



Systemy IBM - iSeries

IBM Directory Server (LDAP)

Verze 5, vydání 4





Systemy IBM - iSeries

IBM Directory Server (LDAP)

Verze 5, vydání 4

Poznámka

Před použitím těchto informací a produktu, ke kterému se vztahují, si nezapomeňte přečíst informace uvedené v části “Poznámky”, na stránce 275 a v publikaci *IBM eServer Safety Information*.

Osmé vydání (únor 2006)

Toto vydání se vztahuje na verzi 5, vydání 4, modifikaci 0 operačního systému IBM i5/OS (číslo produktu 5722-SS1) a na veškerá následná vydání a modifikace, dokud nebude v nových vydáních uvedeno jinak. Tato verze nefunguje na všech modelech počítačů RISC (reduced instruction set computer) ani na modelech CISC.

© Copyright International Business Machines Corporation 1998, 2006. Všechna práva vyhrazena.

Obsah

Kapitola 1. IBM Directory Server for iSeries (LDAP)	1
Kapitola 2. Co je nového ve verzi V5R4	3
Kapitola 3. Tisk PDF	5
Kapitola 4. Koncepce serveru adresářů	7
Adresáře	7
Rozlišovací jména (DN)	11
Přípona (kontext pojmenování)	14
Schéma	15
Schéma serveru adresářů IBM	16
Podpora obecného schématu	17
Třídy objektů	18
Atributy	19
Identifikátor objektu (OID)	26
Záznamy podschématu	27
Třída objektu IBMsubschema	27
Dotazy na schéma	27
Dynamické schéma	27
Zakázané změny schématu	28
Kontrola schématu	31
Kompatibilita s iPlanet	33
Zobecněný čas a UTC čas	33
Publikování	34
Replikace	36
Přehled replikací	36
Terminologie replikace	39
Ujednání o replikacích	40
Způsob uložení informací replikace na serveru	41
Hlediska zabezpečení ochrany dat pro informace replikace	41
Replikace v prostředí s vysokou dostupností	41
Sféry a uživatelské šablony	41
Parametry prohledávání	42
Pravidla pro podporu národního jazyka (NLS)	44
Jazykové příznaky	44
Odkazy v adresáři LDAP	45
Transakce	46
Server adresářů - Zabezpečení ochrany dat	46
Monitorování	46
SSL (Secure Sockets Layer) a TLS (Transport Layer Security) u serveru adresářů	47
Autentizace Kerberos na serveru adresářů	47
Skupiny a role	48
Administrace	54
Proxy autorizace	55
Seznamy přístupových práv	55
Vlastnictví objektů adresáře LDAP	67
Zásada pro správu hesel	67
Autentizace	70
Odmítnutí služeb	73
Procedura Backend projektovaná operačním systémem	74
Stromová struktura adresáře projektovaná uživatelem	74
Operace LDAP	75
Připojovací DN administrátora a repliky	79
Schéma projektované uživatelem	79
Server adresářů a podpora žurnálování i5/OS	80
Jedinečné atributy	80
Operační atributy	80
Serverové paměti cache	81
Paměť cache atributů	81
Paměť cache filtrů	82
Paměť cache záznamů	82
Paměť cache seznamů ACL	82
Ovladače a přídavné operace	83
Kapitola 5. Začínáme s produktem Server adresářů	85
Pokyny pro migraci	85
Provedení migrace z V5R3 nebo V5R2 na verzi V5R4	85
Provedení migrace dat z verzí V4R4, V4R5 nebo V5R1 na verzi V5R4	86
Provedení migrace sítě replikačních serverů	87
Změna jména služby Kerberos	89
Plánování serveru adresářů	89
Konfigurace serveru adresářů	90
Předvolená konfigurace produktu Server adresářů	91
Naplnění adresáře	92
Publikování informací na serveru adresářů	92
Import a export souboru LDIF	93
Kopírování uživatelů z ověřovacího seznamu HTTP serveru do serveru adresářů	94
Doporučené postupy pro strukturu adresáře	96
Webová administrace	97
První nastavení webové administrace	98
Webový nástroj administrace	99
Kapitola 6. Scénář: Nastavení serveru adresářů	101
Podrobnosti scénáře: Nastavení serveru adresářů	102
Podrobnosti scénáře: Vytvoření adresářové databáze	103
Podrobnosti scénáře: Publikace dat iSeries do adresářové databáze	105
Podrobnosti scénáře: Zadávání informací do adresářové databáze	106
Podrobnosti scénáře: Testování adresářové databáze	107
Kapitola 7. Jak provádět správu serveru adresářů	109
Jak spustit/zastavit server adresářů	110
Jak kontrolovat stav serveru adresářů	111
Jak kontrolovat úlohy na serveru adresářů	111
Jak spravovat připojení serveru	111
Jak spravovat vlastnosti připojení	112
Jak aktivovat oznámení o události	114
Jak specifikovat nastavení transakcí	115
Jak změnit port nebo IP adresu	115

