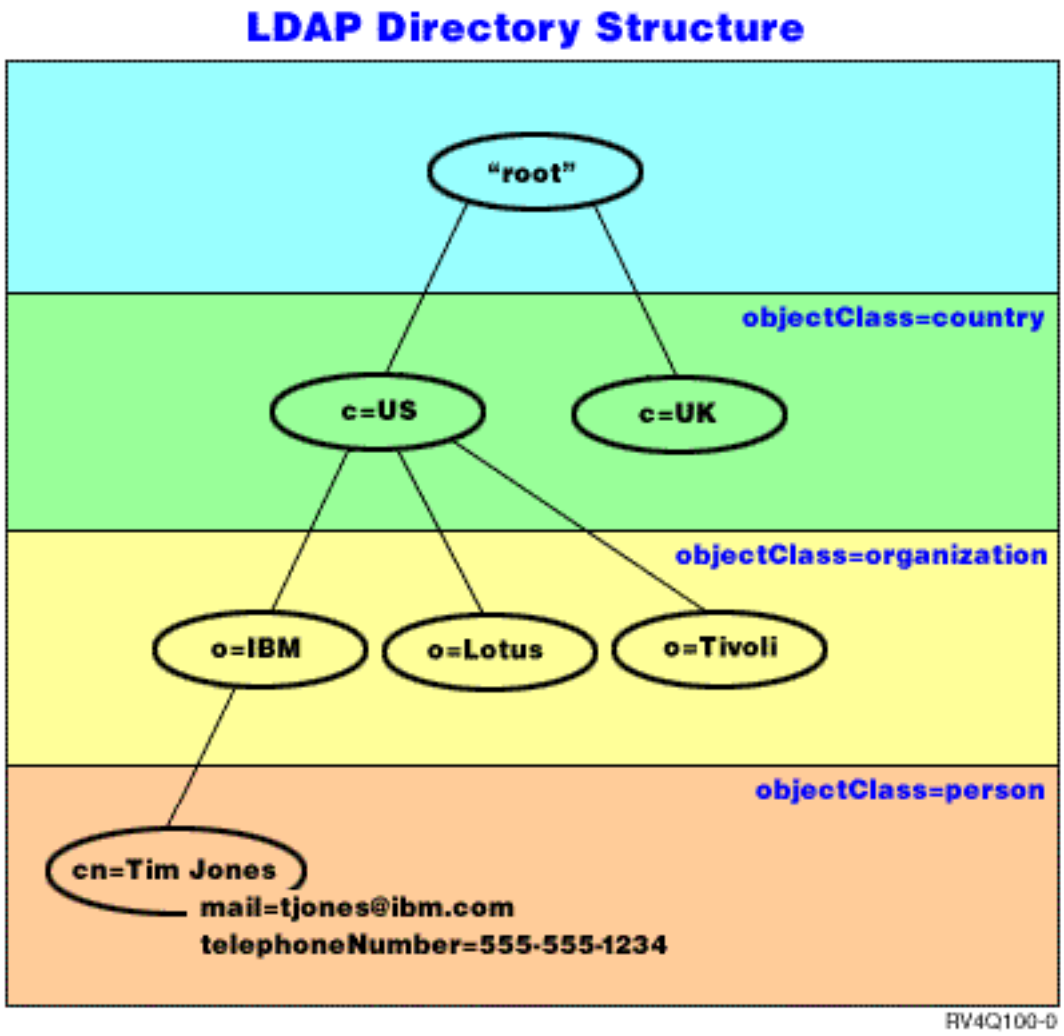
- CreatorsName, s väzbou, ktorú DN použil pri vytváraní položky.
- CreateTimestamp, ktorý obsahuje čas, kedy bola položka vytvorená.
- modifiersName, ktorý obsahuje väzbu, ktorú DN použil pri poslednej modifikácii položky (pôvodne sa zhoduje s CreatorsName).
- modifyTimestamp, obsahuje čas, kedy bol záznam naposledy modifikovaný (na začiatku je zhodný s CreateTimestamp).

Položky adresára LDAP sú bežne zoradené v hierarchickej štruktúre, ktorá rešpektuje politické, geografické a organizačné hranice (pozrite Obrázok 1 na strane 10). Položky predstavujúce krajiny sa zobrazujú navrchu. Položky predstavujúce štáty alebo národné organizácie sú pod nimi. Dole uvedené položky potom môžu predstavovať ľudí, organizačné jednotky, tlačiarne, dokumenty alebo iné položky.

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

LDAP sa odvoláva na položky s **Rozoznaným názvom** (DN). Rozoznané názvy sa skladajú z názvu samotnej položky, ako aj z názvov v poradí zhora i nadol, z objektov nad nimi v adresári. Napríklad úplné DN záznamu v spodnom ľavom rohu Obrázok 1 na strane 10 je cn=Tim Jones, o=IBM, c=US. Každý záznam má najmenej jeden atribút, ktorý sa používa na nazvanie položky. Tento názvový atribút sa uvádza ako **relatívny rozdelený názov (RDN)** položky. Vyššie uvedené položka, daná RDN sa uvádza ako jeho **rodičovský rozlíšený názov**. Vo vyššie uvedenom príklade cn=Tim Jones pomenúva položku na RDN. o=IBM, c=US je rodičovský DN pre cn=Tim Jones.

Ak chcete dať adresárovému serveru možnosť riadiť adresár LDAP, v konfigurácii servera špecifikujte najvyššiu úroveň rodičovských rozoznaných názvov (DN). Tieto rozoznané názvy (DN) sú **prípony**. Server môže mať prístup ku všetkým objektom v adresári, ktoré sú pod špecifickou príponou v hierarchii adresára. Ak napríklad server LDAP obsahoval adresár zobrazený v Obrázok 1 na strane 10, musel by mať príponu o=ibm, c=us uvedenú v svojej konfigurácii, aby mohol odpovedať na dotazy klienta týkajúce sa Tima Jonesa.



Obrázok 1. Základná štruktúra adresára LDAP

Poznámky k LDAP a Directory Services:

- Počnúc od V4R5, OS/400 LDAP server aj OS/400 LDAP klient sú založení na LDAP verzie 3. So serverom V3 môžete použiť klienta V2. Nemôžete však použiť V3 klienta s V2 serverom, pokiaľ nie ste viazaný ako V2 klient a používate len V2 API. Viac informácií nájdete v časti Úvahy pre LDAP V2/V3.
- Windows LDAP klient je tiež založený na LDAP verzie 3.
- Pretože LDAP predstavuje štandard, servery LDAP majú rovnaké mnohé základné charakteristiky. Vzhľadom na rozdiely v implementáciách však nie sú úplne kompatibilné. Server LDAP poskytovaný Directory Services je úzko kompatibilný s ostatnými adresárovými servermi LDAP v skupine produktov IBM SecureWay Directory a IBM Directory. Avšak nemusí byť tak kompatibilný s inými servermi LDAP.
- Údaje pre server LDAP, ktoré poskytuje Directory Services, sa nachádzajú v databáze OS/400.

Viac informácií:

Príklady použitia adresárov LDAP nájdete v týchto častiach:

- Časť 1.6 Rýchly začiatok: Príklad verejného LDAP v červenej knihe *Pochopenie LDAP*.
- Časť 3.3 Vzorové scenáre, v červenej knihe Pochopenie LDAP.

Ak sa chcete dozvedieť viac o mechanizme LDAP, pozrite si Kapitola 5, “Koncepty Directory Services a referenčné informácie” na strane 33.

Úvahy o používaní LDAP V2 s LDAP V3

Počnúc od V4R5, OS/400 LDAP server aj OS/400 LDAP klient sú založení na LDAP verzie 3. So serverom V2 nemôžete použiť klienta V3. Môžete však použiť ldap_set_option() API pre zmenu verzie V3 klienta na V2. Potom môžete úspešne odosielať klientske požiadavky serveru V2.

So serverom V3 môžete použiť V2 klienta. Dávajte však pozor na to, že v požiadavke vyhľadávania V3 server môže odoslať späť údaje v plnom rozsahu vo formáte UTF-8, kým V2 klient môže mať schopnosť obsluhovať údaje v sade znakov IA5.

Poznámka: LDAP verzia 2 je formálne definovaná v Internet Engineering Task Force (IETF) Request for Comments (RFC) 1777, *Lightweight Directory Access Protocol*. LDAP verzia 3 je formálne definovaná v IETF RFC 2251, *Lightweight Directory Access Protocol (v3)*. LDAP verzia 3 je formálne definovaná v IETF RFC 2251, *Lightweight Directory Access Protocol (v3)*. Tieto RFC si môžete pozrieť na internete na nasledujúcich URL:

http://www.ietf.org

Plánovanie vášho adresárového servera LDAP

Kým nainštalujete Directory Services a začnete konfigurovať svoj adresár LDAP, mali by ste pár minút venovať naplánovaniu adresára. Mali by ste zvážiť tieto faktory:

- **Organizáciu adresára**. Naplánujte si štruktúru vášho adresára a určite, ktoré prípony a atribúty bude váš server vyžadovať.
- **Rozhodnite o veľkosti vášho adresára**. Potom budete môcť odhadnúť, koľko pamäte potrebujete. Veľkosť adresára závisí od:
  - Počtu atribútov v schéme serverov.
  - Počtu položiek na serveri.
  - Typu informácií, ktoré na server ukladáte.

  Napríklad prázdny adresár, ktorý používa štandardnú schému Directory Services vyžaduje približne 10 MB pamäťového priestoru. Adresár, ktorý používa štandardnú schému a obsahuje 1000 položiek bežných informácií o zamestnancoch, vyžaduje asi 30 MB pamäťového priestoru. Tento počet sa bude líšiť v závislosti od presných atribútov, ktoré ste použili. Dané číslo sa tiež značne zvýši, ak ste uložili do adresára veľké objekty, napríklad obrázky.
- **Rozhodnite sa, ktoré bezpečnostné opatrenia prijmete**. Directory Services podporuje pre bezpečnosť komunikácie použitie SSL (Secure Sockets Layer) a digitálnych certifikátov, ako aj TLS (Translation Layer Security). Od V5R1 sa podporuje aj autentifikácia Kerberos.
- Directory Services vám umožňuje riadiť prístup k objektom adresára pomocou ACL (zoznamov riadenia prístupov). Na ochranu adresára môžete použiť aj OS/400 auditovanie bezpečnosti.

Migrácia na V5R2 zo staršieho vydania Directory Services

V5R2 OS/400 predstavuje nové vlastnosti a schopnosti na Directory Services. Tieto zmeny sa týkajú tak adresárového LDAP servera, ako aj grafického užívateľského prostredia (GUI) iSeries Navigator. Ak chcete využívať výhody nových vlastností GUI, musíte nainštalovať iSeries Navigator na PC, ktoré môže komunikovať cez TCP/IP s vašim serverom iSeries. iSeries Navigator je komponent iSeries Access for Windows. Ak máte nainštalovanú staršiu verziu iSeries Navigator, mali by ste prejsť na V5R2.

V5R2 OS/400 podporuje rozšírenia z V4R5 a V5R1. Keď prechádzate na V5R2 OS/400, údaje adresára LDAP a adresárové súbory schém sú automaticky migrované tak, aby vyhovovali formátom V5R2. Ak máte server LDAP Directory Services spustený pod V4R3 alebo V4R4 OS/400 a chcete migrovať server na V5R2, musíte vykonať niektoré ďalšie úlohy migrácie.

Keď prechádzate na V5R2 OS/400, mali by ste poznať niektoré problémy migrácie:

- Keď prechádzate na V5R2, Directory Services automaticky migruje vaše súbory schém na V5R2 a vymazáva staré súbory schém. Ak ste však vymazali alebo premenovali súbory schém, Directory Services ich nemôže migrovať. Môžete dostať chybu alebo Directory Services môže predpokladať, že súbory už boli migrované.
- Directory Services migruje adresárové údaje do formátu V5R2 pri vašom prvom spustení servera alebo importe súboru LDIF. Rátajte s tým, že chvíľu bude trvať, kým sa migrácia ukončí. Ak prechádzate na V5R2 z V4R4 alebo staršej verzie, musíte vedieť, že údaje adresára budú vyžadovať približne dvakrát toľko pamäťového priestoru vo V5R2, než vyžadovali predtým. Dôvodom je, že vo V4R4 alebo starších verziách Directory Services podporovala len znakovú sadu IA5 a ukladala údaje v ccsid 37 (jednobajtový formát). Directory Services podporuje úplnú znakovú sadu ISO 10646.

  Potom, ako prejdete na V5R2, mali by ste svoj server spustiť a migrovať existujúce údaje, kým naimportujete nové. Ak sa pokúsite importovať údaje pred spustením servera a nemáte dostatočné oprávnenie, import nemusí prebehnúť.
- Vydania Directory Services V4R4 a staršie pri vytváraní záznamov s časovou značkou nebrali do úvahy časové pásma. Od vydania V4R5 sa používa časové pásmo pri všetkých pridaných a zmenených údajoch adresára. Preto, keď prechádzate na V5R2 z V4R4 alebo staršej verzie, Directory Services upraví existujúce atribúty createtimestamp a modifytimestamp tak, aby odrážali správnu časovú zónu. Zrealizuje to tak, že odpočíta časové pásmo, ktoré je práve nastavené na systéme iSeries od časových značiek, ktoré sú uložené v adresári. Všimnite si, že ak aktuálna časová zóna nie je rovnaká ako časová zóna, ktorá bola aktívna, keď sa položky pôvodne vytvárali alebo modifikovali, hodnoty novej časovej značky nebudú odrážať pôvodnú časovú zónu.
- Po migrácii sa bude adresárový LDAP server automaticky spúšťať, keď sa spustí TCP/IP. Ak nechcete, aby sa adresárový server spúšťal automaticky, použite iSeries Navigator na zmenu nastavenia.

Migrácia z V4R3 alebo V4R4 Directory Services na V5R2

V5R2 OS/400 nepodporuje priame rozšírenie z V4R3. Ak chcete migrovať server LDAP V4R3 alebo V4R4 Directory Services na V5R2, môžete postupovať podľa jednej z nasledujúcich procedúr:

- Presunúť inštaláciu OS/400 z V4R3 alebo V4R4 do dočasného vydania
- Uloženie databázovej knižnice a vynulovanie inštalácie OS/400 z V4R3 alebo V4R4 na V5R2

Presun inštalácie OS/400 z V4R3 alebo V4R4 do dočasného vydania

Aj keď rozšírenia z V4R3 a V4R4 OS/400 na V5R2 nie sú podporované, podporujú sa nasledujúce rozšírenia:

- V4R3 a V4R4 rozšírené na V4R5
- V4R4 a V4R5 rozšírené na V5R1
- V4R5 a V5R1 rozšírené na V5R2

Jedným zo spôsobov migrácie vášho servera Directory Services je rozšírenie do dočasného vydania (V4R5 alebo V5R1) a potom V5R2. Podrobnejšie informácie o procedúrach inštalácie OS/400 obsahuje časť

Inštalácia softvéru . Pri migrácii postupujte podľa nasledujúcich krokov:

1. Zaznamenajte si všetky zmeny, ktoré ste vykonali v súboroch schém do adresára /QIBM/UserData/OS400/DirSrv. Súbory schém sa migrujú automaticky.
2. Pre V4R4 alebo V4R3 vykonajte inštaláciu V4R5 alebo V5R1 OS/400.
3. Vykonajte inštaláciu OS/400 na V5R2.
4. Spustite server Adresárových služieb, ak už nie je spustený.

5. Použite Nástroj na správu adresárov, aby ste zmenili súbory schém pre všetky užívateľské zmeny, ktoré ste si poznačili v kroku 1 na strane 12.
6. Reštartujte server adresárových služieb.

Uloženie databázovej knižnice a vynulovanie inštalácie OS/400 z V4R3 alebo V4R4 na V5R2

Ďalším spôsobom migrácie vášho servera Directory Services je uložiť databázovú knižnicu, ktorú Directory Services používa vo V4R3 alebo V4R4 a potom ju obnoviť po nulovej inštalácii V5R2. Týmto ušetríte krok inštalácie medzivydania. Nastavenia serverov sa však nemigrujú, takže ich musíte znova nastaviť.

Podrobnejšie informácie o inštalačných procedúrach OS/400 nájdete v časti *Inštalácia softvéru* . Pri migrácii postupujte podľa týchto krokov:

1. Zaznamenajte si všetky zmeny, ktoré ste vykonali v súboroch schém do adresára /QIBM/UserData/OS400/DirSrv. Súbory schém nie sú migrované automaticky, takže ak chcete zachovať svoje zmeny, musíte ich znovu manuálne implementovať.
2. Zaznamenajte si rôzne nastavenia konfigurácie vo vlastnostiach serverov Directory Services vrátane názvu databázovej knižnice.
3. Uložte databázovú knižnicu, ktorá je uvedená v konfigurácii serverov Directory Services.
4. Poznačte si konfiguráciu publikovania.
5. Nainštalujte systém na V5R2 OS/400.
6. Pre konfiguráciu servera adresárových služieb použite EZ-Setup.
7. Obnovte knižnicu databázy, ktorú ste uložili v kroku 3.
8. Použite Nástroj na správu adresárov, aby ste zmenili súbory schém pre všetky užívateľské zmeny, ktoré ste si poznačili v kroku 1.
9. Na opätovnú konfiguráciu adresárových služieb použite iSeries Navigator. Zadajte knižnicu databázy, ktorú ste uložili a obnovili.
10. Na konfiguráciu publikovania použite iSeries Navigator.
11. Reštartujte server adresárových služieb.

Problémy pri prechode na vyššiu verziu

Keď aktualizujete z V4R3 na akékoľvek novšie vydanie, môžu nastať uvedené situácie:

- **Migrácia súboru kľúčov do databázy kľúčov:**

  Klient prístupu V3R2 používal súbory zväzkov kľúčov na nastavenie pripojení Secure Sockets Layer (SSL) k adresárovému LDAP serveru. iSeries Access for Windows používa sklady certifikátov, ktoré sa niekedy nazývajú databázy kľúčov, na vytvorenie pripojení SSL. Ak ste predtým použili súbor kľúčov s vaším LDAP adresárovým serverom, súbor kľúčov musíte previesť na databázu kľúčov, aby bolo možné pokračovať použitím SSL. Keď sa pokúšate naštartovať spojenie SSL k adresárovému serveru, iSeries Navigator vás na túto zmenu upozorní. Ak si zvolíte konvertovať kľúč, pred vykonaním konverzie budete musieť zadať niektoré informácie pre databázu kľúčov.

  Adresárový LDAP server tiež pre vlastné pripojenia SSL v V4R3 používal súbor zväzku kľúčov. Od V4R4, používa systémovú pamäť certifikátov. Ak bol váš server v V4R3 nastavený na používanie SSL, obsah súboru kľúčov sa presunie do pamäte certifikátov.
- **Dva prúdové súbory boli odstránené:**

  Nasledujúce prúdové súbory používané s Directory Services v V4R3 už nie sú potrebné a automaticky sa odstránia, keď nainštalujete novšie vydanie:

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

  S týmito súbormi nemusíte vyriešiť žiadnu úlohu. Uvádzajú sa tu len pre vašu informáciu, že sa na vašom systéme nenachádzajú.

Uvedomte si, že sa môžu vyskytnúť ďalšie problémy súvisiace s prechodom z iných vydaní na súčasné vydanie.

Inštalácia a konfigurácia Directory Services

Directory Services(LDAP) sa automaticky nainštaluje, keď nainštalujete OS/400. Adresárový server obsahuje štandardnú konfiguráciu, ktorá automaticky spustí adresárový server, keď sa spustí TCP/IP. Adresárový server tiež spúšťa publikovanie počítačových informácií z OS/400 na adresárový server. Ak chcete upraviť nastavenia adresárových serverov LDAP, spustite sprievodcu konfiguráciou Directory Services . Na použitie sprievodcu musíte mať špeciálne oprávnenia *ALLOBJ a *IOSYSCFG.

Od V5R1 sú adresárové služby integrované do základného operačného systému a od V5R2 už voľba 32 nie je prístupná.

