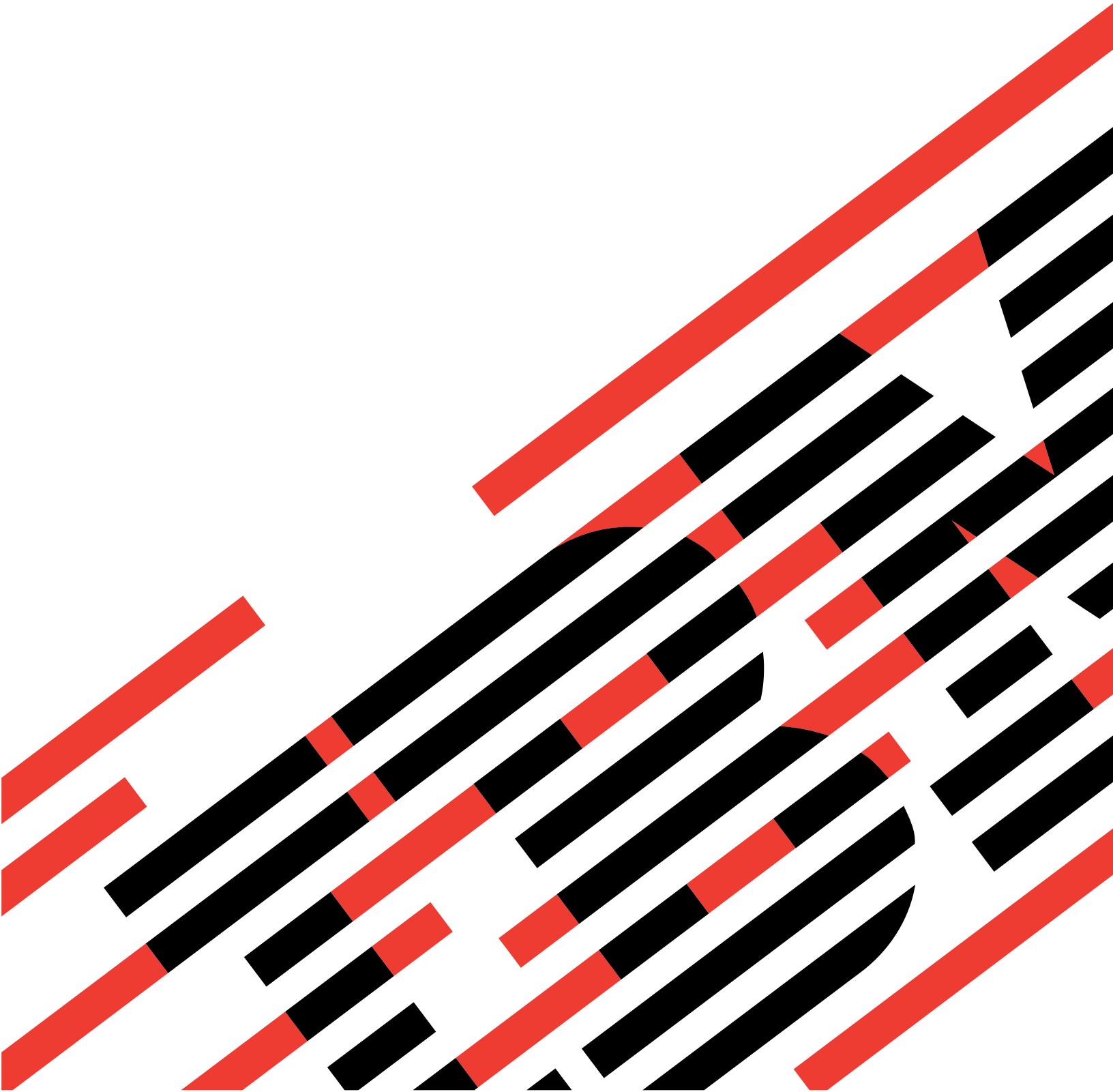
IBM

eserver

iSeries

Networking LDAP (Directory Services)



IBM

@server

iSeries

Networking LDAP (Directory Services)

Obsah

Část 1. Directory Services (LDAP)

Produkt Directory Services poskytuje server LDAP (Lightweight Directory Access Protocol) na serveru iSeries. LDAP využívá protokol TCP/IP (Transmission Control Protocol/Internet Protocol) a je s oblibou stále více používán jako adresářová služba pro internetové a neinternetové aplikace.

Jste-li již s produktem Directory Services obeznámeni, můžete začít s částí Co je nového v tomto vydání. V případě potřeby si můžete vytisknout nebo prohlédnout PDF verzi této dokumentace k produktu Directory Services.

Níže uvedené části vás seznámí s produktem Directory Services a poskytnou vám informace potřebné k administraci serveru LDAP na serveru iSeries:

Kapitola 3, “Začínáme s produktem Directory Services” na stránce 7.

Kapitola 4, “Administrace serveru adresářů LDAP” na stránce 19.

Kapitola 5, “Koncepce a referenční informace týkající se produktu Directory Services” na stránce 33.

Kapitola 6, “Obslužné programy příkazové řádky LDAP” na stránce 47.

Kapitola 7, “Odstraňování problémů s produktem Directory Services” na stránce 61.

Další informace o produktu Directory Services najdete na webové stránce Directory Services 

Server LDAP, který produkt Directory Services obsahuje, je produkt IBM SecureWay Directory. 

Kapitola 1. Co je nového ve verzi V5R2

LDAP (Directory Services) obsahuje tato vylepšení a nové funkce.

- Počínaje verzí V5R1 je LDAP (Directory Services) součástí základního operačního systému. Od verze V5R2 již není k dispozici volba 32.
- Byla provedena nová vylepšení zabezpečení ochrany dat kvůli lepší ochraně dat uložených na serveru adresářů.
- Server adresářů LDAP je nyní možné používat jako řadič domény pro doménu EIM (Enterprise Identity Mapping).
- Pro administrátory je k dispozici nová volba, pomocí níž můžete udělit administrátorovi přístup k serveru adresářů pro uživatele, kteří získali přístup k identifikátoru (ID) funkce QIBM_DIRSRV_ADMIN (Directory Services Administrator) operačního systému prostřednictvím aplikační podpory iSeries Navigator.
- Můžete si zvolit, aby server adresářů používal specifické IP adresy nebo aby používal všechny IP adresy nakonfigurované na serveru. Více informací najdete v části “Jak změnit port nebo IP adresu” na stránce 21.
- Rozhraní API **ldap_set_option** má novou funkci trasování s laděním pro verzi V5R2. Volbu LDAP_OPT_DEBUG je možné použít při diagnostikování problémů s klienty, kteří používají LDAP API. Více informací najdete v tématu “Použití volby LDAP_OPT_DEBUG při sledování chyb” na stránce 63 nebo Directory Services APIs v rámci aplikace iSeries Information Center. 

Jak zjistit, co je nového nebo co se změnilo:

Tyto obrázky v dokumentaci označují, kde byly provedeny technické změny:

-  označuje, kde informace o novinkách nebo změnách začínají.
-  označuje, kde informace o novinkách nebo změnách končí.

Kapitola 2. Tisk tohoto tématu

Chcete-li si prohlédnout nebo stáhnout PDF verzi, vyberte odkaz OS/400 Directory Services (LDAP) (přibližně 323 KB nebo 66 stránek).

Ostatní informace

Můžete si rovněž prohlédnout nebo vytisknout tyto PDF:

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

Chcete-li uložit soubor PDF na pracovní stanici za účelem prohlížení nebo tisku:
1. Otevřete soubor PDF v prohlížeči (klepněte na výše uvedený odkaz).
2. V menu prohlížeče klepněte na volbu **Soubor (File)**.
3. Klepněte na **Uložit jako... (Save As...)**.
4. Vyhledejte adresář, do něhož chcete soubor PDF uložit.
5. Klepněte na **Uložit (Save)**.

Stažení aplikace Adobe Acrobat Reader

Jestliže potřebujete aplikaci Adobe Acrobat Reader k prohlížení nebo vytisknutí těchto souborů PDF, můžete si stáhnout její kopii z webové stránky Adobe (www.adobe.com/products/acrobat/readstep.html).

Kapitola 3. Začínáme s produktem Directory Services

Produkt Directory Services poskytuje server LDAP (Lightweight Directory Access Protocol) na serveru iSeries. LDAP využívá protokol TCP/IP (Transmission Control Protocol/Internet Protocol) a je s oblibou stále více používán jako adresářová služba pro internetové i neinternetové aplikace. Většinu úkolů týkajících se instalace a administrace serveru adresářů LDAP na bázi operačního systému OS/400 lze provádět v grafickém uživatelském rozhraní (GUI) produktu iSeries Navigator. Chcete-li provádět administraci produktu Directory Services, musíte mít PC, který je připojen k serveru iSeries, a dále musíte mít nainstalován produkt iSeries Navigator. Produkt Directory Services lze používat u aplikací s podporou LDAP, jako jsou například poštovní aplikace, které vyhledávají e-mailové adresy na serverech LDAP.

Kromě serveru LDAP nabízí produkt Directory Services i další funkce:

- Klient LDAP na bázi operačního systému OS/400. Tento klient obsahuje sady API, které můžete používat v programech operačního systému OS/400 k vytváření vlastních aplikací typu klient. Informace o těchto API najdete v tématu Directory Services pod tématem Programming v rámci aplikace iSeries Information Center.
- Verze 3.2 produktu IBM SecureWay Directory Client Software Development Kit (SDK). Produkt SDK poskytuje klienta LDAP pro Windows a dále tyto nástroje:
  - Produkt IBM SecureWay Directory Management Tool, který poskytuje grafické uživatelské rozhraní pro správu obsahu adresáře.
  - Obslužné programy příkazové řádky (ldapsearch, ldapadd atd.).
  - Rozhraní C LDAP API (soubory knihoven, soubory záhlaví a vzor zdrojového kódu).
  - Poskytovatel služeb IBM JNDI LDAP (ibmjndi.jar).
  - Online dokumentace ke všem uvedeným položkám. Umístění a názvy těchto HTML souborů jsou uvedeny v souboru readme.

Jestliže jste produkt Directory Services používali v nižší verzi operačního systému OS/400, přečtěte si část “Jak migrovat na verzi V5R2 z předchozí verze produktu Directory Services” na stránce 11.

Úvod k LDAP najdete v části “Základní informace o LDAP” na stránce 8. I když jste již používali LDAP na jiných platformách, měli byste si přečíst tuto část, která uvádí některé informace specifické pro operační systém OS/400.

Až se seznámíte s těmito základními informacemi, přejděte na část “Jak plánovat server adresářů LDAP” na stránce 11.

Informace o instalaci a konfiguraci serveru adresářů najdete v části “Instalace a konfigurace produktu Directory Services” na stránce 14.

Dokumentace

Téma Directory Services v rámci aplikace Information Center podává přehled o LDAP s důrazem na správu serveru adresářů LDAP v operačním systému OS/400. Tato dokumentace obsahuje také kompletní dokumentaci k produktu SecureWay Directory Client SDK. Další informace o LDAP najdete pod odkazy k LDAP, například:

- *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* (autoři: Tim Howes a Mark Smith).
- *Understanding and Deploying LDAP Directory Services* (autoři: Mark C. Smith, Gordon S. Good a Tim Howes).

Další informace o produktu Directory Services na serveru iSeries jsou k dispozici na domovské stránce iSeries server Directory Services.

Poznámka: Některé z materiálů obsažených v tomto dokumentu jsou převzaty z dokumentace Michiganské univerzity: Copyright © 1992-1996, Správa Michiganské univerzity, všechna práva vyhrazena.

Základní informace o LDAP

LDAP (Lightweight Directory Access Protocol) je protokol adresářových služeb, který pracuje nad protokolem TCP/IP (Transmission Control Protocol/Internet Protocol). LDAP verze 2 je formálně definován v RFC (Request for Comments) č. 1777, *Lightweight Directory Access Protocol*, vydaném společností IETF. LDAP verze 3 je formálně definován v RFC č. 2251, *Lightweight Directory Access Protocol (V3)*, vydaném společností IETF. Tyto RFC najdete na níže uvedené adrese:

http://www.ietf.org

Adresářové služby LDAP jsou vystavěny na modelu klient/server. Jeden nebo více serverů LDAP obsahuje data adresáře. Klient LDAP se připojí k serveru LDAP a vyšle požadavek. Server vrátí buď odpověď, nebo odkaz na jiný server LDAP.

Použití LDAP:

Protože LDAP jsou adresářové služby a nikoli databáze, jsou informace v adresáři LDAP obvykle popisné, založené na atributech. Uživatelé LDAP totiž mnohem častěji informace v adresáři pouze čtou, než aby je měnili. Aktualizace spočívají obvykle v jednoduchých změnách typu všechno nebo nic. K běžnému využití adresářů LDAP patří online telefonní adresáře a adresáře elektronické pošty.

Struktura adresáře LDAP:

Model adresářových služeb LDAP je založen na **záznamech** (kterým se rovněž říká **objekty**). Každý záznam obsahuje jeden nebo více **atributů**, jako je jméno nebo adresa, a **typ**. Typy jsou obvykle mnemonické řetězce, například cn jako common name (obecný název) nebo mail jako e-mailová adresa.

Obrázek 1 na stránce 10 je příkladem adresáře, který obsahuje záznam o Timu Jonesovi s uvedením atributů *mail* a *telephoneNumber*. Dalšími možnými atributy jsou *fax*, *title*, *sn* (jako příjmení) a *jpegPhoto*.

Každý adresář má určité **schéma**, což je sada pravidel, která určují strukturu a obsah adresáře. K editaci souborů schémat pro server LDAP slouží nástroj IBM SecureWay Directory Management Tool (DMT). Po instalaci produktu Directory Services jsou tyto soubory uloženy v systému v adresáři /QIBM/UserData/OS400/DirSrv.

Poznámka: Původní kopie souborů s předvolenými schématy se nacházejí v adresáři /QIBM/ProdData/OS400/DirSrv. Chcete-li nahradit soubory v adresáři UserData, můžete tyto soubory zkopírovat do adresáře QIBM/ProdData/OS400/DirSrv.

Každý záznam obsahuje zvláštní atribut **objectClass**. Tento atribut řídí, které atributy v daném záznamu jsou povinné nebo povolené. Jinými slovy, atribut objectClass určuje pravidla schématu, která musí daný záznam zachovávat.

Každý záznam v adresáři obsahuje tyto **operační atributy**, které server LDAP udržuje automaticky:

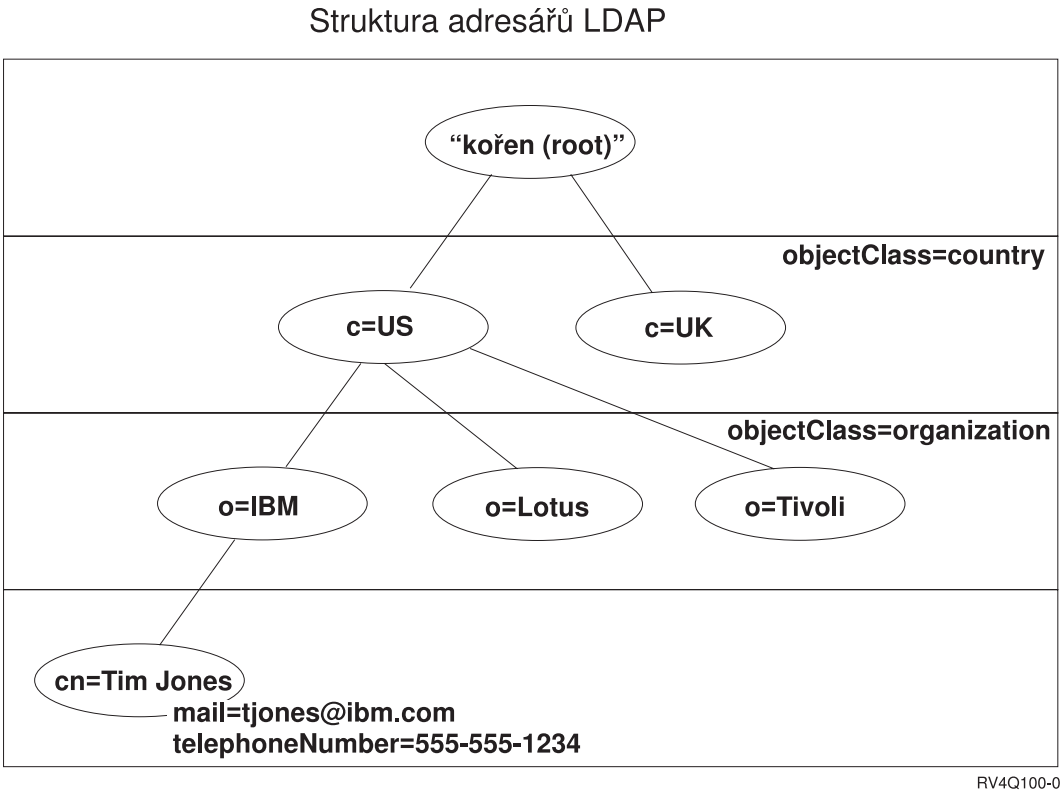
- CreatorsName obsahující DN (rozlišovací jméno), které bylo použito při vytváření záznamu.
- CreateTimestamp obsahující čas, kdy byl záznam vytvořen.
- modifiersName obsahující DN, které bylo použito při poslední modifikaci záznamu (na počátku je tato hodnota shodná s atributem CreatorsName).
- modifyTimestamp obsahující čas, kdy byl záznam naposledy modifikován (na počátku je tato hodnota shodná s atributem CreateTimestamp).

Záznamy v adresáři LDAP jsou tradičně uspořádány do hierarchické struktury, která odráží politické, geografické nebo organizační hranice (viz Obrázek 1 na stránce 10). Záznamy, které představují země, jsou na nejvyšší úrovni této hierarchické struktury. Záznamy, které představují státní a národní organizace, zaujímají v hierarchii druhou úroveň. Záznamy na dalších úrovních mohou představovat osoby, organizační jednotky, tiskárny, dokumenty nebo jiné položky.

Při tvorbě struktury adresáře nejste vázáni touto tradiční hierarchií. Oblibu získává například struktura doménových komponent. V této struktuře se záznamy skládají z částí jmen domén TCP/IP. Například dc=ibm, dc=com může být vhodnější než o=ibm, c=us.

LDAP se na záznamy odkazuje pomocí **rozlišovacího jména**, neboli DN (Distinguished Name). Rozlišovací jména jsou tvořena jménem záznamu a jmény nadřazených objektů v adresáři směrem zdola nahoru. Například plné DN pro záznam v levém dolním rohu je cn=Tim Jones, o=IBM, c=US (Obrázek 1 na stránce 10). Každý záznam obsahuje minimálně jeden atribut, který pojmenovává vlastní záznam. Tento atribut se nazývá **relativní rozlišovací jméno, neboli RDN (Relative Distinguished Name)** záznamu. Záznam nad tímto RDN se nazývá **nadřazené rozlišovací jméno**. Ve výše uvedeném příkladu je vlastní záznam pojmenován cn=Tim Jones, je to tedy RDN. o=IBM, c=US je nadřazené DN pro cn=Tim Jones.

Aby server LDAP mohl spravovat část adresáře LDAP, je třeba v konfiguraci serveru specifikovat nadřazená rozlišovací jména nejvyšší úrovně. Tato rozlišovací jména se nazývají **přípony**. Server má přístup ke všem objektům, které se v hierarchii adresáře nacházejí pod zadanou příponou. Obsahuje-li server LDAP například adresář, který znázorňuje Obrázek 1 na stránce 10, měl by mít v konfiguraci zadánu příponu o=ibm, c=us, aby mohl uspokojit dotazy klienta týkající se Tima Jonese.



Obrázek 1. Základní struktura adresáře LDAP

Poznámky k LDAP a produktu Directory Services:

- Počínaje verzí V4R5 jsou server i klient LDAP pro OS/400 založeny na LDAP verze 3. Klientem verze 2 se lze připojit k serveru verze 3. Nelze se však připojit klientem V3 k serveru V2. To je možné pouze tak, že se připojíte jako klient V2 a používáte pouze rozhraní API pro V2. Podrobnější informace najdete v části Pokyny k LDAP V2/V3.
- Klient LDAP pro Windows je rovněž založen na LDAP verze 3.
- Protože je LDAP standardem, všechny servery LDAP mají mnoho společných charakteristik. Vlivem rozdílů v implementacích však nemusí být navzájem plně kompatibilní. Server LDAP produktu Directory Services je dokonale kompatibilní s ostatními servery adresářů LDAP ze skupiny produktů IBM SecureWay Directory a IBM Directory. Nemusí však být tak dobře kompatibilní s jinými servery LDAP.
- Data serveru LDAP, který obsahuje produkt Directory Services, jsou uložena v databázi operačního systému OS/400.

Další informace:

Příklady použití adresářů LDAP najdete v následujících částech těchto červených knih:

- Část 1.6 - The Quick Start: A Public LDAP Example v červené knize *Understanding LDAP*.
- Část 3.3 - Example Scenarios v červené knize Understanding LDAP.

Více informací o koncepcích LDAP uvádí Kapitola 5, “Koncepce a referenční informace týkající se produktu Directory Services” na stránce 33.

Pokyny pro používání LDAP V2 v kombinaci s LDAP V3

Počínaje verzí V4R5 jsou server i klient LDAP pro OS/400 založeny na LDAP verze 3. Nemůžete použít klienta V3 se serverem V2. Můžete však pomocí rozhraní API ldap_set_option() změnit verzi klienta z V3 na V2. Potom můžete úspěšně posílat požadavky z tohoto klienta na server verze 2.

Klienta V2 můžete použít se serverem V3. Pamatujte si však, že u požadavku na vyhledání může server V3 vracet data v plném formátu UTF-8, avšak klient může pracovat pouze s daty ve znakové sadě IA5.

Poznámka: LDAP verze 2 je formálně definován v RFC (Request for Comments) č. 1777, *Lightweight Directory Access Protocol*, vydaném společností IETF. LDAP verze 3 je formálně definován v RFC č. 2251, *Lightweight Directory Access Protocol (V3)*, vydaném společností IETF. Tyto RFC najdete na níže uvedené adrese:

http://www.ietf.org

Jak plánovat server adresářů LDAP

Než přikročíte k instalaci produktu Directory Services a ke konfiguraci adresáře LDAP, měli byste tento adresář předem naplánovat. Přitom byste měli věnovat pozornost několika důležitým aspektům:

- **Organizace adresáře**. Naplánujte strukturu adresáře a určete, jaké přípony a atributy bude server vyžadovat.
- **Rozhodnutí, jak bude adresář velký**. Potom můžete odhadnout, kolik paměti budete potřebovat. Velikost adresáře závisí na těchto faktorech:
  - Počet atributů ve schématu serveru.
  - Počet záznamů na serveru.
  - Typ informací, které budou na serveru uloženy.