Jak specifikovat server pro adresářové odkazy	116	Jak kopírovat schéma na jiné servery	164
Jak přidávat a odstraňovat přípony serveru adresářů	116	Jak provádět správu záznamů adresáře	165
Jak uložit a obnovit informace o produktu Server adresářů	117	Jak procházet strom	165
Jak poskytnout administrátorský přístup projektovaným uživatelům	117	Jak přidat záznam	165
Jak pracovat s administrační skupinou	118	Jak přidat záznam obsahující atribut s jazykovým příznakem	166
Jak povolit administrační skupinu	118	Jak vymazat záznam	167
Jak přidávat, upravovat a odstraňovat členy administrační skupiny	119	Jak editovat záznam	167
Jak spravovat skupiny s limity hledání	119	Jak kopírovat záznam	167
Jak vytvořit skupinu s limity hledání	120	Jak editovat seznamy přístupových práv	168
Jak měnit skupinu s limity hledání	120	Jak přidat pomocnou třídu objektu	168
Jak kopírovat skupinu s limity hledání	121	Jak vymazat pomocnou třídu	168
Jak odstranit skupinu s limity hledání	121	Jak změnit skupinové členství	169
Jak spravovat skupiny s proxy autorizací	121	Jak prohledávat záznamy adresáře	169
Jak vytvořit skupinu s proxy autorizací	121	Jak změnit binární atributy	171
Jak měnit skupinu s proxy autorizací	122	Jak provádět správu uživatelů a skupin	172
Jak kopírovat skupinu s proxy autorizací	122	Jak provádět správu uživatelů	172
Jak odstranit skupinu s proxy autorizací	122	Jak provádět správu skupin	173
Jak spravovat jedinečné atributy	122	Jak provádět správu sfér a uživatelských šablon	174
Jak vytvořit seznam jedinečných atributů	122	Jak vytvořit sféru	175
Jak odstranit záznam ze seznamu jedinečných atributů	123	Jak vytvořit administrátora sféry	175
Jak sledovat přístup a změny u adresáře LDAP	123	Jak vytvořit šablonu	176
Jak aktivovat monitorování objektů pro server adresářů	124	Jak přidat šablonu do sféry	177
Jak přizpůsobit nastavení vyhledávání	124	Jak vytvářet skupiny	178
Jak přizpůsobit nastavení výkonu	125	Jak přidat uživatele do sféry	178
Jak nastavit databázová připojení a nastavení paměti cache	126	Jak provádět správu sfér	178
Jak konfigurovat paměť cache atributu	126	Jak provádět správu šablon	179
Jak konfigurovat nastavení transakcí	128	Jak provádět správu seznamů přístupových práv (ACL)	181
Jak provádět správu replikací	129	Efektivní seznamy ACL	182
Jak vytvořit topologii hlavní server-replika	129	Efektivní vlastníci	182
Jak vytvořit topologii hlavní server-předávací server-replika	134	Nefiltrované seznamy ACL	182
Přehled tvorby úplné replikační topologie	136	Filtrované seznamy ACL	184
Jak vytvořit úplnou topologii s peerovou replikací	136	Vlastníci	185
Jak nastavit topologii brány	139	Kapitola 8. Odkazy 187	
Jak provádět správu topologií	140	Obslužné programy pro příkazový řádek	187
Jak měnit vlastnosti replikace	143	ldapmodify a ldapadd	187
Jak vytvářet časové plány replikací	144	ldapdelete	191
Jak provádět správu front	146	ldapexop	194
Jak nastavit replikaci přes zabezpečené spojení	146	ldapmodrdn	199
Jak spravovat vlastnosti zabezpečení	147	ldapsearch	202
Jak spravovat hesla	147	ldapchangepwd	211
Jak aktivovat SSL a TLS (Transport Layer Security) na serveru adresářů	151	ldapdiff	213
Jak aktivovat autentizaci Kerberos na serveru adresářů	153	Jak používat SSL s obslužnými programy příkazového řádku LDAP	216
Jak aktivovat autentizaci DIGEST-MD5 na serveru adresářů	154	LDAP data interchange format (LDIF)	216
Jak provádět správu schématu	154	Příklad: LDIF	217
Jak prohlížet třídy objektů	155	Podpora LDIF verze 1	217
Jak přidat třídu objektu	155	Příklad: LDIF verze 1	218
Jak editovat třídu objektu	156	Schéma konfigurace serveru adresářů	219
Jak kopírovat třídu objektu	157	Informační strom adresáře (DIT - Directory information tree)	219
Jak vymazat třídu objektu	158	Atributy	228
Jak prohlížet atributy	159	Identifikátory objektů (OID)	259
Jak přidat atribut	160	Kapitola 9. Odstraňování problémů s produktem Server adresářů 265	
Jak editovat atribut	161	Sledování chyb a přístupů v produktu Server adresářů pomocí protokolu úloh	266
Jak kopírovat atribut	162	Použití příkazu TRCTCPAPP k vyhledání problémů	266
Jak vymazat atribut	163		

Použití volby LDAP_OPT_DEBUG při sledování chyb	267		Chyby související se zásadou pro správu hesel	272
Identifikátory zpráv GLEnnnn	267		Odstraňování problémů s rozhraním API QGLDCPYVL	272
Běžné chyby klienta LDAP	270			
ldap_search: Timelimit exceeded	270			
[Selhávající operace LDAP]: Operations error	271			
ldap_bind: No such object	271			
ldap_bind: Inappropriate authentication	271			
[Selhávající operace LDAP]: Insufficient access	271			
[Selhávající operace LDAP]: Cannot contact LDAP server	271			
[Selhávající operace LDAP]: Failed to connect to SSL server	271			

Kapitola 10. Související informace . . . 273

Dodatek. Poznámky. 275

Ochranné známky 276

| Ustanovení a podmínky 277

Kapitola 1. IBM Directory Server for iSeries (LDAP)

Server adresářů IBM Directory Server for iSeries (dále označovaný jako Server adresářů) poskytuje funkce serveru LDAP (Lightweight Directory Access Protocol) na serveru iSeries. LDAP využívá protokol TCP/IP (Transmission Control Protocol/Internet Protocol) a je stále častěji používán jako adresářová služba pro internetové i neinternetové aplikace.

V následujících tématech najdete informace, které vám pomohou s pochopením produktu Directory Server a jeho použitím na serveru iSeries:

Kapitola 2, “Co je nového ve verzi V5R4”, na stránce 3

Informace o změnách a vylepšeních provedených na serveru adresářů od posledního vydání.

Kapitola 3, “Tisk PDF”, na stránce 5

PDF verze tohoto informačního hesla.

Kapitola 4, “Koncepce serveru adresářů”, na stránce 7

Informace o koncepcích serveru adresářů.

Kapitola 5, “Začínáme s produktem Server adresářů”, na stránce 85

Informace týkající se konfigurování serveru adresářů.

Kapitola 6, “Scénář: Nastavení serveru adresářů”, na stránce 101

Příklad nastavení adresáře LDAP na serveru adresářů.