Konfigurácia adresárového servera LDAP

Ak nebol váš systém nakonfigurovaný na publikovanie informácií ďalšiemu serveru LDAP a serveru TCP/IP DNS nie sú známe žiadne servery LDAP, Directory Services je automaticky nainštalovaný s obmedzenou štandardnou konfiguráciou. Directory Services poskytuje sprievodcu na pomoc pri konfigurácii adresárového servera LDAP pre vaše osobitné potreby. Tohto sprievodcu môžete spustiť ako súčasť EZ-Setup, alebo ho môžete spustiť neskôr z iSeries Navigator. Použite ho, keď po prvýkrát konfigurujete adresárový server. Môžete ho použiť aj pri zmene konfigurácie adresárového servera.

Poznámka: Ak použijete sprievodcu na prekonfigurovanie adresárového servera, začnete konfigurovať znova. Pôvodná konfigurácia sa vymaže a nedá sa meniť. Údaje adresára však nebudú vymazané, ale namiesto toho zostanú uložené v knižnici, ktorú ste si zvolili pri inštalácii (štandardne QUSRDIRDB). Protokol zmeny zostane tiež zachovaný štandardne v knižnici QUSRDIRCL.

Ak chcete začať úplne nanovo, vymažte tieto dve knižnice pred spustením pomocníka.

Ak chcete zmeniť konfiguráciu adresárového servera, ale nechcete ho úplne vymazať, kliknite pravým tlačidlom myši na **Directory** a vyberte **Vlastnosti**. Tak nevymažete pôvodnú konfiguráciu.

Ak chcete konfigurovať server, musíte mať špeciálne oprávnenia *ALLOBJ a *IOSYSCFG. Ak chcete konfigurovať OS/400 auditovanie bezpečnosti, musíte mať tiež zvláštne oprávnenie *AUDIT.

Ak chcete spustiť Sprievodcu konfiguráciou Directory Services, postupujte podľa nasledujúcich krokov:

1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Pravým tlačidlom kliknite na **Adresár** a vyberte **Konfigurovať**.

Poznámka: Ak ste adresárový server nakonfigurovali, kliknite na **Zmeniť konfiguráciu**, nie na **Konfigurovať**.

Ak chcete nakonfigurovať váš adresárový server LDAP, postupujte podľa inštrukcií v sprievodcovi konfiguráciou adresárového servera.

Poznámka: Knižnicu, ktorá ukladá údaje adresára, radšej vložte do dočasnej užívateľskej pomocnej pamäťovej oblasti (ASP) než do systémovej ASP. Túto knižnicu však nemožno uložiť v nezávislej ASP a každý pokus o konfiguráciu, prekonfigurovanie alebo spustenie servera s knižnicou, ktorá sa nachádza v nezávislej ASP, bude neúspešný.

Po dokončení sprievodcu bude mať adresárový server LDAP základnú konfiguráciu. Ak spúšťate vo vašom systéme Lotus Domino, port 389 (štandardný port pre server LDAP) už môže používať funkcia Dominos LDAP. Musíte vykonať jeden z nasledujúcich krokov:

- Zmeňte port, ktorý Lotus Domino používa
- Zmeňte port, ktorý Directory Servicespoužíva
- Použite špecifické adresy IP

Možno budete chcieť spustiť server v tomto bode. Pred spustením servera budete možno chcieť urobiť niektoré alebo všetky nasledujúce kroky:

- Do servera importujete údaje
- Povolíte zabezpečenie Secure Sockets Layer (SSL)
- Aktivovať autentifikáciu Kerberosom
- Nastavíte odkaz

Povolenie SSL na adresárovom serveri LDAP

Ak máte na svojom systéme inštalovaného Správcu digitálnych certifikátov, môžete na ochranu prístupu k svojmu adresárovému LDAP serveru použiť zabezpečenie Secure Sockets Layer (SSL). Kým povolíte SSL na adresárovom serveri, bude užitočné prečítať si Prehľad o použití SSL so Directory Services.

Ak chcete použiť pripojenie SSL, keď spravujete váš adresárový server LDAP z iSeries Navigator alebo ak chcete použiť SSL s klientom LDAP Windows, musíte mať na vašom PC nainštalovaný jeden z produktov šifrovania klienta (5722CE2 alebo 5722CE3).

Ak chcete umožniť SSL pre váš adresárový server, použite rozhranie Správcu digitálnych certifikátov. Manažéra digitálnych certifikátov môžete spustiť z **internetového** adresára v iSeries Navigator alebo zo stránky **Sieť** dialógového okna **Vlastnosti** adresárových serverov.

Ak chcete spustiť rozhranie digitálneho certifikátu zo stránky **Sieť**, postupujte takto:

1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Kliknite pravým tlačidlom na **Adresár** a zvoľte **Vlastnosti**.
5. Kliknite na záložku **Sieť**.
6. Kliknite na **Správca digitálnych certifikátov**.

   Správca digitálnych certifikátov sa spustí vo vašom štandardnom internetovskom prehliadači.

V Securing the LDAP directory server sa uvádzajú špecifické kroky, ktoré treba uskutočniť, aby ste pridelili digitálny certifikát k adresárovému serveru.

Ak ste umožnili SSL, môžete zmeniť port, ktorý pre bezpečnostné pripojenia používa adresárový LDAP server.

Povolenie autentifikácie Kerberos na adresárovom serveri LDAP

Ak máte vo svojom systéme nakonfigurovanú službu sieťovej autentifikácie, môžete nastaviť svoj adresárový server LDAP na použitie autentifikácie Kerberos. Kým povolíte Kerberos na adresárovom serveri, bude užitočné prečítať si Prehľad o používaní Kerberos s Directory Services.

Ak chcete umožniť autentifikáciu Kerberosom, postupujte takto:

1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Kliknite pravým tlačidlom na **Adresár** a zvoľte **Vlastnosti**.
5. Kliknite na zložku **Kerberos**.
6. Začiarknite **Umožniť autentifikáciu Kerberosom**.

7. Podľa vašej konkrétnej situácie špecifikujte ďalšie nastavenia na strane **Kerberos**. Pozrite si stránky s online pomocou, kde nájdete informácie k jednotlivým poliam.

Štandardná konfigurácia pre Directory Services

Adresárový server LDAP sa nainštaluje automaticky, keď inštalujete OS/400. Táto inštalácia obsahuje štandardnú konfiguráciu. Adresárový server používa štandardnú konfiguráciu, ak sú pravdivé všetky nasledujúce body:

- Administrátori nespustili Directory Services Sprievodcu konfiguráciou alebo nezmenili nastavenia adresárov pomocou strán vlastností.
- Directory Services nie je nakonfigurované publikovanie.
- Adresárový LDAP server nemôže nájsť žiadne informácie o LDAP DNS.

Ak adresárový server LDAP používa štandardnú konfiguráciu, nastane toto:

- Adresárový server sa automaticky spustí, keď sa spustí TCP/IP.
- Systém vytvorí štandardného správu cn=Administrator. Tiež vygeneruje heslo, ktoré sa bude interne používať. Ak potrebujete neskôr použiť, môžete definovať nové zo Directory Services strany vlastností.
- Na základe názvu IP systémov sa vytvorí štandardná prípona. Na základe systémového názvu sa vytvorí aj prípona systémových objektov. Ak je napríklad názov IP vašich systémov mary.acme.com, prípona bude dc=mary,dc=acme,dc=com.
- Adresárový LDAP server používa štandardnú dátovú knižnicu QUSRDIRDB. Túto systém vytvorí v ASP systéme.
- Pre nezabezpečenú komunikáciu používa systém port 389. Ak bol pre LDAP nakonfigurovaný digitálny certifikát, pre bezpečnú komunikáciu bude povolené SSL (secure sockets layer) a použije sa port 636.

Pre Directory Services publikovanie potom existujú nasledujúce štandardné nastavenia:

- Systém publikuje informácie o lokálnom adresárovom serveri LDAP.
- Publikovanie nepoužíva SSL
- Publikovanie používa kontajnery pod štandardnou príponou
- Na autentifikáciu adresárového servera OS/400 používa cn=Administrator ID a systémom generované heslo.
- Systém publikuje len systémové informácie.

DMT (program riadenia adresárov) IBM SecureWay

DMT (program riadenia adresárov) IBM SecureWay vám poskytuje grafické užívateľské rozhranie pre riadenie obsahu adresárov LDAP. Úlohy, ktoré môžete vykonávať s DMT, zahŕňajú:

- Prehľadávanie schémy adresára
- Pridávanie, editovanie a vymazávanie objektových tried
- Pridávanie, editovanie a vymazávanie atribútov
- Prehľadávanie a vyhľadávanie v strome adresára
- Pridávanie, editovanie, prezeranie a vymazávanie položiek
- Editovanie RDN položiek
- Riadenie ACL

DMT je súčasťou klienta LDAP Windows LDAP, ktorý je zahrnutý do Directory Services. Klient sa dodáva v adresári integrovaného súborového systému.

Ak chcete nainštalovať klienta LDAP Windows vrátane DMT na PC, postupujte takto:
1. V iSeries Navigator rozviňte **Súborové systémy**.
2. Rozviňte **Zdieľania súborov**.

3. Kliknite dvakrát na **Qdirsrv**.
4. Kliknite dvakrát na **UserTools**.
5. Kliknite dvakrát na **Windows**.
6. Kliknite dvakrát na **setup.exe**, čím spustíte inštaláciu DMT. Postupujte podľa pokynov na obrazovke a dokončite inštaláciu.

Dokumentácia DMT (nástroja na riadenie adresárov IBM SecureWay sa nachádza v súbore dparent.htm. Tento súbor sa kopíruje do zložky adresára IBM SecureWay na vašom PC, keď inštalujete klienta.

Kapitola 4. Správa adresárového servera LDAP

Ak chcete vykonávať správu adresárového servera LDAP, musíte mať nasledujúce sady oprávnení.

- Ak chcete server nakonfigurovať alebo zmeniť jeho konfiguráciu, musíte mať špeciálne oprávnenia na všetky objekty (*ALLOBJ) a na I/O konfiguráciu systému (*IOSYSCFG).
- Ak chcete spustiť alebo zastaviť server, musíte mať oprávnenie na riadenie úlohy (*JOBCTL) a oprávnenie na objekt na príkazy ENDTCP (End TCP/IP), STRTCP (Start TCP/IP), STRTCPSVR (Start TCP/IP Server) a ENDTCPSVR (End TCP/IP Server).
- Ak chcete nastaviť správanie auditovania pre adresárový server, musíte mať špeciálne oprávnenie na audit (*AUDIT).
- Ak si chcete prezerať protokol úlohy servera, musíte mať špeciálne oprávnenie na spoolové riadenie (*SPLCTL).

Na spravovanie objektov adresára (vrátane zoznamov riadenia prístupu, vlastníctva objektov, a replík) sa do adresára pripojte buď s DN, správcu alebo s takým DN, ktoré má zodpovedajúce oprávnenie LDAP. Ak sa používa integrácia oprávnenia, správca môže byť aj projektovaným užívateľom, ktorý má oprávnenie na ID funkcie správcu adresárových služieb.

Spravovanie adresárového servera zahŕňa nasledujúce úlohy:

Spustenie adresárového servera LDAP

Na naštartovanie adresárového LDAP servera vykonajte nasledujúce kroky:

1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Kliknite pravým tlačidlom na **Adresár** a vyberte **Naštartovať**.

   Spustenie adresárového servera môže trvať niekoľko minút v závislosti od rýchlosti vášho servera a rozsahu dostupnej pamäte. Spustenie adresárového servera po prvýkrát môže trvať o niekoľko minút dlhšie než zvyčajne, pretože server musí vytvoriť nové súbory. Podobne pri prvom spustení adresárového servera po aktualizovaní zo staršej verzie Directory Services to môže trvať o niekoľko minút dlhšie ako zvyčajne, pretože server musí migrovať súbory. Stav servera môžete kontrolovať pravidelne a zistiť tak, či už bol spustený.

Poznámka: Adresárový server môže byť naštartovaný z relácie 5250 zadaním príkazu STRTCPSVR *DIRSRV.

Prípadne, ak ste váš adresárový server nakonfigurovali na naštartovanie počas spúšťania TCP/IP, môžete ho naštartovať zadaním príkazu STRTCP.

Zastavenie adresárového servera LDAP

Zastavenie adresárového servera má vplyv na všetky aplikácie používajúce server v čase jeho zastavenia. Zahŕňa to aj aplikácie EIM (Enterprise Identity Mapping), ktoré momentálne používajú adresárový server pre operácie EIM. Všetky aplikácie sú z adresárového servera odpojené, avšak môžu sa snažiť o opätovné pripojenie k serveru.

Ak chcete zastaviť adresárový LDAP server, vykonajte tieto kroky:
1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Kliknite pravým tlačidlom na **Adresár** a vyberte **Zastaviť**.

   Zastavenie adresárového servera môže trvať niekoľko minút v závislosti od rýchlosti vášho systému, množstva aktivít servera a množstva voľnej pamäte. Kontrolu stavu servera môžete vykonávať periodicky, aby ste sa presvedčili, či sa už nezastavil.

Poznámka: Adresárový server sa tiež dá zastaviť z relácie 5250 zadaním príkazov ENDTCPSVR *DIRSRV, ENDTCPSVR *ALL alebo ENDTCP. ENDTCPSVR *ALL a ENDTCP tiež ovplyvňujú všetky ďalšie TCP/IP servery, ktoré pracujú na vašom systéme. ENDTCP tiež ukončí samotný TCP/IP.

Kontrola stavu adresárového servera

iSeries Navigator zobrazí stav adresárového servera v stĺpci **Stav** v ľavom rámiku.

Na kontrolu stavu adresárového servera vykonajte nasledujúce kroky:
1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**. iSeries Navigator zobrazí stav všetkých TCP/IP serverov, vrátane adresárového servera v stĺpci **Stav**. Na aktualizovanie stavu serverov kliknite na menu **Zobraziť** a vyberte **Aktualizovať**.
4. Ak si chcete pozrieť viac informácií o stave adresárového servera, kliknite pravým tlačidlom na **Adresár** a vyberte **Stav**. Ten zobrazí počet aktívnych spojení, ako aj iné informácie, ako napríklad minulé a aktuálne úrovne aktivity.

   Okrem získania ďalších informácií môžete prezeraním stavu touto voľbou ušetriť čas. Stav adresára môžete aktualizovať bez zbytočného plytvania časom, ktorý sa vyžaduje pri zisťovaní stavu iných serverov TCP/IP.

Kontrola úloh na adresárovom serveri LDAP

Niekedy budete chcieť monitorovať úlohy adresárového LDAP servera. Ak to chcete urobiť, vykonajte nasledujúce kroky:
1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Pravým tlačidlom myši kliknite na **Adresár** a zvoľte **Úlohy servera**.

Povoliť notifikáciu udalostí

Directory Services podporuje notifikáciu udalostí, čo klientom umožňuje registrovať sa na serveri LDAP a dostávať notifikáciu o určitej udalosti, ako je napríklad pridanie položky do adresára.

Ak chcete umožniť notifikáciu udalostí pre váš server, postupujte podľa nasledujúcich krokov:
1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Kliknite pravým tlačidlom na **Adresár** a zvoľte **Vlastnosti**.
5. Kliknite na **Udalosti**.
6. Zvoľte **Umožniť klientom registráciu notifikácie udalostí**.

Tiež môžete stanoviť maximálny povolený počet registrácií pre každé pripojenie a maximálny povolený počet registrácií, ktoré server umožňuje.

Ďalšie informácie o notifikácii udalostí nájdete v dodatku C: Notifikácia udalostí v manuále IBM SecureWay Directory Version 3.2: Client SDK Programming Reference .

Uviesť nastavenie transakcie

Directory Services podporuje transakcie, ktoré umožňujú, aby sa so skupinou operácií adresára LDAP postupovalo, ako s jednou jednotkou. Ďalšie informácie obsahuje časť “Transakcie” na strane 37.

Ak chcete nakonfigurovať nastavenia transakcií svojich serverov, postupujte takto:
1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Kliknite pravým tlačidlom na **Adresár** a zvoľte **Vlastnosti**.
5. Kliknite na **Transakcie**.
6. Špecifikujte svoje nastavenia transakcií.

Poznámka: Nastavenia transakcií môžu ovplyvniť výkon vašich serverov LDAP, takže možno budete chcieť experimentovať s inými nastaveniami.

Zmena portu alebo adresy IP

Adresárový LDAP server povolený Directory Services štandardne používa nasledujúce porty:
- 389 pre nezabezpečené pripojenia.
- 636 pre zabezpečené pripojenia (ak ste použili Správcu digitálnych certifikátov na povolenie Directory Services, ako tej aplikácie, ktorá môže použiť bezpečný port).

Poznámka: Štandardne sú všetky adresy IP definované na lokálnom systéme pripojené na server.

Ak už tieto porty používate pre ďalšie aplikácie, môžete k Directory Services priradiť iný port, alebo môžete pre tieto dva servery použiť iné adresy IP, ak aplikácie podporujú pripojenie k špecifickej adrese IP.

Príklad servera LDAP Domino, ktorý je v rozpore so iSeriesserverom LDAP adresárových služieb obsahuje Hostiteľský Domino LDAP a adresárové služby na tom istom iSeries

Na zmenu portov použitých adresárovým serverom LDAP vykonajte tieto kroky:
1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Kliknite pravým tlačidlom na **Adresár** a zvoľte **Vlastnosti**.

5. Kliknite na záložku **Sieť**.
6. Zadajte vhodné čísla portov a potom kliknite na **OK**.

Ak chcete zmeniť adresu IP, na ktorej adresárový server prijíma pripojenia, vykonajte tieto kroky:
1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Kliknite pravým tlačidlom na **Adresár** a zvoľte **Vlastnosti**.
5. Kliknite na záložku **Sieť**.
6. Kliknite na tlačidlo **Adresy IP...**.
7. Vyberte si **Použiť vybranú adresu IP** a zvoľte si adresy IP pre server, ktoré sa majú použiť, keď sa prijímajú pripojenia.

Presun údajov adresára LDAP medzi systémami

Directory Services LDAP server môže pracovať nezávisle od iných serverov. Možno vám bude vyhovovať spolupracovať s inými servermi. Spolupráca môže zahŕňať:
- "Import súboru LDIF"
- "Export súboru LDIF"
- "Nastavenie novej repliky adresárového servera" na strane 23
- "Publikovanie informácií na adresárový server" na strane 26

Import súboru LDIF

Informácie medzi viacerými adresárovými servermi LDAP môžete presúvať použitím súborov LDAP Data Interchange Format (LDIF). Kým začnete túto procedúru, presuňte súbor LDIF na váš server iSeries ako súbor toku.

Pri importovaní súboru LDIF do adresárového servera vykonajte nasledujúce kroky:
1. Ak je spustený adresárový server, zastavte ho. Informácie o zastavení adresárového servera nájdete v "Zastavenie adresárového servera LDAP" na strane 20
2. V iSeries Navigator rozviňte **Sieť**.
3. Rozviňte **Servery**.
4. Kliknite na **TCP/IP**.
5. Pravým tlačidlom kliknite na **Adresár,** vyberte **Nástroje,** potom **Importovať súbor**.

Poznámka: Na importovanie súborov LDIF môžete použiť službu ldapadd .

Export súboru LDIF

Informácie možno presúvať medzi rôznymi adresárovými servermi LDAP použitím súborov LDAP vo formáte Data Interchange Format (LDIF), pozrite "Formát výmeny údajov LDAP" na strane 34. Do súboru LDIF môžete exportovať celý alebo jeho časť.

Ak chcete exportovať súbor LDIF z adresárového servera, postupujte takto:
1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Pravým tlačidlom kliknite na **Adresár,** vyberte **Nástroje**, potom **Exportovať Súbor**.

Poznámka: Ak nezadáte umiestnenie, kam má byť súbor LDIF exportovaný, uloží sa do štandardného adresára, ktorý je zadaný vo vašom OS/400 užívateľskom profile. Ak nezmeníte svoj štandardný adresár, štandardný adresár je root adresár.

Poznámky:

1. Uistite sa, že ste pre súbor LDIF nastavili také oprávnenie, ktoré zabráni neoprávnenému prístupu k údajom adresára. Ak to chcete urobiť, pravým tlačidlom kliknite na súbor v iSeries Navigator, potom vyberte **Povolenia**.
2. Úplný alebo čiastočný súbor LDIF môžete vytvoriť aj použitím služby ldapsearch, pozrite “Funkcia ldapsearch” na strane 52. Použite voľbu -L a presmerujte výstup do súboru.