  Například prázdný adresář používající předvolené schéma produktu Directory Services vyžaduje asi 10 MB paměťového prostoru. Adresář, který používá předvolené schéma a obsahuje přibližně 1000 záznamů s běžnými informacemi o zaměstnancích, vyžaduje asi 30 MB paměťového prostoru. Toto číslo se bude lišit v závislosti na konkrétních použitých atributech. Jeho velikost též rapidně vzroste v případě, že adresář obsahuje velké objekty, jako například obrázky.
- **Rozhodnutí, jaká bezpečnostní opatření použijete**. Produkt Directory Services podporuje použití SSL (Secure Sockets Layer) a digitálních certifikátů i TLS (Translation Layer Security), které zajišťují bezpečnost komunikací. Počínaje verzí V5R1 je také podporována autentizace Kerberos.
- Produkt Directory Services umožňuje řídit přístup k objektům adresáře pomocí přístupových seznamů (ACL). K zabezpečení adresáře můžete použít i funkci monitorování zabezpečení poskytovanou operačním systémem OS/400.

Jak migrovat na verzi V5R2 z předchozí verze produktu Directory Services

V operačním systému OS/400 verze V5R2 byl produkt Directory Services rozšířen o nové funkce a možnosti. Tyto změny se týkají jak serveru adresářů LDAP, tak i grafického uživatelského rozhraní (GUI) produktu iSeries Navigator. Chcete-li využít nových možností GUI, je třeba nainstalovat produkt iSeries Navigator na PC, který s vaším serverem iSeries komunikuje přes TCP/IP. iSeries Navigator je komponentou produktu iSeries Access for Windows. Máte-li nainstalovánu nižší verzi produktu iSeries Navigator, měli byste přejít na verzi V5R2.

Operační systém OS/400 verze V5R2 podporuje přechod z verzí V4R5 a V5R1. Přecházíte-li na verzi V5R2 operačního systému OS/400, provede se automaticky migrace dat adresáře LDAP i souborů schémat adresáře tak, aby odpovídaly formátům verze V5R2. Pracuje-li váš server LDAP produktu Directory Services pod operačním systémem OS/400 verze V4R3 nebo V4R4 a chcete-li migrovat na verzi V5R2, je třeba provést několik dalších úkolů migrace.

Když přecházíte na verzi V5R2 operačního systému OS/400, mějte na paměti několik skutečností spojených s migrací:

- Při přechodu na verzi V5R2 produkt Directory Services automaticky provede migraci souborů schémat na verzi V5R2 a staré soubory schémat vymaže. Pokud jste však původní soubory schémat odstranili nebo

přejmenovali, produkt Directory Services nemůže provést jejich migraci. Buď se zobrazí chyba, nebo produkt Directory Services usoudí, že tyto soubory již byly migrovány.

- Produkt Directory Services migruje data adresáře na formát V5R2 v okamžiku prvního spuštění serveru nebo prvního importu souboru LDIF. Při plánování vyhraďte určitý čas, aby se migrace dat mohla dokončit. Přecházíte-li na verzi V5R2 z verze V4R4 nebo nižší, uvědomte si, že data adresáře budou ve verzi V5R2 potřebovat přibližně dvakrát více prostoru. Důvod je ten, že ve verzi V4R4 nebo v nižších verzích produkt Directory Services podporoval pouze znakovou sadu IA5 a data ukládal ve formátu ccsid 37 (jednobajtový formát). Produkt Directory Services podporuje plnou znakovou sadu ISO 10646.

  Po přechodu na verzi V5R2 byste měli nejprve jednou spustit server, aby se provedla migrace existujících dat, a teprve potom importovat nová data. Pokusíte-li se o import bez předchozího spuštění serveru, a nemáte-li patřičné oprávnění, může import selhat.
- Verze V4R4 a nižší verze produktu Directory Services nebraly při vytváření záznamů s časovým označením v úvahu časová pásma. Počínaje verzí V4R5 se již při všech doplňcích i změnách počítá s časovými pásmy. Přecházíte-li tedy na verzi V5R2 z verze V4R4 nebo nižší, upraví produkt Directory Services existující atributy createtimestamp a modifytimestamp tak, aby odpovídaly správnému časovému pásmu. Provede to odečtením časového pásma, které je definováno na serveru iSeries, od časových údajů, které jsou uloženy v adresáři. Pamatujte si, že pokud aktuální časové pásmo není shodné s časovým pásmem, které bylo aktivní při původním vytvoření nebo modifikaci záznamů, nové hodnoty časových údajů nebudou odpovídat původnímu časovému pásmu.
- Po migraci se server adresářů LDAP bude spouštět automaticky při spuštění TCP/IP. Nechcete-li, aby se server adresářů spouštěl automaticky, můžete pomocí produktu iSeries Navigator toto nastavení změnit.

Jak migrovat z verze V4R3 nebo V4R4 produktu Directory Services na verzi V5R2

Verze V5R2 operačního systému OS/400 nepodporuje přímý přechod z verze V4R3. Chcete-li provést migraci verze V4R3 nebo V4R4 serveru LDAP produktu Directory Services na verzi V5R2, použijte jeden z těchto postupů:

- Postupná instalace operačního systému OS/400 (s mezikrokem) z verze V4R3 nebo V4R4 na prozatímní verzi.
- Uložení databázové knihovny a instalace typu scratch operačního systému OS/400 z verze V4R3 nebo V4R4 na verzi V5R2.

Postupná instalace operačního systému OS/400 z verze V4R3 nebo V4R4 na prozatímní verzi

Ačkoli není podporován přechod z verze V4R3 a V4R4 operačního systému OS/400 na verzi V5R2, jsou podporovány tyto přechody:

- Přechod z vrze V4R3 a V4R4 na verzi V4R5.
- Přechod z verze V4R4 a V4R5 na verzi V5R1.
- Přechod z verze V4R5 a V5R1 na verzi V5R2.

Jedním ze způsobů, jak migrovat server Directory Services, je přejít na prozatímní verzi (V4R5 nebo V5R1) a potom na verzi V5R2. Podrobné informace o postupech při instalaci operačního systému OS/400 najdete v publikaci *Instalace software.*  Chcete-li provést migraci, postupujte takto:

1. Zaznamenejte si všechny změny, které jste provedli u souborů schémat v adresáři /QIBM/UserData/OS400/DirSrv. Migrace souborů schémat se provádí automaticky.
2. Pro verzi V4R4 nebo V4R3 proveďte postupnou instalaci (s mezikrokem) na verzi V4R5 nebo V5R1 operačního systému OS/400.
3. Proveďte postupnou instalaci na verzi V5R2 operačního systému OS/400.
4. Spusťte server Directory Services, není-li již spuštěn.
5. Pomocí nástroje DMT (Directory Management Tool) změňte soubory schémat podle uživatelských změn, které jste si poznamenali v kroku 1.

6. Znovu spusťte server Directory Services.

Uložení databázové knihovny a instalace typu scratch operačního systému OS/400 z verze V4R3 nebo V4R4 na verzi V5R2

Další způsob migrace serveru Directory Services je uložit databázovou knihovnu, kterou server Directory Services používá ve verzi V4R3 nebo V4R4, a obnovit ji po instalaci typu scratch verze V5R2. To vám ušetří jeden krok - instalaci prozatímní verze. Neprovede se však migrace nastavení serveru, a proto je ho třeba znovu nakonfigurovat. Podrobné informace o postupech při instalaci operačního systému OS/400 najdete v publikaci *Instalace software.*  Chcete-li provést migraci, postupujte takto:

1. Poznamenejte si všechny změny, které jste provedli u souborů schémat v adresáři /QIBM/UserData/OS400/DirSrv. Soubory schémat nejsou totiž migrovány automaticky, takže chcete-li zachovat provedené změny, musíte je ručně znovu implementovat.
2. Poznamenejte si různá konfigurační nastavení ve vlastnostech serverů Directory Services, včetně jména databázové knihovny.
3. Uložte databázovou knihovnu, která je uvedena v konfiguraci serveru Directory Services.
4. Poznamenejte si konfiguraci publikování.
5. Proveďte instalaci typu scratch systému na verzi V5R2 operačního systému OS/400.
6. Pomocí produktu EZ-Setup nakonfigurujte server Directory Services.
7. Obnovte databázovou knihovnu, kterou jste uložili v kroku 3.
8. Pomocí nástroje DMT (Directory Management Tool) změňte soubory schémat podle uživatelských změn, které jste si poznamenali v kroku 1.
9. Pomocí produktu iSeries Navigator znovu nakonfigurujte produkt Directory Services. Zadejte databázovou knihovnu, kterou jste uložili a obnovili.
10. Pomocí produktu iSeries Navigator znovu nakonfigurujte publikování.
11. Znovu spusťte server Directory Services.

Aspekty přechodu na vyšší verzi

Při přechodu z verze V4R3 na jakoukoli vyšší verzi byste si měli uvědomit tyto skutečnosti:

- **Migrace souboru řetězců klíčů na databázi klíčů:**

  Soubory řetězců klíčů ve verzi V3R2 produktu Client Access sloužily k vytváření připojení k serveru adresářů LDAP přes SSL. Produkt iSeries Access for Windows používá k vytváření připojení přes SSL paměti certifikátů, kterým se také říká databáze klíčů. Jestliže jste na serveru adresářů LDAP používali soubor řetězců klíčů, musí být tento soubor konvertován na databázi klíčů, aby bylo možné nadále používat SSL. Když se poprvé pokusíte připojit k serveru adresářů LDAP přes SSL, produkt iSeries Navigator vás upozorní na nutnost této změny. Rozhodnete-li se klíče konvertovat, budete vyzváni k zadání údajů týkajících se databáze klíčů, a poté se konverze provede.

  Server adresářů LDAP ve verzi V4R3 používal soubor řetězců klíčů i pro svá vlastní připojení přes SSL. Počínaje verzí V4R4 používá tento server paměť certifikátů systému. Byl-li ve verzi V4R3 server nastaven na používání SSL, provede se migrace obsahu souboru řetězců klíčů na paměť certifikátů systému.
- **Odstraní se dva proudové soubory:**

  Tyto dva proudové soubory používané verzí V4R3 produktu Directory Services již nejsou po instalaci vyšší verze potřebné a automaticky se odstraní:

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

  Stěmito soubory nemusíte vůbec nic dělat. Zmiňujeme se o nich pouze proto, abyste nebyli překvapeni, že již v systému nejsou.

Uvědomte si rovněž, že s přechodem na současnou verzi z jiných verzí souvisejí ještě další aspekty.

Instalace a konfigurace produktu Directory Services

Produkt Directory Services (LDAP) se automaticky instaluje při instalaci operačního systému OS/400. Server adresářů obsahuje předvolenou konfiguraci, která automaticky spouští server adresářů při spuštění TCP/IP. Server adresářů rovněž spustí publikování informací o počítači z operačního systému OS/400 na server adresářů. Chcete-li přizpůsobit nastavení serveru adresářů LDAP vlastním potřebám, spusťte Průvodce konfigurací produktu Directory Services. K použití tohoto průvodce musíte mít zvláštní oprávnění *ALLOBJ a *IOSYSCFG.

Počínaje verzí V5R1 je produkt Directory Services integrován do základního operačního systému a od verze V5R2 již není dostupná volba 32.

Jak konfigurovat server adresářů LDAP

Pokud systém nebyl nakonfigurován pro publikování informací na jiném serveru LDAP a na serveru DNS TCP/IP nejsou uvedeny žádné servery LDAP, nainstaluje se produkt Directory Services automaticky s omezenou předvolenou konfigurací. Produkt Directory Services obsahuje průvodce, který vám pomůže nakonfigurovat server adresářů LDAP podle vašich potřeb. Tohoto průvodce můžete spustit jako součást funkce EZ-Setup nebo jej můžete spustit později v prostředí produktu iSeries Navigator. Použijte jej při počáteční konfiguraci serveru adresářů. Můžete jej použít i k překonfigurování serveru adresářů.

Poznámka: Jestliže pomocí tohoto průvodce provádíte překonfigurování serveru adresářů, zahajujete konfiguraci z pracovního média. Původní konfigurace se nezmění, ale vymaže. Data z adresáře však nejsou vymazána, ale zůstávají uložena v knihovně, kterou jste zvolili při instalaci (předvolená je QUSRDIRDB). Protokol o změnách zůstane rovněž neporušený v předvolené knihovně QUSRDIRCL.

Chcete-li začít zcela znovu z pracovního média, vyčistěte tyto dvě knihovny, než spustíte průvodce.

Chcete-li pouze změnit konfiguraci serveru adresářů, nikoli jej zcela vyčistit, klepněte pravým tlačítkem myši na **Adresář** a vyberte volbu **Vlastnosti**.Tím se nevymaže původní konfigurace.

Ke konfiguraci serveru adresářů musíte mít zvláštní oprávnění *ALLOBJ a *IOSYSCFG. Chcete-li konfigurovat monitorování zabezpečení operačního systému OS/400, musíte mít i zvláštní oprávnění *AUDIT.

Ke spuštění průvodce konfigurací produktu Directory Services použijte tento postup:

1. V prostředí produktu iSeries Navigator rozbalte položku **Síť**.
2. Rozbalte položku **Servery**.
3. Klepněte na **TCP/IP**.
4. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Konfigurovat**.

   Poznámka: Máte-li již server adresářů nakonfigurován, vyberte namísto volby **Konfigurovat** volbu **Překonfigurovat**.

Podle instrukcí, které zobrazuje průvodce konfigurací serveru adresářů, proveďte konfiguraci serveru adresářů LDAP.

Poznámka: Knihovnu, která uchovává data adresáře, můžete uložit i do uživatelského ASP namísto systémového ASP. Tato knihovna však nemůže být uložena jako nezávislé ASP a všechny pokusy o konfiguraci, opětovnou konfiguraci nebo spuštění serveru s knihovnou, která existuje jako nezávislé ASP, selžou.

Po ukončení průvodce bude mít server adresářů LDAP základní konfiguraci. Spouštíte-li v systému produkt Lotus Domino, může se stát, že port 389 (předvolený port pro server LDAP) je již používán funkcí LDAP produktu Domino. Musíte provést jeden z následujících kroků:

| • Změnit port, který používá produkt Lotus Domino.
| • Změnit port, který používá produkt Directory Services.
| • Použít specifické IP adresy.

Chcete-li tak učinit, můžete v tomto okamžiku spustit server. Ještě předtím však lze provést některé z těchto akcí:
- Importovat data na server.
- Aktivovat zabezpečení pomocí SSL (Secure Sockets Layer).
- Aktivovat autentizaci Kerberos.
- Nastavit odkazy.

Jak aktivovat SSL na serveru adresářů LDAP

| Máte-li v systému nainstalován produkt Digital Certificate Manager, můžete k zabezpečení přístupů
| k serveru adresářů LDAP použít SSL (Secure Sockets Layer). Než aktivujete SSL na serveru adresářů,
| můžete si přečíst informace o používání SSL s produktem Directory Services.

Pokud chcete používat připojení přes SSL při administraci serveru adresářů LDAP z produktu iSeries Navigator nebo používat SSL u klienta LDAP pro Windows, musíte mít na PC nainstalován jeden z produktů Client Encryptions (5722CE2 nebo 5722CE3).

| K aktivaci SSL na serveru LDAP použijte rozhraní Digital Certificate Manager. Produkt Digital Certificate
| Manager můžete spustit z pořadače **Internet** v prostředí produktu iSeries Navigator nebo ze stránky **Síť**
| v dialogu **Vlastnosti** pro daný server adresářů.

| Při spouštění ze stránky **Síť** použijte tento postup:
1. V prostředí produktu iSeries Navigator rozbalte položku **Síť**.
2. Rozbalte položku **Servery**.
3. Klepněte na **TCP/IP**.
4. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Vlastnosti**.
5. Klepněte na ouško **Síť**.
6. Klepněte na volbu **Digital Certificate Manager**.

   Produkt Digital Certificate Manager se spustí v předvoleném internetovém prohlížeči.

V tématu Zabezpečení serveru adresářů LDAP najdete specifický postup, Podle něhož můžete serveru adresářů přidělit digitální certifikáty.

Po aktivaci SSL můžete změnit port, který server adresářů LDAP používá pro zabezpečená připojení.

Jak aktivovat autentizaci Kerberos na serveru adresářů LDAP

| Máte-li v systému nakonfigurovány služby síťové autentizace, můžete nastavit server adresářů LDAP pro
| používání autentizace Kerberos. Než aktivujete Kerberos na serveru adresářů, můžete si přečíst informace
| o používání Kerberos v produktu Directory Services.

K aktivaci autentizace Kerberos použijte tento postup:
1. V prostředí produktu iSeries Navigator rozbalte položku **Síť**.
2. Rozbalte položku **Servery**.
3. Klepněte na **TCP/IP**.
4. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Vlastnosti**.
5. Klepněte na ouško **Kerberos**.
6. Zaškrtněte volbu **Umožnit autentizaci Kerberos**.
7. Na stránce **Kerberos** zadejte dle potřeby také ostatní nastavení. Informace o jednotlivých polích najdete v online nápovědě k této stránce.

Standardní konfigurace produktu Directory Services

Server adresářů LDAP se automaticky nainstaluje při instalaci operačního systému OS/400. Tato instalace zahrnuje i předvolenou konfiguraci. Server adresářů používá předvolenou konfiguraci za těchto okolností:

- Administrátor nespustil průvodce konfigurací produktu Directory Services ani nezměnil nastavení adresáře ve stránkách vlastností.
- U produktu Directory Services není nakonfigurováno publikování.
- Server adresářů LDAP nenalezl žádné informace o DNS LDAP.

Má-li server adresářů LDAP předvolenou konfiguraci, nastane toto:

- Server adresářů LDAP se automaticky spustí při spuštění TCP/IP.
- Systém vytvoří předvoleného administrátora ″cn=Administrator″. Vygeneruje i heslo, které se bude používat interně. Budete-li chtít později použít heslo administrátora, můžete nastavit nové na stránce vlastností produktu Directory Services.
- Automaticky se vytvoří přípona, která vychází z IP jména systému. Vytvoří se také systémová přípona objektu vycházející ze jména systému. Je-li například IP jméno systému ″mary.acme.com″, bude přípona ″dc=mary, dc=acme, dc=com″.
- Server adresářů LDAP používá předvolenou datovou knihovnu QUSRDIRDB. Systém vytvoří tuto knihovnu v systémovém ASP.
- Pro nezabezpečené komunikace server používá port 389. Je-li pro LDAP nakonfigurován digitální certifikát, je aktivováno SSL a pro zabezpečené komunikace se používá port 636.

Pro publikování existují v produktu Directory Services tyto předvolby:

- Systém publikuje informace na lokálním serveru adresářů LDAP.
- Publikování nepoužívá SSL.
- Publikování používá pořadače pod předvolenou příponou.
- K autentizaci na serveru adresářů používá operační systém OS/400 ID cn=Administrator a systémem generované heslo.
- Systém publikuje pouze systémové informace.

Produkt IBM SecureWay Directory Management Tool

Produkt IBM SecureWay Directory Management Tool (DMT) poskytuje grafické uživatelské rozhraní pro správu obsahu adresáře LDAP. Pomocí DMT můžete vykonávat tyto činnosti:

- Procházet schéma adresáře.
- Přidávat, editovat a mazat třídy objektů.
- Přidávat, editovat a mazat atributy.
- Procházet a prohledávat adresářový strom.
- Přidávat, editovat a mazat záznamy.
- Editovat RDN záznamů.
- Spravovat ACL.

DMT je součást klienta LDAP pro Windows, který je dodáván s produktem Directory Services. Tento klient je dodáván jako adresář integrovaného systému souborů.

K instalaci klienta LDAP pro Windows včetně DMT na PC použijte tento postup:

1. V prostředí produktu iSeries Navigator rozbalte položku **Systémy souborů**.
2. Rozbalte položku **Sdílení souborů**.
3. Dvakrát klepněte na volbu **Qdirsrv**.
4. Dvakrát klepněte na volbu **UserTools**.
5. Dvakrát klepněte na volbu **Windows**.

6. Dvojím klepnutím na **setup.exe** spusťte instalaci DMT. Podle instrukcí na obrazovce dokončete instalaci.

Dokumentace k produktu IBM SecureWay Directory Management Tool (DMT) je umístěna v souboru dparent.htm. Tento soubor se zkopíruje do pořadače produktu IBM SecureWay Directory na PC při instalaci klienta.

Kapitola 4. Administrace serveru adresářů LDAP

K administraci serveru adresářů LDAP potřebujete tyto sady oprávnění:

- Pro konfiguraci serveru nebo pro změnu konfigurace serveru: zvláštní oprávnění *ALLOBJ (All Object) a *IOSYSCFG (I/O System Configuration).
- Pro spuštění a zastavení serveru: oprávnění *JOBCTL (Job Control) a oprávnění k objektu pro příkazy ENDTCP (End TCP/IP), STRTCP (Start TCP/IP), STRTCPSVR (Start TCP/IP Server) a ENDTCPSVR (End TCP/IP Server).
- Pro nastavení režimu monitorování pro server adresářů: zvláštní oprávnění *AUDIT (Audit).
- Pro prohlížení protokolu úlohy serveru: zvláštní oprávnění *SPLCTL (Spool Control).

Chcete-li spravovat objekty adresáře (včetně přístupových seznamů, vlastnictví objektů a replik), připojte se k adresáři administrátorským DN nebo jiným DN, které má odpovídající oprávnění LDAP. Jestliže používáte integraci oprávnění, může být administrátorem také projektovaný uživatel, který má oprávnění k ID funkce Directory Services Administrator.

Administrace serveru adresářů zahrnuje úkoly popsané v těchto částech:

Jak spustit server adresářů LDAP

Ke spuštění serveru adresářů LDAP použijte tento postup:

1. V prostředí produktu iSeries Navigator rozbalte položku **Síť**.
2. Rozbalte položku **Servery**.
3. Klepněte na **TCP/IP**.
4. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Spustit**.

   Může trvat několik minut, než se server adresářů spustí. Závisí to na rychlosti serveru a velikosti dostupné paměti. Při prvním spuštění serveru adresářů může být tato doba ještě o několik minut delší než obvykle, protože server vytváří nové soubory. Podobně i po migraci serveru z nižší verze produktu Directory Services trvá jeho první spuštění o několik minut déle, protože server musí migrovat soubory. Můžete čas od času zkontrolovat stav serveru, abyste zjistili, jestli je již spuštěn.