Kapitola 7, “Jak provádět správu serveru adresářů”, na stránce 109

Informace o práci se serverem adresářů.

Kapitola 8, “Odkazy”, na stránce 187

Referenční materiál související se serverem adresářů, jako např. obslužné programy pro příkazový řádek a informace o LDIF.

Kapitola 9, “Odstraňování problémů s produktem Server adresářů”, na stránce 265

Informace pomáhající při řešení problémů. Obsahuje návrhy pro činnost shromažďování servisních údajů a řešení specifických problémů.

Kapitola 10, “Související informace”, na stránce 273

Další informace související se serverem adresářů.

Kapitola 2. Co je nového ve verzi V5R4

Produkt Directory Server for iSeries má ve verzi V5R4 tato vylepšení a nové funkce:

Replikace

- **Replikace přes brány:** Replikaci lze v rámci replikovaných sítí provádět za použití serverů bran. Servery bran mohou efektivněji shromažďovat a distribuovat informace, a zároveň se tak redukuje objem síťového provozu. Další informace najdete v části "Replikace přes brány" v tématu "Přehled replikací" na stránce 36.
- **cn=IBMpolicies:** Nový objekt zásobníku pro záznamy, které se mají sdílet mezi replikačními servery. Na rozdíl od cn=localhost, zásobníku pro záznamy, které se nereplikují, obsahuje cn=IBMpolicies informace konfiguračního typu, které je někdy potřeba replikovat. Další informace najdete v tématu "Přípona (kontext pojmenování)" na stránce 14.

Zabezpečení

- **Autentizace DIGEST-MD5:** DIGEST-MD5 je autentizační mechanismus využívající protokol SASL (simple authentication security layer). Když klient použije volbu Digest-MD5, heslo se nepřenáší jako čistý text a protokol zabrání útokům na bázi přehrávání. Další informace najdete v tématu "Autentizace" na stránce 70.
- **Transport layer security (TLS):** Byla přidána rozšířená operace StartTLS, která klientu umožňuje, aby převedl nezabezpečené připojení na připojení zabezpečené pomocí TLS. Kromě toho server podporuje 256bitovou šifrovací sadu AES TLS. Další informace najdete v tématu "SSL (Secure Sockets Layer) a TLS (Transport Layer Security) u serveru adresářů" na stránce 47.

Vyhledávání

- **Prohledávání podstromu na nulové bázi:** Všechny přípony definované v konfiguračním souboru lze prohledávat pomocí pouze jednoho vyhledávacího požadavku. Tím se eliminuje potřeba vícenásobného hledání (vždy pro jednotlivé přípony jako výchozí bod hledání) při prohledávání celého adresáře. Další informace najdete v tématu "Jak prohledávat záznamy adresáře" na stránce 169.
- **Skupiny s limity hledání:** Tato funkce umožňuje, aby administrátor přiřadil specifickým skupinám odlišné limity vyhledávání navíc k obecným limitům uplatněným vůči všem uživatelům. Administrátoři tak mají vyšší flexibilitu při určování, kdo bude mít jaká vyhledávací omezení na konkrétním serveru. Další informace najdete v tématu "Parametry prohledávání" na stránce 42.
- **Vylepšení zpracování dereference aliasů:** Výkon vyhledávání, které používá volby dereference, se výrazně zlepšil, když adresář neobsahuje žádné aliasy. Kromě toho nyní existují konfigurační volby, které přepišou volby dereference specifikované ve vyhledávacím požadavku klienta. Další informace najdete v tématu "Parametry prohledávání" na stránce 42.
- **Paměť cache atributů:** Funkce paměti cache atributů představuje zdokonalení výkonu, neboť řešení vyhledávacího filtru probíhá v paměti namísto toho, že by počáteční řešení bylo provedeno v databázi a uloženo se do paměti cache filtru. Paměť cache atributu se na rozdíl od paměti cache filtru nevymaže pokaždé, když se provede operace LDAP pro přidání, modifikaci nebo vymazání. Když je server takto nakonfigurován, provádí automaticky v nakonfigurovaných intervalech úpravy paměti cache atributu a ukládá do paměti cache ty atributy, které by byly nejužitečnější, v rámci maximálního objemu paměti konfigurovaného pro paměti cache atributů. Další informace najdete v tématu "Paměť cache atributů" na stránce 81.

Atributy

- **Jedinečné atributy:** Funkce jedinečných atributů zajišťuje, aby specifikované atributy měly v rámci adresáře vždy jedinečnou hodnotu. Například administrátor může chtít specifikovat, že atribut, který obsahuje číslo sociálního zabezpečení, musí být jedinečný, protože není možné, aby dva lidé měli stejné číslo. Další informace najdete v tématu "Jedinečné atributy" na stránce 80.
- **Zachování operačních atributů:** Operační atributy creatorsName, createTimestamp, modifiersName a modifyTimestamp se nyní replikují na odběratelské servery a jsou importovány a exportovány do souborů LDIF. Další informace najdete v tématu "Operační atributy" na stránce 80.

- **Jazykové příznaky:** Jazykové příznaky jsou mechanismy, které umožňují adresáři asociovat kódy přirozeného jazyka s hodnotami uloženými v adresáři a které umožňují klientům dotazovat se v adresáři na hodnoty, které odpovídají požadavkům určitého přirozeného jazyka. Další informace najdete v tématu “Jazykové příznaky” na stránce 44.

Skupiny

- **Skupina administračních uživatelů:** Více uživatelských DN nyní může mít téměř stejný rozsah administračního přístupu jako administrátor LDAP serveru. Tato funkce umožňuje, aby administrační úlohy provádělo několik uživatelů, aniž by museli sdílet jeden ID uživatele a heslo. Další informace najdete v tématu “Administrační přístup” na stránce 54.
- **Proxy autorizace:** Proxy autorizace poskytuje způsob, jak se může LDAP klient připojit jako jeden uživatel ale přistupovat k cílovému adresáři jako jiný uživatel. To poskytuje klientským aplikacím více flexibility, protože mohou provádět operace jménem více uživatelů, aniž by se musely za každého uživatele opětovně připojovat. Další informace najdete v tématu “Proxy autorizace” na stránce 55.