Nastavenie novej repliky adresárového servera

Môžete nastaviť repliky adresárového servera LDAP na adresárové servery na ďalších serveroch iSeries. Directory Services používa na replikáciu štandardný protokol LDAP verzia 3.

Poznámky:

1. Nie je možná replikácia medzi servermi LDAP verzie 3 a verzie 2. Preto je potrebné, aby systém, do ktorého replikujete, používal tú istú verziu LDAP ako systém, z ktorého replikujete. V4R3 a V4R4 OS/400 podporujú LDAP verziu 2. V4R1 a novšie vydania podporujú LDAP verziu 3.
2. Môžete replikovať Directory Services adresár na IBM SecureWay V3.2 alebo novšie servery na iných platformách. Aby ste to mohli vykonať, váš adresárový server OS/400 musí byť nakonfigurovaný na použitie mechanizmu 3.2 ACI. Ak sa server stretne s problémom počas toho, ako sa snaží replikovať, zastaví replikáciu. Ak to nastane, vaša replika bude neúplná.

Pri nastavení novej repliky adresárového servera vykonajte tieto kroky:

1. Ak ste to už predtým nespravili, nakonfigurujte hlavný aj replikačný server.

   Poznámka: Skontrolujte, či sa na oboch serveroch zhodujú schéma a prípony.
2. Zastavte hlavný server.
3. (voliteľné) Pre počiatočnú replikáciu nastavte údaje LDAP. Tento krok môžete preskočiť, ak nemáte žiadne počiatočné údaje, ktoré by ste chceli presunúť z hlavného servera na jeho repliku.
4. (voliteľné) Na hlavný server presuňte údaje LDAP. Tento krok preskočte, ak sa niečo z ďalej uvedeného vzťahuje na vašu repliku servera:
   - Je novým adresárovým serverom LDAP.
   - Neobsahuje údaje, ktoré by ste chceli ďalej udržiavať.
5. Nastavte novú repliku servera.
6. Nastavte hlavný server tak, aby mal novú repliku.
7. Uistite sa, že hlavný server povoľuje aktualizácie:
   a. V iSeries Navigator rozviňte systém, na ktorom pracuje hlavný adresárový server.
   b. Rozviňte **Sieť**.
   c. Rozviňte **Servery**.
   d. Kliknite na **TCP/IP**.
   e. Kliknite pravým tlačidlom na **Adresár** a zvoľte **Vlastnosti**.
   f. Ak nie je začiarknuté **Povoliť aktualizovanie adresára**, začiarknite to.

Poznámka: Tento návod predpokladá, že obidva servery, hlavný aj replikovaný sú na systémoch, ktoré spravujete z iSeries Navigator na tom istom PC. Ak spravujete systémy z dvoch rôznych PC, môžete sa pre vykonanie tejto úlohy presúvať medzi dvoma PC. Ak sú hlavný alebo replikačný server spustené na operačnom systéme IBM inom než OS/400, pozrite si dokumentáciu pre túto platformu a nastavte tento server.

Nastavenie údajov LDAP pre úvodnú replikáciu

V hlavnom adresárovom LDAP serveri možno máte údaje, ktoré chcete pridať k novej replike servera. Najskôr musíte exportovať adresár do súboru LDIF. Kým sa súbor LDIF exportuje, musíte predísť aktualizácii hlavného servera. Môžete tak urobiť jedným z nasledujúcich spôsobov:

- Zastavte adresárový LDAP server. V závislosti od rozsahu údajov vo vašom adresári sa môže vyžadovať, aby váš server zostal zastavený po dlhšiu dobu.

- Zmeňte vlastnosti servera tak, aby sa nepovoľovali aktualizácie, čo umožní serveru ďalej odpovedať na požiadavky vyhľadávania, kým sa súbor LDIF exportuje. K tejto voľbe sa môžete dostať uvedeným postupom:
  1. V iSeries Navigator rozviňte systém, na ktorom pracuje hlavný adresárový server.
  2. Rozviňte **Sieť**.
  3. Rozviňte **Servery**.
  4. Kliknite na **TCP/IP**.
  5. Kliknite pravým tlačidlom na **Adresár** a zvoľte **Vlastnosti**.
  6. Ak je začiarknuté **Povoliť aktualizácie adresára**, odčiarknite to. Takto zabránite aktualizáciám adresára, až kým nie je replika úplne nastavená.
  7. Kliknite na **OK**.
  8. Zastavte a reštartujte adresárový LDAP server.

Ak ste zastavili server alebo zmenili vlastnosti servera, takže ste zablokovali aktualizácie adresára, vykonajte tieto úlohy:

1. Adresár exportujte do súboru LDIF.
2. Premiestnite LDIF súbor na systém, na ktorom bude pracovať replika servera.

Po premiestnení LDIF súboru na systém, na ktorom bude pracovať replika servera, je potrebné importovať dáta na repliku servera:

1. V iSeries Navigator rozviňte systém, na ktorom pracuje replika adresárového servera.
2. Ak ešte nie je zastavená replika servera, zastavte ju teraz. Stav serverov obnovujte dovtedy, pokiaľ nie je **Zastavený**.
3. Rozviňte **Sieť**.
4. Rozviňte **Servery**.
5. Kliknite na **TCP/IP**.
6. Kliknite pravým tlačidlom na **Adresár** a zvoľte **Vlastnosti**.
7. Ak ste nezačiarkli **Povoliť aktualizáciu adresára**, začiarknite to. Umožníte tak import údajov.
8. Kliknite na **OK**.
9. Importujte súbor LDIF, ktorý ste presunuli v kroku 2.
10. Kliknite pravým tlačidlom na **Adresár** a zvoľte **Vlastnosti**.
11. Odškrtnite **Povoliť aktualizácie adresára**.

Presun údajov LDAP na hlavný server

Ak nastavíte adresárový LDAP server ako repliku servera, strácate možnosť na ňom aktualizovať údaje. Ak máte údaje na serveri nakonfigurované tak, aby boli replikou adresárového LDAP servera, pravdepodobne ich presuniete na hlavný server, aby ste ich mohli naďalej uchovávať. V tomto prípade, postupujte podľa nasledujúcich krokov:

1. V iSeries Navigator rozviňte systém, na ktorom pracuje replika adresárového servera.
2. Rozviňte **Sieť**.
3. Rozviňte **Servery**.
4. Kliknite na **TCP/IP**.
5. Kliknite pravým tlačidlom na **Adresár** a zvoľte **Vlastnosti**.
6. Ak je začiarknuté **Povoliť aktualizácie adresára**, odškrtnite. Zabránite, aby sa aktualizoval adresár, pokiaľ nie je replika úplne nastavená.
7. Kliknite na **OK**.
8. Zastavte adresárový LDAP server.
9. Adresár exportujte do súboru LDIF.
10. Premiestnite LDIF súbor na systém, na ktorom bude pracovať hlavný server.

Po premiestnení LDIF súboru na systém, na ktorom bude pracovať hlavný server, je potrebné importovať dáta na hlavný server:

1. V iSeries Navigator rozviňte systém, na ktorom pracuje hlavný adresárový server.
2. Ak ešte nie je adresárový server zastavený, zastavte ho teraz. Stav serverov obnovujte dovtedy, pokiaľ nie je **Zastavený**.
3. Rozviňte **Sieť**.

4. Rozviňte **Servery**.
5. Kliknite na **TCP/IP**.
6. Kliknite pravým tlačidlom na **Adresár** a zvoľte **Vlastnosti**.
7. Ak ste nezaškrtli **Povoliť aktualizáciu adresára**, odškrtnite. Umožníte tak import údajov.
8. Kliknite na **OK**.
9. Importujte súbor LDIF, ktorý ste presunuli v kroku 10 na strane 24 predchádzajúceho postupu.
10. Kliknite pravým tlačidlom na **Adresár** a zvoľte **Vlastnosti**.
11. Odškrtnite **Povoliť aktualizácie adresára**.

Nastavenie novej repliky

Tento postup vykonajte pri nastavení novej repliky servera.

Poznámka: Replika servera musí byť nakonfigurovaná a zastavená predtým, ako vykonáte tento postup.

1. V iSeries Navigator rozviňte systém, na ktorom pracuje replika adresárového servera.
2. Rozviňte **Sieť**.
3. Rozviňte **Servery**.
4. Kliknite na **TCP/IP**.
5. Ak ešte nie je server zastavený, zastavte ho teraz. Stav serverov obnovujte dovtedy, pokiaľ nie je **Zastavený**.
6. Kliknite pravým tlačidlom na **Adresár** a zvoľte **Vlastnosti**.
7. Kliknite na záložku **Replikácia**.
8. Zvoľte **Použiť ako replika servera.**
9. V poli **Názov používaný hlavným serverom na aktualizácie** zvoľte názov hlavného servera, ktorý sa použije pri prihlasovaní na repliku servera pri vykonávaní aktualizácií. Môže to byť prihlasovacie meno (DN) alebo používateľ Kerberosu.

   Ak zvolíte DN:

   - Kliknite na tlačidlo **Heslo** vedľa poľa **Názov používaný hlavným serverom pre aktualizácie**. Zadajte heslo hlavného servera, ktoré použije pri prihlasovaní k replike servera pri vykonávaní aktualizácií.

     Poznámka: Poznačte si heslo a názov, ktorý ste zadali v kroku 9. Budete ich potrebovať pri nastavovaní hlavného servera na replikáciu.

   Ak zvolíte **Pridať používateľa Kerberos**:

   - Budete vyzvaný, aby ste zadali názov Kerberos (v tvare LDAP/*názov_hostiteľa*, kde *názov_hostiteľa* je plne kvalifikovaný názov hostiteľa hlavného servera) a štandardný realm (ako napríklad ACME.COM) hlavného servera.

     Poznámka: Ak chcete používať Kerberos, musíte mať povolený Kerberos na hlavnom aj replika serveri.
10. V poli **URL hlavného servera** zadajte názov hlavného servera vo formáte URL. Ak váš hlavný server používa port iný ako štandardný, zadajte číslo tohto portu ako časť URL.
11. Kliknite na záložku **Databáza/Prípony**. Ak sa prípona, ktorú chcete replikovať, nenachádza v zozname, pridajte ju tam.
12. (voliteľné) Ak chcete počas replikovania použiť Secure Sockets Layer (SSL) na povolenie SSL servera, použite Správcu digitálnych certifikátov. Správcu digitálnych certifikátov môžete naštartovať zo záložky **Sieť**. Ďalšie informácie o povoľovaní SSL adresárovému serveru nájdete v “Povolenie SSL na adresárovom serveri LDAP” na strane 15.
13. Kliknite na **OK**.

Nastavenie hlavného servera tak, aby ste mali novú repliku

Pri nastavovaní novej repliky hlavného servera vykonajte nasledujúce kroky.

Poznámka: Kým budete môcť vykonať túto procedúru, musíte mať svoj hlavný server nakonfigurovaný a spustený.

1. V iSeries Navigator rozviňte systém, na ktorom pracuje hlavný adresárový server.

2. Rozviňte **Sieť**.
3. Rozviňte **Servery**.
4. Kliknite na **TCP/IP**.
5. Kliknite pravým tlačidlom na **Adresár** a zvoľte **Vlastnosti**.
6. Ak nie je začiarknuté **Povoliť aktualizovanie adresára**, začiarknite to.
7. Kliknite na **OK**.
8. Zastavte, potom znovu naštartujte adresárový LDAP server. Obnovujte stav serverov dovtedy, kým nie je **Naštartovaný**.
9. Pravým tlačidlom znovu kliknite na **Adresár** a vyberte **Vlastnosti**.
10. Kliknite na záložku **Replikácia**. iSeries Navigator môže vyzvať, aby ste zadali informácie o pripojení. Zadajte tieto informácie a kliknite na **OK**.
11. Kliknite na **Pridať**.
12. V poli **Server** zadajte názov repliky servera vo formáte URL.
13. Zvoľte spôsob autentifikácie.

    Ak chcete použiť prihlasovacie meno (DN) a heslo:

    a. Zvoľte **Použiť DN a heslo**.

    b. V poli **Pripojiť ako** zadajte názov, ktorý ste špecifikovali v kroku 9 na strane 25 pri nastavovaní repliky servera.

    c. Kliknite na **Heslo** a zadajte heslo, ktoré ste špecifikovali v kroku 9 na strane 25 pri nastavovaní repliky servera.

    Ak chcete použiť Kerberos:

    - Zvoľte si **Použiť konto Kerberos hlavných serverov**. Hlavný server použije svoj názov principála Kerberos na autentifikáciu.

      Poznámka: Ak chcete používať Kerberos, musíte mať povolený Kerberos na hlavnom aj replika serveri.
14. Ak chcete pri replikovaní pre server použiť Secure Sockets Layer (SSL), použite Správcu digitálnych certifikátov. Správcu digitálnych certifikátov môžete naštartovať zo záložky **Sieť**. Ďalšie informácie o povoľovaní SSL adresárovému serveru nájdete v kapitole “Povolenie SSL na adresárovom serveri LDAP” na strane 15.
15. Ak replikačný server nepoužíva štandardný port, uveďte číslo portu v poli **Port**.
16. Ak nechcete repliku servera aktualizovať vždy, keď sa zmení záznam na hlavnom serveri, zvoľte **Čas**. Potom špecifikujte, frekvenciu aktualizácie repliky hlavným serverom.
17. Kliknite na **OK**.
18. Kliknite na záložku **Databáza**/**Prípony**. Ak sa prípona, ktorú chcete replikovať, nenachádza v zozname, pridajte ju tam.
19. Pre každú repliku servera povoľte aktualizáciu adresára:
    a. V iSeries Navigator rozviňte systém, na ktorom pracuje replika adresárového servera.
    b. Rozviňte **Sieť**.
    c. Rozviňte **Servery**.
    d. Kliknite na **TCP/IP**.
    e. Kliknite pravým tlačidlom na **Adresár** a zvoľte **Vlastnosti**.
    f. Ak ste nezačiarkli **Povoliť aktualizáciu adresára**, začiarknite to.
    g. Kliknite na **OK**.
20. Ak ešte nie je každá replika servera naštartovaná, naštartujte ich.

Poznámka: Server nemôže byť súčasne hlavným serverom aj replikačným serverom.

Publikovanie informácií na adresárový server

Váš systém môžete nakonfigurovať na publikovanie určitých informácií na adresárový server LDAP na tom istom alebo inom systéme. OS/400 tieto informácie automaticky publikuje na adresárový server LDAP, keď použijete iSeries Navigator na zmenu týchto informácií na OS/400. Informácie, ktoré možno publikovať,

zahŕňajú informácie o systéme (systémoch a tlačiarňach), zdieľaniach tlače a užívateľoch, ako aj politiku kvality služieb TCP/IP. Ďalšie informácie o kvalite služieb obsahuje časť Konfigurácia LDAP a QoS.

Ak rodičovský DN, do ktorého sa údaje publikujú, neexistuje, Directory Services ho automaticky vytvorí. Tiež si môžete inštalovať iné aplikácie OS/400, ktoré publikujú informácie do LDAP adresára. Prípadne z vlastných programov môžete zavolať rozhrania aplikačného programu (API) a uverejniť iné typy informácií do adresára LDAP.

Poznámky:

1. Keď konfigurujete OS/400 na publikovanie typu informácií užívateľov do adresárového servera LDAP, systém automaticky exportuje položky zo systémového distribučného adresára na server LDAP. AS/400 použije aplikačné rozhranie programu (API) QGLDSSDD. AS/400 tiež synchronizuje adresár LDAP so zmenami vykonanými v systémovom distribučnom adresári. Informácie o QGLDSSDD API obsahuje téma OS/400 adresárové služby pod Programovaním v iSeries Information Center. Dostupné informácie obsahujú toto:
   - Ako manuálne zavolať toto API.
   - Ako zabrániť exportovaniu špecifických používateľov na LDAP server.
   - Ako exportuje polia systémového distribučného adresára.
2. Keď konfigurujete OS/400 na publikovanie typu informácií systému do adresárového servera LDAP a vyberáte si na publikovanie jednu alebo viacero tlačiarní, systém automaticky zosynchronizuje adresár LDAP so zmenami vykonanými na týchto tlačiarňach na systéme. Publikovateľné informácie o tlačiarni môžu obsahovať umiestnenie tlačiarne, jej rýchlosť v stránkach za minútu, či podporuje duplex alebo farbu, jej typ a model a opis. Táto informácia pochádza z popisu zariadenia na systéme, ktorý je publikovaný. V sieťovom prostredí môžu používatelia použiť túto informáciu pri výbere tlačiarne.
3. Publikovať možno aj informácie OS/400 do adresárového servera, ktorý nie je na OS/400, ak konfigurujete tento server na použitie schémy IBM.

Postup konfigurácie vášho systému pre publikovanie informácií OS/400 na adresárovom LDAP serveri je takýto:

1. V iSeries Navigator kliknite pravým tlačidlom myši na váš systém a zvoľte **Vlastnosti**.
2. Kliknite na záložku **Directory Services**.
3. Kliknite na typy informácií, ktoré chcete uverejňovať.

   Tip: Ak na jedno miesto plánujete uverejňovať viac ako jeden typ informácií, ušetríte čas, ak počas jednej konfigurácie vyberiete viaceré typy informácií. Operations Navigator použije vami zadané hodnoty počas konfigurovania jedného typu informácií ako štandardné hodnoty pri konfigurácii ďalších typov informácií.
4. Kliknite na **Podrobnosti**.
5. Kliknite na začiarkovacie políčko **Publikovať systémové informácie**.
6. Špecifikujte **Metódu autentifikácie**, ktorú má váš server používať, ako aj dostatočné autentifikačné informácie.
7. Kliknite na tlačidlo **Upraviť** vedľa políčka **(Aktívny) Adresárový server**. Do dialógového okna, ktoré sa zobrazí, zadajte názov adresárového LDAP servera, kam chcete publikovať informácie OS/400 a potom kliknite na **OK**.
8. Do políčka **Pod DN** zadajte rodičovské prihlasovacie meno (DN), kam na adresárovom serveri chcete dané informácie pridať.
9. Vyplňte políčka v okne **Pripojenie servera**, ktoré sa týkajú vašej konfigurácie.

   Poznámka: Ak chcete publikovať informácie OS/400 na adresárovom serveri pomocou SSL alebo Kerberos, musíte mať predtým váš adresárový server nakonfigurovaný pre použitie daného protokolu. Viac informácií o SSL a Kerberose nájdete v “Použitie autentifikácie Kerberos s adresárovým serverom LDAP” na strane 39.
10. Ak váš adresárový server nepoužíva štandardný port, v poli **Port** zadajte správne číslo portu.
11. Kliknite na **Potvrdiť**, aby ste sa uistili, že rodičovské DN na serveri existuje a že informácie o pripojení sú správne. Ak adresárová cesta neexistuje, dialóg vás vyzve k jej vytvoreniu.

Poznámka: Ak neexistuje rodičovský DN a vy ho nevytvoríte, uverejňovanie nebude úspešné.

12. Kliknite na **OK**.

Poznámka: Publikovať možno aj informácie OS/400 do adresárového servera LDAP, ktorý sa nachádza na inej platforme. Musíte publikovať užívateľské a systémové informácie na adresárový server, ktorý používa schému kompatibilnú so schémou Directory Services. Definície schémy IBM SecureWay Directory zahŕňajúce adresárové služby iSeries možno nájsť na webovej stránke adresárových služieb.

Zdieľania tlače musíte publikovať do adresárového servera, ktorý podporuje schému aktívneho adresára Microsoftu. Publikovanie zdieľaní tlače do aktívneho adresára umožňuje užívateľom nakonfigurovať tlačiarne iSeries priamo z pracovnej plochy Windows 2000 pomocou sprievodcu pridávaním tlačiarne Windows 2000. Aby ste to mohli v sprievodcovi pridania tlačiarne urobiť, špecifikujte, že chcete nájsť tlačiareň v aktívnom adresári Windows 2000.

API pre publikovanie informácií OS/400 na adresárovom serveri

Directory Services poskytuje zabudovanú podporu publikovania užívateľských a systémových informácií. Tieto položky sú uvedené na stránke **Adresárové služby** systémového dialógu **Vlastnosti**. Môžete použiť konfiguráciu LDAP servera a publikačné API na to, aby mohli OS/400 programy, ktoré napíšete, publikovať iné typy informácií. Tieto typy informácií sa potom objavia aj na stránke **Adresárové služby**. Podobne ako užívatelia a systémy sú tieto na začiatku zakázané a pomocou rovnakej procedúry ich môžete nakonfigurovať. Program, ktorý pridáva údaje do adresára LDAP, sa nazýva uverejňujúci agent. Typ uverejnených informácií, zobrazený na stránke **Directory Services** sa nazýva názov agenta.