Poznámka: Server adresářů lze spustit i z relace 5250 zadáním příkazu STRTCPSVR *DIRSRV.

V případě, že máte server adresářů nastaven tak, aby se spouštěl při spuštění TCP/IP, můžete jej spustit i příkazem STRTCP.

Jak zastavit server adresářů LDAP

Zastavení serveru adresářů ovlivňuje všechny aplikace, které server používají v době jeho zastavení. Týká se to také aplikací EIM (Enterprise Identity Mapping), které server právě používají pro operace EIM. Všechny aplikace jsou odpojeny od serveru adresářů, není jim však zabráněno, aby se znovu nepokoušely o připojení k serveru.

K zastavení serveru adresářů LDAP použijte tento postup:
1. V prostředí produktu iSeries Navigator rozbalte položku **Síť**.
2. Rozbalte položku **Servery**.
3. Klepněte na **TCP/IP**.
4. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Zastavit**.

   Může trvat několik minut, než se server adresářů zastaví. Závisí to na rychlosti systému, na rozsahu aktivity serveru a na velikosti dostupné paměti. Můžete čas od času zkontrolovat stav serveru, abyste zjistili, jestli je již zastaven.

Poznámka: Server adresářů lze zastavit i z relace 5250 zadáním příkazu ENDTCPSVR *DIRSRV, ENDTCPSVR *ALL nebo ENDTCP. Příkazy ENDTCPSVR *ALL a ENDTCP platí i pro ostatní servery TCP/IP, které běží v systému. Příkaz ENDTCP ukončí i samotný protokol TCP/IP.

Jak zkontrolovat stav serveru adresářů

Stav serveru adresářů se zobrazuje v prostředí produktu iSeries Navigator ve sloupci **Stav** v pravém rámečku.

Ke zjištění stavu serveru adresářů použijte tento postup:
1. V prostředí produktu iSeries Navigator rozbalte položku **Síť**.
2. Rozbalte položku **Servery**.
3. Klepněte na **TCP/IP**. Produkt iSeries Navigator zobrazí stav všech serverů TCP/IP včetně serveru adresářů ve sloupci **Stav**. Pokud chcete aktualizovat zobrazení stavu serverů, klepněte na menu **Zobrazení** a vyberte volbu **Obnovit**.
4. Chcete-li zobrazit více informací o stavu serveru adresářů, klepněte pravým tlačítkem myši na volbu **Adresář** a vyberte volbu **Stav**. Zobrazí se počet aktivních připojení a další informace, jako jsou např. minulé a aktuální úrovně aktivity.

   Kromě toho, že získáte další informace, může vám tento způsob prohlížení stavu ušetřit čas. Můžete totiž aktualizovat zobrazení stavu serveru adresářů, aniž byste strávili další čas nutný ke kontrole stavu ostatních serverů TCP/IP.

Jak kontrolovat úlohy na serveru adresářů LDAP

Občas je třeba na serveru adresářů LDAP monitorovat určité úlohy. Ke kontrole úloh serveru použijte tento postup:
1. V prostředí produktu iSeries Navigator rozbalte položku **Síť**.
2. Rozbalte položku **Servery**.
3. Klepněte na **TCP/IP**.
4. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Úlohy serveru**.

Jak aktivovat oznámení o události

Produkt Directory Services podporuje oznámení o události, které umožňuje klientům registrovat se u serveru LDAP a být upozorněn v případě výskytu specifikované události, například když je něco přidáno do adresáře.

Chcete-li aktivovat oznámení o události ve vašem serveru, použijte tento postup:
1. V prostředí produktu iSeries Navigator rozbalte položku **Síť**.

2. Rozbalte položku **Servery**.
3. Klepněte na **TCP/IP**.
4. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Vlastnosti**.
5. Klepněte na **Události**.
6. Vyberte volbu **Povolit klientům registraci za účelem oznámení o události**.

Rovněž lze specifikovat maximální počet povolených registrací pro každé připojení a maximální celkový počet registrací, které server povolí.

Další informace o oznámení události najdete v příloze C: Event Notification příručky IBM SecureWay Directory Version 3.2: Client SDK Programming Reference.

Jak specifikovat nastavení transakcí

Produkt Directory Services podporuje transakce, které umožňují, aby se se skupinou operací adresáře LDAP pracovalo jako s jedinou jednotkou. Více informací najdete v části “Transakce” na stránce 37.

Ke konfiguraci nastavení transakcí na serveru použijte tento postup:
1. V prostředí produktu iSeries Navigator rozbalte položku **Síť**.
2. Rozbalte položku **Servery**.
3. Klepněte na **TCP/IP**.
4. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Vlastnosti**.
5. Klepněte na volbu **Transakce**.
6. Zadejte požadovaná nastavení transakcí.

Poznámka: Způsob nastavení transakcí má vliv na výkon serveru LDAP, a proto můžete vyzkoušet více různých nastavení.

Jak změnit port nebo IP adresu

Server adresářů LDAP, který je povolen produktem Directory Services, používá tyto předvolené porty:
- 389 pro nezabezpečená připojení.
- 636 pro zabezpečená připojení (jestliže jste pomocí produktu Digital Certificate Manager povolili Directory Services jako aplikaci, která může používat zabezpečený port).

Poznámka: Standardně jsou všechny IP adresy definované v lokálním systému svázány se serverem.

Používáte-li již tyto porty pro jiné aplikace, můžete buď přiřadit produkt Directory Services jiný port, nebo můžete použít pro dva servery jinou IP adresu, pokud aplikace podporují vazbu na specifickou IP adresu.

Pokud je například server Domino LDAP v rozporu se serverem iSeries Directory Services LDAP, prohlédněte si Host Domino LDAP a Directory Services na stejném serveru iSeries.

Ke změně portů, které používá server adresářů LDAP, použijte tento postup:
1. V prostředí produktu iSeries Navigator rozbalte položku **Síť**.
2. Rozbalte položku **Servery**.
3. Klepněte na **TCP/IP**.
4. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Vlastnosti**.
5. Klepněte na ouško **Síť**.
6. Zadejte příslušná čísla portů a klepněte na **OK**.

Chcete-li změnit IP adresu, na které server adresářů přijímá připojení, proveďte následující kroky:
1. V prostředí produktu iSeries Navigator rozbalte položku **Síť**.
2. Rozbalte položku **Servery**.

3. Klepněte na **TCP/IP**.
4. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Vlastnosti**.
5. Klepněte na ouško **Síť**.
6. Klepněte na tlačítko **IP adresa...**.
7. Vyberte volbu **Použít vybrané IP adresy** a vyberte IP adresy, které má server použít, když potvrzuje připojení.

Jak přesouvat data adresáře LDAP mezi systémy

Server LDAP produktu Directory Services může běžet nezávisle na dalších serverech. Je však výhodné využít jej ve spolupráci s ostatními servery. Tato spolupráce zahrnuje činnosti popsané v následujících částech:

- "Import souboru LDIF".
- "Export souboru LDIF".
- "Jak nastavit novou repliku serveru adresářů" na stránce 23.
- "Publikování informací na server adresářů" na stránce 26.

Import souboru LDIF

Informace lze přenášet mezi různými servery adresářů LDAP pomocí souborů LDIF (LDAP Data Interchange Format). Než spustíte tuto proceduru, přesuňte soubor LDIF na server iSeries jako proudový soubor.

K importu souboru LDIF na server adresářů LDAP použijte tento postup:

1. Je-li spuštěn server adresářů, zastavte jej. Informace o zastavení serveru adresářů najdete v části "Jak zastavit server adresářů LDAP" na stránce 20.
2. V prostředí produktu iSeries Navigator rozbalte položku **Síť**.
3. Rozbalte položku **Servery**.
4. Klepněte na **TCP/IP**.
5. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Nástroje** a potom volbu **Importovat soubor**.

Poznámka: K importu souborů LDIF můžete také použít obslužný program ldapadd.

Export souboru LDIF

Informace lze přenášet mezi různými servery adresářů LDAP pomocí souborů LDIF (LDAP Data Interchange Format), viz část "LDIF (LDAP data interchange format)" na stránce 34. Do souboru LDIF můžete exportovat celý adresář LDAP nebo jeho část.

K exportu souboru LDIF ze serveru adresářů použijte tento postup:

1. V prostředí produktu iSeries Navigator rozbalte položku **Síť**.
2. Rozbalte položku **Servery**.
3. Klepněte na **TCP/IP**.
4. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Nástroje** a potom volbu **Exportovat soubor**.

   Poznámka: Nezadáte-li místo, kam má být soubor LDIF exportován, soubor se uloží do předvoleného adresáře, který je uveden v uživatelském profilu operačního systému OS/400. Pokud jste nezměnili předvolený adresář, je jím kořenový adresář.

Poznámky:

1. Nezapomeňte nastavit oprávnění k souboru LDIF, abyste zabránili neoprávněnému přístupu k datům adresáře. Oprávnění nastavíte tak, že v prostředí produktu iSeries Navigator klepnete na tento soubor pravým tlačítkem myši a vyberete volbu **Povolení**.

2. K vytvoření úplného nebo částečného souboru LDIF můžete použít také obslužný program ldapsearch, jehož popis najdete v části “Obslužný program ldapsearch” na stránce 52. Použijte volbu -L a přesměrujte výstup na soubor.

Jak nastavit novou repliku serveru adresářů

Na serverech adresářů v jiných systémech iSeries můžete založit repliky serveru adresářů LDAP. Produkt Directory Services používá k replikaci standardní protokol LDAP verze 3.

Poznámky:

1. Nelze provádět replikaci mezi servery LDAP verze 3 a verze 2. Systém, na který replikujete, musí mít tedy stejnou verzi LDAP jako systém, ze kterého replikujete. Verze V4R3 a V4R4 operačního systému OS/400 podporují LDAP verze 2. Verze V4R5 a vyšší podporují LDAP verze 3.
2. Adresář produktu Directory Services můžete replikovat i na servery IBM SecureWay V3.2 nebo na novější servery na jiných platformách. K tomu musí být server adresářů operačního systému OS/400 nakonfigurován tak, aby používal mechanismus 3.2 ACI. Narazí-li server při pokusu o replikaci na problém, replikace se přeruší. Jestliže k tomu dojde, replika nebude úplná.

K nastavení nové repliky serveru adresářů použijte tento postup:

1. Pokud jste to již neučinili, nakonfigurujte hlavní i replikační server.

   Poznámka: Zkontrolujte, zda se schéma přípon na obou serverech shoduje.
2. Zastavte hlavní server.
3. (volitelné) Připravte data LDAP pro první replikaci. Tento krok můžete vynechat v případě, že nemáte žádná data, která byste chtěli přenést z hlavního serveru na repliku.
4. (volitelné) Přesuňte data LDAP z replikačního serveru na hlavní server. Tento krok vynechte v případě, že pro replikační server platí, že:
   - je to nový server adresářů LDAP.
   - neobsahuje data, která chcete nadále udržovat.
5. Nastavte nový replikační server.
6. Nastavte hlavní server na novou repliku.
7. Ověřte si, že hlavní server povoluje aktualizace:
   a. V prostředí produktu iSeries Navigator rozbalte systém, ve kterém je spuštěn hlavní server adresářů.
   b. Rozbalte položku **Síť**.
   c. Rozbalte položku **Servery**.
   d. Klepněte na **TCP/IP**.
   e. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Vlastnosti**.
   f. Zaškrtněte políčko **Umožnit aktualizaci adresáře**.

Poznámka: Tyto instrukce předpokládají, že se oba servery, hlavní i replikační, nacházejí v systémech, které jsou spravovány pomocí produktu iSeries Navigator z téhož PC. Jestliže systémy spravujete z různých PC, můžete se při provádění uvedených úkolů mezi těmito dvěma PC přesouvat. Jestliže hlavní nebo replikační server používá jiný operační systém IBM než OS/400, prostudujte si dokumentaci k této platformě ještě předtím, než server nastavíte.

Jak nastavit data LDAP pro první replikaci

Na hlavním serveru adresářů LDAP již možná máte data, která chcete přidat na nový replikační server. Nejprve exportujte adresář do souboru LDIF. V průběhu exportu souboru LDIF je třeba zabránit aktualizaci hlavního serveru. K tomu můžete použít jeden z těchto způsobů:

- Zastavte server adresářů LDAP. V závislosti na množství dat v adresáři to může vyžadovat, aby byl server zastaven po delší časový úsek.
- Změňte vlastnosti serveru tak, aby nepovoloval aktualizace. Tak bude server moci pokračovat v odpovědích na požadavky na vyhledání i v průběhu exportu souboru LDIF. Pro tuto volbu použijte tento postup:
  1. V prostředí produktu iSeries Navigator rozbalte systém, ve kterém je spuštěn hlavní server adresářů.
  2. Rozbalte položku **Síť**.

3. Rozbalte položku **Servery**.
4. Klepněte na **TCP/IP**.
5. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Vlastnosti**.
6. Je-li políčko **Umožnit aktualizaci adresáře** zaškrtnuté, zaškrtnutí zrušte. Tím zabráníte aktualizacím adresáře, dokud nebude replikace dokončena.
7. Klepněte na **OK**.
8. Zastavte a znovu spusťte server adresářů LDAP.

Po zastavení serveru nebo změně vlastností serveru tak, aby se zabránilo aktualizacím, proveďte tento postup:

1. Exportujte adresář do souboru LDIF.
2. Přeneste soubor LDIF do systému, ve kterém se bude spouštět replikační server.

Po přenesení souboru LDIF do systému, ve kterém se bude spouštět replikační server, je třeba importovat data na replikační server:

1. V prostředí produktu iSeries Navigator rozbalte systém, ve kterém je spuštěn replikační server.
2. Není-li replikační server dosud zastaven, zastavte jej. Několikrát obnovte zobrazení stavu serverů a počkejte, až bude jeho stav **Zastaven**.
3. Rozbalte položku **Síť**.
4. Rozbalte položku **Servery**.
5. Klepněte na **TCP/IP**.
6. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Vlastnosti**.
7. Není-li políčko **Umožnit aktualizaci adresáře** zaškrtnuté, zaškrtněte je. To umožní import dat.
8. Klepněte na **OK**.
9. Importujte soubor LDIF, který jste přenesli v kroku 2.
10. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Vlastnosti**.
11. Zrušte zaškrtnutí políčka **Umožnit aktualizaci adresáře**.

Jak přemístit data LDAP na hlavní server

Když vytvoříte na replikačním serveru server adresářů LDAP, nemůžete na něm již provádět aktualizace. Máte-li na serveru, který konfigurujete jako replikační server, nějaká data, můžete je přesunout na hlavní server, abyste je mohli nadále spravovat. Použijte k tomu tento postup:

1. V prostředí produktu iSeries Navigator rozbalte systém, ve kterém je spuštěn replikační server.
2. Rozbalte položku **Síť**.
3. Rozbalte položku **Servery**.
4. Klepněte na **TCP/IP**.
5. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Vlastnosti**.
6. Je-li políčko **Umožnit aktualizaci adresáře** zaškrtnuté, zaškrtnutí zrušte. Tím zabráníte aktualizacím adresáře, dokud nebude replikace dokončena.
7. Klepněte na **OK**.
8. Zastavte server adresářů LDAP.
9. Exportujte adresář do souboru LDIF.
10. Přeneste soubor LDIF do systému, ve kterém se bude spouštět hlavní server.

Po přenesení souboru LDIF do systému, ve kterém se bude spouštět hlavní server, je třeba importovat data na hlavní server:

1. V prostředí produktu iSeries Navigator rozbalte systém, ve kterém je spuštěn hlavní server adresářů.
2. Není-li hlavní server adresářů dosud zastaven, zastavte jej. Několikrát obnovte zobrazení stavu serverů a počkejte, až bude jeho stav **Zastaven**.
3. Rozbalte položku **Síť**.
4. Rozbalte položku **Servery**.
5. Klepněte na **TCP/IP**.
6. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Vlastnosti**.
7. Není-li políčko **Umožnit aktualizaci adresáře** zaškrtnuté, zaškrtněte je. To umožní import dat.
8. Klepněte na **OK**.
9. Importujte soubor LDIF, který jste přenesli v kroku 10 v předchozím postupu.

10. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Vlastnosti**.
11. Zrušte zaškrtnutí políčka **Umožnit aktualizaci adresáře**.

Jak nastavit novou repliku

K nastavení replikačního serveru použijte následující postup.

Poznámka: Než začnete tento postup provádět, musí být replikační server nakonfigurován a zastaven.

1. V prostředí produktu iSeries Navigator rozbalte systém, ve kterém je spuštěn replikační server.
2. Rozbalte položku **Síť**.
3. Rozbalte položku **Servery**.
4. Klepněte na **TCP/IP**.
5. Není-li server dosud zastaven, zastavte jej. Několikrát obnovte zobrazení stavu serverů a počkejte, až bude jeho stav **Zastaven**.
6. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Vlastnosti**.
7. Klepněte na ouško **Replikace**.
8. Vyberte volbu **Použít jako replikační server**.
9. Do pole **Jméno použité hlavním serverem pro aktualizace** zadejte jméno hlavního serveru, který se má použít při přihlášení k replikačnímu serveru při aktualizaci záznamů. Může to být rozlišovací jméno (DN) nebo uživatel Kerberos.

   Zvolíte-li DN:

   - Klepněte na tlačítko **Heslo** vedle pole **Jméno použité hlavním serverem pro aktualizace**. Zadejte heslo pro hlavní server, které se má použít při přihlášení k replikačnímu serveru při aktualizaci záznamů.

     Poznámka: Poznamenejte si jméno a heslo, které jste zadali v kroku 9. Budete je potřebovat k nastavení hlavního serveru pro replikace.

   Zvolíte-li **Přidat uživatele Kerberos**:

   - Budete vyzváni k zadání jména Kerberos (ve formátu LDAP/*hostname*, kde *hostname* je plně kvalifikované jméno hlavního serveru) a předvolené sféry (např. ACME.COM) hlavního serveru.

     Poznámka: Chcete-li Kerberos použít, musíte ho mít aktivován na hlavním i replikačním serveru.
10. Do pole **URL hlavního serveru** zadejte jméno hlavního serveru ve formátu URL. Používá-li váš hlavní server jiný než předvolený port, zadejte tento port jako součást URL.
11. Klepněte na ouško **Databáze/Přípony**. Jestliže se přípona, kterou chcete replikovat, nenachází v tomto seznamu, přidejte ji.
12. (volitelné) Chcete-li při replikaci používat SSL, aktivujte ho pro tento server pomocí produktu Digital Certificate Manager. Digital Certificate Manager můžete spustit pod ouškem **Síť**. Informace o tom, jak aktivovat SSL na serveru adresářů, najdete v části “Jak aktivovat SSL na serveru adresářů LDAP” na stránce 15.
13. Klepněte na **OK**.

Jak nastavit hlavní server na novou repliku

K nastavení hlavního serveru na novou repliku použijte následující postup.

Poznámka: Než začnete provádět tento postup, musí být server nakonfigurován a zastaven.

1. V prostředí produktu iSeries Navigator rozbalte systém, ve kterém je spuštěn hlavní server adresářů.
2. Rozbalte položku **Síť**.
3. Rozbalte položku **Servery**.
4. Klepněte na **TCP/IP**.
5. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Vlastnosti**.
6. Zaškrtněte políčko **Umožnit aktualizaci adresáře**.
7. Klepněte na **OK**.
8. Zastavte a potom znovu spusťte server adresářů LDAP. Několikrát obnovte zobrazení stavu serverů a počkejte, až bude jeho stav **Spuštěn**.
9. Opět klepněte pravým tlačítkem myši na **Adresář** a vyberte volbu **Vlastnosti**.

10. Klepněte na ouško **Replikace**. iSeries Navigator vás pravděpodobně vyzve k zadání informací o připojení. Zadejte tyto informace a klepněte na **OK**.
11. Klepněte na tlačítko **Přidat**.
12. Do pole **Server** zadejte jméno replikačního serveru ve formátu URL.
13. Vyberte metodu autentizace.

    Chcete-li použít rozlišovací jméno (DN) a heslo:

    a. Vyberte volbu **Použít DN a heslo**.
    b. Do pole **Připojit jako** zadejte jméno, které jste uvedli v kroku 9 na stránce 25, když jste nastavovali replikační server.
    c. Klepněte na volbu **Heslo** a zadejte heslo, které jste uvedli v kroku 9 na stránce 25, když jste nastavovali replikační server.

    Chcete-li použít Kerberos:

    - Vyberte volbu **Použít konto Kerberos hlavního serveru**. Hlavní server bude k autentizace používat své hlavní jméno Kerberos.

    Poznámka: Chcete-li Kerberos použít, musíte ho mít aktivován na hlavním i replikačním serveru.
14. Chcete-li při replikaci používat SSL, aktivujte ho pro tento server pomocí produktu Digital Certificate Manager. Digital Certificate Manager můžete spustit pod ouškem **Síť**. Další informace o tom, jak aktivovat SSL na serveru adresářů, najdete v části “Jak aktivovat SSL na serveru adresářů LDAP” na stránce 15.
15. Nepoužívá-li replikační server předvolený port, zadejte správné číslo portu do pole **Port**.
16. Jestliže nechcete aktualizovat replikační server při každé změně záznamu na hlavním serveru, vyberte volbu **Čas**. Potom zadejte, jak často má hlavní server provádět aktualizaci repliky.
17. Klepněte na **OK**.
18. Klepněte na ouško **Databáze/Přípony**. Jestliže se přípona, kterou chcete replikovat, nenachází v tomto seznamu, přidejte ji.
19. Povolte aktualizace adresáře na každém replikačním serveru:
    a. V prostředí produktu iSeries Navigator rozbalte systém, ve kterém je spuštěn replikační server.
    b. Rozbalte položku **Síť**.
    c. Rozbalte položku **Servery**.
    d. Klepněte na **TCP/IP**.
    e. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Vlastnosti**.
    f. Není-li políčko **Umožnit aktualizaci adresáře** zaškrtnuté, zaškrtněte je.
    g. Klepněte na **OK**.
20. Jestliže nejsou ještě spuštěny všechny replikační servery, spusťte je.

Poznámka: Jeden server nemůže být současně hlavním i replikačním serverem.

Publikování informací na server adresářů

Můžete konfigurovat systém tak, aby publikoval určité informace na server adresářů LDAP v témže nebo jiném systému. Operační systém OS/400 bude automaticky publikovat tyto informace na server adresářů LDAP vždy, když pomocí produktu iSeries Navigator změníte údaje v operačním systému OS/400. Publikovatelné informace zahrnují systém (systémy a tiskárny), sdílení tisku a uživatele a metody QoS (Quality of Service) TCP/IP. Více informací o QoS najdete v části Konfigurace LDAP a QoS.