Další

- **Zdokonalení monitoru:** Pomocí webového administračního nástroje lze nyní zobrazit informace o serveru a připojení. U podpory monitoru byla provedena tato vylepšení:
 - Obslužnost a odmítnutí služeb
 - Do výstupu monitoru byly přidány nové informace, které zahrnují počty provedených operací podle typu (BIND, MODIFY, COMPARE, SEARCH atd.), délku pracovní fronty, počet dostupných pracovních vláken, počet zpráv přidaných do protokolu serveru, protokol monitorování, chyby rozhraní příkazového řádku (CLI), počet připojení SSL i TSL, informace o nečinných připojeních a statistiku nouzového vlákna.
 - Je dodán nový výchozí bod hledání “cn=workers,cn=monitor”, který vrací informace o pracovních vláknech.
 - Paměť cache atributu
 - Informace o paměti cache a attributech v paměti cache (konfigurovaná velikost, celková velikost, poměrná četnost odkazů) se zaznamenává.
 - Pro návrat informací o paměti cache atributu pro protokol změn se používá nový výchozí bod hledání “cn=changelog,cn=monitor”.
- **Podpora pro autentizování klientských aplikací jako aktuální uživatel:** Klient LDAP a obslužné programy příkazového řádku jsou rozšířeny tak, aby podporovaly autentizaci na lokální server adresářů jako aktuální uživatel. Toto je obzvláště užitečné pro vykonávání administračních úloh při přihlášení jako uživatel i5/OS, který má k adresáři administrační oprávnění.
- **Kontrola přístupu k systémovým a omezeným atributům:** Nyní můžete kontrolovat přístup k systémovým a omezeným atributům souvisejícím s kontrolou přístupu a dalším atributům záznamů LDAP spravovaným serverem.
- **Kopírování uživatelů z ověřovacího seznamu do adresáře LDAP:** Server adresářů lze naplnit objekty adresáře na základě uživatelů definovaných v ověřovacím seznamu stylu HTTP. Kromě toho může server adresářů autentizovat uživatele na základě pověření zkopírovaných z ověřovacích seznamů HTTP. Tento proces umožňují nová rozhraní API. Další informace najdete v tématu “Kopírování uživatelů z ověřovacího seznamu HTTP serveru do serveru adresářů” na stránce 94.
- **Odmítnutí služeb a zrušení vazby u připojeného DN:** Nová vylepšení umožňují, aby server identifikoval mnoho forem útoků způsobujících odmítnutí služeb (DoS, denial of service), zotavil se po nich a překonal je. Tato vylepšení poskytují administrátorům možnost větší kontroly a automatických úprav serveru. Další informace najdete v tématu “Odmítnutí služeb” na stránce 73.
- **Více administračních funkcí prováděných přes web:** Více úloh lze provádět pomocí webového administračního nástroje. Většina nových funkcí se nachází v rámci nové kategorie **Server administration**.

Kapitola 3. Tisk PDF

Chcete-li prohlížet nebo stáhnout PDF verzi tohoto dokumentu, vyberte si téma Server adresářů (LDAP) (přibližně 2700 KB).

Ostatní informace


Chcete-li prohlížet nebo vytisknout soubory PDF souvisejících publikací a červených knih (Redbooks), prostudujte si část Kapitola 10, “Související informace”, na stránce 273.

Ukládání souborů PDF

Chcete-li uložit soubor PDF na pracovní stanici za účelem prohlížení nebo tisku:

1. Klepněte pravým tlačítkem myši na soubor PDF v prohlížeči (klepněte pravým tlačítkem myši na výše uvedený odkaz).
2. Klepněte na volbu, která lokálně ukládá soubor PDF.
3. Vyhledejte adresář, do něhož chcete soubor PDF uložit.
4. Klepněte na **Uložit (Save)**.

Stažení aplikace Adobe Reader

- | K tomu, abyste mohli prohlížet nebo vytisknout tyto soubory PDF ve vašem systému, potřebujete aplikaci Adobe Reader. Kopii je možné bezplatně stáhnout z webových stránek společnosti Adobe
- | (www.adobe.com/products/acrobat/readstep.html)  .

Kapitola 4. Koncepte serveru adresářů

Server adresářů implementuje specifikace LDAP V3 asociace Internet Engineering Task Force (IETF). Obsahuje rovněž vylepšení v oblasti funkčnosti a výkonu doplněná společností IBM. Tato verze využívá pro zálohování IBM DB2 Universal Database for iSeries, což zabezpečuje pro činnost LDAP integritu transakce, vysoký výkon operací a možnost zálohování a obnovy on-line. Spolupracuje s klienty připojenými prostřednictvím protokolu LDAP V3 IETF. Informace o konceptech a aspektech souvisejících se serverem adresářů najdete v těchto částech:

- “Adresáře”
- “Rozlišovací jména (DN)” na stránce 11
- “Přípona (kontext pojmenování)” na stránce 14
- “Schéma” na stránce 15
- “Publikování” na stránce 34
- “Replikace” na stránce 36
- “Sféry a uživatelské šablony” na stránce 41
- “Parametry prohledávání” na stránce 42
- “Pravidla pro podporu národního jazyka (NLS)” na stránce 44
- “Jazykové příznaky” na stránce 44
- “Odkazy v adresáři LDAP” na stránce 45
- “Transakce” na stránce 46
- “Server adresářů - Zabezpečení ochrany dat” na stránce 46
- “Procedura Backend projektovaná operačním systémem” na stránce 74
- “Server adresářů a podpora žurnálování i5/OS” na stránce 80
- “Jedinečné atributy” na stránce 80
- “Operační atributy” na stránce 80
- “Serverové paměti cache” na stránce 81
- “Ovladače a přídatné operace” na stránce 83

Adresáře

Server adresářů umožňuje přístup do takového typu databáze, která ukládá informace v hierarchické struktuře podobným způsobem, jakým je uspořádán integrovaný systém souborů operačního systému i5/OS.