Uverejňovanie vám do vlastných programov umožnia zabudovať nasledujúce API :

QgldChgDirSvrA
Aplikácia používa formát CSVR0500 s cieľom pridať na začiatku názov agenta, ktorý je označený ako zakázaná položka. Inštrukcie pre užívateľov aplikácie by im mali dať pokyn na použitie iSeries Navigator na prechod na stránku vlastností adresárových služieb na konfiguráciu publikujúceho agenta. Príklady názvov agentov sú názvy agentov systémov a používateľov automaticky dostupné na strane **Adresárové služby**.

QgldLstDirSvrA
Pomocou tohto formátu API LSVR0500 uveďte, ktorí agenti sú momentálne dostupní na vašom systéme.

QgldPubDirObj
Toto API použite na aktuálne uverejnenie informácií.

Podrobné informácie o týchto API obsahuje téma LDAP (Lightweight Directory Access Protocol) pod Programovaním v iSeries Information Center.

Zadanie servera pre adresárové referály

Na pridelenie referenčných serverov pre adresárový server vykonajte nasledujúce kroky:

1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Pravým tlačidlom kliknite na **Adresár**, potom vyberte **Vlastnosti**.
5. Kliknite na **Pridať**.
6. Uveďte názov referenčného servera vo formáte URL. Nasledujú príklady prijateľných LDAP URL:
   - ldap://test.server.com
   - ldap://test.server.com:400
   - ldap://9.9.99.255

   Poznámka: Ak referálový server nepoužíva štandardný port, uveďte správne číslo portu ako súčasť adresy, keďže port 400 je uvedený v druhom vyššie uvedenom príklade.

7. Kliknite na **OK**.

Pridávanie prípon do adresárového servera LDAP

Pridaním prípony do adresárového LDAP serveru umožníte serveru riadiť danú časť adresárového stromu.

Poznámka: Nemôžete pridávať príponu, ktorá sa už nachádza na serveri pod ďalšou príponou. Ak boli napríklad o=ibm, c=us príponou na vašom serveri, nemôžete pridávať ou=rochester, o=ibm, c=us.

Na pridanie prípony do adresárového servera vykonajte tieto kroky:
1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Kliknite pravým tlačidlom na **Adresár** a zvoľte **Vlastnosti**.
5. Kliknite na záložku **Databáza**/**Prípony**.
6. V poli **Nová prípona** napíšte názov novej prípony.
7. Kliknite na **Pridať**.
8. Kliknite na **OK**.

Poznámka: Pridanie prípony nasmeruje server do časti adresára, ale nevytvorí žiadne objekty. Ak objekt, ktorý zodpovedá novej prípone predtým neexistoval, musíte ho vytvoriť rovnako, ako by ste vytvorili hocijaký iný objekt.

Odstraňovanie prípon z adresárového servera

Na odstránenie prípony z adresárového LDAP servera vykonajte nasledujúce kroky:
1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Kliknite pravým tlačidlom na **Adresár** a zvoľte **Vlastnosti**.
5. Kliknite na záložku **Databáza**/**Prípony**.
6. Kliknite na príponu, ktorú chcete odstrániť a vyberte ju.
7. Kliknite na **Odstrániť**.

Poznámka: Môžete si zvoliť vymazanie prípony bez vymazania objektov adresára, ktoré sú pod ňou. To zmení údaje na neprístupné z adresárového servera. Avšak spätným pridaním prípony môžete neskôr tieto údaje získať znova.

Ukladanie a obnova Directory Services informácií

Directory Services ukladá informácie na nasledujúce miesta:

- Knižnica databázy (QUSRDIRDB by default), ktorá obsahuje obsah adresárových serverov.
- Knižnica QDIRSRV2, ktorá slúži na ukladanie publikačných informácií.
- Knižnica QUSRSYS, ktorá uchováva rôzne položky v objektoch začínajúcich na QGLD (pre ich uloženie zadajte QUSRSYS/QGLD*).
- Ak konfigurujete adresárový server na protokolovanie zmien adresára, používa sa databázový server s názvom QUSRDIRCL, ktorý používa protokol zmien.

Ak sa obsah adresára pravidelne mení, mali by ste si pravidelne ukladať databázovú knižnicu a objekty v nej. Konfiguračné údaje sú uložené v adresári:

```
/QIBM/UserData/OS400/Dirsrv/
```

Pri každej zmene konfigurácie alebo používaní PTF by ste mali uložiť v tomto adresári aj súbory.

Pozrite si Zálohovanie a obnova, SC41-5304 , kde nájdete informácie o ukladaní a obnove OS/400 údajov.

Riadenie vlastníctva a prístupu k adresárovým údajom

Riadenie vlastníctva a prístupu k adresárovým údajom pozostáva z nasledujúcich činností:
- "Práca s vlastnosťami vlastníctva adresárových objektov"
- "Práca s ACL (zoznamami riadenia prístupov)"
- "Práca so skupinami ACL"

Práca s vlastnosťami vlastníctva adresárových objektov

Na nastavenie vlastností vlastníctva adresárových objektov vykonajte tieto kroky:
1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Kliknite pravým tlačidlom na **Adresár** a vyberte **Oprávnenia**.

   Ak ešte nie ste pripojený k adresárovému serveru, objaví sa dialóg **Pripojiť k adresárovému serveru**. Pripojte sa ako správca servera alebo ako vlastník objektu, s ktorého vlastnosťami vlastníctva chcete pracovať.
5. Z adresárového stromu vyberte objekt, s ktorého vlastnosťami vlastníctva chcete pracovať a kliknite na **OK**.

Práca s ACL (zoznamami riadenia prístupov)

Práca so zoznamami riadenia prístupu (ACL) zahŕňa pripojenie explicitných a implicitných objektov adresára, pridanie používateľov ACL, odstránenie z ACL a prehľadávanie objektov adresára. Všimnite si, že od V5R1 Directory Services podporuje nový model ACL, takže, aj keď ste už predtým používali ACL, možno sa budete chcieť s nimi znova oboznámiť.

Ak chcete pracovať s ACL, vykonajte nasledujúce kroky:
1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Kliknite pravým tlačidlom na **Adresár** a vyberte **Oprávnenia**.

   Ak ešte nie ste pripojený k adresárovému serveru, objaví sa dialóg **Pripojiť k adresárovému serveru**. Pripojte sa ako správca servera alebo ako vlastník objektu, s ktorého ACL chcete pracovať.
5. Z adresárového stromu vyberte objekt, s ktorého ACL chcete pracovať, potom kliknite na **OK**.
6. Kliknite na záložku **ACL**.

Práca so skupinami ACL

Ak chcete pracovať so Skupinami ACL, vykonajte nasledujúce kroky:
1. V iSeries Navigator vyberte **Sieť**.
2. Vyberte **Servery**.
3. Kliknite na **TCP/IP**.
4. Kliknite pravým tlačidlom na **Adresár** a vyberte **Skupiny ACL**.

Práca s prístupom správcu pre oprávnených užívateľov

| Od V5R2 môžete udeliť správcovi prístup na užívateľské profily, ktorým bol udelený prístup na identifikátor
| (ID) funkcie správcu adresárových služieb (QIBM_DIRSRV_ADMIN).

| Ak je napríklad užívateľskému profilu JOHNSMITH udelený prístup na ID funkcie správcu adresárových
| služieb a z dialógu Vlastnosti adresára bola vybraná voľba Udeliť prístup správcu oprávneným užívateľom,
| profil JOHNSMITH má potom oprávnenie správcu LDAP. Keď sa tento profil použije na pripojenie k
| adresárovému serveru pomocou nasledujúceho DN, os400-profile=JOHNSMTH,cn=accounts,os400-

sys=systemA.acme.com, užívateľ bude mať oprávnenie správcu. Prípona systémových objektov bude v tomto príklade os400-sys=systemA.acme.com. Ďalšie informácie o projektovaných užívateľoch obsahuje časť “Projektované pozadie operačného systému” na strane 40.

Ak si chcete zvoliť túto voľbu, postupujte takto:

1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite pravým tlačidlom myši na **Adresár** a zvoľte si **Vlastnosti**.
4. Na záložke **Všeobecné** pod **Informáciami správcu** si zvoľte voľbu **Udeliť prístup správcu oprávneným užívateľom**.

Ak chcete nastaviť ID funkcie oprávnenia správcu adresárových služieb, postupujte takto:

1. V iSeries Navigator kliknite pravým tlačidlom myši na systémový názov a zvoľte si **Správu aplikácie**.
2. Kliknite na záložku **Hostiteľské aplikácie**.
3. Rozviňte **Operating System/400**.
4. Kliknite na **Správcu adresárových služieb** a vysvieťte voľbu.
5. Kliknite na tlačidlo **Upraviť**.
6. Rozviňte **Užívateľov**, **Skupiny** alebo **Použitia, ktoré nie sú v skupine**, podľa toho, čo sa hodí pre užívateľa, ktorého si želáte.
7. Zvoľte si užívateľa alebo skupinu, ktorú chcete pridať na zoznam **Povolených prístupov**.
8. Kliknite na tlačidlo **Pridať**.
9. Kliknutím na **OK** uložte zmeny.
10. Kliknite na **OK** v dialógu **Správa aplikácie**.

Sledovanie prístupu a zmien v adresári LDAP

Možno budete chcieť sledovať prístup a zmeny na vašom adresári LDAP. Ak chcete sledovať zmeny v adresári, môžete použiť protokol zmien adresárov LDAP. Protokol zmien je umiestnený pod špeciálnou príponou cn=changelog. Je uložený v knižnici QUSRDIRCL.

Pri sprístupňovaní protokolu zmien vykonajte nasledujúce kroky:

1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Kliknite pravým tlačidlom na **Adresár** a zvoľte **Vlastnosti**.
5. Kliknite na záložku **Adresár/Prípony**.
6. Vyberte **Protokolovať zmeny adresára**.
7. (voliteľné) V možnosti **Maximum položiek** zadajte maximálny počet položiek, ktoré má protokol zmien uchovať.

   Poznámka: Hoci je tento parameter voliteľný, dobre zvážte zadanie maximálneho počtu položiek. Ak nezadáte maximálny počet položiek, protokol zmien uchová všetky položky a môže sa príliš zväčšiť.

Trieda objektov changeLogEntry sa používa na reprezentovanie zmien použitých v adresárovom serveri. Súbor zmien je daný nariadeným súborom všetkých položiek v rámci kontajnera changelog, ako sa definuje v changeNumber. Informácie protokolu zmien sú určené len na čítanie.

Ktorýkoľvek používateľ, ktorý je na Zozname riadeného prístupu pre príponu cn=changelog, môže vyhľadávať v položkách v protokole zmien. Mali by ste vyhľadávať iba príponu protokolu zmien, cn=changelog. Nepokúšajte sa pridávať, meniť alebo vymazať príponu protokolu zmien, aj keď na to máte oprávnenie. Spôsobí to nepredvídateľné následky.

Príklad:

Nasledujúci príklad používa vlastnosť príkazového riadka ldapsearch na obnovu všetkých položiek protokolu zmien, zaprotokolovaných v serveri:

```
ldapsearch -h ldaphost -D cn=admininistrator -w password -b cn=changelog  (changetype=*)
```

Povoliť auditovanie objektu pre adresárový server

Directory Services podporuje OS/400 auditovanie bezpečnosti. Ak je systémová hodnota QAUDCTL nastavená na *OBJAUD, môžete aktivovať audit objektov pomocou iSeries Navigator.

Ak chcete umožniť audit objektov pre Directory Services, postupujte podľa nasledujúcich krokov:
1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Kliknite pravým tlačidlom na **Adresár** a zvoľte **Vlastnosti**.
5. Kliknite na zložku **Auditovanie**.
6. Zvoľte nastavenie auditovania, ktoré chcete pre svoj server používať.

Zmeny nastavení auditovania budú platné hneď po kliknutí na **OK**. Nie je potrebné reštartovať LDAP adresárový server. Ďalšie informácie obsahuje časť “Directory Services bezpečnosť” na strane 38

Úprava výkonu adresárového servera LDAP

Výkon adresárového LDAP servera môžete nastaviť zmenou nasledujúcich premenných:
- Veľkosť hľadania
- Maximálny čas povolený na hľadanie
- Nastavenie transakcie serverov
- Počet databázových pripojení a serverových vláken

Pri nastavovaní výkonnostných hodnôt adresárového servera vykonajte tieto kroky:
1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Kliknite pravým tlačidlom na **Adresár** a zvoľte **Vlastnosti**.
5. Kliknite na záložku **Výkonnosť**.

Výkon adresárového servera môžete upraviť aj zmenou počtu databázových pripojení a serverových vláken, ktoré server používa. Túto hodnotu zmeníte nasledujúcim postupom:
1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Kliknite pravým tlačidlom na **Adresár** a zvoľte **Vlastnosti**.
5. Kliknite na záložku **Databáza**/**Prípony**.

Kapitola 5. Koncepty Directory Services a referenčné informácie

Nasledujúce koncepčné a referenčné informácie vám pomôžu spoznať a spúšťať váš LDAP server Directory Services:

Základné informácie o LDAP a plánovaní vášho LDAP servera nájdete v Kapitola 3, "Začíname s Directory Services" na strane 7.

Zoznamy riadenia prístupu (ACL) LDAP

Vo väčšine prípadov pravdepodobne nebudete chcieť zamedziť prístup k údajom v adresári vášho LDAP servera. Napríklad: LDAP server intranetu vašej firmy môže obsahovať telefónny zoznam zamestnancov firmy. Asi chcete, aby si všetci zamestnanci mohli prezrieť údaje v tomto adresári.

Prezident spoločnosti však nechce, aby mali všetci zamestnanci prístup na jeho telefón. V tomto prípade môžete vytvoriť **zoznam riadenia prístupu (ACL)**. S takýmto ACL môžete obmedziť prístup k jeho serveru len na tých ľudí, od ktorých chce riaditeľ prijímať hovory.

S ACL tiež môžete kontrolovať práva osôb na pridávanie a vymazávanie objektov adresára. Ďalej môžete určovať, či používatelia môžu čítať, zapisovať, prehľadávať a porovnávať adresárové atribúty. ACL môže byť zdedený alebo explicitný. Znamená to, že môžete použiť ACL jedným z nasledujúcich spôsobov:

- Pre daný objekt explicitne nastavte ACL.
- Určte, že objekty zdedia ACL od objektov, ktoré sa nachádzajú vyššie v hierarchii adresára LDAP.

Možno prezident v predchádzajúcom príklade nechcel, aby mali všetci zamestnanci prístup k jeho telefónu. Želal si ale, aby tento prístup mali všetci manažéri. V takomto prípade môžete použiť **Skupinu ACL** na zjednodušenie udeľovania práv manažérom. Skupiny ACL vám umožňujú udeliť prístup špecifickým skupinám používateľov a vy nemusíte udeľovať práva jednotlivcom. Toto je vhodné v tých prípadoch, keď rovnaká skupina ľudí potrebuje prístup k viac ako jednému súboru objektov. Ak tí istí manažéri, ktorí mali prístup k telefónu prezidenta, potrebovali neskôr prístup napríklad k platovým položkám, mohli by ste znova použiť skupinu ACL.

Modely ACL

Všetky verzie Directory Services podporujú model povolení úrovne triedy prístupu. Pod týmto modelom má každý typ atribútu LDAP normálnu, citlivú alebo dôležitú klasifikáciu. Schéma atribútov súborov túto klasifikáciu kontroluje. Keď ste pridali užívateľa na ACL objektov, uvediete, ktoré klasifikácie môže užívateľ čítať, zapisovať, hľadať a porovnávať. Vo väčšine schém by bolo telefónne číslo klasifikované ako normálny atribút. Preto, ak chcete poskytnúť manažérom vo vyššie uvedenom príklade prístup na prezidentovo telefónne číslo, mali by ste im poskytnúť prístup na čítanie na normálne atribúty v objekte adresára prezidenta. Ešte stále by však nemali prístup k citlivým a dôležitým informáciám. Všetky verzie Directory Services podporujú nastavenie povolení úrovne triedy prístupu.

Directory Services tiež podporuje model povolení úrovne atribútov. Pri tomto modeli môžete špecifikovať právomoci na čítanie, zapisovanie, vyhľadávanie a porovnávanie pre špecifické atribúty, nezávisle od ich triedy prístupu. Predstavte si znovu vyššie uvedený príklad. Pod modelom povolení úrovne atribútov by ste mohli manažérom poskytnúť prístup na čítanie na atribút telephoneNumber aj vtedy, keď vo všeobecnosti nemali prístup k normálnym atribútom.

Model povolení úrovne atribútov je kompatibilný len so SecureWay Directory Services verziou 3.2 a vyššie uvedenými servermi. Štandardne toto nie je povolené. Voľbu povoliť budete mať, keď pracujete s ACLwork with ACLs. Po jeho aktivovaní môže byť model deaktivovaný len rekonfiguráciou servera a obnovením databázy adresárov. Predtým, ako sa rozhodnete aktivovať tento model, uvedomte si, že ho nebudete môcť spravovať zo žiadneho LDAP V2 klienta (vrátane starších verzií iSeries Navigator ako je V5R1), a že ak sa o to pokúsite, môže dôjsť k poškodeniu ACL záznamov.

Špeciálne hodnoty ACL

Všetky objekty v adresári Directory Services servera majú pôvodne ACL, ktoré obsahuje špeciálnu skupinu ACL, CN=Anybody, obsahujúcu všetkých používateľov adresára. Štandardne má táto skupina nastavený prístup na čítanie, vyhľadávanie a porovnávanie k atribútom normálnej triedy pre všetky objekty.

Možno chcete, aby niektoré objekty mali rovnaké prístupové povolenia pre všetkých používateľov, ktorí sú viazaní k adresárovému serveru spojením, ktoré nie je anonymné. V tomto prípade použite špeciálny zoznam riadeného prístupu (ACL) skupina cn=Authenticated.

Ak chcete určiť, aké prístupové povolenia má objekt pre seba, môžete použiť špeciálny cn=this. To umožňuje ″detským″ položkám, ktoré zdedia ich ACL, aby boli automaticky oprávnené vykonať operácie na svojich vlastných objektoch.

Ďalšie informácie

Pri spravovaní ACL pomocou iSeries Navigator nemusíte poznať všetky podrobnosti, napríklad ako Directory Services implementuje ACL. Avšak, ak chcete pri používaní súborov LDIF špecifikovať atribúty súvisiace s ACL alebo chcete používať ACL s programami príkazového riadka LDAP, budete sa potrebovať zoznámiť s atribútmi, ktoré používa ACL. Informácie o atribútoch ACL nájdete v časti Referenčný dokument ACL dokumentácie IBM SecureWay Directory Management Tool documentation.

Ďalšie informácie o nastavovaní a zmene ACL a skupín ACL, nájdete v častiach:
“Práca s ACL (zoznamami riadenia prístupov)” na strane 30
“Práca so skupinami ACL” na strane 30

Formát výmeny údajov LDAP

Formát výmeny údajov ODAP (LDIF) poskytuje jednoduchý spôsob prenosu adresárových informácií medzi adresárovými servermi LDAP. Súbory LDIF obsahujú položky adresárov LDAP v jednoduchom textovom formáte. Formát LDIF súborov, ktoré používa adresárový server, sa mierne od V4R5 pre AS/400 Directory Services zmenil. Directory Services Súbory LDIF obsahujú postupnosť riadkov, ktoré popisujú položku adresára alebo súbor zmien do položky adresára. Nemôžu popisovať obe.

Všeobecný formát položky LDIF je:

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

kde:

- *verzia* zobrazuje verziu formátu LDIF pre súbor. Číslo verzie musí byť 1. Ak chýba, predpokladá sa, že súbor LDIF sa nachádza v staršom formáte súboru LDIF. Keď má súbor LDIF verziu 1, obsah MUSÍ byť zakódovaný prostredníctvom UTF-8.
- *rozoznaný názov (DN)* je rozoznaný názov (DN) adresárovej položky
- *attrtype1* je typ atribútu LDAP (buď cn alebo ou)
- *attrvalue1* je hodnota atribútu

Každý záznam má niekoľko atribútov. Každý atribút sa objavuje na samostatnom riadku. Ak je hodnota atribútu dlhšia ako jeden riadok, táto môže pokračovať na nasledujúcom riadku a predchádza jej znak medzery alebo tabelátora.