Pokud nadřazené DN, na kterém mají být data publikována, neexistuje, produkt Directory Services je automaticky vytvoří. I jiné nainstalované aplikace OS/400 mohou publikovat informace v adresáři LDAP. Kromě toho můžete z vlastních programů volat API pro publikování dalších typů informací v adresáři LDAP.

Poznámky:

1. Když nastavíte operační systém OS/400 tak, aby na serveru adresářů LDAP publikoval informace typu Users (Uživatelé), budou se automaticky exportovat záznamy ze systémového distribučního adresáře na server adresářů LDAP. K tomu slouží rozhraní API QGLDSSDD. Toto nastavení také synchronizuje

adresář LDAP se změnami prováděnými v systémovém distribučním adresáři. Informace o API QGLDSSDD najdete v tématu OS/400 Directory Services pod tématem Programming v rámci aplikace iSeries Information Center. K dispozici jsou tyto informace:
   - Jak toto API ručně vyvolat.
   - Jak ochránit určité uživatele před jejich exportem na server LDAP.
   - Jak exportovat pole systémového distribučního adresáře.
2. Když nastavíte operační systém OS/400 tak, aby na serveru adresářů LDAP publikoval informace typu System (Systém), a k publikování vyberete jednu nebo více tiskáren, bude systém automaticky synchronizovat adresář LDAP se změnami prováděnými na těchto tiskárnách v systému. K informacím o tiskárně, které lze publikovat, patří umístění tiskárny, rychlost vyjádřená počtem stránek za minutu, zda podporuje oboustranný a barevný tisk, typ a model tiskárny a popis tiskárny. Tyto informace pocházejí z popisu zařízení v systému, který je publikován. V síťovém prostředí slouží tyto informace uživatelům při výběru tiskárny.
3. Publikovat informace o operačním systému OS/400 lze i na serveru adresářů LDAP, který se nenachází v operačním systému OS/400, je-li tento server nakonfigurován se schématem IBM.

Ke konfiguraci systému tak, aby mohl publikovat informace o operačním systému OS/400 na serveru adresářů LDAP, použijte tento postup:

1. V prostředí produktu iSeries Navigator klepněte pravým tlačítkem myši na požadovaný systém a vyberte volbu **Vlastnosti**.
2. Klepněte na ouško **Adresářové služby**.
3. Klepnutím označte typy informací, které chcete publikovat.

   Rada:

   Máte-li v úmyslu publikovat více než jeden typ informací na stejném místě, můžete ušetřit čas tím, že vyberete ke konfiguraci více typů informací současně. Produkt Operations Navigator potom použije hodnoty, které jste zadali při konfiguraci jednoho typu, jako předvolené hodnoty pro konfiguraci dalších typů informací.
4. Klepněte na volbu **Podrobnosti**.
5. Klepněte na zaškrtávací políčko **Publikovat systémové informace**.
6. Zadejte **Metodu autentizace**, kterou bude server používat, a odpovídající informace o autentizaci.
7. Klepněte na tlačítko **Editovat** vedle pole **(Aktivní) Server adresářů**. Do dialogu, který se objeví, zadejte jméno serveru adresářů LDAP, na kterém chcete publikovat informace o operačním systému OS/400, a klepněte na **OK**.
8. Do pole **Pod DN** zadejte nadřazené rozlišovací jméno (DN) na serveru adresářů, pod které chcete přidávat informace.
9. V rámečku **Připojení na server** vyplňte pole, která odpovídají vaší konfiguraci.

   Poznámka: Chcete-li publikovat informace o operačním systému OS/400 na serveru adresářů s využitím SSL nebo Kerberos, je třeba nejprve nakonfigurovat daný server adresářů tak, aby používal odpovídající protokol. Více informací o produktech SSL a Kerberos najdete v části “Jak používat autentizaci Kerberos u serveru adresářů LDAP” na stránce 39.
10. Nepoužívá-li váš server adresářů předvolený port, zadejte správné číslo portu do pole **Port**.
11. Klepnutím na volbu **Ověřit** se přesvědčte, že zadané nadřazené DN na serveru existuje a že informace pro připojení jsou správné. Jestliže zadaná cesta neexistuje, objeví se výzva k jejímu vytvoření.

    Poznámka: Jestliže nadřazené DN neexistuje a vy je nevytvoříte, publikování nebude úspěšné.
12. Klepněte na **OK**.

Poznámka: Publikovat informace o operačním systému OS/400 lze i na serveru adresářů LDAP, který je postaven na jiné platformě. Informace o uživateli a o systému můžete však publikovat pouze na serveru adresářů, který používá schéma kompatibilní se schématem produktu Directory Services. Definici schémat IBM SecureWay Directory, která zahrnuje produkt iSeries Directory Services, najdete na webové stránce Directory Services.

Sdílení tisku je třeba publikovat na serveru adresářů, který podporuje schéma aktivního adresáře Microsoftu (Microsofts Active Directory). Publikování sdílení tisku v aktivním adresáři umožňuje uživatelům konfigurovat tiskárny iSeries přímo z pracovní plochy Windows 2000 pomocí průvodce přidáním tiskárny Windows 2000. K tomu je třeba, abyste v průvodci přidáním tiskárny zadali, že chcete tiskárnu vyhledat v aktivním adresáři Windows 2000.

API pro publikování informací o operačním systému OS/400 na serveru adresářů

Produkt Directory Services poskytuje vestavěnou podporu pro publikování informací o uživateli a systému. Tyto položky jsou vypsány na stránce **Adresářové služby** systémového dialogu **Vlastnosti**. Pomocí konfigurace serveru LDAP a rozhraní API pro publikování můžete umožnit i publikování jiných typů informací prostřednictvím vlastních uživatelských programů OS/400. Tyto typy informací se potom rovněž zobrazují na stránce **Adresářové služby**. Stejně jako uživatelé a systémy nejsou tyto typy zpočátku povoleny a je třeba je nakonfigurovat pomocí stejného postupu. Program, který přidává data do adresáře LDAP, se nazývá Publishing Agent. Typ informací, které jsou publikovány tak, jak se zobrazují na stránce **Adresářové služby**, se nazývá jméno agenta.

Rozhraní API, která zde uvádíme, vám umožní zahrnout publikování do vašich vlastních programů:

QgldChgDirSvrA
Aplikace používá formát CSVR0500 pro první přidání jména agenta, které je označeno jako nepovolený záznam. Pokyny pro uživatele této aplikace doporučují použít produkt iSeries Navigator k přechodu na stránku vlastností Adresářové služby, kde je možné konfigurovat program Publishing Agent. Jako příklad jmen agentů slouží jména agentů pro systémy a uživatele, která se automaticky zobrazují na stránce **Adresářové služby**.

QgldLstDirSvrA
Formát LSVR0500 tohoto API použijte k zobrazení agentů, kteří jsou v systému aktuálně k dispozici.

QgldPubDirObj
Toto API použijte ke skutečnému publikování informací.

Podrobné informace o API najdete v tématu LDAP (Lightweight Directory Access Protocol) pod tématem Programming v rámci aplikace iSeries Information Center.

Jak specifikovat server pro adresářové odkazy

K přiřazení referenčních serverů pro server adresářů použijte tento postup:
1. V prostředí produktu iSeries Navigator rozbalte položku **Síť**.
2. Rozbalte položku **Servery**.
3. Klepněte na **TCP/IP**.
4. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Vlastnosti**.
5. Klepněte na tlačítko **Přidat**.
6. Do náznaku zadejte jméno referenčního serveru ve formátu URL. Zde jsou příklady přípustných URL pro LDAP:
   - ldap://test.server.com
   - ldap://test.server.com:400
   - ldap://9.9.99.255

   Poznámka: Jestliže referenční server nepoužívá předvolený port, zadejte správné číslo portu jako součást URL tak, jako bylo zadáno číslo portu 400 ve druhém příkladu.
7. Klepněte na **OK**.

Jak přidat přípony na server adresářů LDAP

Přidáním přípony na server adresářů LDAP umožníte serveru spravovat příslušnou část adresářového stromu.

Poznámka: Nemůžete přidávat příponu podřízenou příponě, která se již na serveru nachází. Jestliže například o=ibm, c=us je existující přípona na serveru, nemůžete přidat ou=rochester, o=ibm, c=us.

K přidání přípony na server adresářů použijte tento postup:
1. V prostředí produktu iSeries Navigator rozbalte položku **Síť**.
2. Rozbalte položku **Servery**.
3. Klepněte na **TCP/IP**.
4. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Vlastnosti**.
5. Klepněte na ouško **Databáze/Přípony**.
6. Do pole **Nová přípona** napište jméno nové přípony.
7. Klepněte na tlačítko **Přidat**.
8. Klepněte na **OK**.

Poznámka: Přidání přípony odkáže server na adresář, ale nevytvoří žádný objekt. Jestliže objekt, který odpovídá nové příponě, zatím neexistoval, je třeba jej vytvořit stejně jako jiný objekt.

Jak odstranit přípony ze serveru adresářů

K odstranění přípony ze serveru adresářů LDAP použijte tento postup:
1. V prostředí produktu iSeries Navigator rozbalte položku **Síť**.
2. Rozbalte položku **Servery**.
3. Klepněte na **TCP/IP**.
4. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Vlastnosti**.
5. Klepněte na ouško **Databáze/Přípony**.
6. Klepnutím vyberte příponu, kterou chcete odstranit.
7. Klepněte na tlačítko **Odstranit**.

Poznámka: Můžete se rozhodnout odstranit příponu, aniž byste odstranili objekty adresáře, které pod ni patří. Tato data potom nebudou ze serveru adresářů přístupná. Přístup k nim však můžete později obnovit tím, že znovu přidáte tuto příponu.

Jak uložit a obnovit informace produktu Directory Services

Produkt Directory Services uchovává informace v těchto místech:

- Databázová knihovna (standardně QUSRDIRDB) - obsahuje obsah serveru adresářů.
- Knihovna QDIRSRV2 - slouží k uchovávání informací o publikování.
- Knihovna QUSRSYS - uchovává různé položky v objektech začínajících na QGLD (k jejich uložení zadejte QUSRSYS/QGLD*).
- Databázová knihovna QUSRDIRCL - obsahuje protokol změn (je-li server adresářů nastaven na použití protokolu změn).

Mění-li se obsah adresáře pravidelně, měli byste ukládat databázovou knihovnu a objekty v ní obsažené rovněž pravidelně. Konfigurační data jsou uložena i v tomto adresáři:

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

Soubory v tomto adresáři byste měli ukládat při každé změně konfigurace nebo aplikaci PTF.

Informace o ukládání a obnově dat operačního systému OS/400 najdete v části Zálohování a obnova, SC09-3599.

Jak spravovat vlastnictví a přístup k datům v adresáři

Správa vlastnictví a přístupu k datům v adresáři zahrnuje tyto činnosti:
- "Práce s vlastnostmi vlastnictví objektů adresáře".
- "Práce s přístupovými seznamy (ACL)".
- "Práce se skupinami ACL".

Práce s vlastnostmi vlastnictví objektů adresáře

K nastavení vlastností vlastnictví objektů adresáře použijte tento postup:
1. V prostředí produktu iSeries Navigator rozbalte položku **Síť**.
2. Rozbalte položku **Servery**.
3. Klepněte na **TCP/IP**.
4. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Oprávnění**.

   Nejste-li v daném okamžiku připojeni k serveru adresářů, objeví se dialog **Připojení na server adresářů**. Připojte se jako administrátor serveru nebo jako vlastník objektu, s jehož vlastnostmi vlastnictví chcete pracovat.
5. Z adresářového stromu vyberte objekt, s jehož vlastnostmi vlastnictví chcete pracovat, a klepněte na **OK**.

Práce s přístupovými seznamy (ACL)

Práce s přístupovými seznamy (ACL) zahrnuje přiřazení explicitních a implicitních ACL k objektům adresáře, přidání uživatelů do ACL, odstranění uživatelů z ACL a procházení objektů v adresáři. Uvědomte si, že od verze V5R1 podporuje produkt Directory Services nový model ACL, takže i když jste již dříve používali ACL, měli byste se s nimi znovu seznámit.

Chcete-li pracovat s ACL, použijte tento postup:
1. V prostředí produktu iSeries Navigator rozbalte položku **Síť**.
2. Rozbalte položku **Servery**.
3. Klepněte na **TCP/IP**.
4. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Oprávnění**.

   Nejste-li v daném okamžiku připojeni k serveru adresářů, objeví se dialog **Připojení na server adresářů**. Připojte se jako administrátor serveru nebo jako vlastník objektu, s jehož ACL chcete pracovat.
5. Z adresářového stromu vyberte objekt, s jehož ACL chcete pracovat, a klepněte na **OK**.
6. Klepněte na ouško **ACL**.

Práce se skupinami ACL

Chcete-li pracovat se skupinami ACL, použijte tento postup:
1. V prostředí produktu iSeries Navigator rozbalte položku **Síť**.
2. Rozbalte položku **Servery**.
3. Klepněte na **TCP/IP**.
4. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Skupiny ACL**.

Práce s přístupovými seznamy pro oprávněné uživatele

| Počínaje verzí V5R2 můžete administrátorovi udělit přístup k uživatelským profilům, které dostaly přístup
| k ID funkce Directory Services Administrator (QIBM_DIRSRV_ADMIN).

| Pokud například dostane uživatelský profil JOHNSMITH přístup k ID funkce Directory Services
| Administrator a v dialogu Vlastnictví adresáře je vybrána volba Udělení administrátorského přístupu
| oprávněným uživatelům, získá profil JOHNSMITH oprávnění administrátora LDAP. Když vyberete tento profil
| pro připojení k serveru adresářů pomocí DN os400-profile=JOHNSMTH, cn=accounts,
| os400-sys=systemA.acme.com, získá uživatel oprávnění administrátora. Systémová přípona objektu

v tomto příkladu je os400-sys=systemA.acme.com. Více informací o projektovaných uživatelích najdete v části “Procedura Backend projektovaná operačním systémem” na stránce 40.

Chcete-li vybrat tuto volbu, použijte tento postup:

1. V prostředí produktu iSeries Navigator rozbalte položku **Síť**.
2. Rozbalte položku **Servery**.
3. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Vlastnosti**.
4. V oušku **Obecné** pod položkou **Informace pro administrátora** vyberte volbu **Udělení administrátorského přístupu oprávněným uživatelům**.

Při nastavení ID funkce Directory Services Administrator v uživatelském profilu postupujte takto:

1. V prostředí produktu iSeries Navigator klepněte pravým tlačítkem myši na jméno systému a vyberte volbu **Administrativa aplikací**.
2. Klepněte na ouško **Hostitelské aplikace**.
3. Rozbalte položku **Operating System/400**.
4. Klepnutím zvýrazněte volbu **Directory Services Administrator**.
5. Klepněte na tlačítko **Přizpůsobit**.
6. Rozbalte položky **Uživatelé**, **Skupiny** nebo **Uživatelé, kteří nejsou ve skupině** podle toho, která položka je pro uživatele vhodná.
7. Vyberte uživatele nebo skupinu, kteří mají být přidáni do seznamu **Povolený přístup**.
8. Klepněte na tlačítko **Přidat**.
9. Klepněte na **OK** a uložte změny.
10. Klepněte na **OK** v dialogu **Administrativa aplikací**.

Jak sledovat přístup a změny u adresáře LDAP

Možná budete chtít sledovat přístup k adresáři LDAP a v něm prováděné změny. Pomocí protokolu změn adresáře LDAP můžete sledovat změny provedené v tomto adresáři. Protokol změn se nachází pod zvláštní příponou cn=changelog. Je uchováván v knihovně QUSRDIRCL.

Chcete-li aktivovat protokol změn, použijte tento postup:

1. V prostředí produktu iSeries Navigator rozbalte položku **Síť**.
2. Rozbalte položku **Servery**.
3. Klepněte na **TCP/IP**.
4. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Vlastnosti**.
5. Klepněte na ouško **Databáze/Přípony**.
6. Vyberte volbu **Protokolovat změny adresáře**.
7. (volitelné) Do pole **Maximum záznamů** zadejte maximální počet záznamů, které může protokol udržovat.

   Poznámka: I když je tento parameter nepovinný, doporučujeme vám tento maximální počet záznamů zadat. Nezadáte-li maximální počet záznamů, bude protokol změn uchovávat všechny záznamy a jeho velikost bude značně narůstat.

Třída objektů changeLogEntry slouží k reprezentaci změn provedených na serveru adresářů. Sada změn je dána sadou všech záznamů uspořádanou v rámci zásobníku changelog, jak je definováno atributem changeNumber. Informace v protokolu změn jsou určeny ″pouze pro čtení″.

Každý uživatel, který je zapsán v přístupovém seznamu pro příponu cn=changelog, může procházet záznamy v protokolu změn. V příponě protokolu změn cn=changelog byste měli pouze vyhledávat. Nezkoušejte přidávat, měnit nebo mazat záznamy nebo měnit příponu protokolu, i kdybyste k tomu měli oprávnění. Mohlo by to mít nepředvídatelné následky.

Příklad:

Tento příklad ukazuje, jak pomocí obslužného programu příkazové řádky ldapsearch vyhledat v protokolu změn všechny záznamy zapsané na serveru:

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

Jak aktivovat monitorování objektů pro server adresářů

Produkt Directory Services podporuje monitorování zabezpečení operačního systému OS/400. Je-li u systémové hodnoty QAUDCTL zadáno *OBJAUD, můžete aktivovat monitorování objektů prostřednictvím produktu iSeries Navigator.

Chcete-li aktivovat monitorování objektů pro produkt Directory Services, použijte tento postup:
1. V prostředí produktu iSeries Navigator rozbalte položku **Síť**.
2. Rozbalte položku **Servery**.
3. Klepněte na **TCP/IP**.
4. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Vlastnosti**.
5. Klepněte na ouško **Monitorování**.
6. Vyberte požadované nastavení monitorování pro váš server.

Změny v nastavení monitorování se projeví, jakmile klepnete na tlačítko **OK**. Není třeba restartovat server adresářů LDAP. Více informací najdete v části “Zabezpečení produktu Directory Services” na stránce 38.

Jak upravit výkon serveru adresářů LDAP

Výkon serveru adresářů LDAP můžete upravit změnou některé z těchto položek:
- Objemy vyhledávání.
- Maximální povolený čas pro vyhledávání.
- Nastavení transakcí serveru.
- Počet databázových připojení a vláken na serveru.

K úpravě hodnot výkonu serveru adresářů použijte tento postup:
1. V prostředí produktu iSeries Navigator rozbalte položku **Síť**.
2. Rozbalte položku **Servery**.
3. Klepněte na **TCP/IP**.
4. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Vlastnosti**.
5. Klepněte na ouško **Výkon**.

Výkon serveru adresářů můžete upravit i změnou počtu databázových připojení a vláken na serveru, která tento server využívá. Ke změně této hodnoty použijte tento postup:
1. V prostředí produktu iSeries Navigator rozbalte položku **Síť**.
2. Rozbalte položku **Servery**.
3. Klepněte na **TCP/IP**.
4. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Vlastnosti**.
5. Klepněte na ouško **Databáze**/**Přípony**.

Kapitola 5. Koncepce a referenční informace týkající se produktu Directory Services

Následující informace o koncepcích a referencích vám přiblíží server LDAP produktu Directory Services a pomohou vám s jeho provozem:

Informace o základech LDAP a o plánování serveru LDAP obsahuje také Kapitola 3, "Začínáme s produktem Directory Services" na stránce 7.

Přístupové seznamy (ACL) LDAP

V mnohých případech není třeba omezovat přístup k datům na serveru adresářů. Server LDAP na intranetu vaší firmy může například obsahovat telefonní seznam zaměstnanců. Za normálních okolností by všichni zaměstnanci měli mít přístup k prohlížení těchto údajů.

Prezidentka společnosti však nechce, aby měli všichni zaměstnanci přístup k jejímu telefonnímu číslu. V tom případě byste měli vytvořit **přístupový seznam (ACL)**. Pomocí tohoto ACL můžete omezit přístup uživatelů k jejímu záznamu na serveru tak, že k němu budou mít přístup pouze ti zaměstnanci, kteří jí smějí telefonovat.

Pomocí ACL můžete řídit i to, kdo má právo přidávat a mazat objekty adresáře. Můžete rovněž určit, zda uživatelé mají možnost číst, zapisovat, vyhledávat a porovnávat atributy adresáře. ACL mohou být buď zděděné, nebo explicitní. To znamená, že je lze používat jedním z těchto způsobů:

- Explicitně nastavit ACL pro určitý objekt.
- Zadat, že objekty zdědí ACL z objektů vyšší úrovně v hierarchii adresáře LDAP.

Je možné, že prezidentka v předchozím příkladu nechce, aby měli všichni zaměstnanci přístup k jejímu telefonnímu číslu. Přeje si však, aby k němu měli přístup všichni ředitelé. V tom případě můžete k udělení oprávnění pro ředitele využít **skupinu ACL**. Skupiny ACL umožňují poskytnout přístup určitým skupinám uživatelů hromadně namísto jednotlivých oprávnění. To je užitečné v případech, kdy stejná skupina osob má mít přístup k více než jedné sadě objektů. Jestliže ředitelé, kteří mají přístup k telefonnímu číslu prezidentky, budou později potřebovat přístup například k mzdovým záznamům, můžete znovu využít tutéž skupinu ACL.

Modely ACL

Všechny verze produktu Directory Services podporují model povolení přístupu na úrovni přístupových tříd. V tomto modelu má každý typ atributu LDAP kategorii ″Normální″, ″Citlivý″ nebo ″Kritický″. Tyto kategorie jsou řízeny soubory schémat atributů. Při přidávání uživatele do ACL objektu specifikujete, v které kategorii může uživatel číst, zapisovat, vyhledávat a porovnávat. Ve většině schémat je telefonní číslo klasifikováno atributem kategorie ″Normální″. Proto pro ředitele z uvedeného příkladu, kteří mají mít přístup k telefonnímu číslu prezidentky, nastavte v objektu prezidentky přístup pro čtení k atributům kategorie ″Normální″. Tak nebudou mít přístup k ″Citlivým″ ani ″Kritickým″ údajům. Všechny verze produktu Directory Services podporují nastavení povolení přístupu na úrovni přístupových tříd.