Jestliže je známo jméno některého objektu, je možné načíst jeho charakteristiky. Pokud jméno konkrétního jednotlivého objektu známo není, je možné adresář prohledávat a nalézt seznam objektů, které vyhovují určitému požadavku. Adresáře se mohou obvykle prohledávat podle specifických kritérií, nikoli pouze podle předdefinovaných množin kategorií.

Adresář je specializovaná databáze mající charakteristiky, které ji odlišují od relačních databází pro všeobecné účely. Charakteristika adresáře je taková, že je k němu prováděn přístup (čte se nebo prohledává) mnohem častěji, než je aktualizován (zapisuje se do něj). Protože musejí být adresáře schopny podporovat velké objemy požadavku na čtení, jsou typicky optimalizovány pro přístup ke čtení. Jelikož adresáře nejsou určeny k tomu, aby umožňovaly tolik funkcí jako databáze pro všeobecné účely, je možné je optimalizovat tak, aby úspěšně poskytovaly rychlý přístup více aplikacím k datům adresáře ve velkých distribuovaných prostředích.

Adresář je možné centralizovat nebo distribuovat. Jestliže je adresář centralizovaný, potom jednomu místu existuje server adresářů (nebo klastr serverů), který poskytuje přístup do příslušného adresáře. Pokud je adresář distribuovaný, existuje několik serverů, obvykle geograficky rozptýlených, které zajišťují přístup do tohoto adresáře.

V případě, že je adresář distribuovaný, informace uložené v adresáři mohou být rozdělené na logické části nebo replikované. Když jsou informace rozdělené na logické části, každý server adresářů uchovává jedinečnou a nepřekrývající se podmnožinu informací. To znamená, že každý záznam adresáře je uchováván v jednom a pouze jednom serveru. Metoda pro rozdělení adresáře využívá odkazy LDAP. Odkazy LDAP umožňují uživatelům odkazovat požadavky LDAP (Lightweight Directory Access Protocol) buď na tytéž, nebo na odlišné prostory jmen uložené na jiném (nebo tomtéž) serveru. Když jsou informace replikované, je tentýž záznam adresáře uložen na více než jednom serveru. V distribuovaném adresáři mohou být některé informace rozdělené na logické části a některé informace mohou být replikované.

Model serveru adresářů LDAP je založen na záznamech (které se rovněž označují jako objekty). Každý záznam sestává z jednoho nebo více atributů, jako je např. jméno nebo adresa, a z typu. Typy jsou obvykle mnemotechnické řetězce, například "cn" pro "common name" (obecné jméno) nebo "mail" pro adresu elektronické pošty.

Příklad adresáře, který uvádí Obrázek 1 na stránce 9, znázorňuje záznam pro Tima Jonese, který obsahuje atributy mail a telephoneNumber. Některé další možné atributy jsou fax, title (titul), sn (pro surname - příjmení) a jpegPhoto.

Každý adresář má určité schéma, což je sada pravidel, která určují strukturu a obsah adresáře. Toto schéma můžete zobrazit pomocí webového administračního nástroje. Další informace o schématu najdete v tématu "Schéma" na stránce 15.

Každý záznam adresáře obsahuje zvláštní atribut zvaný třída objektu (objectClass). Tento atribut řídí, které atributy v daném záznamu jsou povinné nebo povolené. Jinými slovy, hodnota atributu třídy objektu určuje pravidla schématu, která musí daný záznam zachovávat.

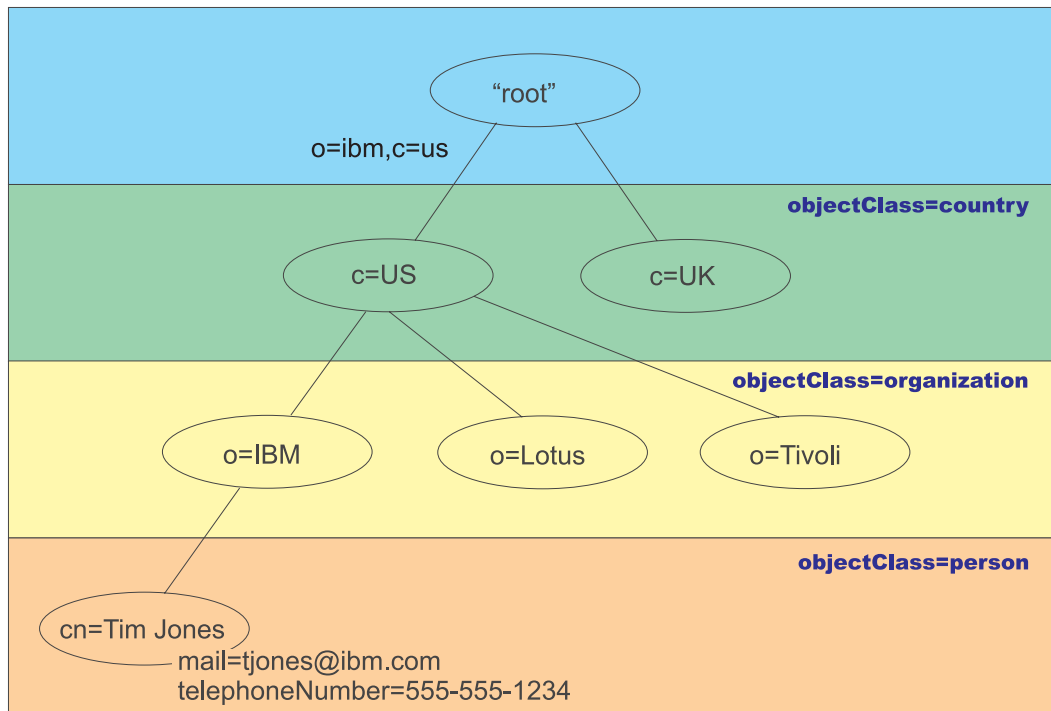
Kromě atributů definovaných příslušným schématem obsahují záznamy také sadu atributů, které jsou uchovávány na serveru. Tyto atributy, označované jako operační atributy, obsahují např. údaje o čase vytvoření záznamu a informace o řízení přístupu. Další informace o operačních attributech najdete v tématu "Operační atributy" na stránce 80.