Prázdne riadky oddeľujú viaceré položky v rámci jedného súboru LDIF. Každý riadok, ktorý sa začína znakom libry (#), je komentárovým riadkom a pri analýze súboru LDIF musí byť ignorovaný.

Všetky rozoznané názvy alebo hodnoty atribútu, ktoré spĺňajú jednu z nasledujúcich podmienok, by mali byť zakódované na základe 64:
- Obsahuje návraty vozíka alebo riadkovače.
- Začína sa dvojbodkou (:), SPACE alebo menej než (<).
- Končí medzerou.

Atribúty zakódované na základe 64 sú určené použitím dvoch dvojbodiek medzi názvom atribútu a hodnotou.

Externé referencie sú vo formáte súbor:// URL. Znaky dvojbodky a menej než (:<) by sa mali nachádzať medzi typom atribútu a externou referenčnou hodnotou.

Vzory súborov LDIF:

Príklad 1: Jeden súbor LDAP s dvoma položkami

```
verzia: 1
   dn: cn=Barbara Jensen, ou=Rochester, o=Big Company, c=US
   objectclass: top
   objectclass: person
   objectclass: organizationalPerson
   cn: Barbara Jensen
   cn: Barbara J Jensen
   cn: Babs Jensen
   sn: Jensen
   uid: bjensen
   telephonenumber: +1 408 555 1212
   description: Veľký fanúšik plachtenia.

   dn: cn=Bjorn Jensen, ou=Rochester, o=Big Company, c=US
   objectclass: top
   objectclass: person
   objectclass: organizationalPerson
   cn: Bjorn Jensen
   sn: Jensen
   telephonenumber: +1 408 555 1212
   description:Babs je fanúšik plavby a veľa cestuje za
   vyhľadávaním dokonalých plavebných podmienok.
   title:Product Manager, Rod and Reel Division
```

Príklad 2: Súbor obsahujúci hodnotu zakódovanú na základe 64

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

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

Príklad 3: Súbor obsahujúci sériu záznamov zmien a komentárov

Poznámka: LDIF súbory so záznamami zmien sa nedajú importovať do servera priamo. Sú však podporované shell programami LDAP.

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

   # Vymazať existujúcu položku
   dn: cn=Robert Jensen, ou=Rochester, o=Big Company, c=US
   changetype: delete

   # Zmeniť položky týkajúce sa charakteristického názvu
   dn: cn=Paul Jensen, ou=Rochester, o=Big Company, c=US
   changetype: modrdn
   newrdn: cn=Paula Jensen
   deleteoldrdn: 1
```

Poradie položiek v súbore LDIF je dôležité. Ak má byť pridanie položky špecifikovanej v súbore LDIF k adresáru LDAP úspešné, musí jeho rodičovský záznam najprv existovať v priestore názvov adresára. V predchádzajúcom príklade by druhý a tretí záznam nemohli byť pridané, keby neexistoval prvý záznam.

Podobne, na importovanie súboru LDIF do servera podporujúceho isté prípony, musí súbor LDIF obsahovať záznamy pre tieto prípony. Napríklad ak váš server mal príponu ou=Rochester, o=Big Company, c=US, súbor LDIF ukázal, že predtým uvedené záznamy možno importovať. Ak mal váš server príponu o=Big Company, c=US, musíte mať záznam pre danú príponu najprv špecifikovaný v súbore LDIF, ako sa uvádza v tomto prípade:

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

Špecifický formát a obsah súborov LDIF je určený schémou servera, z ktorého sú exportované. Súbor LDIF môžete importovať do akéhokoľvek LDAP servera používajúceho identickú schému ako server, z ktorého bol súbor exportovaný. Rôzni predajcovia serverov LDAP používajú rozdielnu schému (s rozdielnymi triedami objektov a atribútmi). Preto sa vám nemusí podariť import súboru LDIF, vytvoreného na jednom serveri, na iný server.

Požiadavka na komentáre (RFC) pre špecifikácie súborov LDIF je dostupná na nasledujúcej URL:

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

Podobné postupy:

“Import súboru LDIF” na strane 22
“Export súboru LDIF” na strane 22

Charakteristiky národnej jazykovej podpory (NLS)

Od V4R5 je OS/400 server adresárových služieb LDAP aj OS/400 klient LDAP založený na verzii 3 LDAP. Oboznámte sa s nasledujúcimi úvahami NLS.

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

Ďalšie informácie o UCS-2 obsahuje téma Globalizácia pod Plánovaním v iSeries Information Center.

Vlastníctvo objektov adresára LDAP

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

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

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

Podobné postupy:

"Práca s vlastnosťami vlastníctva adresárových objektov" na strane 30

Odkazy adresára LDAP

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

Directory Services vám umožňuje použiť dva rôzne typy odvoláviek. Môžete zadať štandardné referenčné servery, kde LDAP server ohlási klientovi vždy, keď v adresári nebude žiadny DN. Vášho klienta LDAP môžete použiť aj na pridávanie položiek do adresárového servera, ktorý má referál objectClass. Umožní vám to uviesť referály založené na tom, ktorý špecifický DN klient požaduje.

Poznámka: Pri Directory Services musia obsahovať objekty odvoláviek len tieto atribúty: prihlasovacie meno (dn), triedu objektu (objectClass) a odvolávku (ref). Ak si chcete pozrieť príklady, ktoré ilustrujú toto obmedzenie, nájdite "Funkcia ldapsearch" na strane 52.

Odvolávkové servery sa vzťahujú na replikačné servery. Pretože údaje na replikačných serveroch nemôžu klienti meniť, replikačný server odkáže každú požiadavku na zmenu servera na hlavný server.

Transakcie

Môžete nakonfigurovať adresárový server LDAP vašich systémov na povolenie klientom používať transakcie. Transakcia je skupina adresárových operácií LDAP, s ktorými sa narába ako s jedným celkom. Žiadna z jednotlivých operácií LDAP, ktoré tvoria transakciu, nie je trvalá, pokiaľ neboli všetky operácie v transakcii dokončené úspešne a celá transakcia dokončená. Ak zlyhá hociktorá z operácií alebo je transakcia zrušená, ostatné operácie sa vrátia späť. Táto schopnosť môže pomôcť používateľom udržať LDAP operácie organizované. Napríklad, používateľ môže vytvoriť transakciu na svojom klientovi, ktorá vymaže niekoľko

adresárových záznamov. Ak klient stratí spojenie so serverom počas tejto transakcie, žiadny zo záznamov nie je vymazaný. Používateľ môže preto jednoducho začať transakciu znovu namiesto toho, aby musel kontrolovať, ktoré záznamy boli úspešne zmazané.

Časťou transakcie môžu byť nasledujúce LDAP operácie:

- pridať
- upraviť
- upraviť RDN
- vymazať

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

Ďalšie informácie o transakciách obsahuje dodatok Obmedzená podpora transakcií IBM SecureWay Directory Client SDK Programming Reference .

Replika adresárového LDAP servera

Informácie uložené na replikačných adresárových serveroch LDAP sú totožné s informáciami na vašom hlavnom adresárovom serveri LDAP. Ak máte jednu alebo viacero replík svojho adresára LDAP, môžete využiť dve výhody:

- Repliky umožňujú rýchlejšie prehľadávanie adresárov. Namiesto toho, aby všetci klienti smerovali vyhľadávacie požiadavky na jeden hlavný server, môžete požiadavky rozdeliť medzi hlavný server a repliky servera.
- Repliky poskytujú hlavnému serveru zálohu. Ak je hlavný server nedostupný, replika stále môže odpovedať na vyhľadávacie požiadavky a poskytnúť prístup k údajom adresára.

Repliky servera sú len na čítanie. Keď sa oprávnený používateľ pokúša zmeniť záznam na replike servera, replika sa s požiadavkou odvolá na hlavný server.

Podobné postupy:

"Nastavenie novej repliky adresárového servera" na strane 23

Directory Services bezpečnosť

Auditovanie bezpečnosti

Od verzie V5R1, Directory Services podporuje OS/400 auditovanie bezpečnosti. Auditovateľné sú nasledujúce položky:

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

Možno budete musieť vykonať zmeny nastavenia auditu vášho OS/400, až potom môže audit položiek adresára fungovať. Ak je systémová hodnota QAUDTL nastavená na *OBJAUD, môžete umožniť

auditovanie objektov pomocou iSeries Navigator. Informácie o audite si pozrite v časti *Bezpečnosť - odkaz*  alebo v téme Auditovanie bezpečnosti v iSeries Information Center.

Autentifikácia pripojenia a bezpečnosti

Directory Services zabezpečuje nasledujúce mechanizmy, ktoré môžete použiť na podporenie bezpečnosti komunikácie medzi klientmi LDAP a adresárovým serverom LDAP:

- Pripojenia Secure Sockets Layer (SSL)
- Autentifikácia Kerberosom
- Šifrovanie hesiel CRAM-MD5

Použitie SSL (Secure Sockets Layer) a Translation Layer Security s adresárovým serverom LDAP

Ak chcete s vašim adresárovým serverom bezpečnejšie komunikovať, Directory Services môže použiť zabezpečenie Secure Sockets Layer (SSL).

Aby ste mohli používať SSL s Directory Services, musíte mať na svojom systéme nainštalovaný jeden z produktov Poskytovateľa šifrovaného prístupu (5722-ACx). Ak chcete používať SSL z iSeries Navigator, musíte tiež mať na svojom PC nainštalovaný jeden z produktov šifrovania klientov (5722-CEx). Tento softvér potrebujete vtedy, ak chcete vykonávať jednu z nasledujúcich činností:

- Z vašej pracovnej stanice použitím spojenia SSL konfigurovať a spravovať Directory Services. Tento postup obsahuje úlohy, ktoré vykonávate s iSeries Navigator.
- Použiť pripojenie SSL s aplikáciami, ktoré vytvárate s aplikačnými programovými rozhraniami (API) klienta Windows.

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

Ak chcete použiť SSL, musíte mať na vašom systéme nainštalovanú voľbu 34 DCM (Manažér digitálnych certifikátov) OS/400. DCM je rozhraním na vytváranie a riadenie digitálnych certifikátov a skladov certifikátov. Informácie o digitálnych certifikátoch a o použití DCM (Správca digitálnych certifikátov) nájdete v dokumentácii pre Správca digitálnych certifikátov. Informácie o SSL na iSeries nájdete v Zabezpečenie aplikácií pomocou SSL. Informácie o TLS na serveri iSeries nájdete v protokoloch podporovaných SSL a TLS (Transport Layer Security).

Použitie autentifikácie Kerberos s adresárovým serverom LDAP

Directory Services vám umožňuje nastaviť adresárový server LDAP na použitie autentifikácie Kerberos. Kerberos je sieťový autentifikačný protokol, ktorý používa kryptografiu tajnými kľúčmi, čím sa zabezpečuje silná autentifikácia klient/server aplikácií.

Aby ste mohli umožniť autentifikáciu Kerberosom, musíte mať na vašom systéme inštalovaný jeden z produktov poskytovateľa kryptografických služieb (5722AC2 alebo 5722AC3). Tiež musíte mať nakonfigurovanú službu sieťovej autentifikácie.

Podpora Kerberosu pre Directory Services zabezpečuje podporu pre mechanizmus GSSAPI SASL. To povoľuje klientom SecureWay a Windows 2000 LDAP používať autentifikáciu Kerberos s adresárovým serverom LDAP.

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

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

názov služby je LDAP, názov hostiteľa je plne kvalifikovaný názov TCP/IP systému a realm je štandardný realm uvedený v konfigurácii systémov Kerberos.

Napríklad, pre systém s názvom my-as400 v TCP/IP doméneacme.com, so štandardným realmom Kerberosu ACME.COM, by bol názov principálu Kerberosu LDAP servera LDAP/my-as400.acme.com@ACME.COM. Štandardný realm Kerberos je uvedený v konfiguračnom súbore Kerberos (štandardne /QIBM/UserData/OS400/NetworkAuthentication/krb5.conf) s direktívou default_realm (default_realm = ACME.COM). Podľa konvencie používajú názvy realmov Kerberosu veľké písmená a názvy hostiteľov používajú malé písmená. LDAP/ musí mať veľké písmená. Adresárový server nemožno nakonfigurovať, aby používal autentifikáciu Kerberosom, ak nebol nakonfigurovaný štandardný realm.

Pri použití autentifikácie Kerberosom priraďuje adresárový LDAP server rozoznaný názov (DN) k pripojeniu, ktoré určuje prístup k údajom adresárov. Môžete si zvoliť, aby bol rozoznaný názov servera priraďovaný jedným z nasledujúcich postupov:

- Server môže vytvoriť DN založený na ID Kerberosu. Keď si vyberáte túto voľbu, identita Kerberos v tvare principal@realm generuje DN v tvare ibm-kn=principal@realm. ibm-kn= je ekvivalent k ibm-kerberosName=.
- Server môže hľadať v adresári rozoznaný názov (DN), ktorý obsahuje záznam pre principál Kerberosu a realm. Ak si zvolíte túto možnosť, server hľadá v adresári záznam, ktorý špecifikuje identitu Kerberos takto:
  - Server hľadá adresár pre objekt krbRealm-V2 s atribútom krbRealmName-V2 vyhovujúcim realmu Kerberos. Ak sa takáto položka nájde, potom hľadá DN uvedené v atribúte princSubtree pre položku s atribútom krbPrincipalName, ktorá sa zhoduje s názvom principálu a realmu. Ak DN nakonfigurované v krbAliasedObjectName obsahuje DN predtým nájdenej položky, použije sa DN nakonfigurované v krbAliasedObjectName. V opačnom prípade sa použije DN položky. Tento postup sa zvyčajne používa, keď KDC Kerberosu ukladá do adresára LDAP informácie o principále Kerberosu.
  - Ak vyššie uvedené hľadanie zlyhá, server bude hľadať položku adresára, ktorá používa pomocnú triedu ibm-securityIdentities a má hodnotu atribútu altSecurityIdentities KERBEROS:principal@realm. Tento postup sa môže použiť na priradenie identít Kerberos k záznamom adresárov, keď KDC neukladá do adresára principály.

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

Projektované pozadie operačného systému

Projektované pozadie systému má schopnosť mapovať objekty OS/400 ako položky v rámci adresárového stromu prístupného LDAP. Projektované objekty sú reprezentácie LDAP objektov OS/400 namiesto skutočných položiek uložených v databáze servera LDAP. Vo V5R2 sú užívateľské profily OS/400 jedinými objektmi, ktoré sa mapujú alebo projektujú ako položky v adresárovom strome. Mapovanie objektov užívateľského profilu sa označuje ako projektované pozadie užívateľa OS/400.

Operácie LDAP sa mapujú do nižšie sa nachádzajúcich objektov OS/400 a operácie LDAP vykonávajú funkcie operačného systému s cieľom mať prístup k uvedeným objektom. Všetky operácie LDAP vykonávané na užívateľských profiloch sa vykonávajú pod oprávnením užívateľského profilu priradeného ku pripojeniu klienta.

Podrobnejšie informácie o projektovanom pozadí operačného systému nájdete v nasledujúcich témach:

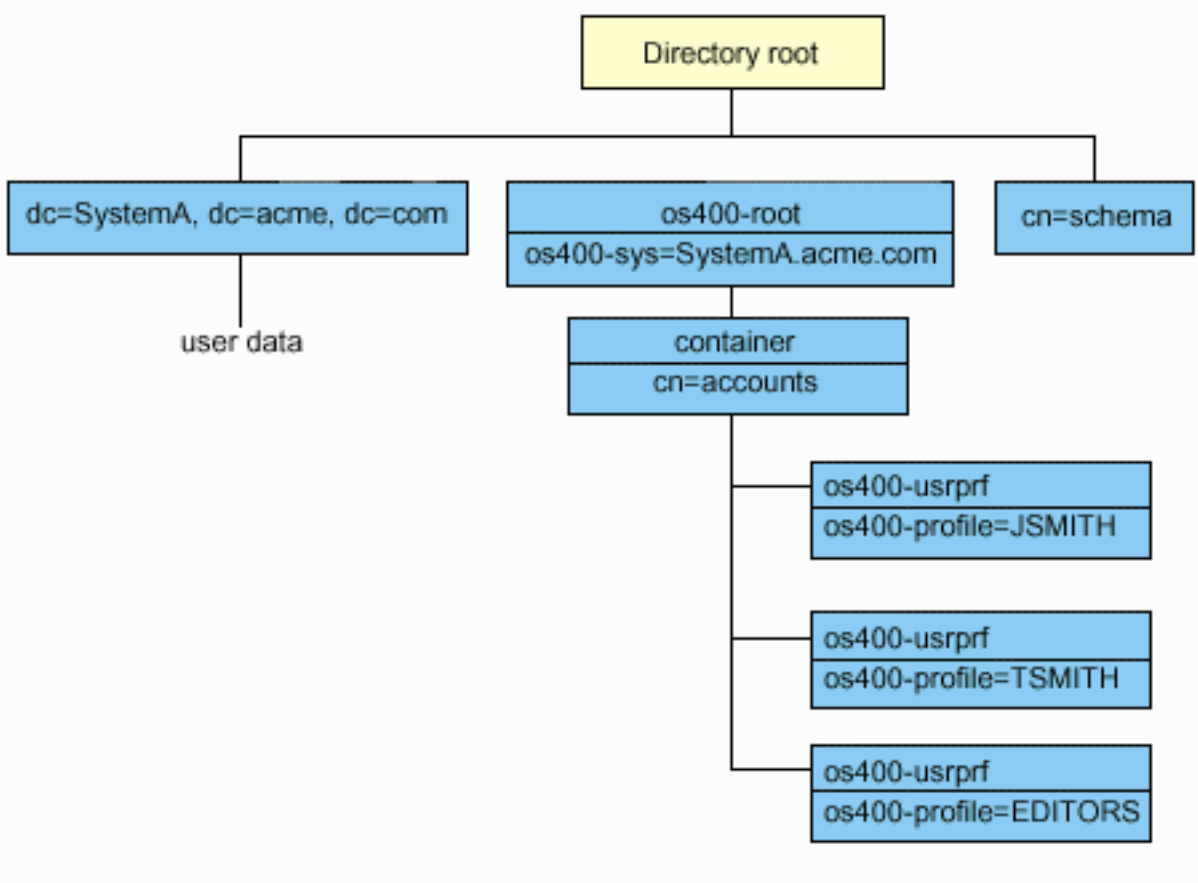
- “OS/400” na strane 41
- “Operácie LDAP” na strane 42
- “DN pripojenia správcu a repliky” na strane 45
- “OS/400” na strane 45

OS/400

OS/400

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

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



Koreňom stromu je prípona na os400-sys=*SystemA.acme.com*, kde *SystemA.acme.com* je názov vášho systému. Trieda objektu je os400-root. Aj keď DIT nemožno zmeniť alebo vymazať, je možné prekonfigurovať príponu systémového objektu. Musíte však skontrolovať, či sa aktuálna prípona nepoužíva v ACL alebo niekde inde v systéme, kde keď sa zmení prípona, bude potrebné zmeniť aj položky.

Na predchádzajúcom obrázku sa kontajner cn=accounts zobrazí pod koreňom. Tento objekt nemožno modifikovať. Kontajner je umiestnený na tejto úrovni za predpokladu, že operačný systém môže v budúcnosti naprojektovať iné druhy informácií alebo objektov. Pod kontajnerom cn=accounts sa nachádzajú užívateľské profily, ktoré sú naprojektované ako objectclass=os400-usrprf. Tieto užívateľské profily sa nazývajú projektované užívateľské profily a sú LDAP známe v tvare os400-profile=JSMITH,cn=accounts,os400-sys=SystemA.acme.com.

Operácie LDAP

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

Vytváranie väzieb

Klient LDAP sa môže pripojiť (autentifikovať) k serveru LDAP pomocou projektovaného užívateľského profilu. Uvedené možno vykonať zadaním DN (charakteristického názvu) projektovaného užívateľského profilu pre DN vytvorenia väzby a správneho hesla užívateľského profilu OS/400 na autentifikáciu. Príkladom DN používaného v požiadavke na vytvorenie väzby je os400-profile=jsmith,cn=accounts,os400-sys=systemA.acme.com.

Klient sa musí pripojiť ako projektovaný užívateľ, aby mohol mať prístup k informáciám v systémovom projektovanom pozadí. Server vykonáva všetky operácie pomocou oprávnenia na daný užívateľský profil. DN projektovaného užívateľského profilu možno použiť v ACL LDAP ako iné DN položky LDAP. Jednoduchá metóda vytvorenia väzby je jedinou povolenou metódou vytvorenia väzby, keď je na požiadavke vytvorenia väzby uvedený projektovaný užívateľský profil.

Hľadanie

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

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

Nasledujúca tabuľka opisuje správanie projektovaného pozadia systému pre operácie hľadania.

Tabuľka 1. Správanie projektovaného pozadia systému pre operácie hľadania

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

Tabuľka 1. Správanie projektovaného pozadia systému pre operácie hľadania (pokračovanie)

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

Tabuľka 1. Správanie projektovaného pozadia systému pre operácie hľadania (pokračovanie)

Požadované hľadanie	Základ hľadania	Rozsah hľadania	Vyhľadávací filter	Komentáre
Návrat všetkých skupinových profilov začínajúcich sa na G.	cn=accounts, os400-sys=SystemA.acme.com	one alebo sub	(&(!(os400-gid=0)) (os400-profile=G*))	Pre projektované užívateľské profily sa vracajú len hodnoty DN (charakteristický názov), objectclass a os400-profile. Ak je uvedený akýkoľvek iný filter, vráti sa LDAP_UNWILLING_TO_PERFORM.
Návrat všetkých užívateľských profilov začínajúcich sa na A.	cn=accounts, os400-sys=SystemA.acme.com	one alebo sub	(&(os400-gid=0) (os400-profile=A*))	Pre projektované užívateľské profily sa vracajú len hodnoty DN (charakteristický názov), objectclass a os400-profile. Ak je uvedený akýkoľvek iný filter, vráti sa LDAP_UNWILLING_TO_PERFORM.

Porovnávanie

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

Pridávanie a modifikácia

Užívateľské profily môžete vytvoriť pomocou operácie pridávania LDAP a môžete ich zmeniť pomocou operácie modifikácie LDAP.

Vymazávanie

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

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

- os400-dltusrprf-ownobjopt 1.3.18.0.2.10.8

  Nasleduje hodnota ovládacieho prvku:
  - controlValue ::= ownObjOpt [newOwner]
  - ownObjOpt ::= *NODLT / *DLT / *CHGOWN

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

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

Nasledujú príklady hodnoty ovládacieho prvku:

- *NODLT: uvádza, že profil nemožno vymazať, ak vlastní nejaké objekty.
- *CHGOWN SMITH: uvádza prenos vlastníctva ľubovoľných objektov na užívateľský profil SMITH.

- Identifikátor objektu (OID) je definovaný v ldap.h as LDAP_OS400_OWNOBJOPT_CONTROL_OID.
  - os400-dltusrprf-pgpopt 1.3.18.0.2.10.9

Hodnota ovládacieho prvku je definovaná takto:

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

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

Nasledujú príklady hodnoty ovládacieho prvku:

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

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

ModRDN

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

API importu a exportu

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

DN pripojenia správcu a repliky

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

Ďalšie informácie nájdete v “Práca s prístupom správcu pre oprávnených užívateľov” na strane 30.

OS/400

OS/400

Triedy a atribúty objektov z projektovaného pozadia možno nájsť v serverovej schéme. Názvy atribútov LDAP sú vo formáte os400–*nnn*, kde *nnn* je zvyčajne kľúčové slovo atribútu (napríklad CRTUSRPRF alebo CHGUSRPRF) na príkazoch užívateľského profilu. Ďalšie informácie nájdete v téme “OS/400” na strane 41.

Directory Services a OS/400

Directory Services a OS/400

Directory Services používa podporu databázy OS/400 na ukladanie adresárových informácií. Directory Services používa riadenie potvrdenia na ukladanie adresárových položiek v databáze. To si vyžaduje podporu žurnálovania OS/400.

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

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

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

Vaše prostredie, veľkosť a štruktúra adresárov alebo stratégia ukladania alebo obnovovania môže vyžadovať niektoré rozdiely vzhľadom na štandardné nastavenia, vrátane spôsobu, ako sú tieto objekty spravované a použitej prahovej hodnoty veľkosti. Ak je to potrebné, môžete zmeniť parametre príkazov žurnálovania. Žurnálovanie LDAP je štandardne nastavené na vymazávanie starých prijímačov. Ak je nakonfigurovaný protokol zmien a chcete si ponechať staré prijímače, vykonajte z príkazového riadka OS/400 nasledujúci príkaz:

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

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

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

Informácie o príkazoch žurnálovania obsahuje téma príkazy OS/400 pod Programovaním v iSeries Information Center.

Kapitola 6. Služby príkazového riadka LDAP

Directory Services obsahuje päť programov, ktoré umožňujú vykonávať akcie na adresárovom LDAP serveri z príkazového prostredia Qshell na OS/400. Tieto služby používajú API LDAP. Tieto programy môžete používať z príkazového riadka QSH alebo ich zavolať z vašich programov. Možno vám pomôžu ako vhodné príklady. Keď nainštalujete Windows klienta LDAP, ktorý je súčasťou Directory Services, inštalujete aj kód, ktorý je veľmi podobný zdrojovému kódu pre plášťové pomocné programy.

Tieto služby sú:
- "Vlastnosti ldapmodify a ldapadd", ktorá pridáva a mení položky adresára LDAP.
- "Funkcia ldapdelete" na strane 50, ktorá odstraňuje položky z adresára LDAP.
- "Funkcia ldapsearch" na strane 52, ktorá v adresári LDAP vyhľadáva položky.
- "Funkcia ldapmodrdn" na strane 56, ktorá modifikuje relatívny rozoznaný názov (RDN) položiek adresára.

Viac informácií o použití SSL so službami príkazového riadka, nájdete v "Poznámky k používaniu SSL s pomocnými programami príkazového riadku LDAP" na strane 58.

Vlastnosti ldapmodify a ldapadd

Ldapmodify vám umožňuje zmeniť alebo pridať záznamy do adresárového servera LDAP z QSH príkazového shellu vo vašom systéme a používa API (aplikačné programové rozhrania ldap_modify, ldap_add a ldap_delete. Pomocný program ldapadd pracuje takmer rovnako ako ldapmodify s výnimkou toho, že príznak -a sa zapína automaticky.

Formát:

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

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

Poznámka: Ak zo *súboru* použitím voľby **-f** neposkytnete informácie o položke, funkcia počká na načítanie položiek zo štandardného vstupu. Ak chcete prerušiť čakanie, stlačte kláves SysReq, potom vyberte 2. Ukončiť predchádzajúcu požiadavku.

Diagnostika:

Ak sa nevyskytne chyba, stav ukončenia je 0. Chyby sa prejavia v nenulovom stave ukončenia a diagnostická správa sa zapíše do štandardnej chyby.

Kliknite sem, ak si chcete pozrieť príklady použitia týchto služieb.

Parametre:

-V	Označuje verziu LDAP, ktorú používa táto vlastnosť na väzbu k LDAP serveru. Štandardne používa spojenie LDAP V3. Ak chcete explicitne vybrať LDAP V3, uveďte -V 3. Ak chcete bežať ako aplikácia LDAP V2, uveďte -V 2.
-a	Tento parameter používa iba ldapmodify a určuje, že pomocný program radšej pridá štandardné položky, než by ich menil. Použitie tohto parametra je rovnaké, ako použitie ldapadd.

-b	Predpokladajme, že všetky hodnoty, ktoré sa začínajú na `/ sú binárne a že skutočná hodnota je v súbore, ktorého cesta je uvedená na mieste, kde sa zvyčajne objavujú hodnoty.
-c	Nepretržitý prevádzkový režim. Chyby sa ohlásia, ale ldapmodify alebo ldapadd naďalej modifikujú alebo pridávajú. Štandardne je po ohlásení chyby nastavené ukončenie.
-r	Nahrádza existujúce hodnoty štandardnými.
-M	Spravovať objekty odvoláviek ako štandardné záznamy.
-n	Ukáže, aký by bol výsledok, ale záznamy nemodifikuje. Používa sa pri ladení spolu s -v.
-v	Použije sa viacslovný režim s veľkým množstvom diagnostík zapísaných do štandardného výstupu.
-F	Vynúti aplikáciu všetkých zmien bez ohľadu na obsah vstupných riadkov, ktoré začínajú replikou: (štandardne replika: riadky sa porovnajú s hostiteľom a portom LDAP servera pri rozhodovaní, či sa má aplikovať záznam protokolu replikácie).
-R	Určuje, že odvolávky automaticky nenasledujú.
-C *charset*	Označuje, že reťazce dodávané ako vstup k vlastnostiam sú reprezentované v miestnej sade znakov (*charset*) a musia sa skonvertovať na UTF-8. Použite možnosť **-C** charset, ak sa kódová strana vstupného reťazca odlišuje od hodnoty kódovej strany úlohy. V dokumentácii pre ldap_set_iconv_local_charset() API sa uvádzajú podporované hodnoty *charset*.
-d *debuglevel*	Nastavuje úroveň ladenia na *debuglevel*.
-D *binddn*	*Viazať dn* použite na zviazanie s adresárom LDAP. *binddn* by malo byť reťazcovo reprezentovaným DN.
-w *passwd*	Použiť *passwd* ako heslo pre autentifikáciu.
-m *mechanism*	Použite *mechanism*, aby ste špecifikovali SASL mechanizmus, ktorý používa klient na pripojenie k serveru. Klient používa ldap_sasl_bind_s() API. Dostupné mechanizmy sú CRAM-MD5 (šifruje heslo), EXTERNAL (používa sa s SSL) a GSSAPI (Kerberos). Príkaz ignoruje **-m** parameter ak je nastavené **-V 2**. Ak nezadáte **-m**, použije sa jednoduchá autentifikácia.
-O*hopcount*	Špecifikujte *hopcount*, čím nastavíte maximálny počet preskočení, ktoré urobí knižnica klienta pri hľadaní odkazov. Štandardný počet preskočení je 10.
-h *ldaphost*	Určite alternatívneho hostiteľa, na ktorom je spustený LDAP server.
-p *ldapport*	Určite alternatívny port Transmission Control protocol (TCP), ktorý sleduje LDAP server. Štandardný port LDAP je 389. Ak port nie je špecifikovaný a je špecifikované **-Z**, použije sa štandardný port LDAP SSL 636.
-f *file*	Prečítať informácie o modifikácii položky v súbore LDIF namiesto štandardného vstupu. Ak súbor LDIF nie je špecifikovaný, musíte použiť štandardný vstup na špecifikovanie aktualizovaných položiek vo formáte LDIF.
-Z	Na komunikáciu so serverom LDAP použije bezpečné spojenie SSL. Voľbu **-Z** podporujú len tie verzie tohto nástroja, ktoré môžu disponovať SSL.
-K *keyfile*	Zadajte názov databázového súboru kľúčov SSL. Ak databázový súbor kľúčov nie je v aktuálnom adresári, zadajte úplný názov databázového súboru kľúčov. Ak pomocný program nemôže lokalizovať databázu kľúčov, použije náročne kódovanú sadu štandardných dôveryhodných koreňov certifikačnej autority. Databázový súbor kľúčov zvyčajne obsahuje jeden alebo viac certifikátov z certifikačných autorít (CA), ktoré sú dôveryhodné pre klienta. Tieto typy certifikátov X.509 sú známe aj ako dôveryhodné zdroje. Tento parameter efektívne umožní prepínač **-Z**.
-P *keyfilepw*	Zadajte heslo databázy kľúčov. Toto heslo sa vyžaduje pre prístup k zakódovaným informáciám v databázovom súbore kľúčov (zahŕňajúc súkromný kľúč). Ak je súbor s uloženými heslami pridružený k súboru kľúčov databázy, heslo sa získa z tohto súboru uložených hesiel a tento parameter nie je potrebný. Tento parameter sa ignoruje, ak nie je zadefinované **-Z** ani **-K**.

-N *certificatename*	Zadajte návestie prislúchajúce klientskemu certifikátu v databázovom súbore kľúčov. Všimnite si, že ak je LDAP server nakonfigurovaný len na vykonanie Autentifikácie servera, nepožaduje sa klientsky certifikát. Ak je LDAP server nakonfigurovaný na vykonanie Autentifikácie klienta a servera, požaduje sa klientsky certifikát. *Názov certifikátu* sa nepožaduje, ak bol štandardný pár certifikát/privátny kľúč nastavený ako štandardný. Podobne, *certificatename* nie je potrebné, ak v označenom súbore kľúčov databázy existuje jeden pár certifikát/súkromný kľúč. Tento parameter sa ignoruje, ak nie je zadefinované **-Z** ani **-K**.

Alternatívny vstupný formát:

Pomocný program ldapmodify podporuje alternatívny vstupný formát s cieľom udržiavať kompatibilitu so staršími verziami pomocného programu. Tento formát pozostáva z jedného alebo viacerých záznamov, ktoré sú oddelené prázdnymi riadkami. Každý záznam má nasledujúci formát:

```
Distinguished Name (DN)
attr=value
[attr=value ...]
```

kde *attr* je názvom atribútu a *value* je hodnota. Štandardne sa hodnoty pridajú. Ak použijete príznak príkazového riadka **-r**, štandardne sa nastaví nahrádzanie existujúcich hodnôt novými. Všimnite si, že pre dané atribúty je povolené objaviť sa viac ako raz (napríklad môžete pridať viac ako jednu hodnotu pre atribút). Všimnite si, že môžete použiť aj počiatočný znak lomeno (\), aby mohli hodnoty pokračovať cez riadky a aby sa nové riadky zachovali v hodnote samotnej. Ak chcete odstrániť hodnotu, pred hodnotu *attr* umiestnite pomlčku (-). Znak rovná sa (=) a hodnota treba vynechať, ak chcete odstrániť celý atribút. *attr* by mal predchádzať znak (+), ak chcete pridať hodnotu v prítomnosti príznaku **-r**.

Príklady: ldapmodify a ldapadd

Príklad 1:

Ak existuje súbor /**tmp**/**entrymods** s nasledujúcim obsahom:

```
dn: cn=Modify Me, o=University of Higher Learning, c=US
changetype: modify
replace: mail
mail: modme@student.of.life.edu
-
add: title
title: Grand Poobah
-
add: jpegPhoto
jpegPhoto:< file:///tmp/modme.jpeg
-
delete: description
-
```

Príkaz ldapmodify -b -r -f /tmp/entrymods urobí nasledujúce zmeny:

- Nahradí obsah atribútu Modify Me entrys mail hodnotou modme@student.of.life.edu.
- Pridá titul Grand Poobah.
- Pridá obsah súboru /**tmp**/**modme.jpeg** ako jpegPhoto.
- Úplne odstráni atribút description.

Také isté úpravy môžete vykonať so starším vstupným formátom 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
```

Príkaz pre použitie starého formátu bude:

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

Príklad 2:

Predpokladajme, že existuje súbor /**tmp**/**newentry** s nasledujúcim obsahom:

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

Príkaz ldapadd -f /tmp/entrymods pridá nový záznam Johna Doea použitím hodnôt zo súboru /tmp/newentry.

Príklad 3:

Ak existuje súbor /**tmp**/**newentry** s obsahom:

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

Príkaz ldapmodify -f /tmp/entrymods odstráni záznam Johna Doea.

Funkcia ldapdelete

Funkcia ldapdelete vám umožňuje vymazať jednu alebo viac položiek z adresárového LDAP servera. Pracuje cez príkazový shell QSH na OS/400. Používa rozhranie aplikačného programu (API) ldap_delete.

Formát:

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

Poznámka: Ak neposkytnete argumenty *dn*, príkaz ldapdelete bude čakať na prečítanie zoznamu DN zo štandardného vstupu. Ak chcete prerušiť čakanie, stlačte kláves SysReq, potom vyberte 2. Ukončiť predchádzajúcu požiadavku.

Diagnostika:

Ak sa nevyskytne chyba, stav ukončenia je 0. Chyby sa prejavia v nenulovom stave ukončenia a diagnostická správa sa zapíše do štandardnej chyby.

Kliknite sem, aby ste si pozreli príklad použitia služby ldapdelete.

Parametre:

-V	Určuje verziu LDAP, ktorú používa táto vlastnosť na väzbu so serverom LDAP. Štandardne používa spojenie LDAP V3. Ak chcete explicitne vybrať LDAP V3, uveďte -V 3. Ak chcete bežať ako aplikácia LDAP V2, uveďte -V 2.
-M	Spravovať objekty odvoláviek ako štandardné záznamy.
-n	Ukáže, čo by sa vykonalo, ale nevymaže položky. Používa sa pri ladení spolu s **-v**.
-v	Použije sa viacslovný režim s veľkým množstvom diagnostík zapísaných do štandardného výstupu.

-c	Nepretržitý prevádzkový režim. Chyby sa hlásia, ale ldapdelete vymazáva ďalej. Štandardne je po ohlásení chyby nastavené ukončenie.
-R	Určuje, že odvolávky sa automaticky nenasledujú.
-C *charset*	Určuje, že rozoznané názvy (DN) dodané ako vstup pre funkciu ldapdelete sú reprezentované v lokálnej znakovej sade (*charset*). Použite **-C** *charset* na prekrytie štandardnej hodnoty, kde reťazce musia byť dodané v UTF-8. Použite voľbu **-C** charset, ak sa kódová stránka vstupného reťazca líši od hodnoty kódovej stránky úlohy. V dokumentácii pre ldap_set_iconv_local_charset() API nájdete podporované hodnoty *charset*.
-d *debuglevel*	Nastavuje úroveň ladenia na *debuglevel*.
-f *súbor*	Zo *súboru* prečíta skupinu riadkov, pričom vykoná jedno vymazanie LDAP pre každý riadok súboru. Každý riadok súboru by mal obsahovať jeden rozoznaný názov (DN).
-D *binddn*	Použite *binddn* na zviazanie s adresárom LDAP. *binddn* by malo byť reťazcovo reprezentovaným DN.
-w *passwd*	Použiť *passwd* ako heslo pre autentifikáciu.
-m *mechanism*	Použite *mechanism* na zadanie mechanizmu SASL, ktorý sa použije na väzbu k serveru. Bude použitý ldap_sasl_bind_s() API. Dostupné mechanizmy sú CRAM-MD5 (šifruje heslo), EXTERNAL (používa sa s SSL) a GSSAPI (Kerberos). Parameter -m sa ignoruje, ak je nastavené -V 2. Ak nezadáte **-m**, použije sa jednoduchá autentifikácia.
-O *hopcount*	Zadajte *hopcount* pre nastavenie maximálneho počtu preskočení, ktoré vykoná klientska knižnica pri hľadaní odporúčaní. Štandardný počet preskočení je 10.
-h *ldaphost*	Určite alternatívneho hostiteľa, na ktorom je spustený LDAP server.
-p *ldapport*	Určite alternatívny port Transmission Control protocol (TCP), ktorý sleduje LDAP server. Štandardný port LDAP je 389. Ak port nie je špecifikovaný, a je špecifikované **-Z**, použije sa štandardný port LDAP SSL 636.
-Z	Na komunikáciu so serverom LDAP použije bezpečné spojenie SSL. Voľba **-Z** je podporovaná len tými verziami tohto nástroja, ktoré môžu disponovať SSL.
-K *keyfile*	Zadajte názov databázového súboru kľúčov SSL. Ak databázový súbor kľúčov nie je v aktuálnom adresári, zadajte úplný názov databázového súboru kľúčov. Ak pomocný program nemôže lokalizovať databázu kľúčov, použije náročne kódovanú sadu štandardných dôveryhodných koreňov certifikačnej autority. Databázový súbor kľúčov zvyčajne obsahuje jeden alebo viac certifikátov z certifikačných autorít (CA), ktoré sú dôveryhodné pre klienta. Tieto typy certifikátov X.509 sú tiež známe ako dôveryhodné zdroje. Tento parameter efektívne umožní prepínač **-Z**.
-P *keyfilepw*	Zadajte heslo databázy kľúčov. Toto heslo sa vyžaduje pre prístup k zakódovaným informáciám v databázovom súbore kľúčov (vrátane súkromného kľúča). Ak je súbor s uloženými heslami pridružený k súboru kľúčov databázy, heslo sa získa z tohto súboru uložených hesiel a tento parameter nie je potrebný. Tento parameter sa ignoruje, ak nie je zadaný **-Z** ani **-K**.
-N *certificatename*	Zadajte návestie prislúchajúce klientskemu certifikátu v databázovom súbore kľúčov. Všimnite si, že ak je LDAP server nakonfigurovaný len na vykonanie Autentifikácie servera, nepožaduje sa klientsky certifikát. Ak je LDAP server nakonfigurovaný na vykonanie Autentifikácie klienta a servera, požaduje sa klientsky certifikát. *Názov certifikátu* sa nepožaduje, ak bol štandardný pár certifikát/privátny kľúč nastavený ako štandardný. Podobne, *certificatename* nie je potrebné, ak v označenom súbore kľúčov databázy existuje jeden pár certifikát/súkromný kľúč. Tento parameter sa ignoruje, ak nie je zadefinované **-Z** ani **-K**.
dn	Označuje jeden alebo viac argumentov *dn*. Každý *dn* by mal byť znakovo reprezentovaným DN.