Produkt Directory Services podporuje i model povolení přístupu na úrovni atributů. V tomto modelu můžete specifikovat oprávnění ke čtení, zápisu, vyhledávání a porovnávání pro určité atributy bez ohledu na jejich přístupovou třídu. Vraťme se znovu k výše uvedenému příkladu. V modelu povolení přístupů na úrovni přístupových tříd jste mohli udělit ředitelům přístup za účelem čtení k atributu telephoneNumber (telefonní číslo), i kdyby obecně neměli přístup k atributům kategorie ″Normální″.

Model povolení na úrovni atributů je kompatibilní pouze se servery SecureWay Directory Services verze 3.2 a vyšší. Standardně není tento model povolen. Máte možnost ho povolit při práci s ACL. Když je tento model jednou povolen, můžete jej zakázat pouze tak, že překonfigurujete server a obnovíte databázi adresáře. Než se rozhodnete tento model povolit, uvědomte si, že jej nebudete moci spravovat z žádného klienta LDAP V2 (ani pomocí nižších verzí produktu iSeries Navigator než V5R1), a jestliže se o to pokusíte, může dojít k poškození záznamů ACL.

Zvláštní hodnoty ACL

Všechny objekty na serveru adresářů produktu Directory Services mají výchozí ACL, který obsahuje zvláštní skupinu ACL CN=Anybody, jež zahrnuje všechny uživatele adresáře. Standardně má tato skupina přístup za účelem čtení, vyhledávání a porovnávání k atributům kategorie Normální pro všechny objekty.

K některým objektům můžete ponechat stejná přístupová práva všem uživatelům, kteří se připojují k serveru adresářů neanonymně. K tomu použijte zvláštní skupinu ACL cn=Authenticated.

Ke specifikaci, jaká přístupová práva bude mít objekt sám k sobě, použijte zvláštní DN cn=this. To umožní, aby i podřízené záznamy, které zdědí jejich ACL, byly automaticky oprávněny k provádění operací s jejich vlastními objekty.

Další informace

Spravujete-li ACL pomocí produktu iSeries Navigator, nemusíte znát podrobnosti o implementaci ACL v produktu Directory Services. Chcete-li však v souborech LDIF specifikovat atributy, které se týkají ACL, nebo chcete používat ACL u obslužných programů příkazové řádky LDAP, měli byste se s atributy používanými v ACL seznámit. Informace o atributech ACL najdete v dokumentu Access Control Lists příručky The IBM SecureWay Directory Management Tool.

Informace o tom, jak nastavovat a měnit ACL a skupiny ACL, najdete v těchto částech:

“Práce s přístupovými seznamy (ACL)” na stránce 30.
“Práce se skupinami ACL” na stránce 30.

LDIF (LDAP data interchange format)

Formát LDIF (LDAP data interchange format) umožňuje jednoduchým způsobem přenášet informace adresářů mezi servery adresářů LDAP. Soubory LDIF uchovávají záznamy adresářů LDAP v jednoduchém textovém formátu. Formát souborů LDIF používaný serverem adresářů se od verze V4R5 produktu Directory Services změnil. Soubory LDIF se skládají ze sekvence řádek, které popisují buď záznam adresáře, nebo sadu změn provedených v záznamu. Nemohou popisovat obojí.

Obecný formát záznamu LDIF je:

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

kde:

- *version* udává verzi formátu souboru LDIF. Číslo verze musí být 1. Jestliže číslo verze chybí, předpokládá se, že soubor LDIF je ve starším formátu. Je-li soubor LDIF ve verzi 1, jeho obsah MUSÍ být v kódu UTF-8.
- *distinguished name* je rozlišovací jméno záznamu.
- *attrtype1* je typ atributu LDAP (například cn nebo ou).
- *attrvalue1* je hodnota tohoto atributu.

Každý záznam má několik atributů. Každý atribut je na samostatné řádce. Je-li hodnota atributu delší než jedna řádka, může hodnota pokračovat na další řádce, a je před ní uvedena mezera nebo znak tabelátoru.

Prázdné řádky oddělují jednotlivé vstupy v témže souboru LDIF. Všechny řádky začínající znakem ″#″ jsou komentáře a při analýze souboru LDIF musejí být ignorovány.

Všechna rozlišovací jména a atributy by měly být kódovány podle algoritmu base-64, když:
- Obsahují návrat vozíku (CR) nebo posun řádky (LF).
- Začínají dvojtečkou (:), mezerou nebo znakem méně než (<).
- Končí mezerou.

Atributy kódované podle base-64 se vyznačují dvěma dvojtečkami mezi jménem atributu a jeho hodnotou.

Externí odkazy mají formát file:// URL. Mezi typem atributu a hodnotou externího odkazu by měla být dvojtečka a znak méně než (″:<″).

Zde uvádíme příklady souborů LDIF:

Příklad 1: Jednoduchý soubor LDAP se dvěma záznamy

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

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

Příklad 2: Soubor obsahuje hodnotu kódovanou podle base-64

```
version: 1
   dn: cn=Gern Jensen, ou=Rochester, o=Big Company, c=US
   objectclass: top
   objectclass: person
   objectclass: organizationalPerson
   cn: Gern Jensen
   cn: Gern O Jensen
   sn: Jensen
   uid: gernj
   telephonenumber: +1 408 555 1212
```

```
   description:: V2hhdCBhIGNhcmVmdWwgcmVhZGVyIHlvdSBhcmUhICBUaGlzIHZhbHVlIGlzIGJ
    hc2UtNjQtZW5jb2RlZCBiZWNhdXNlIGl0IGhhcyBhIGNvbnRyb2wgY2hhcmFjdGVyIGluIGl0ICh
    hIENSKS4NICBCeSB0aGUgd2F5LCB5b3Ugc2hvdWxkIHJlYWxseSBnZXQgb3V0IG1vcmUu
```

Příklad 3: Soubor obsahuje řadu záznamů o změnách a komentáře

Poznámka: Soubory LDIF se záznamy o změnách nelze přímo importovat na server. Jsou však podporovány obslužnými programy shellu LDAP.

```
version: 1
   # Přidání nového záznamu
   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

   # Smazání existujícího záznamu
   dn: cn=Robert Jensen, ou=Rochester, o=Big Company, c=US
   changetype: delete

   # Modifikace relativního rozlišovacího jména záznamů
   dn: cn=Paul Jensen, ou=Rochester, o=Big Company, c=US
   changetype: modrdn
   newrdn: cn=Paula Jensen
   deleteoldrdn: 1
```

Pořadí záznamů v souboru LDIF je důležité. Aby mohl být záznam uvedený v souboru LDIF úspěšně přidán do adresáře LDAP, musí v adresáři existovat jeho nadřazený záznam. V uvedeném příkladu by druhý a třetí záznam nemohl být přidán, kdyby neexistoval první záznam.

Podobně při importu souboru LDIF na server, který podporuje určité přípony, musí soubor LDIF obsahovat záznamy pro tyto přípony. Kdyby server měl například příponu ou=Rochester, o=Big Company, c=US, soubor LDIF uvedený v daném příkladu by nemohl být importován. Kdyby však tento server měl místo toho příponu o=Big Company, c=US, musel by být záznam pro tuto příponu uveden nejprve v souboru LDIF takto:

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

Formát a obsah souborů LDIF je dán schématem serveru, ze kterého jsou soubory LDIF exportovány. Soubor LDIF může být importován na jakýkoli server LDAP, který používá stejné schéma jako server, z něhož byl tento soubor exportován. Různí dodavatelé serverů LDAP používají různá schémata (s různými třídami objektů a atributy). Proto se může stát, že soubor LDIF vytvořený na jednom serveru nebude možné importovat na jiný server.

RFC (Request for Comments) týkající se specifikací souboru LDIF jsou k dispozici na této adrese:

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

Související postupy:

“Import souboru LDIF” na stránce 22.
“Export souboru LDIF” na stránce 22.

Pravidla pro podporu národního jazyka (NLS)

Počínaje verzí V4R5 jsou server Directory Services LDAP pro OS/400 i klient LDAP pro OS/400 založeny na LDAP verze 3. Uvědomte si tato pravidla pro NLS:

- Data mezi servery LDAP a klienty se přenášejí ve formátu UTF-8. Jsou povoleny všechny znaky ISO 10646.
- Server adresářů LDAP používá k ukládání dat do databáze metodu mapování UTF-16.
- Server a klient provádějí porovnání řetězců bez rozlišení velikosti písmen. Algoritmy používající velká písmena nemusejí být správné ve všech jazycích (lokalitách).

Více informací o UCS-2 najdete v tématu Globalization pod tématem Planning v rámci aplikace iSeries Information Center.

Vlastnictví objektů adresáře LDAP

Každý objekt v adresáři LDAP má minimálně jednoho vlastníka. Vlastník objektu má právo objekt vymazat. Vlastníci a administrátor serveru jsou z uživatelů jediní, kdo mohou změnit vlastnosti vlastnictví a atributy ACL daného objektu. Vlastnictví objektů může být buď zděděné, nebo explicitní. To znamená, že chcete-li přidělit vlastnictví, můžete použít jeden z těchto způsobů:

- Explicitně nastavit vlastnictví pro určitý objekt.
- Zadat, že objekty zdědí vlastníky z objektů nadřazených v hierarchii adresáře LDAP.

Produkt Directory Services umožňuje zadat pro jeden objekt více vlastníků. Můžete též zadat, že objekt vlastní sám sebe, když do seznamu vlastníků objektu přidáte zvláštní DN cn=this. Předpokládejme například, že objekt cn=A má vlastníka cn=this. Každý uživatel, který se připojí k serveru jako cn=A, bude mít přístup k objektu cn=A jako vlastník.

Související postup:

"Práce s vlastnostmi vlastnictví objektů adresáře" na stránce 30.

Odkazy v adresáři LDAP

Odkazy umožňují serverům adresářů LDAP pracovat v týmech. Jestliže se DN, které klient požaduje, nenachází v jednom adresáři, může daný server automaticky poslat (odkázat) tento požadavek na jiný server LDAP.

Produkt Directory Services umožňuje používat dva různé typy odkazů. Můžete zadat předvolené referenční servery, kam server LDAP odkazuje klienty, kdykoli není požadované DN v jeho adresáři. Pomocí klienta LDAP také můžete přidat záznamy na server adresářů, který má odkaz objectClass. To umožňuje specifikovat odkazy na základě toho, jaké konkrétní DN klient požaduje.

Poznámka: V produktu Directory Services smí referenční objekt obsahovat pouze rozlišovací jméno (dn), třídu objektu (objectClass) a atribut odkazu (ref). V části "Obslužný program ldapsearch" na stránce 52 najdete příklad s ukázkou tohoto omezení.

Referenční servery úzce souvisejí s replikačními servery. Protože data na replikačních serverech nemohou být modifikována z klientů, odkazuje replika všechny požadavky na změnu dat adresáře na hlavní server.

Transakce

Server adresářů LDAP můžete v systému konfigurovat tak, aby klientům umožnil používání transakcí. Transakce je skupina operací adresáře LDAP, s kterými se pracuje jako s jedinou jednotkou. Žádné z operací LDAP, které tvoří transakci, nejsou provedeny trvale, dokud nejsou všechny operace v transakci úspěšně dokončeny a transakce není potvrzena. Jestliže některá operace selže nebo je transakce zrušena, všechny ostatní operace se anulují. Tato schopnost umožňuje uživatelům udržovat operace LDAP organizované. Uživatel například spustí z klienta transakci, která vymaže z adresáře několik záznamů.

Jestliže uživatel ztratí spojení se serverem v průběhu této transakce, nevymažou se žádné záznamy. Uživatel může znovu spustit transakci a nemusí kontrolovat, které záznamy byly skutečně vymazány.

Součástí transakce mohou být tyto operace:

- přidání
- změna
- změna RDN
- mazání

Poznámka: Do transakcí byste neměli zahrnovat změny ve schématu adresáře (přípona cn=schema). I když tuto operaci lze v rámci transakce použít, nemůže být vzata zpět v případě selhání transakce. To by mohlo na serveru způsobit nepředvídatelné problémy.

Další informace o transakcích najdete v dodatku Limited Transaction Support příručky IBM SecureWay Directory Client SDK Programming Reference.

Replikační servery adresářů LDAP

Informace uložené na replikačních serverech adresářů LDAP jsou identické s informacemi na hlavním serveru adresářů LDAP. Používání jedné nebo více replik adresáře LDAP má dvě hlavní přednosti:

- Repliky urychlují vyhledávání v adresářích. Místo aby všechny klienty posílaly své požadavky na vyhledání přímo na hlavní server, můžete je rozdělit mezi hlavní server a replikační servery.
- Repliky jsou vlastně zálohou hlavního serveru. Když je hlavní server nedostupný, může replika plnit požadavky na vyhledání a poskytovat přístup k datům adresáře.

Replikační servery jsou určeny pouze pro čtení. Pokusí-li se oprávněný uživatel změnit záznam na replikačním serveru, je jeho požadavek odkázán na hlavní server adresářů.

Související postup:

"Jak nastavit novou repliku serveru adresářů" na stránce 23.

Zabezpečení produktu Directory Services

Monitorování zabezpečení

Počínaje verzí V5R1 produkt Directory Services podporuje monitorování zabezpečení operačního systému OS/400. Monitorovat můžete:

- Připojení a odpojení od serveru adresářů.
- Změny povolení pro objekty adresáře LDAP.
- Změny vlastnictví objektů adresáře LDAP.
- Vytváření, odstranění, vyhledávání a změny objektů adresáře LDAP.
- Změny hesla administrátora a aktualizace rozlišovacích jmen (DN).
- Změny hesel uživatelů.
- Import a export souborů.

Ještě před zahájením monitorování záznamů adresáře můžete změnit nastavení funkce monitorování operačního systému OS/400. Je-li u systémové hodnoty QAUDCTL zadáno *OBJAUD, můžete aktivovat monitorování objektů prostřednictvím produktu iSeries Navigator. Další informace o monitorování najdete v publikaci *Security - Reference* nebo v tématu Security auditing v rámci aplikace iSeries Information Center.

Autentizace a zabezpečení připojení

Produkt Directory Services obsahuje následující mechanismus, který slouží ke zdokonalení zabezpečení komunikací mezi klienty LDAP a serverem adresářů LDAP:

- Připojení přes SSL.
- Autentizace Kerberos.
- Kódování hesla CRAM-MD5.

Jak používat zabezpečení SSL a TLS u serveru adresářů LDAP

K lepšímu zabezpečení komunikací se serverem adresářů LDAP může produkt Directory Services použít zabezpečení SSL (Secure Sockets Layer).

K tomu, abyste mohli v produktu Directory Services používat SSL, je třeba mít v systému nainstalován jeden z produktů Cryptographic Access Provider (5722-ACx). Chcete-li používat SSL z prostředí produktu iSeries Navigator, je třeba mít na PC nainstalovaný i jeden z produktů Client Encryption (5722-CEx). Tento software je nutný k provádění následujících činností:

- Konfigurace a administrace produktu Directory Services z pracovní stanice pomocí připojení přes SSL. To zahrnuje úkoly, které se provádějí z prostředí produktu iSeries Navigator.
- Používání připojení přes SSL s aplikacemi, která vytváříte pomocí rozhraní API klienta Windows.

SSL je standardem pro bezpečnost Internetu. SSL můžete používat ke komunikaci s klienty LDAP i s replikačními servery LDAP. Kromě autentizace serveru můžete používat i autentizaci klienta a dále tak zvýšit bezpečnost připojení přes SSL. Autentizace klienta vyžaduje, aby klient LDAP předložil digitální certifikát, kterým potvrdí serveru svoji identitu, než bude vytvořeno připojení.

Chcete-li používat SSL, je třeba mít v systému nainstalován produkt DCM (Digital Certificate Manager), což je volba 34 operačního systému OS/400. DCM poskytuje rozhraní, které slouží k vytváření a správě digitálních certifikátů a pamětí certifikátů. Informace týkající se digitálních certifikátů a používání DCM najdete v dokumentaci k produktu Digital Certificate Manager. Informace týkající se SSL na serveru iSeries najdete v tématu Zabezpečení aplikací pomocí SSL. Informace o TLS (Transport Layer Security) na serveru iSeries najdete v tématu Podporované protokoly SSL a TLS.

Jak používat autentizaci Kerberos u serveru adresářů LDAP

Produkt Directory Services umožňuje nastavit server adresářů LDAP pro používání autentizace Kerberos. Kerberos je síťový autentizační protokol, který pomocí šifrování tajným klíčem zajišťuje přísnou autentizaci pro aplikace typu klient/server.

Chcete-li aktivovat autentizaci Kerberos, je třeba mít nainstalován jeden z produktů Cryptographic Service Provider (5722AC2 nebo 5722AC3). Je rovněž třeba mít nastavenou službu síťové autentizace.

Podpora produktu Directory Services protokolem Kerberos obsahuje podporu mechanismu GSSAPI SASL. Ten umožňuje klientům LDAP SecureWay a Windows 2000 používat u serveru adresářů LDAP autentizaci Kerberos.

Hlavní jméno pro Kerberos, které server používá, má tento formát:

```
jméno-služby/jméno-hostitele@sféra
```

Jméno-služby je ″LDAP″, jméno-hostitele je plně kvalifikované TCP/IP jméno systému a sféra je předvolená sféra zadaná v systémové konfiguraci Kerberos.

Například u systému, který má jméno my-as400 v TCP/IP doméně acme.com a s předvolenou sférou Kerberos ACME.COM, bude hlavní jméno pro Kerberos LDAP/my-as400.acme.com@ACME.COM. Předvolená sféra Kerberos je uvedená v konfiguračním souboru produktu Kerberos (standardně je to soubor /QIBM/UserData/OS400/NetworkAuthentication/krb5.conf) s direktivou ″default_realm″ (default_realm =

ACME.COM). Podle konvence se pro jména sfér Kerberos používají velká písmena a pro jména hostitelů malá písmena. ″LDAP/″ musí být velkými písmeny. Server adresářů nelze pomocí autentizace Kerberos nakonfigurovat, není-li předtím nastavena předvolená sféra.

Při použití autentizace Kerberos sváže server adresářů LDAP rozlišovací jméno (DN) s připojením, které určuje přístup k datům adresáře. Můžete si vybrat, zda má být DN serveru svázáno s některou z těchto metod:

- Server může vytvořit DN založené na ID Kerberos. Vyberete-li tuto volbu, identita Kerberos ve formátu ″principal@realm″ vygeneruje DN ve formátu ″ibm-kn=principal@realm″. ibm-kn= je ekvivalentem k ibm-kerberosName=.
- Server může v adresáři vyhledat rozlišovací jméno (DN), které obsahuje záznam o hlavním jménu a sféře Kerberos. Vyberete-li tuto volbu, bude server v adresáři hledat záznam, který udává tuto identitu Kerberos takto:
  - Server vyhledá v adresáři objekt ″krbRealm″, který má atribut ″krbRealmName″ shodný se sférou Kerberos. Nalezne-li tento záznam, vyhledá v DN, která jsou uvedena v atributu ″princSubtree″, záznam s atributem ″krbPrincipalName″, který je shodný s hlavním jménem. Jestliže DN nakonfigurované v ″krbAliasedObjectName″ obsahuje DN dříve nalezeného záznamu, použije se DN nakonfigurované v ″krbAliasedObjectName″. Jinak se použije DN tohoto záznamu. Tato metoda se obvykle používá, když KDC Kerberos ukládá hlavní informace do adresáře LDAP.
  - Jestliže uvedené vyhledávání selže, bude server hledat v adresáři záznam, který používá pomocnou třídu ibm-securityIdentities a jehož atribut altSecurityIdentities má hodnotu KERBEROS:principal@realm. Tato metoda slouží ke svázání identit Kerberos se záznamy v adresáři, pokud KDC neukládá hlavní jména do adresáře.

Je třeba, abyste měli k dispozici soubor s tabulkou klíčů (keytab), který obsahuje klíč pro hlavní jméno služeb LDAP. Více informací o produktu iSeries Kerberos na serveru iSeries najdete v rámci aplikace Information Center pod tématem Network authentication service v tématu Security. Toto téma popisuje, jak přidávat informace do souboru s tabulkou klíčů.

Procedura Backend projektovaná operačním systémem

Procedura Backend projektovaná systémem má schopnost mapovat objekty operačního systému OS/400 jako záznamy v rámci adresářového stromu přístupného z LDAP. Plánované objekty jsou LDAP reprezentacemi objektů operačního systému OS/400 namísto skutečných záznamů uložených v databázi serveru LDAP. U verze V5R2 jsou uživatelské profily operačního systému OS/400 jedinými objekty, které jsou mapovány nebo projektovány jako záznamy v adresářovém stromu. Mapování objektů uživatelských profilů se nazývá procedura Backend projektovaná uživatelem OS/400.

Operace LDAP jsou mapovány do objektů operačního systému OS/400. Operace LDAP provádějí funkce operačního systému, aby měly přístup k těmto objektům. Všechny operace LDAP prováděné v uživatelských profilech jsou uskutečňovány s oprávněním uživatelského profilu asociovaným s připojením klienta.