Záznamy v adresáři LDAP jsou tradičně uspořádány do hierarchické struktury, která odráží politické, geografické nebo organizační hranice (viz Obrázek 1 na stránce 9). Záznamy, které představují země nebo regiony, se zobrazují 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.

LDAP na záznamy odkazuje pomocí rozlišovacích jmen, neboli DN (Distinguished Names). Rozlišovací jména jsou tvořena jménem samotného záznamu a jmény nadřazených objektů v adresáři směrem zdola nahoru. Například plné DN pro záznam v levém dolním rohu Obrázek 1 na stránce 9 je cn=Tim Jones, o=IBM, c=US. Každý záznam obsahuje minimálně jeden atribut, který pojmenovává vlastní záznam. Tomuto atributu pojmenování se říká relativní rozlišovací jméno, neboli RDN (Relative Distinguished Name) záznamu. Záznam nad tímto RDN se označuje jako nadřazené rozlišovací jméno. Ve výše uvedeném příkladu je vlastní záznam pojmenován cn=Tim Jones, je to tedy RDN. Nadřazené DN pro cn=Tim Jones je o=IBM, c=US. Další informace o DN najdete v tématu "Rozlišovací jména (DN)" na stránce 11.

K tomu, aby mohl server LDAP spravovat část adresáře LDAP, je nutné 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 9, měl by mít v konfiguraci zadanou příponu o=ibm, c=us, aby mohl uspokojit dotazy klienta týkající se Tima Jonese.

Struktura adresářů LDAP



RV4Q100-1

Obrázek 1. Struktura adresáře LDAP

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

Řekněme, že chcete vytvořit adresář pomocí struktury doménových komponent, která bude obsahovat data zaměstnance, jako např. jména, čísla telefonu a e-mailové adresy. Používáte příponu nebo kontext pojmenování na základě domény TCP/IP. Tento adresář je možné znázornit asi takto:

```

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

Když se tato data zadávají do serveru adresářů, mohou ve skutečnosti vypadat nějak takto:

```

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

# adresar zamestnancu
dn: cn=employees,dc=ibm,dc=com
objectclass: top
  
```

```

objectclass: container
cn: employees

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

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

```

Asi si všimnete, že každý záznam obsahuje hodnoty atributů nazvané třída objektu (objectclass). Hodnoty třídy objektu definují, které atributy jsou v záznamu povolené, jako například telephonenumber nebo givenname. Povolené třídy objektů (object classes) jsou definovány ve schématu. Schéma je sestava pravidel, která definují typ záznamů povolených v příslušné databázi.

Klienti a servery adresáře

K adresářům se obvykle získává přístup pomocí komunikačního modelu klient-server. Klientské i serverové procesy mohou nebo nemusí běžet na stejném počítači. Server je schopen obsloužit mnoho klientů. Aplikace, která chce zapisovat nebo číst informace v adresáři, nezískává přístup k adresáři přímo. Namísto toho volá funkci nebo rozhraní API, které zprostředkuje odeslání zprávy jinému procesu. Tento druhý proces získává přístup k informacím v adresáři jménem žádající aplikace. Výsledky zápisu nebo čtení jsou potom vráceny do žádající aplikace.

Rozhraní API definuje programovací rozhraní, které konkrétní programovací jazyk používá k získání přístupu k dané službě. Formát a obsah zpráv vyměňovaných mezi klientem a serverem se musí řídit dohodnutým protokolem. LDAP definuje protokol zpráv používaný klienty a servery adresáře. K dispozici je rovněž rozhraní API pro LDAP přiřazené jazyku C nebo například způsoby přístupu k adresáři z aplikací Java využívajících rozhraní pojmenování a adresářů JNDI (Naming and Directory Interface) systému Java.

Zabezpečení adresářů

Adresář by měl podporovat základní schopnosti potřebné k implementaci zásad zabezpečení dat. Adresář nemusí přímo zajišťovat vlastní schopnosti zabezpečení, ale může být začleněn do služby důvěryhodné sítě, která poskytuje základní služby zabezpečení. Především je zapotřebí metoda pro autentizaci uživatelů. Autentizace ověřuje, zda jsou uživatelé těmi, za které se vydávají. Základním schématem autentizace je ID uživatele a heslo. Jakmile jsou uživatelé autentizováni, je nutné určit, zda mají oprávnění nebo povolení k provádění požadované činnosti na specifickém objektu.

Autorizace je často založena na seznamech přístupových práv (ACL). ACL je seznam oprávnění, která mohou být připojena k objektům a atributům v příslušném adresáři. Seznamy ACL uvádějí, který typ přístupu má každý z uživatelů nebo skupin uživatelů povolen nebo odepřen. K tomu, aby bylo možné seznamy ACL vytvořit co nejkratší a snadněji spravovatelné, jsou často uživatelé se stejnými přístupovými právy soustředováni do skupin.

Rozlišovací jména (DN)

Každý záznam v adresáři má rozlišovací jméno (DN - distinguished name). DN je jméno, které jednoznačně určuje záznam v adresáři. DN je tvořeno z párů atribut=hodnota, oddělených čárkami, například:

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

K vytvoření DN je možné použít jakýkoli z atributů definovaných ve schématu adresáře. Důležité je však pořadí párů hodnot atributů komponent. DN obsahuje jednu komponentu pro každou úroveň hierarchie adresáře od kořene až po úroveň, kde je záznam umístěn. Jména DN používaná pro LDAP začínají nejspécifičtějším atributem (obvykle některým typem jména) a pokračují postupně širšími atributy a často končí atributem země. První z komponent DN se označuje jako RDN (relativní rozlišovací jméno - Relative Distinguished Name). To jasně odlišuje příslušný záznam od jakýchkoli jiných záznamů, které mají stejné nadřazené atributy. Ve výše uvedených příkladech odlišuje jméno RDN "cn=Ben Gray" první záznam od druhého záznamu (se jménem RDN "cn=Lucille White"). Jména DN v těchto dvou příkladech jsou jinak rovnocenná. V příslušném záznamu musí být rovněž přítomen pár atribut=hodnota tvořící RDN pro daný záznam (to neplatí pro ostatní komponenty DN).

Vytvořte podle tohoto příkladu záznam pro nějakou osobu:

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

Pravidla pro uvolnění DN

Některé znaky mají v DN speciální význam. Například znak "=" (rovnítko) odděluje jméno a hodnotu atributu a znak ", " (čárka) odděluje páry atribut=hodnota. Speciálními znaky jsou , (čárka), = (rovnítko), + (plus), < (menší než), > (větší než), # (křížek), ; (středník), \ (zpětné lomítko) a " (uvozovka, ASCII 34).

Speciální znak může být v hodnotě atributu "uvolněn", tím se odstraní jeho speciální význam. Uvolnění těchto speciálních znaků nebo jiných znaků v hodnotě atributu v řetězci DN se provádí těmito způsoby:

1. V případě, že znak, který má být uvolněn, je jeden ze speciálních znaků, zapíšte před něj zpětné lomítko ('\` ASCII 92). Tento příklad znázorňuje způsob uvolnění čárky v názvu organizace:

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

To je preferovaný způsob.

2. Jiným způsobem je nahrazení uvolňovaného znaku zpětným lomítkem a dvěma hexadecimálními číslicemi, které tvoří jediný bajt v kódu znaku. Kód znaku **musí** být ve znakové sadě UTF-8.