Príklad: ldapdelete

Nasledujúci príkaz sa pokúsi vymazať položku s názvom commonName Delete Me priamo pod organizačnou položkou University of Life.

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

Môže byť nevyhnutné zadať *binddn* a *passwd* (pozrite voľby **-D** a **-w**).

Funkcia ldapsearch

Program ldapsearch umožňuje vyhľadávať záznamy na vašom adresárovom LDAP serveri z príkazového shellu QSH na OS/400. Používa rozhranie aplikačného programu (API) ldap_search.

Vyhľadávanie používa filter, ktorý vyhovuje reprezentácii reťazca pre filtre LDAP. Ďalšie informácie o vyhľadávacích filtroch LDAP obsahujú informácie API ldap_search v téme OS/400 adresárové služby pod Programovaním v iSeries Information Center.

Ak funkcia ldapsearch nájde jeden alebo viac záznamov, získa atribúty, ktoré sú špecifikovanými *atribútmi* a záznamy a hodnoty vytlačí do štandardného výstupu. Ak neuvediete žiadne atribúty, vráti všetky atribúty.

Formát:

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

Diagnostika:

Ak sa nevyskytne chyba, stav ukončenia je 0. Chyby sa prejavia v nenulovom stave ukončenia a diagnostická správa sa zapíše do štandardnej chyby.

Výstupný formát:

Ak ldapsearch nájde jeden alebo viac položiek, každá položka zapíše do štandardného výstupu vo formáte:

```
Rozoznaného názvu (DN).
názov atribútu=hodnota
názov atribútu=hodnota
názov atribútu=hodnota
...
```

Viacnásobné položky sú oddelené jedným prázdnym riadkom. Ak na určenie oddeľovacieho znaku použijete voľbu **-F**, výstup zobrazí tento znak a nie znak (=). Ak použijete voľbu **-t**, názov dočasného súboru nahradí aktuálna hodnota. Ak špecifikujete voľbu **-A**, zapíše sa len časť názov atribútu.

Kliknite sem, ak si chcete pozrieť príklady použitia služby ldapsearch.

Parametre:

-V	Určuje verziu LDAP, ktorú používa táto vlastnosť na väzbu so serverom LDAP. Štandardne používa spojenie LDAP V3. Ak si chcete explicitne zvoliť LDAP V3, zadajte -V 3. Uveďte -V 2, aby ste bežali ako aplikácia LDAP V2.
-n	Ukáže, čo by sa vykonalo, ale záznamy nevyhľadá. Používa sa pri ladení spolu s **-v**.
-v	Použije sa viacslovný režim s veľkým množstvom diagnostík zapísaných do štandardného výstupu.
-t	Získané hodnoty zapíše do niekoľkých dočasných súborov. To je výhodné pri práci s binárnymi hodnotami, ako napríklad jpegPhoto alebo audio.

-A	Získava len atribúty (nie hodnoty). Možno ho použiť vtedy, keď sa chcete uistiť, či sa atribút v zázname nachádza, ale nezaujíma vás konkrétna hodnota.
-B	Nepotlačí zobrazenie binárnych hodnôt. Toto sa dá použiť pri práci s hodnotami, ktoré sa zobrazujú v alternatívnej znakovej sade, napríklad ISO-8859.1. Táto voľba sa zapína s **-L.**
-L	Výsledky vyhľadávania zobrazí vo formáte LDIF. Táto voľba tiež zapína voľbu **-B** a zapríčiní ignorovanie voľby **-F**.
-M	Spravovať objekty odvoláviek ako štandardné záznamy.
-R	Určuje, že odvolávky automaticky nenasledujú.
-C *charset*	Určuje, že reťazce dodávané ako vstup do vlastnosti ldapsearch sú reprezentované v miestnej sade znakov (*charset*). Reťazcový vstup zahŕňa filter, DN väzby a DN základne. Podobne, keď sa zobrazujú údaje, ldapsearch konvertuje údaje prijaté zo servera LDAP na zadané znaky. Použite možnosť **-C** charset, ak sa kódová strana vstupného reťazca odlišuje od hodnoty kódovej strany úlohy. V dokumentácii si pozrite ldap_set_iconv_local_charset() API, kde nájdete podporované hodnoty *charset*. Takisto, ak sú zadané obe voľby -C aj -L, predpokladá sa, že vstup je v zadanej sade znakov, ale údaje výstupu z ldapsearch majú vždy zachovaný formát UTF-8, alebo zakódovaný formát na základe 64, keď sa nájdu netlačiteľné znaky. Tento prípad existuje, odkedy štandardné súbory LDIF obsahujú len formát údajov UTF-8 (alebo UTF-8 zakódovaný na základe 64).
-d *debuglevel*	Nastavuje úroveň ladenia na *debuglevel*.
-F *sep*	Použite *sep* ako oddeľovač poľa medzi názvami a hodnotami atribútov. Štandardný oddeľovač je `=, pokiaľ nebol zadaný príznak **-L**. V takom prípade bude táto voľba ignorovaná.
-f *súbor*	Zo súboru prečíta skupinu riadkov, vykoná jedno vyhľadanie LDAP pre každý riadok súboru. Každý riadok súboru by mal obsahovať jeden rozlíšený názov (DN).
-D *binddn*	*Viazať dn* použite na zviazanie s adresárom LDAP. *binddn* by malo byť reťazcovo reprezentovaným DN.
-w *passwd*	Použiť *passwd* ako heslo pre autentifikáciu.
-m *mechanism*	Použite *mechanism* na zadanie mechanizmu SASL, ktorý sa použije na väzbu k serveru. Použije sa ldap_sasl_bind_s() API. Dostupné mechanizmy sú CRAM-MD5 (šifruje heslo), EXTERNAL (používa sa s SSL) a GSSAPI (Kerberos). Parameter **-m** sa ignoruje, ak je zadané **-V** 2. Ak **-m** nie je zadaný, použije sa jednoduché preverenie.
-O *hopcount*	Zadajte *hopcount* pre nastavenie maximálneho počtu preskočení, ktoré vykoná klientska knižnica pri hľadaní odporúčaní. Štandardný počet preskočení je 10.
-h *ldaphost*	Určte alternatívneho hostiteľa, na ktorom je spustený LDAP server.
-p *ldapport*	Určite alternatívny port Transmission Control protocol (TCP), ktorý sleduje LDAP server. Štandardný port LDAP je 389. Ak port nie je špecifikovaný, a je špecifikovaný **-Z**, použije sa štandardný port LDAP Secure Socket Layer (SSL) 636.
-Z	Na komunikáciu so serverom LDAP použije bezpečné spojenie SSL. Voľba **-Z** je podporovaná len tými verziami tohto nástroja, ktoré môžu disponovať SSL.
-K *keyfile*	Zadajte názov databázového súboru kľúčov SSL. Ak databázový súbor kľúčov nie je v aktuálnom adresári, zadajte úplný názov databázového súboru kľúčov. Ak pomocný program nemôže lokalizovať databázu kľúčov, použije náročne kódovanú sadu štandardných dôveryhodných koreňov certifikačnej autority. Databázový súbor kľúčov zvyčajne obsahuje jeden alebo viac certifikátov z certifikačných autorít (CA), ktorým dôveruje klient. Tieto typy certifikátov X.509 sú tiež známe ako dôveryhodné zdroje. Tento parameter efektívne umožní prepínač **-Z**.
-P *keyfilepw*	Zadajte heslo databázy kľúčov. Toto heslo sa vyžaduje pre prístup k zakódovaným informáciám v databázovom súbore kľúčov (zahŕňajúc súkromný kľúč). Ak súbor na úschovu hesiel je pripojený k databázovému súboru kľúčov, heslo sa získa z tohto úschovného súboru a tento parameter sa nevyžaduje. Tento parameter sa ignoruje, ak nie je zadaný **-Z** ani **-K**.

-N *certificatename*	Zadajte návestie prislúchajúce klientskemu certifikátu v databázovom súbore kľúčov. Všimnite si, že ak LDAP server je nakonfigurovaný len na vykonanie Autentifikácie servera, nepožaduje sa klientsky certifikát. Ak je LDAP server nakonfigurovaný na vykonanie Autentifikácie klienta a servera, požaduje sa klientsky certifikát. *Názov certifikátu* sa nepožaduje, ak bol štandardný pár certifikát/privátny kľúč nastavený ako štandardný. Podobne, *certificatename* nie je potrebné, ak v označenom súbore kľúčov databázy existuje jeden pár certifikát/súkromný kľúč. Tento parameter sa ignoruje, ak nie je zadefinované **-Z** ani **-K**.
-b *searchbase*	Použite *searchbase* ako štartovací bod pre vyhľadávanie namiesto štandardu. Ak **-b** nie je zadaný, táto služba použije premennú prostredia LDAP_BASEDN pre definíciu *searchbase*.
-s *scope*	Špecifikuje rozsah hľadania. *scope* by mal byť jeden z base, one alebo sub na špecifikovanie vyhľadávania základného objektu, jednej úrovne alebo podstromu. Štandardné je sub.
-a *deref*	Špecifikuje, ako sa rušia referencie na alias. *deref* by malo byť nikdy, vždy, vyhľadať alebo nájsť, ak chcete špecifikovať, že referencie na alias nie sú nikdy zrušené, sú zrušené vždy, zrušené pri vyhľadávaní alebo zrušené len pri lokalizovaní objektu bázy, v ktorom sa bude vyhľadávať. Štandard je nikdy nerušiť referencie na alias.
-l *timelimit*	Čaká sa najviac *timelimit* sekúnd pre dokončenie vyhľadávania.
-z *sizelimit*	Obmedzuje výsledky hľadania na najväčší *limit veľkosti* položiek, čo umožňuje určiť hornú hranicu pre počet položiek, ktoré sú vrátené operáciou hľadania.
filter	Označuje názov filtra, ktorý sa používa pre vyhľadávanie.
attrs...	Označuje atribúty, ktoré táto služba obnovuje, ak vyhľadávanie nájde jednu alebo viac položiek. Ak pre *attrs* neurčíte žiadnu hodnotu, funkcia vráti všetky hodnoty.

Príklady: ldapsearch

Príklad 1:

Príkaz ldapsearch cn=john doe cn telephoneNumber prehľadáva podstrom (pomocou štandardnej vyhľadávacej bázy) kvôli položkám s commonName john doe. Vyhľadávanie získa a do štandardného výstupu vytlačí hodnoty názvu a telefónneho čísla (telephoneNumber). Ak vyhľadávanie nájde dve položky, výstup vyzerá takto:

```
cn=John E Doe, ou=College of Literature, Science, and the Arts,
ou=Students, ou=People, o=University of Higher Learning, c=US
cn=John Doe
cn=John Edward Doe
cn=John E Doe 1
cn=John E Doe
telephoneNumber=+1 313 555-5432

cn=John B Doe, ou=Information Technology Division,
ou=Faculty and Staff,
ou=People, o=University of Higher Learning, c=US
cn=John Doe
cn=John B Doe 1
cn=John B Doe
telephoneNumber=+1 313 555-1111
```

Príklad 2:

Príkaz ldapsearch -t uid=jed jpegPhoto audio prehľadáva podstrom pomocou štandardnej vyhľadávacej bázy kvôli položkám s ID užívateľa jed. Vyhľadávanie získa hodnoty jpegPhoto a audio values a zapíše ich do dočasných súborov. Ak vyhľadávanie nájde jednu položku s jednou hodnotou pre každý z požadovaných atribútov, výstup vyzerá takto:

```
cn=John E Doe,
ou=Information Technology Division,
ou=Faculty and Staff,
ou=People, o=University of Higher Learning, c=US
audio=/tmp/ldapsearch-audio-a19924
jpegPhoto=/tmp/ldapsearch-jpegPhoto-a19924
```

Príklad 3:

Príkaz ldapsearch -L -s one -b c=US o=university* o description vykonáva jednoúrovňové hľadanie na úrovni c=US. Vyhľadávajú sa všetky organizácie, ktorých názov (organizationName) začína na university. Výsledky vyhľadávania sa zobrazia vo formáte LDIF. Získa sa hodnota atribútu názvu a hodnoty atribútu deskriptora a vytlačia sa do štandardného výstupu, ktorý vyzerá:

```
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
...
```

Príklad 4:

Ako sa uvádza v “Odkazy adresára LDAP” na strane 37, Directory Services adresáre LDAP môžu obsahovať objekty odvolávok len vtedy, ak obsahujú len:

- Rozoznaný názov (dn).
- Triedu objektov (objectClass).
- Atribút (ref) odvolávky.

Tento príkaz ukazuje vyhľadávania, keď sa týkajú objektu odvolávky.

Predpokladajme, že System_A má položku referálu:

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

Všetky atribúty priradené k tejto položke by sa mali nachádzať na System_B.

Systém_B obsahuje záznam:

```
dn: cn=Barb Jensen, ou=Rochester, o=Big Company, c=US
cn: Barb Jensen
objectclass: organizationalPerson
sn: Jensen
telephonenumber: (800) 555 1212
```

Keď klient zadá požiadavku do System_A a nepoužije riadenie manageDsaIT, server vráti referál. Napríklad použitím -M na ldapsearch server LDAP na System_A odpovedá klientovi s nasledujúcou adresou:

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

Klient použije tieto informácie na zadanie požiadavky System_B. Ak položka na System_A obsahuje atribúty okrem dn, objectclass a ref, server ich bude ignorovať.

Keď klient od servera získava odvolávkovú odpoveď, túto požiadavku vydá opäť serveru, na ktorý sa odvoláva vrátené URL. Ak sa vyhľadávanie vykonalo v jednoúrovňovom rozsahu, požiadavka referálu použije základný rozsah. Výsledky tohto vyhľadávania sa menia podľa hodnoty, ktorú špecifikujete pre rozsah vyhľadávania (**-b**).

Ak špecifikujete -s sub, ako v tomto prípade:

```
ldapsearch -h System_A -b ou=Rochester, o=Big Company, c=US
     -s sub sn=Jensen
```

Vyhľadávanie vráti všetky atribúty pre všetky položky so sn=Jensen, ktoré sa nachádzajú v alebo pod ou=Rochester, o=Big Company, c=US na System_A a System_B. Klient príjme referál zo System_A a prehľadáva System_B vracajúc cn=Barb Jense,ou=Rochester,o=Big Company,c=US.

Ak špecifikujete -s one, ako v tomto prípade:

```
ldapsearch -h System_A -b ou=Rochester, o=Big Company, c=US
     -s one sn=Jensen
```

vyhľadávanie nevráti položky ani z jedného systému. Namiesto toho server klientovi vráti odvolávku na URL:

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

Potom klient vydá požiadavku:

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

Táto vráti položku cn=Barb Jensen,ou=Rochester,o=Big Company,c=US.

Funkcia ldapmodrdn

Funkcia ldapmodrdn vám umožní zmeniť relatívny rozoznaný názov (RDN) záznamov adresárového LDAP servera. Je možné ju použiť z QSH príkazového shellu na OS/400. Používa aplikačné rozhranie programu (API) ldap_modrdn.

Formát:

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

Poznámky:

1. Ak použijete argumenty príkazového riadka *dn* a *rdn*, *rdn* nahradí RND položky, ktorá je špecifikovaná DN, *dn*. Inak by sa mal obsah súboru (alebo štandardného vstupu, ak neudáte príznak **-f**) skladať z jednej alebo viacerých položiek.

   ```
   Rozoznaného názvu (DN).

   Relatívneho rozoznaného názvu (RDN)
   ```

   Každý pár DN/RDN oddeľuje jeden alebo viacero riadkov.

2. Ak nedodáte informácie o položke zo *súboru* pomocou voľby **-f** (alebo z páru príkazových riadkov *dn* a *rdn*), príkaz ldapmodrdn bude čakať na čítanie týchto položiek zo štandardného vstupu. Ak chcete prerušiť čakanie, stlačte kláves SysReq, potom vyberte 2. Ukončiť predchádzajúcu požiadavku.

Diagnostika:

Ak sa nevyskytne chyba, stav ukončenia je 0. Chyby sa prejavia v nenulovom stave ukončenia a diagnostická správa sa zapíše do štandardnej chyby.

Kliknite sem, ak si chcete pozrieť príklady na použitie služby ldapmodrdn.

Parametre:

-V	Určuje verziu LDAP, ktorú používa táto vlastnosť na väzbu so serverom LDAP. Štandardne používa spojenie LDAP V3. Ak si chcete explicitne zvoliť LDAP V3, zadajte -V 3. Uveďte -V 2, aby ste bežali ako aplikácia LDAP V2.
-r	Zo záznamu odstraňuje staré hodnoty relatívnych rozoznaných názvov (RDN). Štandardne sa staré hodnoty uchovávajú.
-M	Spravovať objekty odvoláviek ako štandardné záznamy.
-n	Ukáže, aký by bol výsledok, ale záznamy nemodifikuje. Používa sa pri ladení spolu s **-v**.
-v	Použije sa viacslovný režim s veľkým množstvom diagnostík zapísaných do štandardného výstupu.
-c	Nepretržitý prevádzkový režim. Chyby sa hlásia, ale ldapmodrdn modifikuje ďalej. Štandardne je po ohlásení chyby nastavené ukončenie.
-R	Určuje, že odvolávky automaticky nenasledujú.
-C *charset*	Označuje, že reťazce dodávané ako vstup k vlastnostiam sú reprezentované v miestnej sade znakov (*charset*) a musia sa skonvertovať na UTF-8. Použite možnosť **-C** charset, ak sa kódová strana vstupného reťazca odlišuje od hodnoty kódovej strany úlohy. V dokumentácii pre ldap_set_iconv_local_charset() API nájdete podporované hodnoty *charset*.
-d *debuglevel*	Nastavuje úroveň ladenia na *debuglevel*.
-D *binddn*	Použite *binddn* na zviazanie s adresárom LDAP. *binddn* by malo byť reťazcovo reprezentovaným DN.
-w *passwd*	Použiť *passwd* ako heslo pre autentifikáciu.
-m *mechanism*	Použite *mechanism* na zadanie mechanizmu SASL, ktorý sa použije na väzbu k serveru. Bude použitý ldap_sasl_bind_s() API. Dostupné mechanizmy sú CRAM-MD5 (šifruje heslo), EXTERNAL (používa sa s SSL) a GSSAPI (Kerberos). Parameter -m sa ignoruje, ak je nastavené -V 2. Ak nezadáte **-m**, použije sa jednoduchá autentifikácia.
-O *hopcount*	Zadajte *hopcount* pre nastavenie maximálneho počtu preskočení, ktoré vykoná klientska knižnica pri hľadaní odporúčaní. Štandardný počet preskočení je 10.
-h *ldaphost*	Určte alternatívneho hostiteľa, na ktorom je spustený LDAP server.
-p *ldapport*	Určite alternatívny port Transmission Control protocol (TCP), ktorý sleduje LDAP server. Štandardný port LDAP je 389. Ak sa port nešpecifikuje a je špecifikované **-Z**, použije sa štandardný port LDAP SSL 636.
-Z	Na komunikáciu so serverom LDAP použije bezpečné spojenie SSL. Voľbu **-Z** podporujú len tie verzie tohto nástroja, ktoré môžu disponovať SSL.