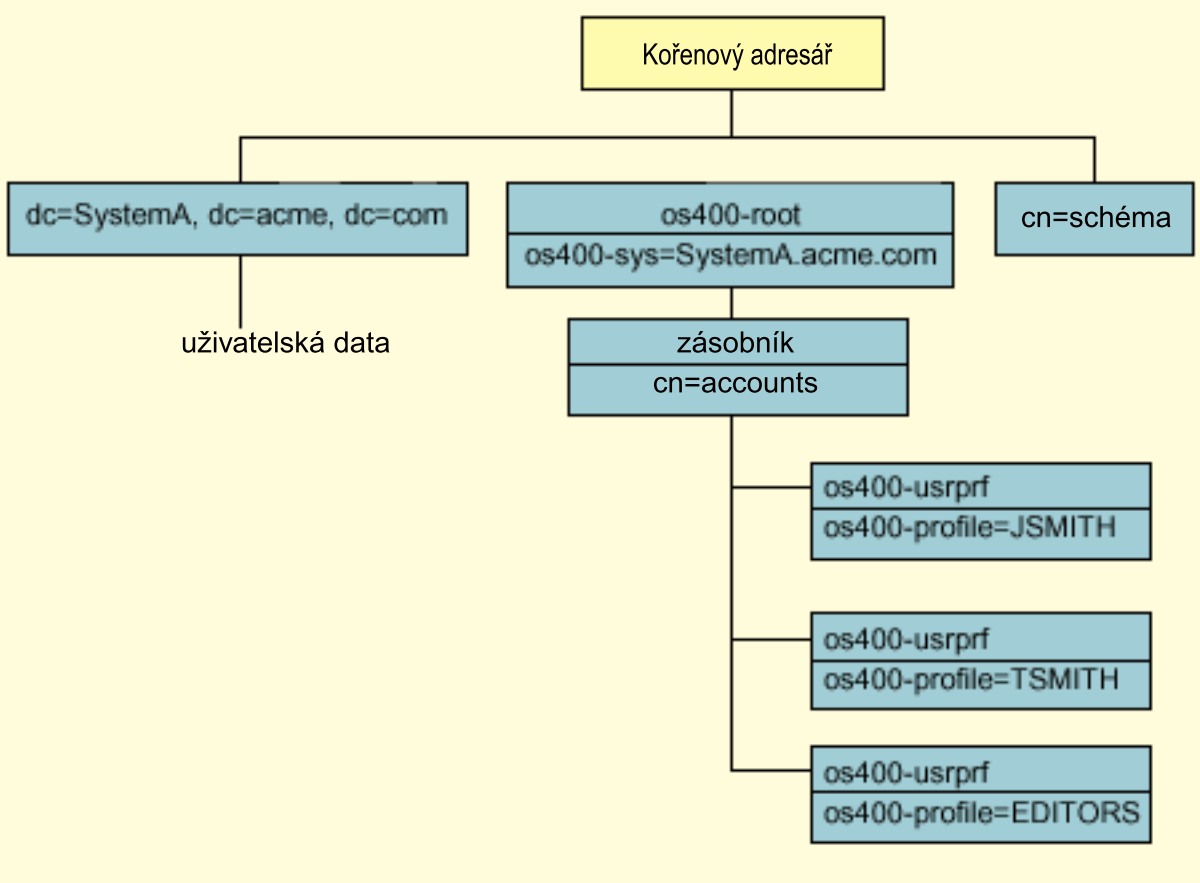
Podrobnější informace o proceduře Backend projektované operačním systémem najdete v těchto částech:

- “Struktura adresářů projektovaná uživatelem OS/400”.
- “Operace LDAP” na stránce 41.
- “Připojená DN administrátora a repliky” na stránce 45.
- “Uživatelem projektované schéma OS/400” na stránce 45.

Struktura adresářů projektovaná uživatelem OS/400

Níže uvedený obrázek ukazuje příklad adresářového stromu, neboli DIT (directory information tree) pro the proceduru Backend projektovanou uživatelem Obrázek zobrazuje individuální i skupinové profily. Na obrázku jsou JSMITH a TSMITH uživatelské profily, což je interně označeno pomocí identifikátoru skupiny (GID), GID=*NONE (nebo 0). EDITORS je skupinový profil, který je interně označen nenulovým GID.

Přípona dc=SystemA, dc=acme, dc=com je na obrázku kvůli odkazům. Tato přípona představuje Backend aktuální databáze, který spravuje ostatní záznamy LDAP. Přípona cn=schema reprezentuje aktuální používané schéma pro celý server.



Kořenem stromu je přípona, která nabývá předem stanovenou hodnotu os400-sys=*SystemA.acme.com*, kde *SystemA.acme.com* je jméno vašeho systému. Atribut objectclass je os400-root. Ačkoli DIT nemůže být upraven nebo vymazán, můžete konfigurovat systémovou příponu objektů. Musíte však zajistit, aby se aktuální přípona nepoužila v ACL nebo jinde v systému, kde je potřeba modifikovat wntries v případě, že by se přípona změnila.

Na předchozím obrázku je zásobník cn=accounts zobrazen pod kořenem. Tento objekt nemůže být modifikován. Zásobník je na této úrovni umístěn v očekávání dalších druhů informací nebo objektů, které mohou být v budoucnu plánovány operačním systémem. Pod zásobníkem jsou umístěny uživatelské profily, které jsou projektovány jako objectclass=os400-usrprf. Na uživatelské profily se odkazuje jako na projektované uživatelské profily a LDAP je registruje ve formě os400-profile=JSMITH, cn=accounts, os400-sys=SystemA.acme.com.

Operace LDAP

Následující operace LDAP mohou být prováděny pomocí projektovaných uživatelských profilů.

Připojení

Klient LDAP může být připojen (autentizován) na server LDAP pomocí projektovaného uživatelského profilu. Provede se to pomocí specifikace rozlišovacího jména (DN) projektovaného uživatelského profilu pro připojené DN a správného hesla uživatelského profilu OS/400 pro autentizaci. Příkladem DN použitého v požadavku na připojení je os400-profile=jsmith, cn=accounts, os400-sys=systemA.acme.com.

Klient se musí připojit jako projektovaný uživatel, aby měl přístup k informacím v proceduře Backend projektované systémem. Server provádí všechny operace pomocí oprávnění tohoto uživatelského profilu. DN projektovaného uživatelského profilu může být použito také v LDAP ACL jako DN ostatních položek LDAP. Jednoduchá metoda připojení je jedinou povolenou metodou připojení v případě, když je projektovaný uživatelský profil specifikován v požadavku na připojení.

Vyhledávání

Procedura Backend projektovaná systémem podporuje některé základní vyhledávací filtry. Ve vyhledávacích filtrech můžete určit atributy objectclass, os400-profile a os400-gid. Atribut os400-profile podporuje zástupné znaky. Atribut os400-gid je omezen na zadání (os400-gid=0), což je individuální uživatelský profil, nebo na zadání !(os400-gid=0), což je skupinový profil. Můžete vyhledat všechny atributy uživatelského profilu kromě hesla a podobných atributů.

U některých filtrů se vrátí pouze hodnoty DN objectclass a os400-profile. Po provedení následujícího vyhledávání se však mohou vrátit podrobnější informace.

Tato tabulka popisuje chování procedury Backend projektované systémem při operacích vyhledávání.

Tabulka 1. Chování procedury Backend projektované systémem při operacích vyhledávání

Požadováno vyhledávání	Základna vyhledávání	Rozsah vyhledávání	Filtr vyhledávání	Poznámky
Vrátit informace pro os400-sys=SystemA, (volitelně) pro zásobníky pod ním a (volitelně) pro objekty v těchto zásobnících.	os400-sys=SystemA.acme.com	base, sub nebo one	objectclass=* objectclass=os400-root objectclass=container objectclass=os400-usrprf	Vrátí odpovídající atributy a jejich hodnoty podle zadaného rozsahu a filtru. Pevně naprogramované atributy a jejich hodnoty se vrátí pro systémovou příponu objektů a zásobník pod ní.
Vrátit všechny uživatelské profily.	cn=accounts, os400-sys=SystemA.acme.com	one nebo sub	os400-gid=0	Pro projektované uživatelské profily se vrátí pouze hodnoty rozlišovací jméno (DN), objectclass a os400-profile. Pokud je zadán jakýkoli jiný filtr, vrátí se LDAP_UNWILLING_TO_PERFORM.
Vrátit všechny skupinové profily.	cn=accounts, os400-sys=SystemA.acme.com	one nebo sub	(!(os400-gid=0))	Pro projektované uživatelské profily se vrátí pouze hodnoty rozlišovací jméno (DN), objectclass a os400-profile. Pokud je zadán jakýkoli jiný filtr, vrátí se LDAP_UNWILLING_TO_PERFORM.

Tabulka 1. Chování procedury Backend projektované systémem při operacích vyhledávání (pokračování)

Požadováno vyhledávání	Základna vyhledávání	Rozsah vyhledávání	Filtr vyhledávání	Poznámky
Vrátit všechny uživatelské a skupinové profily.	cn=accounts, os400-sys=SystemA.acme.com	one nebo sub	os400-profile=*	Pro projektované uživatelské profily se vrátí pouze hodnoty rozlišovací jméno (DN), objectclass a os400-profile. Pokud je zadán jakýkoli jiný filtr, vrátí se LDAP_UNWILLING_TO_PERFORM.
Vrátit informace pro konkrétní uživatelský nebo skupinový profil, jako je například uživatelský profil JSMITH.	cn=accounts, os400-sys=SystemA.acme.com	one nebo sub	os400-profile=JSMITH	Mohou být specifikovány jiné atributy, které se mají vrátit.
Vrátit informace pro konkrétní uživatelský nebo skupinový profil, jako je například uživatelský profil JSMITH.	os400-profile=JSMITH, cn=accounts, os400-sys=SystemA.acme.com	bas, sub nebo one	objectclass=os400-usrprf objectclass=* os400-profile=JSMITH	Mohou být specifikovány jiné atributy, které se mají vrátit. Přestože může být specifikován rozsah jedné úrovně, výsledek vyhledávání nevrátí žádné hodnoty, protože v DIT se pod uživatelským profilem JSMITH nenachází nic.
Vrátit všechny uživatelské a skupinové profily, které začínají písmenem A.	cn=accounts, os400-sys=SystemA.acme.com	one nebo sub	os400-profile=A*	Pro projektované uživatelské profily se vrátí pouze hodnoty rozlišovací jméno (DN), objectclass a os400-profile. Pokud je zadán jakýkoli jiný filtr, vrátí se LDAP_UNWILLING_TO_PERFORM.
Vrátit všechny skupinové profily, které začínají písmenem G.	cn=accounts, os400-sys=SystemA.acme.com	one nebo sub	(&(!(os400-gid=0)) (os400-profile=G*))	Pro projektované uživatelské profily se vrátí pouze hodnoty rozlišovací jméno (DN), objectclass a os400-profile. Pokud je zadán jakýkoli jiný filtr, vrátí se LDAP_UNWILLING_TO_PERFORM.

Tabulka 1. Chování procedury Backend projektované systémem při operacích vyhledávání (pokračování)

Požadováno vyhledávání	Základna vyhledávání	Rozsah vyhledávání	Filtr vyhledávání	Poznámky
Vrátit všechny uživatelské profily, které začínají písmenem A.	cn=accounts, os400-sys=SystemA.acme.com	one nebo sub	(&(os400-gid=0) (os400-profile=A*))	Pro projektované uživatelské profily se vrátí pouze hodnoty rozlišovací jméno (DN), objectclass a os400-profile. Pokud je zadán jakýkoli jiný filtr, vrátí se LDAP_UNWILLING_TO_PERFORM.

Porovnávání

LDAP operaci porovnávání je možné použít k porovnání hodnoty atributu projektovaného uživatelského profilu. Atributy os400-aut a os400-docpwd nemohou být porovnány.

Přidání a změna

Uživatelský profil můžete vytvořit pomocí LDAP operace přidání nebo ho můžete změnit pomocí LDAP operace změny.

Mazání

Pomocí LDAP operace mazání můžete uživatelský profil vymazat. Aby bylo možné specifikovat chování parametrů DLTUSRPRF OWNOBJOPT a PGPOPT, jsou nyní k dispozici dva ovladače serveru LDAP. Tyto ovladače mohou být zadány v LDAP operaci mazání. Více informací o chování těchto parametrů najdete v části popisující příkaz DLTUSRPRF (Výmaz uživatelského profilu).

V LDAP operaci výmazu klienta mohou být zadány tyto ovladače a jejich identifikátory objektu (OID).

- os400-dltusrprf-ownobjopt 1.3.18.0.2.10.8

  Dále je uvedena hodnota ovladače:
  - controlValue ::= ownObjOpt [newOwner]
  - ownObjOpt ::= *NODLT / *DLT / *CHGOWN

  Hodnota ovladače ownObjOpt určuje operaci, která se má provést, pokud uživatelský profil vlastní nějaké objekty. Hodnota *NODLT určuje, aby se nemazal uživatelský profil, vlastní-li uživatelský profil nějaké objekty. Hodnota *DLT určuje, aby se vymazal vlastněný objekt, a hodnota *CHGOWN určuje, aby se vlastnictví převedlo na jiný profil.

  Hodnota newOwner specifikuje profil, na který se má převést vlastnictví. Tato hodnota je vyžadována, když je ovladač ownObjOpt nastaven na *CHGOWN.

  Toto jsou příklady hodnot ovladačů:
  - *NODLT: určuje, že profil nemůže být vymazán, pokud vlastní nějaké objekty.
  - *CHGOWN SMITH: určuje, aby se vlastnictví všech objektů převedlo na uživatelský profil SMITH.
- Identifikátor objektu (OID) je definován v ldap.h jako LDAP_OS400_OWNOBJOPT_CONTROL_OID.
  - os400-dltusrprf-pgpopt 1.3.18.0.2.10.9

    Hodnota ovladače je definována takto:

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

Hodnota pgpOpt určuje operaci, která se má provést, je-li mazaný profil primární skupinou pro jakékoli objekty. Je-li zadána hodnota *CHGPGP, musí být zadána také hodnota newPgp. Hodnota newPgp určuje jméno profilu primární skupiny nebo *NONE. Jestliže je zadán nový profil primární skupiny, může být zadána také hodnota newPgpAut. Hodnota newPgpAut určuje oprávnění k objektům, které je uděleno nové primární skupině.

Toto jsou příklady hodnot ovladačů:

- *NOCHG: určuje, že profil nemůže být vymazán, pokud je primární skupinou pro některé objekty.
- *CHGPGP *NONE: určuje, aby se odstranila primární skupina pro objekty.
- *CHGPGP SMITH *USE: určuje, aby se změnila primární skupina pro uživatelský profil SMITH a aby se primární skupině udělilo oprávnění *USE.

Není-li některý z těchto ovladačů zadán v operaci mazání, použijí se namísto toho aktuálně platné předvolené ovladače pro příkaz QSYS/DLTUSRPRF.

ModRDN

Plánované uživatelské profily nelze přejmenovat, protože operační systém přejmenování nepodporuje.

Rozhraní API pro import, rozhraní API pro export

Rozhraní API QgldImportLdif a QgldExportLdif nepodporují import a export dat v rámci procedury Backend projektované systémem.

Připojená DN administrátora a repliky

Projektovaný uživatelský profil můžete zadat jako připojená DN konfigurovaného administrátora nebo repliky. Použije se heslo uživatelského profilu. Projektované uživatelské profily se mohou stát také administrátory LDAP, jestliže mají oprávnění k ID funkce Directory Server Administrator (QIBM_DIRSRV_ADMIN). Přístup administrátora může získat několik uživatelských profilů.

Více informací najdete v části “Práce s přístupovými seznamy pro oprávněné uživatele” na stránce 30.

Uživatelem projektované schéma OS/400

Třídy objektů a atributy z projektované procedury Backend je možné najít v schématu pro celý server. Jména atributů LDAP jsou ve formátu os400–*nnn*, kde *nnn* je obvykle klíčové slovo atributu (například CRTUSRPRF nebo CHGUSRPRF) v příkazech uživatelského profilu. Více informací najdete v části “Struktura adresářů projektovaná uživatelem OS/400” na stránce 40.

Produkt Directory Services a podpora zapisování do žurnálu OS/400

Produkt Directory Services používá k uchovávání informací o adresářích databázovou podporu operačního systému OS/400. Adresářové záznamy jsou ukládány do databáze pomocí vázaného zpracování. To vyžaduje podporu zapisování do žurnálů OS/400.

Při prvním spuštění serveru nebo nástroje pro import LDIF se vytvoří tyto položky:

- žurnál
- zásobník žurnálu
- všechny potřebné databázové tabulky

Žurnál QSQJRN je vytvořen v databázové knihovně, kterou jste nakonfigurovali. Zásobník žurnálu QSQJRN0001 je zpočátku vytvořen v databázové knihovně, kterou jste nakonfigurovali.

Vaše prostředí, velikost a struktura adresáře nebo strategie ukládání a obnovy mohou vyžadovat změnu nastavení předvolených hodnot, včetně způsobu správy objektů a velikosti použitého prahu. V případě potřeby můžete změnit uvedené parametry příkazu pro zapisování do žurnálu. Zapisování do žurnálu LDAP je standardně nastaveno tak, aby vymazalo staré zásobníky. Je-li nakonfigurován protokol změn a chcete si ponechat staré zásobníky, zadejte z příkazové řádky operačního systému OS/400 tento příkaz:

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

Je-li nastaven protokol změn, můžete vymazat i jeho zásobníky žurnálu příkazem:

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

Informace o příkazech pro zapisování do žurnálu najdete v tématu OS/400 commands pod tématem Programming v rámci aplikace iSeries Information Center.

Kapitola 6. Obslužné programy příkazové řádky LDAP

Produkt Directory Services obsahuje pět obslužných programů, které umožňují provádět úkoly na serveru adresářů LDAP z příkazového prostředí Qshell v operačním systému OS/400. Tyto obslužné programy využívají API LDAP. Můžete je spustit z příkazové řádky qsh nebo je volat z uživatelských programů. Můžete je využít i jako příklady při programování. Když instalujete klienta LDAP pro Windows, který je začleněn do produktu Directory Services, instaluje se i kód, který je velmi podobný zdrojovému kódu obslužných programů shellu.

Jedná se o tyto obslužné programy:
- "Obslužné programy ldapmodify a ldapadd" přidávají a modifikují záznamy v adresáři LDAP.
- "Obslužný program ldapdelete" na stránce 50 odstraňuje záznamy z adresáře LDAP.
- "Obslužný program ldapsearch" na stránce 52 vyhledává záznamy v adresáři LDAP.
- "Obslužný program ldapmodrdn" na stránce 57 modifikuje RDN záznamů v adresáři LDAP.

Informace o použití SSL u obslužných programů příkazové řádky najdete v části "Poznámky k používání SSL s obslužnými programy příkazové řádky LDAP" na stránce 59.

Obslužné programy ldapmodify a ldapadd

Obslužný program ldapmodify slouží ke změnám záznamů nebo k přidávání záznamů na server adresářů LDAP z příkazového shellu QSH ve vašem systému. Používá rozhraní API ldap_modify, ldap_add a ldap_delete. Obslužný program ldapadd pracuje téměř stejně jako obslužný program ldapmodify, pouze s tou výjimkou, že příznak -a se zapíná 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: Jestliže nedodáte informace o záznamu ze souboru (*file*) použitím volby **-f**, obslužný program bude čekat na přečtení záznamů ze standardního vstupu. Toto čekání můžete přerušit stisknutím klávesy SysReq a výběrem volby 2. End previous request (Ukončit předchozí příkaz).

Diagnostika:

Dokončí-li se program bez chyb, je návratový kód 0. V případě chyby je návratový kód nenulový a pro standardní chybový výstup se zapíše diagnostická zpráva.

Zde si můžete prohlédnout příklady použití těchto obslužných programů.

Parametry:

-V	Specifikuje verzi LDAP, kterou obslužný program použije k připojení na server LDAP. Standardně se používá připojení LDAP V3. Chcete-li explicitně vybrat LDAP V3, zadejte -V 3. Chcete-li spustit aplikaci LDAP V2, zadejte -V 2.

-a	Tento parametr používá pouze obslužný program ldapmodify. Určuje, že obslužný program bude namísto modifikace záznamy standardně přidávat. Použití tohoto parametru je stejné jako u programu ldapadd.
-b	Předpokládá, že všechny hodnoty, které začínají `/ , jsou binární hodnoty a že skutečná hodnota je v souboru, jehož cesta je zadána v místě, kde se hodnoty běžně zobrazují.
-c	Nepřerušený operační režim. Chyby se zaznamenávají, ale program ldapmodify nebo ldapadd pokračuje v přidávání nebo změnách. Standardně je nastaveno ukončení programu po zaznamenání chyby.
-r	Existující hodnoty se standardně přepisují.
-M	Referenční objekty jsou spravovány jako řádné záznamy.
-n	Zobrazuje, co bude vykonáno, ale záznamy se ve skutečnosti nemění. Tento parametr ve spojení s parametrem -v lze využít k ladění.
-v	Používá mnohomluvný režim s mnoha diagnostickými zprávami na standardním výstupu.
-F	Vynutí aplikaci všech změn, bez ohledu na obsah vstupních řádek, které začínají řetězcem replica: (řádky začínající na replica: jsou standardně porovnávány proti serveru LDAP a použitému portu, aby se mohlo rozhodnout, zda záznam v replikačním protokolu bude skutečně aplikován).
-R	Specifikuje, že odkazy nebudou zpracovány automaticky.
-C *charset*	Specifikuje, že řetězce, které jsou dodávány jako vstup do programu, jsou v lokální znakové sadě (*charset*) a musí být konvertovány na kód UTF-8. Volbu **-C** použijte v případě, že je kódová stránka vstupního řetězce jiná než hodnota kódové stránky úlohy. V dokumentaci k API ldap_set_iconv_local_charset() najdete podporované hodnoty *charset*.
-d *debuglevel*	Nastaví úroveň ladění na hodnotu *debuglevel*.
-D *binddn*	Hodnota *binddn* slouží k připojení k adresáři LDAP. *Binddn* by mělo být řetězcem vyjádřené DN.
-w *passwd*	Hodnota *passwd* je heslo pro autentizaci.
-m *mechanism*	Hodnota *mechanism* specifikuje mechanismus SSL, kterým se klient připojuje k serveru. Klient používá API ldap_sasl_bind_s(). Dostupné mechanismy jsou CRAM-MD5 (kódování hesla), EXTERNAL (pro SSL) a GSSAPI (Kerberos). Parametr **-m** je ignorován v případě, že je nastaven parametr **-V 2**. Jestliže parametr **-m** nezadáte, použije se jednoduchá autentizace.
-O*hopcount*	Hodnota *hopcount* nastaví maximální počet přechodů, které knihovna klienta vykoná, když vyhledává odkazy. Standardní hodnota pro počet přechodů je 10.
-h *ldaphost*	Specifikuje alternativního hostitele, na kterém běží server LDAP.
-p *ldapport*	Specifikuje alternativní port TCP, na kterém server LDAP naslouchá. Předvolený port LDAP je 389. Není-li port specifikován a je specifikován parametr **-Z**, použije se předvolený port LDAP SSL 636.
-f *file*	Čte informace o změně záznamu ze souboru LDIF namísto standardního vstupu. Není-li soubor LDIF zadán, musíte pomocí standardního vstupu zadat aktualizované záznamy ve formátu LDIF.
-Z	Ke komunikaci se serverem LDAP se použije připojení přes SSL. Volba **-Z** je podporována pouze ve verzích, které podporují SSL.
-K *keyfile*	Specifikuje jméno souboru databáze klíčů SSL. Není-li soubor databáze klíčů v aktuálním adresáři, zadejte plně kvalifikované jméno souboru databáze klíčů. Jestliže obslužný program nemůže najít databázi klíčů, použije pevně naprogramovanou sadu předvolených důvěryhodných zdrojů vydavatele certifikátů (CA). Soubor databáze klíčů obvykle obsahuje jeden nebo více certifikátů nebo vydavatelů certifikátů ověřených klientem. Tyto typy certifikátů X.509 jsou rovněž známé jako důvěryhodné zdroje. Tento parametr účinně aktivuje přepínač **-Z**.

-P *keyfilepw*	Specifikuje heslo pro databázi klíčů. Toto heslo je požadováno pro přístup ke kódovaným informacím v souboru databáze klíčů (včetně soukromého klíče). Je-li se souborem databáze klíčů asociován soubor pro uložení hesla, získá se heslo ze souboru pro uložení hesla a tento parametr se nevyžaduje. Tento parametr je ignorován v případě, že není zadán parametr **-Z** ani **-K**.
-N *certificatename*	Specifikuje návěští asociované s certifikátem klienta v souboru databáze klíčů. Všimněte si, že jestliže je server LDAP konfigurován pouze pro provádění autentizace serveru, certifikát klienta se nevyžaduje. Je-li server LDAP konfigurován pro provádění autentizace serveru i klienta, je certifikát klienta povinný. *Certificatename* není vyžadováno, jestliže byl standardně označen předvolený pár certifikát/soukromý klíč. Podobně není *certificatename* vyžadováno, jestliže existuje jediný pár certifikát/soukromý klíč v označeném souboru databáze klíčů. Tento parametr je ignorován v případě, že není zadán parametr **-Z** ani **-K**.

Alternativní vstupní formát:

Obslužný program ldapmodify podporuje alternativní vstupní formát za účelem zachování kompatibility s nižšími verzemi tohoto obslužného programu. Tento formát obsahuje jeden nebo více záznamů, které jsou odděleny prázdnými řádky. Každý záznam má tento formát:

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

kde *attr* je jméno atributu a *value* je hodnota. Standardně se hodnoty přidávají. Zadáte-li na příkazovou řádku příznak **-r**, bude předvoleno nahrazování existujících hodnot novými. Všimněte si, že je přípustné, aby se daný parametr objevil více než jednou (například můžete přidat pro atribut několik hodnot). Rovněž si uvědomte, že pokud použijete zpětné lomítko na konci řádky (\), mohou hodnoty pokračovat i na dalších řádcích a mohou být zachovány i nové řádky ve vlastní hodnotě. Chcete-li některou hodnotu odstranit, uveďte před hodnotu *attr* pomlčku (-). Znaménko rovná se (=) a hodnota by se měla vynechat v případě, že chcete odstranit celý atribut. Před hodnotou *attr* by mělo být uvedeno znaménko plus (+), chcete-li přidat hodnotu za přítomnosti příznaku **-r**.

Příklady: ldapmodify a ldapadd

Příklad 1:

Jestliže soubor /**tmp**/**entrymods** obsahuje tento zápis:

```
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
-
```

pak příkaz ldapmodify -b -r -f /tmp/entrymods provede tyto změny:

- Nahradí obsah atributu mail v záznamu ″Modify Me″ hodnotou modme@student.of.life.edu.
- Přidá název Grand Poobah.
- Přidá obsah souboru /**tmp**/**modme.jpeg** jako jpegPhoto.
- Úplně odstraní atribut description.

Tytéž změny můžete provést i ve starším vstupním formátu 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
```

Příkaz pro použití staršího formátu by měl vypadat takto:

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

Příklad 2:

Jestliže soubor /**tmp**/**newentry** obsahuje tento zápis:

```
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
```

pak příkaz ldapadd -f /tmp/entrymods přidá nový záznam pro Johna Doea, přičemž použije hodnoty ze souboru /tmp/newentry.

Příklad 3:

Jestliže existuje soubor /**tmp**/**newentry**, který obsahuje tento zápis:

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

Příkaz ldapmodify -f /tmp/entrymods odstraní záznam pro Johna Doea.

Obslužný program ldapdelete

Obslužný program ldapdelete umožňuje vymazat jeden nebo více záznamů ze serveru adresářů LDAP. Spouští se z příkazového shellu QSH v systému OS/400. Používá 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: Nezadáte-li argumenty *dn*, bude příkaz ldapdelete čekat na přečtení seznamu DN ze standardního vstupu. Toto čekání můžete přerušit stisknutím klávesy SysReq a výběrem volby 2. End previous request (Ukončit předchozí příkaz).

Diagnostika:

Dokončí-li se program bez chyb, je návratový kód 0. V případě chyby je návratový kód nenulový a pro standardní chybový výstup se zapíše diagnostická zpráva.

Zde si můžete prohlédnout příklady použití obslužného programu ldapdelete.

Parametry:

-V	Specifikuje verzi LDAP, kterou obslužný program použije k připojení na server LDAP. Standardně se používá připojení LDAP V3. Chcete-li explicitně vybrat LDAP V3, zadejte -V 3. Chcete-li spustit aplikaci LDAP V2, zadejte -V 2.
-M	Referenční objekty jsou spravovány jako řádné záznamy.
-n	Zobrazuje, co bude vykonáno, ale záznamy se ve skutečnosti nevymažou. Tento parametr ve spojení s parametrem -v lze využít k ladění.
-v	Používá mnohomluvný režim s mnoha diagnostickými zprávami na standardním výstupu.
-c	Nepřerušený operační režim. Chyby jsou oznamovány, ale program ldapdelete pokračuje ve výmazech. Standardně je nastaveno ukončení programu po zaznamenání chyby.
-R	Specifikuje, že odkazy nebudou zpracovány automaticky.
-C *charset*	Specifikuje, že rozlišovací jména (DN), která jsou dodávána jako vstup do programu ldapdelete, jsou v lokální znakové sadě (*charset*). Volba **-C** *charset* potlačí předvolbu, kdy řetězce musí být dodávány v UTF-8. Volbu **-C** použijte v případě, že je kódová stránka vstupního řetězce jiná než hodnota kódové stránky úlohy. V dokumentaci k API ldap_set_iconv_local_charset() najdete podporované hodnoty *charset*.
-d *debuglevel*	Nastaví úroveň ladění na hodnotu *debuglevel*.
-f *file*	Čte se série řádek ze souboru (*file*) a pro každou řádku se provede jeden výmaz LDAP. Každá řádka v tomto souboru by měla obsahovat jedno rozlišovací jméno (DN).
-D *binddn*	Hodnota *binddn* slouží k připojení k adresáři LDAP. *Binddn* by mělo být řetězcem vyjádřené DN.
-w *passwd*	Hodnota *passwd* je heslo pro autentizaci.
-m *mechanism*	Hodnota *mechanism* specifikuje mechanismus SSL, kterým se klient připojuje k serveru. Použije se API ldap_sasl_bind_s(). Dostupné mechanismy jsou CRAM-MD5 (kódování hesla), EXTERNAL (pro SSL) a GSSAPI (Kerberos). Parametr **-m** je ignorován v případě, že je nastaven parametr **-V 2**. Jestliže parametr **-m** nezadáte, použije se jednoduchá autentizace.
-O *hopcount*	Hodnota *hopcount* nastaví maximální počet přechodů, které knihovna klienta vykoná, když vyhledává odkazy. Standardní hodnota pro počet přechodů je 10.
-h *ldaphost*	Specifikuje alternativního hostitele, na kterém běží server LDAP.
-p *ldapport*	Specifikuje alternativní port TCP, na kterém server LDAP naslouchá. Předvolený port LDAP je 389. Není-li port specifikován a je specifikován parametr **-Z**, použije se předvolený port LDAP SSL 636.
-Z	Ke komunikaci se serverem LDAP se použije připojení přes SSL. Volba **-Z** je podporována pouze ve verzích, které podporují SSL.
-K *keyfile*	Specifikuje jméno souboru databáze klíčů SSL. Není-li soubor databáze klíčů v aktuálním adresáři, zadejte plně kvalifikované jméno souboru databáze klíčů. Jestliže obslužný program nemůže najít databázi klíčů, použije pevně naprogramovanou sadu předvolených důvěryhodných zdrojů vydavatele certifikátů (CA). Soubor databáze klíčů obvykle obsahuje jeden nebo více certifikátů nebo vydavatelů certifikátů ověřených klientem. Tyto typy certifikátů X.509 jsou rovněž známé jako důvěryhodné zdroje. Tento parametr účinně aktivuje přepínač **-Z**.
-P *keyfilepw*	Specifikuje heslo pro databázi klíčů. Toto heslo je požadováno pro přístup ke kódovaným informacím v souboru databáze klíčů (včetně soukromého klíče). Je-li se souborem databáze klíčů asociován soubor pro uložení hesla, získá se heslo ze souboru pro uložení hesla a tento parametr se nevyžaduje. Tento parametr je ignorován v případě, že není zadán parametr **-Z** ani **-K**.

-N *certificatename*	Specifikuje návěští asociované s certifikátem klienta v souboru databáze klíčů. Všimněte si, že jestliže je server LDAP konfigurován pouze pro provádění autentizace serveru, certifikát klienta se nevyžaduje. Je-li server LDAP konfigurován pro provádění autentizace serveru i klienta, je certifikát klienta povinný. *Certificatename* není vyžadováno, jestliže byl standardně označen předvolený pár certifikát/soukromý klíč. Podobně není *certificatename* vyžadováno, jestliže existuje jediný pár certifikát/soukromý klíč v označeném souboru databáze klíčů. Tento parametr je ignorován v případě, že není zadán parametr **-Z** ani **-K**.
dn	Specifikuje jeden nebo více argumentů *dn*. *dn* by mělo být řetězcem vyjádřené DN.

Příklad: ldapdelete

Následující příkaz se pokusí vymazat záznam, který má commonName ″Delete Me″ a nachází se přímo pod organizačním záznamem University of Life:

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

Možná budete muset zadat *binddn* a *passwd* (viz volby **-D** a **-w**).

Obslužný program ldapsearch

Obslužný program ldapsearch umožňuje vyhledat záznam na serveru adresářů LDAP z příkazového shellu QSH v systému OS/400. Používá API ldap_search.

Vyhledávání používá filtr, který odpovídá řetězcovému formátu pro filtry LDAP. Více informací o vyhledávacích filtrech LDAP najdete v informacích o ldap_search API v tématu OS/400 Directory Services pod tématem Programming v rámci aplikace iSeries Information Center.

Jestliže obslužný program ldapsearch nalezne jeden nebo více záznamů, načte atributy, které jsou zadány pomocí *attrs* a pošle záznamy a hodnoty na standardní výstup. Nezadáte-li žádné atributy, vrátí příkaz všechny atributy.

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:

Dokončí-li se program bez chyb, je návratový kód 0. V případě chyby je návratový kód nenulový a pro standardní chybový výstup se zapíše diagnostická zpráva.

Výstupní formát:

Jestliže ldapsearch nalezne jeden nebo více záznamů, zapíše každý záznam na standardní výstup ve formátu:

```
Rozlišovací
jméno (DN)
jménoatributu=hodnota
jménoatributu=hodnota
jménoatributu=hodnota
...
```

Více záznamů se odděluje jednou prázdnou řádkou. Použijete-li ke specifikaci znaku pro oddělovač volbu **-F**, zobrazí výstup tento znak namísto znaménka rovná se (=). Použijete-li volbu **-t**, bude skutečná hodnota nahrazena jménem dočasného souboru. Zadáte-li volbu **-A**, zapíše se pouze část attributename (jméno atributu).

Zde si můžete prohlédnout příklady použití obslužného programu ldapsearch.

Parametry:

-V	Specifikuje verzi LDAP, kterou obslužný program použije k připojení na server LDAP. Standardně se používá připojení LDAP V3. Chcete-li explicitně vybrat LDAP V3, zadejte -V 3. Chcete-li spustit aplikaci LDAP V2, zadejte -V 2.
-n	Zobrazuje, co bude vykonáno, ale vyhledání se ve skutečnosti neprovede. Tento parametr ve spojení s parametrem -v lze využít k ladění.
-v	Používá mnohomluvný režim s mnoha diagnostickými zprávami na standardním výstupu.
-t	Zapíše vyhledané hodnoty do sady dočasných souborů. To je výhodné při práci s binárními hodnotami, jako jsou jpegPhoto nebo audio.
-A	Načte pouze atributy (bez hodnot). To je výhodné, když chcete pouze zjistit, zda se v záznamu nachází určitý atribut, a nezajímá vás konkrétní hodnota.
-B	Nebude potlačeno zobrazování binárních hodnot. To je výhodné, když pracujete s hodnotami, které jsou v alternativních znakových sadách, například ISO-8859.1. Tato volba je odvozena od volby **-L**
-L	Zobrazí výsledky vyhledávání ve formátu LDIF. Tato volba rovněž zapíná volbu **-B** a způsobí, že se ignoruje volba **-F**.
-M	Referenční objekty jsou spravovány jako řádné záznamy.
-R	Specifikuje, že odkazy nebudou zpracovány automaticky.
-C *charset*	Specifikuje, že řetězce, které jsou dodávány jako vstup do obslužného programu ldapsearch, jsou v lokální znakové sadě (*charset*). Vstupní řetězec obsahuje filtr, připojovací DN a základní DN. Podobně při zobrazování dat program ldapsearch zkonvertuje data, která obdrží ze serveru LDAP na zadanou znakovou sadu. Volbu **-C** použijte v případě, že je kódová stránka vstupního řetězce jiná než hodnota kódové stránky úlohy. V dokumentaci k API ldap_set_iconv_local_charset() najdete podporované hodnoty *charset*. Rovněž platí, že je-li zadána volba -C i -L, předpokládá se, že vstup je v zadané znakové sadě, ale výstup z programu ldapsearch vždy zachová reprezentaci dat v UTF-8 nebo base-64, když jsou detekovány netisknutelné znaky. Důvod je ten, že standardní soubory LDIF obsahují reprezentace dat řetězců pouze v UTF-8 (nebo v kódování base-64 UTF-8).
-d *debuglevel*	Nastaví úroveň ladění na hodnotu *debuglevel*.
-F *sep*	Hodnota *sep* specifikuje oddělovač mezi jmény atributů a hodnotami. Předvolený oddělovač je `=, pokud nebyl zadán příznak **-L**; v tom případě je tato volba ignorována.
-f *file*	Čte se série řádek ze souboru a pro každou řádku se provede jedno vyhledávání LDAP. Každá řádka v tomto souboru by měla obsahovat jedno rozlišovací jméno (DN).
-D *binddn*	Hodnota *binddn* slouží k připojení k adresáři LDAP.*Binddn* by mělo být řetězcem vyjádřené DN.
-w *passwd*	Hodnota *passwd* je heslo pro autentizaci.
-m *mechanism*	Hodnota *mechanism* specifikuje mechanismus SSL, kterým se klient připojuje k serveru. Použije se API ldap_sasl_bind_s(). Dostupné mechanismy jsou CRAM-MD5 (kódování hesla), EXTERNAL (pro SSL) a GSSAPI (Kerberos). Parametr **-m** je ignorován v případě, že je nastaven parametr **-V 2**. Jestliže parametr **-m** nezadáte, použije se jednoduchá autentizace.
-O *hopcount*	Hodnota *hopcount* nastaví maximální počet přechodů, které knihovna klienta vykoná, když vyhledává odkazy. Standardní hodnota pro počet přechodů je 10.

-h *ldaphost*	Specifikuje alternativního hostitele, na kterém běží server LDAP.
-p *ldapport*	Specifikuje alternativní port TCP, na kterém server LDAP naslouchá. Předvolený port LDAP je 389. Není-li port specifikován a je specifikován parametr **-Z**, použije se předvolený port LDAP SSL 636.
-Z	Ke komunikaci se serverem LDAP se použije připojení přes SSL. Volba **-Z** je podporována pouze ve verzích, které podporují SSL.
-K *keyfile*	Specifikuje jméno souboru databáze klíčů SSL. Není-li soubor databáze klíčů v aktuálním adresáři, zadejte plně kvalifikované jméno souboru databáze klíčů. Jestliže obslužný program nemůže najít databázi klíčů, použije pevně naprogramovanou sadu předvolených důvěryhodných zdrojů vydavatele certifikátů (CA). Soubor databáze klíčů obvykle obsahuje jeden nebo více certifikátů nebo vydavatelů certifikátů ověřených klientem. Tyto typy certifikátů X.509 jsou rovněž známé jako důvěryhodné zdroje. Tento parametr účinně aktivuje přepínač **-Z**.
-P *keyfilepw*	Specifikuje heslo pro databázi klíčů. Toto heslo je požadováno pro přístup ke kódovaným informacím v souboru databáze klíčů (včetně soukromého klíče). Je-li se souborem databáze klíčů asociován soubor pro uložení hesla, získá se heslo ze souboru pro uložení hesla a tento parametr se nevyžaduje. Tento parametr je ignorován v případě, že není zadán parametr **-Z** ani **-K**.
-N *certificatename*	Specifikuje návěští asociované s certifikátem klienta v souboru databáze klíčů. Všimněte si, že jestliže je server LDAP konfigurován pouze pro provádění autentizace serveru, certifikát klienta se nevyžaduje. Je-li server LDAP konfigurován pro provádění autentizace serveru i klienta, je certifikát klienta povinný. *Certificatename* není vyžadováno, jestliže byl standardně označen předvolený pár certifikát/soukromý klíč. Podobně není *certificatename* vyžadováno, jestliže existuje jediný pár certifikát/soukromý klíč v označeném souboru databáze klíčů. Tento parametr je ignorován v případě, že není zadán parametr **-Z** ani **-K**.
-b *searchbase*	Hodnota *searchbase* slouží jako výchozí bod pro vyhledávání namísto předvolené hodnoty. Není-li volba **-b** zadána, obslužný program hledá definici *searchbase* v proměnné prostředí LDAP_BASEDN.
-s *scope*	Specifikuje rozsah vyhledávání. Hodnota *scope* by měla být base, one nebo sub. Tyto hodnoty znamenají vyhledávání v základním objektu, v jedné úrovni nebo v podstromu. Předvolba je sub.
-a *deref*	Určuje, jak se provádí rušení odkazů na aliasy. Hodnota *deref* by měla být never, always, search nebo find. Tyto hodnoty znamenají, že odkazy na aliasy se nikdy neruší, vždy ruší, ruší se při vyhledávání nebo se ruší pouze při nalezení základního objektu pro vyhledávání. Předvolba je nikdy nerušit odkazy na aliasy.
-l *timelimit*	Čeká na dokončení vyhledání maximálně tolik sekund, kolik je uvedeno v hodnotě *timelimit*.
-z *sizelimit*	Omezí výsledky vyhledávání na maximálně takový počet, jaký je uveden v hodnotě *sizelimit*. Tato volba umožňuje stanovit pro operaci vyhledávání horní hranici počtu vrácených záznamů.
filter	Specifikuje jméno filtru, který se použije při vyhledávání.
attrs...	Specifikuje atributy, které obslužný program načte při nalezení jednoho nebo více záznamů. Nezadáte-li pro *attrs* žádné hodnoty, vrátí program všechny atributy.

Příklady: ldapsearch

Příklad 1:

Příkaz ldapsearch cn=john doe cn telephoneNumber vyhledá v podstromu (s použitím předvolené základny vyhledávání) záznamy, ve kterých commonName je john doe. Při vyhledávání se načtou hodnoty commonName a hodnoty telephoneNumber a pošlou se na standardní výstup. Jsou-li nalezeny dva záznamy, bude výstup vypadat přibližně 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
```

Příklad 2:

Příkaz ldapsearch -t uid=jed jpegPhoto audio vyhledá v podstromu (s použitím předvolené základny vyhledávání) záznamy, které mají ID uživatele jed. Vyhledávání načte hodnoty jpegPhoto a audio a zapíše je do dočasných souborů. Jestliže je nalezen jeden záznam s jednou hodnotou pro každý požadovaný atribut, bude výstup vypadat přibližně 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
```

Příklad 3:

Příkaz ldapsearch -L -s one -b c=US o=university* o description provede vyhledání v jedné úrovni (one-level) na úrovni c=US. Budou vyhledány všechny organizace, jejichž organizationName začíná na university. Výsledky vyhledávání se zobrazí ve formátu LDIF. Vyhledávání načte hodnotu atributu organizationName a hodnoty atributu description a pošle je na standardní výstup, který bude vypadat přibližně takto:

```
dn: o=University of Alaska Fairbanks, c=US
o: University of Alaska Fairbanks
description: Preparing Alaska for a brave new tomorrow
description: leaf node only

dn: o=University of Colorado at Boulder, c=US
o: University of Colorado at Boulder
description: No personnel information
description: Institution of education and research

dn: o=University of Colorado at Denver, c=US
o: University of Colorado at Denver
o: UCD
o: CU/Denver
o: CU-Denver
description: Institute for Higher Learning and Research

dn: o=University of Florida, c=US
o: University of Florida
o: UFl
description: Shaper of young minds
...
```

Příklad 4:

Jak bylo uvedeno v části “Odkazy v adresáři LDAP” na stránce 37, adresáře LDAP produktu Directory Services mohou obsahovat referenční objekty, za předpokladu, že obsahují pouze tyto atributy:

- Rozlišovací jméno (dn).
- Třída objektů (objectClass).
- Odkaz (ref).

Následující příklad je ukázkou vyhledávání, kde je zahrnut referenční objekt.

Předpokládejme, že System_A obsahuje referenční záznam:

```
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
```

Všechny atributy, které jsou asociovány s tímto záznamem, by se měly nacházet v systému System_B.

System_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
```

Když klient vyšle požadavek systému System_A a neodešle ovladač manageDsaIT, server vrátí odkaz (referral). Například, když se použije -M v příkazu ldapsearch, odpoví server LDAP v systému System_A klientovi následující adresou URL:

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

Klient použije tuto informaci k vydání příkazu pro systém System_B. Jestliže záznam v systému System_A obsahuje i jiné atributy než dn, objectclass a ref, server je ignoruje.

Když klient přijme referenční odpověď ze serveru, znovu vyšle požadavek, tentokrát na server, na který se odkazuje vrácená URL. Jestliže bylo vyhledávání provedeno v rozsahu jedné úrovně, použije referenční požadavek základní rozsah. Výsledek tohoto vyhledávání se liší v závislosti na hodnotě, kterou zadáte jako rozsah vyhledávání (**-b**).

Zadáte-li -s sub, jak je uvedeno zde:

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

vyhledávání vyhledávání vrátí všechny atributy pro všechny záznamy obsahující sn=Jensen , které se nacházejí v obou systémech (System_A a System_B) na úrovni nebo pod úrovní ou=Rochester, o=Big Company, c=US.

Zadáte-li -s one, jak je uvedeno zde:

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

vyhledávání nevrátí žádné záznamy ani z jednoho systému. Namísto toho server vrátí klientu referenční URL:

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

Klient obratem předá požadavek:

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

Vrátí se záznam cn=Barb Jensen,ou=Rochester,o=Big Company,c=US.