-K *keyfile*	Zadajte názov databázového súboru kľúčov SSL. Ak databázový súbor kľúčov nie je v aktuálnom adresári, zadajte úplný názov databázového súboru kľúčov. Ak pomocný program nemôže lokalizovať databázu kľúčov, použije náročne kódovanú sadu štandardných dôveryhodných koreňov certifikačnej autority. Databázový súbor kľúčov zvyčajne obsahuje jeden alebo viac certifikátov z certifikačných autorít (CA), ktoré sú dôveryhodné pre klienta. Tieto typy certifikátov X.509 sú známe aj ako dôveryhodné zdroje. Tento parameter efektívne umožní prepínač **-Z**.
-P *keyfilepw*	Zadajte heslo databázy kľúčov. Toto heslo sa vyžaduje pre prístup k zakódovaným informáciám v databázovom súbore kľúčov (obsahuje aj súkromný kľúč). Ak je súbor s uloženými heslami pridružený k súboru kľúčov databázy, heslo sa získa z tohto súboru uložených hesiel a tento parameter nie je potrebný. Tento parameter sa ignoruje, ak nie je zadaný **-Z** ani **-K**.
-N *certificatename*	Zadajte návestie patriace klientskemu certifikátu v databázovom súbore kľúčov. Všimnite si, že ak je LDAP server nakonfigurovaný len na vykonanie Autentifikácie servera, nepožaduje sa klientsky certifikát. Ak je LDAP server nakonfigurovaný na vykonanie Autentifikácie klienta a servera, požaduje sa klientsky certifikát. *Názov certifikátu* sa nepožaduje, ak bol štandardný pár certifikát/privátny kľúč nastavený ako štandardný. Podobne, *certificatename* nie je potrebné, ak v označenom súbore kľúčov databázy existuje jeden pár certifikát/súkromný kľúč. Tento parameter sa ignoruje, ak nie je zadefinované **-Z** ani **-K**.
-f *file*	Prečíta informáciu o modifikácii záznamu zo súboru LDIF, a nie zo štandardného vstupu alebo príkazového riadka (špecifikovaním *dn* a nového *rdn*). Štandardný vstup možno dodať aj zo súboru (< file).
dn rdn	Špecifikuje rozoznaný názov (DN) položky na premenovanie a nový relatívny rozoznaný názov položky (RDN).

Príklad: ldapmodrdn

Predpokladajme, že ste vytvorili textový súbor file/**tmp**/**entrymods** s nasledujúcim obsahom:

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

Nasledujúci príkaz:

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

zmení RND Modify Me položky z Modify Me na The New Me. Staré cn, Modify Me sa odstráni.

Poznámky k používaniu SSL s pomocnými programami príkazového riadku LDAP

Aby ste mohli používať vlastnosti SSL (Secure Sockets Layer) programov príkazového riadka, musíte mať inštalovaný jeden z Cryptographic Access Provider Products (5722-ACx).

“Použitie SSL (Secure Sockets Layer) a Translation Layer Security s adresárovým serverom LDAP” na strane 39 sa zaoberá použitím SSL so serverom Directory Services LDAP. Tieto informácie zahŕňajú riadenie a vytváranie dôveryhodných certifikačných autorít manažérom digitálnych certifikátov.

Niektoré servery LDAP, do ktorých vstupujú klienti, používajú len autentifikáciu servera. Pre tieto servery musíte definovať jeden alebo viac dôveryhodných zdrojových certifikátov v pamäti certifikátov. Ak je použitá autentifikácia servera, je klientovi jasné, že cieľovému LDAP serveru bol certifikát vydaný jednou z dôveryhodných Certifikačných autorít (CA). Aj všetky transakcie LDAP, ktoré tečú ponad spojenie SSL so serverom, sú zakódované. Medzi tieto procesy patria aj povoľovacie údaje LDAP, dodávané v aplikačných programových rozhraniach (API), ktoré sa používajú na väzbu s adresárovým serverom. Napríklad, ak LDAP server používa vysoko spoľahlivý certifikát Verisign, mali by ste urobiť nasledujúce:

1. Od Verisign získať certifikát CA.

2. Na jeho importovanie do vašej pamäte certifikátov použite DCM.
3. Na jeho označenie za dôveryhodný certifikát použite DCM.

Ak server LDAP používa súkromne vydaný certifikát servera, správca serverov vám môže dodať kópiu súboru požiadaviek certifikátu serverov. Certifikát požadovaného súboru importujte do vašej pamäti certifikátov a označte ho ako dôveryhodný.

Ak používate na prístup k serverom LDAP funkcie shell, ktoré používajú autentifikáciu klienta aj autentifikáciu servera, musíte urobiť nasledujúce:

- Definujte jeden alebo viacej dôveryhodných zdrojov certifikátov v systémovej pamäti certifikátov. Toto umožňuje klientovi mať istotu, že cieľovému LDAP serveru bol certifikát vydaný jednou z dôveryhodných CA. Aj všetky transakcie LDAP, ktoré tečú ponad spojenie SSL so serverom, sú zakódované. Medzi tieto procesy patria aj povoľovacie údaje LDAP, dodávané v aplikačných programových rozhraniach (API), ktoré sa používajú na väzbu s adresárovým serverom.
- Vytvorte kľúčový pár a od CA vyžiadajte klientsky certifikát. Po prijatí podpísaného certifikátu od CA certifikát umiestnite do súboru kľúčov klienta.

Kapitola 7. Odstraňovanie problémov Directory Services

Aj také spoľahlivé servery, ako sú Directory Services LDAP servery, majú občas problémy. Keď má váš adresárový LDAP server problémy, nasledujúce informácie vám pomôžu zistiť chybu a napraviť ju.

Ďalšie informácie o bežných problémoch Directory Services obsahuje domovská stránka Directory Services  na nasledujúcej adrese:

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

Základné postupy pri odstraňovaní chýb v Directory Services

Spätné kódy chýb LDAP sa nachádzajú v súbore ldap.h, ktorý je umiestnený na vašom systéme v QSYSINC/H.LDAP.

Ak zaznamenáte na svojom adresárovom serveri LDAP chybu a chcete viac podrobností, pozrite si protokol úlohy QDIRSRV. Pre opakované chyby môžete použiť príkaz TRCTCPAPP APP(*DIRSRV) (Trace TCP/IP Application) na spustenie sledovania chýb. Ďalšie informácie nájdete v téme "Použitie TRCTCPAPP na pomoc pri vyhľadávaní problémov" na strane 62.

Directory Services používa niekoľko serverov SQL (Structured Query Language). Keď nastane chyba SQL, protokol úlohy QDIRSRV obyčajne obsahuje nasledujúcu správu:

```
Nastala chyba SQL -1
```

V týchto príkladoch vás bude protokol úlohy QDISRV odkazovať na protokoly úlohy servera SQL. V niektorých prípadoch QDIRSRV nemusí obsahovať túto správu a túto odvolávku, aj keď je SQL server príčinou problému. V týchto prípadoch vám správa pomôže a poskytne informácie o tom, ktoré SQL servery treba naštartovať a na čo ich Directory Services používa.

Ak sa adresárový LDAP server spustí normálne, vygeneruje napríklad takéto správy:

Poznámka: Správy a počet spustených úloh SQL servera sa môžu líšiť v týchto prípadoch:
- Spustíte server po prvýkrát.
- Musí sa objaviť migrácia.
- Váš server používa protokol zmien.
- Váš server je nastavený, aby umožnil vyššie množstvo databázových pripojení.

```
                                                        System:   WARMERS
 Úloha . . :   QDIRSRV       Používateľ . . :   QDIRSRV       Číslo .
. . :   174440

  >> CALL PGM(QSYS/QGLDSVR)
     Úloha 057448/QUSER/QSQSRVR používaná pre spracovanie v režime
SQL servera.
     Úloha 057340/QUSER/QSQSRVR používaná pre spracovanie v režime
SQL servera.
     Úloha 057448/QUSER/QSQSRVR používaná pre spracovanie v režime
SQL servera.
     Úloha 057166/QUSER/QSQSRVR používaná pre spracovanie v režime
SQL servera.
     Úloha 057279/QUSER/QSQSRVR používaná pre spracovanie v režime
   Úloha 057288/QUSER/QSQSRVR používaná na spracovanie režimu servera SQL.
     SQL servera.
     Server adresárových služieb bol úspešne naštartovaný.
```

Directory Services používa prvý SQL server, 057448/QUSER/QSQSRVR, počas spustenia LDAP servera. Directory Services môže spustiť ďalšie SQL servery počas inicializovania LDAP servera podľa potreby, ak ste spustili váš server po prvýkrát, ak sa má objaviť migrácia, alebo ak váš server používa protokol zmien. Po inicializácii sa tieto SQL servery prestanú používať.

V tomto príklade sa nepoužili na migráciu alebo spustenie servera žiadne ďalšie servery SQL a protokol zmien nie je nakonfigurovaný. Directory Services používa na replikáciu ďalší server SQL SQL (057340/QUSER/QSQSRVR).

Úplne posledné pripojenie v tomto príklade (057288/QUSER/QSQSRVR) sa používa na operácie pridávania, modifikácie, modrdn a vymazávania. Ostatné pripojenia sa používajú na vyhľadávanie, vytváranie väzieb a porovnávanie.

Na stránke Vlastnosti **databázy/prípon** adresárových serverov v iSeries Navigator uvádzate celkový počet serverov SQL, ktoré používa Directory Services pre operácie adresára po spustení servera. Okrem toho je jeden server SQL vždy nakonfigurovaný na replikáciu.

Monitorovanie chýb a prístupu pomocou Directory Servicesprotokolu úloh

Prezeranie protokolu úlohy vášho LDAP servera vás môže upozorniť na chyby a môže vám pomôcť monitorovať prístupy na server.

Ak je server naštartovaný, prezrite si protokol úlohy QDIRSRV:
1. V iSeries Navigator rozviňte **Sieť**.
2. Rozviňte **Servery**.
3. Kliknite na **TCP/IP**.
4. Pravým tlačidlom kliknite na **Adresár** a vyberte **Úlohy servera**.
5. Z menu **File** vyberte **Protokol úlohy**.

Ak je server zastavený, prezrite si protokol úlohy QDIRSRV:
1. V iSeries Navigator rozviňte **Základné operácie**.
2. Kliknite na **Výstup na tlačiareň**.
3. QDIRSRV sa objaví v stĺpci **Užívateľ** iSeries Navigators pravého panelu. Ak si chcete prezrieť protokol úlohy, 2x kliknite na **Qpjoblog** naľavo od QDIRSRV v tom istom riadku.

   Poznámka: iSeries Navigator sa dá nakonfigurovať tak, že zobrazí len pripravené súbory. Ak sa na zozname neobjaví QDIRSRV, kliknite na **Výstup na tlačiareň**, potom vyberte **Zahrnúť** v menu **Voľby**. V poli **Používateľ** špecifikujte **Všetko** Potom kliknite na **OK**.

Poznámka: Directory Services používa na vykonanie niektorých úloh iné systémové prostriedky. Ak chyba nastane na jednom z týchto prostriedkov, protokol úlohy označí, kde nájdete potrebné informácie. V niektorých prípadoch Directory Services nemusí byť schopný určiť miesto, kam by ste sa mali pozrieť. V takýchto prípadoch si pozrite protokol úloh serverov SQL (Structured Query Language) a zistite, či sa problém týkal serverov SQL.

Použitie TRCTCPAPP na pomoc pri vyhľadávaní problémov

Váš server poskytuje sledovanie komunikácie a zhromažďuje údaje o komunikačnej linke, ako napríklad rozhranie LAN (local area network) alebo WAN (wide area network). Priemerný užívateľ nemusí porozumieť celému obsahu údajov sledovania. Tieto položky sledovania však môže použiť na to, aby určil, či sa skutočne bude konať výmena údajov medzi dvoma bodmi.

Príkaz TRCTCPAPP (Trace TCP/IP Application) s voľbou *DIRSRV možno na adresárovom serveri použiť na pomoc pri zisťovaní problémov s klientmi alebo aplikáciami.

Podrobnejšie informácie o použití príkazu TRCTCPAPP s LDAP, ako aj o obmedzeniach na požadovaných oprávneniach obsahuje časť Opis príkazu TRCTCPAPP (Trace TCP/IP Application).

Všeobecné informácie o použití sledovania komunikácie obsahuje časť Sledovanie komunikácie.

Použitie voľby LDAP_OPT_DEBUG na sledovanie chýb

Od V5R2 môžete používať voľbu LDAP_OPT_DEBUG rozhrania API **ldap_set_option()** na sledovanie problémov s klientmi, ktorí používajú API LDAP C. Voľba ladenia má nastavenie viacerých úrovní ladenia, ktoré môžete použiť na pomoc pri odstraňovaní problémov s týmito aplikáciami.

Nasleduje príklad povolenia klientskej voľby ladenia sledovania.

```
int  debugvalue=  LDAP_DEBUG_TRACE  |  LDAP_DEBUG_PACKETS;
ldap_set_option(    1d,  LDAP_OPT_DEBUG,  &debugvalue);
```

Iným spôsobom nastavenia úrovne ladenia je nakonfigurovať numerickú hodnotu premennej prostredia LDAP_DEBUG pre úlohu, v ktorej je spustená klientska aplikácia na rovnakú numerickú hodnotu, ktorou by debugvalue bola, ak by sa použilo API **ldap_set_option()** .

Nasleduje príklad povolenia sledovania klienta pomocou premennej prostredia LDAP_DEBUG:

```
ADDENVVAR  ENVVAR(LDAP_DEBUG)  VALUE(0x0003)
```

Po spustení klienta, ktorý spôsobuje váš problém, napíšte do výzvy iSeries toto:

```
DMPUSRTRC    ClientJobNumber
```

kde ClientJobNumber je číslo úlohy klienta.

Ak chcete túto informáciu zobraziť interaktívne, napíšte do výzvy iSeries nasledujúce:

```
DSPPFM  QAPOZDMP  QPOZnnnnnn
```

kde nnnnnn je číslo úlohy.

Ak chcete uložiť tieto informácie s cieľom odoslať ich do servisu, postupujte takto:

1. Pomocou príkazu CRTSAVF (Create SAVF) vytvorte súbor SAVF.
2. Do príkazovej výzvy iSeries napíšte nasledujúce:

   ```
   SAVOBJ  OBJ(QAPOZDMP  LIB(QTEMP)  DEV(*SAVF)  SAVF(xxx)
   ```

   kde *xxx* je názov, ktorý ste uviedli pre súbor SAVF.

Obvyklé chyby klienta LDAP

Poznanie príčin obvyklých problémov klientov LDAP vám pomôže vyriešiť problémy s vaším serverom. Úplný zoznam chybových podmienok klienta LDAP nájdete v téme OS/400 adresárové služby pod Programovaním v iSeries Information Center.

Chybové správy klienta majú nasledujúci formát:

```
[Zlyhanie operácie LDAP]:[chybový stav API klienta LDAP]
```

Poznámka: Vysvetlenie týchto chýb predpokladá, že klient komunikuje so serverom LDAP na OS/400. Klient komunikujúci so serverom na inej platforme sa môže stretnúť s podobnými chybami, ale príčiny a ich náprava budú pravdepodobne odlišné.

Bežné správy majú nasledujúci obsah:

- “ldap_search: Timelimit exceeded”
- “[Zlyhanie operácie LDAP]: Chyba operácií”
- “ldap_bind: Žiadny objekt tohto typu”
- “ldap_bind: Inappropriate authentication”
- “[Failing LDAP operation]: Insufficient access”
- “[neúspešná operácia LDAP]: nemožno kontaktovať server LDAP”
- “[zlyhanie operácie LDAP]: Nepodarilo sa pripojiť k SSL serveru” na strane 65

ldap_search: Timelimit exceeded

Táto chyba nastane pri pomalom vykonávaní ldapsearch. Môžete ju opraviť týmito činnosťami:

- zväčšite časový limit vyhľadávania adresárového LDAP servera. Pozrite si “Úprava výkonu adresárového servera LDAP” na strane 32, ak potrebujete pomoc.
- Znížte aktivitu na vašom systéme. Môžete znížiť aj počet aktívnych spustených úloh klienta LDAP.

[Zlyhanie operácie LDAP]: Chyba operácií

Túto chybu môže spôsobiť viacero príčin. Ak v konkrétnom prípade chcete zistiť príčinu chyby, pozrite si protokoly QDIRSRV a Structured Query Language (SQL) úloh servera, ako sa uvádza v téme “Základné postupy pri odstraňovaní chýb v Directory Services” na strane 61.

ldap_bind: Žiadny objekt tohto typu

Bežnou príčinou tejto chyby je, že keď užívateľ vykonáva operáciu, urobí chybu pri písaní. Ďalšou bežnou príčinou býva, keď sa klient LDAP pokúsi o väzbu s DN, ktorý neexistuje, čo sa často stáva, keď používateľ zadá čosi, o čom sa chybne domnieva, že ide o správcu DN. Užívateľ môže napríklad uviesť QSECOFR alebo Administrator, keď skutočný DN správcu môže byť niečo ako cn=Administrator.

Ak potrebujete informácie o tejto chybe, pozrite sa do protokolu úlohy QDIRSRV, ako je popísané v “Základné postupy pri odstraňovaní chýb v Directory Services” na strane 61.

ldap_bind: Inappropriate authentication

Keď je heslo alebo DN vytvorenia väzby nesprávny, server vráti neplatné oprávnenia. Server vracia nevhodnú autentifikáciu, keď sa klient pokúša vytvoriť väzbu buď ako:

- Položka, ktorá nemá atribút userpassword
- Položka, ktorá reprezentuje užívateľa OS/400, ktorý má atribút UID a nemá atribút userpassword. Tým nastane porovnávanie medzi uvedeným heslom a užívateľským heslom OS/400, ktoré sa nezhodujú.
- Položka, ktorá predstavuje projektovaného užívateľa a inú metódu pripojenia, než bola požadovaná.

Táto chyba sa vyskytne vtedy, keď sa klient pokúša pripojiť použitím hesla, ktoré nie je platné. Ak potrebujete informácie o tejto chybe, pozrite sa do protokolu úlohy QDIRSRV, ako je popísané v “Základné postupy pri odstraňovaní chýb v Directory Services” na strane 61.

[Failing LDAP operation]: Insufficient access

Táto chyba sa zvyčajne vyskytne vtedy, keď pripájané DN nemá oprávnenie na vykonanie operácie (ako napríklad pridať alebo vymazať), ktorú klient požaduje. Ak potrebujete informáciu o tejto chybe, pozrite sa do protokolu úlohy QDIRSRV, ako sa uvádza v téme “Základné postupy pri odstraňovaní chýb v Directory Services” na strane 61.

[neúspešná operácia LDAP]: nemožno kontaktovať server LDAP

Najčastejšie príčiny tejto chyby sú nasledujúce:

- LDAP klient zadá požiadavku predtým, než je LDAP server na danom systéme pripravený a v režime očakávania výberov.
- Používateľ špecifikuje číslo portu, ktoré je neplatné. Napríklad: server je pripravený na porte 386, ale požiadavka klienta smeruje na port 387.

Ak potrebujete informáciu o tejto chybe, pozrite sa do protokolu úlohy QDIRSRV, ako sa uvádza v téme “Základné postupy pri odstraňovaní chýb v Directory Services” na strane 61. Ak bol server adresárových služieb úspešne spustený, jeho správa sa bude nachádzať v protokole úloh QDIRSRV.

[zlyhanie operácie LDAP]: Nepodarilo sa pripojiť k SSL serveru

Táto chyba sa vyskytuje vtedy, keď LDAP server odmietne spojenie s klientom preto, lebo sa nedá nastaviť zásuvka bezpečného spojenia. Môže to byť spôsobené jednou z nasledujúcich príčin:

- Podpora riadenia certifikátov odmietne pokus klienta o pripojenie sa k serveru. Použite Správcu digitálnych certifikátov, aby ste zabezpečili, že vaše certifikáty sú nastavené správne, potom reštartujte server a pokúste sa znovu pripojiť.
- Používateľ možno nemá prístup na čítanie do súboru certifikátov *SYSTEM (štandardne /QIBM/userdata/ICSS/Cert/Server/default.kdb).

Pre aplikácie OS/400 C sú dostupné ďalšie chybové informácie SSL. Detaily pozrite v dokumentácii o jednotlivých Directory Services API.

Vytlačené v USA