Obslužný program ldapmodrdn

Obslužný program ldapmodrdn umožňuje změnit relativní rozlišovací jména (RDN) záznamů na serveru adresářů LDAP. Spouští se z příkazového shellu QSH v systému OS/400. Používá 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. Zadáte-li argumenty příkazové řádky *dn* a *rdn*, nahradí zadané *rdn* původní RDN záznamu, který je určen podle DN zadaného argumentem *dn*. Jinak by obsah souboru (nebo standardního vstupu, když nezadáte příznak **-f**) měl obsahovat jeden nebo více záznamů.

   ```
   Rozlišovací jméno (DN)
   Relativní rozlišovací jméno (RDN)
   ```

   Každý pár DN/RDN je oddělen jednou nebo více řádkami.
2. Jestliže nedodáte informace o záznamu ze souboru (*file*) prostřednictvím volby **-f** (nebo zadáním dvojice *dn* a *rdn* z příkazové řádky), bude příkaz ldapmodrdn čekat na přečtení záznamu ze standardního vstupu. Toto čekání můžete přerušit stisknutím klávesy SysReq a výběrem volby 2. End previous request (Ukončit předchozí příkaz).

Diagnostika:

Dokončí-li se program bez chyb, je návratový kód 0. V případě chyby je návratový kód nenulový a pro standardní chybový výstup se zapíše diagnostická zpráva.

Zde si můžete prohlédnout příklad použití obslužného programu ldapmodrdn.

Parametry:

-V	Specifikuje verzi LDAP, kterou obslužný program použije k připojení na server LDAP. Standardně se používá připojení LDAP V3. Chcete-li explicitně vybrat LDAP V3, zadejte -V 3. Chcete-li spustit aplikaci LDAP V2, zadejte -V 2.
-r	Odstraní ze záznamu všechna relativní rozlišovací jména (RDN). Předvolba je uchovávat staré hodnoty.
-M	Referenční objekty jsou spravovány jako řádné záznamy.
-n	Zobrazuje, co bude vykonáno, ale záznamy se ve skutečnosti nezmění. Tento parametr ve spojení s parametrem -v lze využít k ladění.
-v	Používá mnohomluvný režim s mnoha diagnostickými zprávami na standardním výstupu.
-c	Nepřerušený operační režim. Chyby jsou oznamovány, ale program ldapmodrdn pokračuje v modifikacích. Standardně je nastaveno ukončení programu po zaznamenání chyby.
-R	Specifikuje, že odkazy nebudou zpracovány automaticky.
-C *charset*	Specifikuje, že řetězce, které jsou dodávány jako vstup do programu, jsou v lokální znakové sadě (*charset*) a musí být konvertovány na kód UTF-8. Volbu **-C** použijte v případě, že je kódová stránka vstupního řetězce jiná než hodnota kódové stránky úlohy. V dokumentaci k API ldap_set_iconv_local_charset() najdete podporované hodnoty *charset*.

-d *debuglevel*	Nastaví úroveň ladění na hodnotu *debuglevel*.
-D *binddn*	Hodnota *binddn* slouží k připojení k adresáři LDAP. *Binddn* by mělo být řetězcem vyjádřené DN.
-w *passwd*	Hodnota *passwd* je heslo pro autentizaci.
-m *mechanism*	Hodnota *mechanism* specifikuje mechanismus SSL, kterým se klient připojuje k serveru. Použije se API ldap_sasl_bind_s(). Dostupné mechanismy jsou CRAM-MD5 (kódování hesla), EXTERNAL (pro SSL) a GSSAPI (Kerberos). Parametr **-m** je ignorován v případě, že je nastaven parametr **-V 2**. Jestliže parametr **-m** nezadáte, použije se jednoduchá autentizace.
-O *hopcount*	Hodnota *hopcount* nastaví maximální počet přechodů, které knihovna klienta vykoná, když vyhledává odkazy. Standardní hodnota pro počet přechodů je 10.
-h *ldaphost*	Specifikuje alternativního hostitele, na kterém běží server LDAP.
-p *ldapport*	Specifikuje alternativní port TCP, na kterém server LDAP naslouchá. Předvolený port LDAP je 389. Není-li port specifikován a je specifikován parametr **-Z**, použije se předvolený port LDAP SSL 636.
-Z	Ke komunikaci se serverem LDAP se použije připojení přes SSL. Volba **-Z** je podporována pouze ve verzích, které podporují SSL.
-K *keyfile*	Specifikuje jméno souboru databáze klíčů SSL. Není-li soubor databáze klíčů v aktuálním adresáři, zadejte plně kvalifikované jméno souboru databáze klíčů. Jestliže obslužný program nemůže najít databázi klíčů, použije pevně naprogramovanou sadu předvolených důvěryhodných zdrojů vydavatele certifikátů (CA). Soubor databáze klíčů obvykle obsahuje jeden nebo více certifikátů nebo vydavatelů certifikátů ověřených klientem. Tyto typy certifikátů X.509 jsou rovněž známé jako důvěryhodné zdroje. Tento parametr účinně aktivuje přepínač **-Z**.
-P *keyfilepw*	Specifikuje heslo pro databázi klíčů. Toto heslo je požadováno pro přístup ke kódovaným informacím v souboru databáze klíčů (včetně soukromého klíče). Je-li se souborem databáze klíčů asociován soubor pro uložení hesla, získá se heslo ze souboru pro uložení hesla a tento parametr se nevyžaduje. Tento parametr je ignorován v případě, že není zadán parametr **-Z** ani **-K**.
-N *certificatename*	Specifikuje návěští asociované s certifikátem klienta v souboru databáze klíčů. Všimněte si, že jestliže je server LDAP konfigurován pouze pro provádění autentizace serveru, certifikát klienta se nevyžaduje. Je-li server LDAP konfigurován pro provádění autentizace serveru i klienta, je certifikát klienta povinný. *Certificatename* není vyžadováno, jestliže byl standardně označen předvolený pár certifikát/soukromý klíč. Podobně není *certificatename* vyžadováno, jestliže existuje jediný pár certifikát/soukromý klíč v označeném souboru databáze klíčů. Tento parametr je ignorován v případě, že není zadán parametr **-Z** ani **-K**.
-f *file*	Čte informace o změně záznamu ze souboru LDIF namísto standardního vstupu nebo z příkazové řádky (zadáním *dn* a nového *rdn*). Standardní vstup může být dodáván i ze souboru (< file).
dn rdn	Určuje rozlišovací jméno záznamu, který se má přejmenovat, a nové relativní rozlišovací jméno tohoto záznamu.

Příklad: ldapmodrdn

Předpokládejme, že již máte vytvořen textový soubor /**tmp**/**entrymods**, který obsahuje tento zápis:

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

Příkaz:

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

změní RDN záznamu Modify Me z Modify Me na The New Me. Staré cn Modify Me se vymaže.

Poznámky k používání SSL s obslužnými programy příkazové řádky LDAP

K tomu, abyste mohli používat SSL u obslužných programů příkazové řádky, je třeba mít v systému nainstalován jeden z produktů Cryptographic Access Provider (5722-ACx).

Část “Jak používat zabezpečení SSL a TLS u serveru adresářů LDAP” na stránce 39 popisuje použití SSL na serveru Directory Services LDAP. Tyto informace zahrnují správu a vytváření důvěryhodných vydavatelů certifikátů (CA) pomocí produktu DCM (Digital Certificate Manager).

Některé servery LDAP, ke kterým má klient přístup, používají pouze autentizaci serveru. U těchto serverů je třeba pouze definovat jeden nebo více certifikátů z důvěryhodných zdrojů v paměti certifikátů. Při autentizaci serveru může být klient ujištěn, že cílový server LDAP obdržel certifikát od jednoho z důvěryhodných vydavatelů certifikátů (CA). Kromě toho všechny transakce LDAP, které procházejí přes připojení SSL k tomuto serveru, jsou šifrovány. Patří sem i pověřovací listiny, které jsou obsaženy v rozhraních API, která slouží k připojení k serveru adresářů. Pokud například server LDAP používá certifikát Verisign s vysokou důvěrností, měli byste učinit tyto kroky:

1. Získat certifikát CA od Verisign.
2. Pomocí produktu DCM jej importovat do paměti certifikátů.
3. Pomocí produktu DCM jej označit jako důvěryhodný.

Používá-li server LDAP privátně vydaný certifikát serveru, může vám administrátor serveru poskytnout kopii souboru požadavků na certifikát. Tento soubor požadavků na certifikát importujte do paměti certifikátů a označte jej jako důvěryhodný.

Používáte-li obslužné programy shellu pro přístup na servery LDAP, které používají autentizaci serveru i klienta, měli byste učinit tyto kroky:

- Definovat jeden nebo více certifikátů z důvěryhodných zdrojů v paměti certifikátů systému. Při autentizaci serveru může být klient ujištěn, že cílový LDAP obdržel certifikát od jednoho z důvěryhodných vydavatelů certifikátů (CA). Kromě toho všechny transakce LDAP, které procházejí přes připojení SSL k tomuto serveru, jsou šifrovány. Patří sem i pověřovací listiny, které jsou obsaženy v rozhraních API, která slouží k připojení k serveru adresářů.
- Vytvořit dvojici klíčů a požádat o certifikát pro klienta od CA. Po obdržení podepsaného certifikátu od CA uložte tento certifikát do souboru klíčového řetězce na klientovi.

Kapitola 7. Odstraňování problémů s produktem Directory Services

Bohužel i tak spolehlivé servery, jako jsou servery LDAP Directory Services, mají někdy problémy. Pokud narazíte na problém se serverem adresářů LDAP, mohou vám následující informace pomoci při zjišťování a nápravě chyb.

- “Základní postup při odstraňování problémů s produktem Directory Services”.
- “Obecné chyby klienta LDAP” na stránce 63.

Další informace o obecných problémech produktu Directory Services najdete na domovské stránce Directory Services na adrese:

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

.

Základní postup při odstraňování problémů s produktem Directory Services

Návratové kódy chyb LDAP jsou zapsány v souboru ldap.h, který je v systému uložen v adresáři QSYSINC/H.LDAP.

Když se vyskytne chyba na serveru adresářů LDAP a chcete se dozvědět více podrobností, můžete si také prohlédnout protokol úlohy QDIRSRV. V případě opakujících se chyb můžete ke sledování chyb použít příkaz TRCTCPAPP APP(*DIRSRV) (Trasování aplikace TCP/IP). Více informací najdete v části “Použití příkazu TRCTCPAPP k vyhledání problémů” na stránce 62.

Produkt Directory Services používá několik serverů SQL. Vyskytne-li se chyba SQL, objeví se v protokolu úlohy QDIRSRV obvykle tato zpráva:

```
SQL error -1 occurred
```

V těchto případech vás protokol úlohy QDIRSRV bude odkazovat na protokoly úloh serverů SQL. V některých případech však QDIRSRV nemusí obsahovat tuto zprávu a odkaz, zvláště když příčinou problému je právě server SQL. V těchto případech je dobré vědět, které servery SQL by se měly spouštět a k čemu je produkt Directory Services používá.

Když je server adresářů LDAP normálně spuštěn, generuje zprávy podobné těmto:

Poznámka: Zprávy a počet spuštěných úloh serverů SQL se mohou lišit, když:

- Spouštíte server poprvé.
- Je zapotřebí migrace.
- Server používá protokol změn.
- Server je nastaven tak, že povoluje větší počet připojení k databázi.

```
                                                      System:   WARMERS
 Job . . :   QDIRSRV       User . . :   QDIRSRV       Number . . . :   174440

  >> CALL PGM(QSYS/QGLDSVR)
     Job 057448/QUSER/QSQSRVR used for SQL server mode processing.
     Job 057340/QUSER/QSQSRVR used for SQL server mode processing.
     Job 057448/QUSER/QSQSRVR used for SQL server mode processing.
     Job 057166/QUSER/QSQSRVR used for SQL server mode processing.
     Job 057279/QUSER/QSQSRVR used for SQL server mode processing.
  Job 057288/QUSER/QSQSRVR used for SQL server mode processing.
     Directory Services server started successfully.
```

Produkt Directory Services používá při spuštění serveru LDAP první server SQL 057448/QUSER/QSQSRVR. Produkt Directory Services může při spuštění serveru LDAP spustit i další servery SQL tak, jak je třeba v případě, že spouštíte server LDAP poprvé nebo že je zapotřebí provést migraci nebo že váš server používá protokol změn. Po spuštění se tyto servery SQL opustí.

V tomto příkladu nebyly k migraci nebo spuštění serveru použity žádné další servery SQL a nebyl nakonfigurován protokol změn. Produkt Directory Services používá další server SQL (057340/QUSER/QSQSRVR) pouze k replikaci.

Poslední připojení v tomto příkladu (057288/QUSER/QSQSRVR) se používá pro operaci přidání, změny, mazání a operaci modrdn. Ostatní připojení se používají pro vyhledávání, svázání a porovnávání.

Celkový počet serverů SQL, který server Directory Services po spuštění používá pro adresářové operace, se zadává na serveru LDAP v prostředí produktu iSeries Navigator na stránce vlastností v poli **Databáze/Přípony**. Navíc je jeden server SQL vždy nakonfigurován pro replikaci.

Sledování chyb a přístupů v produktu Directory Services pomocí protokolu úloh

Protokol úloh serveru LDAP vás může upozornit na chyby a pomoci vám sledovat přístupy k serveru.

Je-li server spuštěn, můžete si prohlédnout protokol úloh QDIRSRV pomocí tohoto postupu:
1. V prostředí produktu iSeries Navigator rozbalte položku **Síť**.
2. Rozbalte položku **Servery**.
3. Klepněte na **TCP/IP**.
4. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Úlohy serveru**.
5. Z menu **Soubor** vyberte volbu **Protokol úlohy**.

Je-li server zastaven, můžete si prohlédnout protokol úloh QDIRSRV pomocí tohoto postupu:
1. V prostředí produktu iSeries Navigator rozbalte položku **Základní operace**.
2. Klepněte na volbu **Tiskový výstup**.
3. QDIRSRV se objeví ve sloupci **Uživatel** v pravém panelu produktu iSeries Navigator. Protokol úlohy zobrazíte dvojím klepnutím na položku **Qpjoblog** vlevo od QDIRSRV na téže řádce.

   Poznámka: iSeries Navigator může být konfigurován tak, aby ukazoval pouze soubory pro souběžný tisk. Jestliže se v seznamu QDIRSRV neobjeví, klepněte na volbu **Tiskový výstup** a z menu **Volby** vyberte volbu **Zahrnout**. Do pole **Uživatel** zadejte **Vše** a klepněte na **OK**.

Poznámka: Produkt Directory Services používá k provádění některých úloh další systémové prostředky. Vyskytne-li se chyba u některého z těchto prostředků, můžete z protokolu úlohy zjistit, kde hledat informace. Někdy nemusí být produkt Directory Services schopen určit, kde tyto informace hledat. V takových případech se podívejte do protokolu úlohy serveru SQL, abyste zjistili, zda se problém netýká serverů SQL.

Použití příkazu TRCTCPAPP k vyhledání problémů

Váš server umožňuje sledování komunikace sloužící ke shromažďování dat na komunikační lince, jako je rozhraní LAN nebo WAN. Průměrný uživatel nemusí rozumět celému obsahu trasovacích dat. Záznamy sledování však můžete použít, abyste určili, zda skutečně došlo k výměně dat mezi dvěma body.

Na serveru adresářů LDAP je možné použít příkaz TRCTCPAPP (Trasování aplikace TCP/IP) s volbou *DIRSRV při vyhledávání problémů s klienty nebo aplikacemi.

Podrobnější informace o použití příkazu TRCTCPAPP na serveru LDAP a také o omezeních týkajících se požadovaných oprávnění najdete pod tématem Popis příkazu TRCTCPAPP (Trasování aplikace TCP/IP).

Všeobecné informace o použití sledování komunikace uvádí téma Sledování komunikace.

Použití volby LDAP_OPT_DEBUG při sledování chyb

| Počínaje verzí V5R2 můžete použít volbu LDAP_OPT_DEBUG rozhraní API **ldap_set_option()** ke
| sledování problémů s klienty, kteří používají API LDAP. Volba ladění má několik nastavení úrovní ladění,
| které můžete použít při odstraňování problémů v těchto aplikacích.

| Toto je příklad aktivace volby ladění sledování klienta.

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

| Alternativním způsobem nastavení úrovně ladění je konfigurovat numerickou hodnotu proměnné prostředí
| LDAP_DEBUG pro úlohu, ve které běží klientská aplikace, na stejnou numerickou hodnotu, jakou by měl
| parametr debugvalue v případě použití API **ldap_set_option()** .

| Zde je příklad aktivace sledování klienta pomocí proměnné prostředí LDAP_DEBUG:

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

| Po spuštění klienta, který způsobuje problém, napište do náznaku serveru iSeries:

```
| DMPUSRTRC
| ClientJobNumber
```

| kde ClientJobNumber je počet klientských úloh.

| Chcete-li interaktivně zobrazit tyto informace, napište do náznaku iSeries:

```
| DSPPFM QAPOZDMP QPOZnnnnnn
```

| kde nnnnnn je číslo úlohy.

| Chcete-li uložit tyto informace za účelem jejich odeslání servisnímu středisku, postupujte takto:
| 1. Pomocí příkazu CRTSAVF vytvořte soubor SAVF.
| 2. Na příkazový řádek serveru iSeries napište:

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

| kde *xxx* je jméno, které jste zadali pro soubor SAVF.

Obecné chyby klienta LDAP

Znalost příčin obecných chyb u klienta LDAP vám může pomoci i při řešení problémů se serverem. Kompletní seznam chybových stavů u klienta LDAP najdete v tématu OS/400 Directory Services pod tématem Programming v rámci aplikace iSeries Information Center.

Chybové zprávy klienta mají tento formát:

```
[Selhávající operace LDAP]:[chybový stav API klienta LDAP]
```

Poznámka: Při objasnění těchto chyb předpokládáme, že klient komunikuje se serverem LDAP v operačním systému OS/400. Klient, který komunikuje se serverem na jiné platformě, může obdržet podobné chyby, ale jejich příčiny a řešení se budou pravděpodobně lišit.

Obecné chybové zprávy jsou:

- “ldap_search: Timelimit exceeded”
- “[Selhávající operace LDAP]: Operations error”
- “ldap_bind: No such object”
- “ldap_bind: Inappropriate authentication”
- “[Selhávající operace LDAP]: Insufficient access”
- “[Selhávající operace LDAP]: Cannot contact LDAP server”
- “[Selhávající operace LDAP]: Failed to connect to ssl server” na stránce 65

ldap_search: Timelimit exceeded

K této chybě dochází, když vyhledávání v LDAP probíhají příliš pomalu. K nápravě této chyby můžete učinit jeden z těchto kroků:

- Zvýšit časový limit pro vyhledávání na serveru adresářů LDAP. Informace o tom, jak to provést, najdete v části “Jak upravit výkon serveru adresářů LDAP” na stránce 32.
- Snížit aktivitu ve vašem systému. Můžete též snížit počet aktivních úloh klientů LDAP.

[Selhávající operace LDAP]: Operations error

Tato chyba může mít více příčin. Chcete-li získat informace o této chybě pro konkrétní případ, podívejte se do souboru QDIRSRV a do protokolů úloh serverů SQL, jak je popsáno v části “Základní postup při odstraňování problémů s produktem Directory Services” na stránce 61.

ldap_bind: No such object

Obecnou příčinou této chyby je, že uživatel v průběhu operace udělá chybu při psaní. Další obecná příčina je, že se klient LDAP pokusí připojit s DN, které neexistuje. To se často stává, když uživatel zadá něco, o čem se nesprávně domnívá, že je DN administrátora. Uživatel například zadá QSECOFR nebo Administrator, zatímco skutečné DN administrátora je cn=Administrator.

Podrobné informace o této chybě najdete v protokolu úlohy QDIRSRV, jak je popsáno v části “Základní postup při odstraňování problémů s produktem Directory Services” na stránce 61.

ldap_bind: Inappropriate authentication

Server vrátí neplatné průkazy (credentials) v případě, že je heslo nebo připojené DN nesprávné. Server vrátí nepatřičnou autentizaci v případě, že se klient pokusí připojit:

- Položku, která nemá atribut ″userpassword″.
- Položku, která reprezentuje uživatele operačního systému OS/400, jenž má atribut UID a nemá atribut ″userpassword″. Tím dojde k porovnání zadaného hesla a uživatelského hesla operačního systému OS/400, která se neshodují.
- Položku, která reprezentuje projektovaného uživatele a metodu připojení jinou, než bylo požadováno.

K této chybě obvykle dochází, když se klient pokusí připojit pod heslem, které není platné. Podrobné informace o této chybě najdete v protokolu úlohy QDIRSRV, jak je popsáno v části “Základní postup při odstraňování problémů s produktem Directory Services” na stránce 61.

[Selhávající operace LDAP]: Insufficient access

K této chybě obvykle dochází, když připojované DN nemá oprávnění k operaci (např. přidání nebo výmaz), kterou klient požaduje. Informace o této chybě najdete v protokolu úlohy QDIRSRV, jak je popsáno v části “Základní postup při odstraňování problémů s produktem Directory Services” na stránce 61.

[Selhávající operace LDAP]: Cannot contact LDAP server

Nejběžnější příčiny této chyby jsou:

- Klient LDAP vydá požadavek předtím, než je server LDAP v daném systému připraven a je ve stavu čekání na výběr.
- Uživatel zadal neplatné číslo portu. Server například naslouchá na portu 386, ale požadavek klienta se pokouší použít port 387.

Informace o této chybě najdete v protokolu úlohy QDIRSRV, jak je popsáno v části “Základní postup při odstraňování problémů s produktem Directory Services” na stránce 61. Pokud byl server Directory Services úspěšně spuštěn, objeví se o tom v protokolu úlohy QDIRSRV zpráva.

[Selhávající operace LDAP]: Failed to connect to ssl server

K této chybě dochází, když server LDAP odmítne připojení klienta, protože nebylo vytvořeno připojení přes SSL. To může být způsobeno těmito okolnostmi:

- Podpora správy certifikátů (Certificate Management) odmítne pokus klienta o připojení k serveru. Pomocí produktu Digital Certificate Manager se přesvědčte, že máte správně nastavené certifikáty, a potom restartujte server a znovu se zkuste připojit.
- Uživatel nemá přístup za účelem čtení k paměti certifikátů *SYSTEM (standardně /QIBM/userdata/ICSS/Cert/Server/default.kdb).

Pro aplikace operačního systému OS/400 napsané v jazyce C jsou k dispozici další informace o chybách SSL. Podrobnější údaje najdete v jednotlivých API produktu Directory Services.

Vytištěno v Dánsku společností IBM Danmark A/S.