```
CN=L. Eagle,o=Sue\2C Grabbit and Runn,C=GB
```

3. Celou hodnotu atributu uzavřete uvozovkami "" (ASCII 34), které nejsou součástí hodnoty. Mezi párem uvozovek jsou všechny znaky chápány tak, jak jsou, s výjimkou \ (zpětného lomítka). Zpětné lomítko \ je možné použít pro uvolnění zpětného lomítka (ASCII 92) nebo uvozovek (ASCII 34), kteréhokoli z výše uvedených speciálních znaků nebo párů hexadecimálních číslic jako v metodě 2. Příkladem může být uvolnění uvozovek ve výrazu `cn=xyz"qrs"abc`, ze kterého se stane `cn=xyz\"qrs\"abc`, nebo uvolnění \ :

"jednoduché zpětné lomítko musíte uvolnit takto \\"

Jiný příklad: "\Zoo" je neplatné, protože 'Z' nelze v tomto kontextu uvolnit.

Nepravá DN

Nepravá (pseudo) DN se používají při definování a vyhodnocování řízení přístupu. Adresář LDAP podporuje několik nepravých DN (například "group:CN=THIS" a "access-id:CN=ANYBODY"), které se používají pro odkazování na velké počty DN, která sdílejí společnou charakteristiku, buď v souvislosti s prováděnou činností, nebo s objektem, na kterém se tato činnost provádí. Další informace o řízení přístupu najdete v tématu "Server adresářů - Zabezpečení ochrany dat" na stránce 46.

Server adresářů podporuje tři nepravá DN:

- access-id: CN=THIS

Když je uvedeno jako součást ACL, odkazuje toto DN na bindDN (přípojovací DN), které odpovídá DN, na němž je příslušná činnost prováděna. Jestliže je například nějaká činnost prováděna na objektu "cn=personA, ou=IBM, c=US" a bindDn je "cn=personA, ou=IBM, c=US", jsou poskytnutá práva kombinací práv udělených jménu "CN=THIS" a jménu "cn=personA, ou=IBM, c=US".

- group: CN=ANYBODY

Když je uvedeno jako součást ACL, odkazuje toto DN na všechny uživatele, včetně těch, jejichž identita nebyla ověřena. Uživatele nelze vyjmout z této skupiny a tuto skupinu nelze vyjmout z databáze.

- group: CN=AUTHENTICATED

Toto DN odkazuje na jakékoli DN, které bylo adresářem autentizováno. Na metodu autentizace se nebere zřetel.

Poznámka: "CN=AUTHENTICATED" odkazuje na DN, které bylo autentizováno kdekoli na serveru, bez ohledu na to, kde je umístěn objekt představovaný jménem DN. Toto jméno by se však mělo používat opatrně. Například pod jednou příponou "cn=Secret" by mohl být uzel nazvaný "cn=Confidential Material", který má aclentry "group:CN=AUTHENTICATED:normal:rsc". Pod jinou příponou, "cn=Common" by mohl být uzel "cn=Public Material". Pokud jsou tyto dva stromy umístěny na stejném serveru, připojení k "cn=Public Material" by se považovalo za autentizovanou a dostalo by povolení pro normální třídu v objektu "cn= Confidential Material".

Některé příklady nepravých DN:

Příklad 1

Předpokládejme toto ACL pro objekt: cn=personA, c=US

AclEntry: access-id: CN=THIS:critical:rwc

AclEntry: group: CN=ANYBODY: normal:rsc

AclEntry: group: CN=AUTHENTICATED: sensitive:rsc

Připojení uživatele jako	Obdržel by
cn=personA, c=US	normal:rsc:sensitive:rsc:critical:rwc
cn=personB, c=US	normal:rsc:sensitive:rsc
Anonymous	normal:rsc

V tomto případě obdrží personA práva udělená objektu s ID "CN=THIS" i práva udělená oběma skupinám s nepravými DN, jak "CN=ANYBODY", tak "CN=AUTHENTICATED".

Příklad 2

Předpokládejme toto ACL pro objekt: cn=personA, c=US AclEntry: access-id:cn=personA, c=US: object:ad

AclEntry: access-id: CN=THIS:critical:rwc

AclEntry: group: CN=ANYBODY: normal:rsc

AclEntry: group: CN=AUTHENTICATED: sensitive:rsc

Pro činnost prováděnou na cn=personA, c=US:

Připojení uživatele jako	Obdržel by
cn=personA, c=US	object:ad:critical:rwsc
cn=personB, c=US	normal:rsc:sensitive:rsc
Anonymous	normal:rsc

V tomto případě obdrží personA práva udělená objektu s ID "CN=THIS" i práva udělená DN samotnému "cn=personA, c=US". Pověšimněte si, že práva skupiny nejsou udělena, protože pro připojovací DN ("cn=personA, c=US") existuje specifičtější aclentry ("access-id:cn=personA, c=US").

Zpracování rozšířeného DN

Smišené RDN jména DN se může skládat z několika komponent spojených operátory '+'. Server rozšiřuje podporu pro vyhledávání záznamů, které mají takové DN. Smišené RDN je možné specifikovat v jakémkoli pořadí jako výchozí bod pro operaci vyhledávání.

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

Server podporuje rozšířenou operaci normalizace DN. Rozšířené operace normalizace DN normalizují jména DN pomocí schématu serveru. Tato rozšířená operace může být užitečná u aplikací, které používají jména DN. Další informace o rozšířených operacích najdete v tématu "Ovladače a přídatné operace" na stránce 83.

Syntaxe rozlišovacího jména

Formální syntaxe pro rozlišovací jméno (DN) je založena na RFC 2253. Syntaxe podle BNF (Backus Naur Form) je definována takto:

```
<jméno> ::= <jméno-komponenty> ( <oddělovač-mezera> )
          | <jméno-komponenty> <oddělovač-mezera> <jméno>

<oddělovač-mezera> ::= <volitelná-mezera>
                    <oddělovač>
                    <volitelná-mezera>

<oddělovač> ::= ", " | ";"

<volitelná-mezera> ::= ( <CR> ) *( " " )

<jméno-komponenty> ::= <atribut>
                    | <atribut> <volitelná-mezera> "+"
                    <volitelná-mezera> <jméno-komponenty>

<atribut> ::= <řetězec>
            | <klávesa> <volitelná-mezera> "=" <volitelná-mezera> <řetězec>

<klávesa> ::= 1*( <keychar> ) | "OID." <oid> | "oid." <oid>
<keychar> ::= písmena, číslice a mezera

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

<řetězec> ::= *( <stringchar> | <pár> )
            | "'" *( <stringchar> | <speciální> | <pár> ) "'"
            | "#" <hex>

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

<pár> ::= "\" ( <speciální> | "\" | "'" )
```

<stringchar> ::= jakýkoli znak s výjimkou <speciálního> nebo "\" nebo "'

<hex> ::= 2*<hexchar>

<hexchar> ::= 0-9, a-f, A-F

Pro oddělování jednotlivých RDN v rozlišovacím jménu je možné používat znak středníku (;), ačkoli typickým zápisem je znak čárky (,).

Na obou stranách čárky nebo středníku mohou být použity neviditelné znaky (mezery). Tyto neviditelné znaky se ignorují a středník je nahrazen čárkou.

Kromě toho je možné použít znaky mezery (' ' ASCII 32), buď před, nebo za '+' nebo '='. Tyto znaky mezer se při analýze ignorují.

Následující příklad znázorňuje rozlišovací jméno zapsané pomocí zápisu, který je výhodný pro běžné tvary jmen. První jméno obsahuje tři komponenty. První z komponent je složené RDN. Složené RDN obsahuje více než jeden pár atribut: hodnota a lze je použít pro jednoznačné určení specifického záznamu v případech, ve kterých by mohla být jednoduchá hodnota CN nejednoznačná:

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

Přípona (kontext pojmenování)

Přípona (rovněž označovaná jako kontext pojmenování) je DN, které označuje nejvyšší záznam v hierarchii místně uloženého adresáře. Následkem použití schématu relativního pojmenování v LDAP je toto DN rovněž příponou každého dalšího záznamu v hierarchii tohoto adresáře. Server adresářů může mít mnoho přípon, z nichž každá identifikuje hierarchii místně uloženého adresáře, například o=ibm,c=us.

Do adresáře musí být přidán určitý záznam, který odpovídá příponě. Záznam, který vytvoříte, musí využívat třídu objektu, která obsahuje použitý atribut pojmenování. Pro vytváření záznamu odpovídajícího této příponě můžete použít webový nástroj administrace nebo obslužný program Qshell ldapadd. Další informace najdete v tématu "Jak provádět správu záznamů adresáře" na stránce 165 nebo v tématu "ldapmodify a ldapadd" na stránce 187.

Jednou z koncepcí LDAP je existence globálního prostoru pro jména LDAP. V globálním prostoru pro jména LDAP byste mohli najít DN jako například:

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

Přípona "o=IBM" sděluje serveru, že pouze první DN je v prostoru pro jména uchovávaném příslušným serverem. Pokusy odkazovat na objekty, které nespádají do jedné z přípon, mají za následek chybu "no such object" (žádný takový objekt) nebo odkaz na jiný server adresářů.

Server může mít několik přípon. Server adresářů má několik předdefinovaných přípon, které uchovávají data specifická pro naši implementaci:

- cn=schema obsahuje přístupné znázornění LDAP schématu
- cn=changelog uchovává protokol změn serveru, pokud je povolený
- cn=localhost obsahuje nereplikované informace, které určují některé aspekty činnosti serveru, například konfigurační objekty replikace
- cn=IBMpolicies obsahuje informace o činnosti serveru, které jsou replikovány
- cn=pwdpolicy obsahuje zásadu správy hesel pro celý server
- přípona "os400-sys=system-name.mydomain.com" zajišťuje LDAP s možností přístupu k objektům i5/OS, v současnosti omezený na uživatelské profily a skupiny

Server adresářů se dodává předkonfigurovaný pomocí předvolené přípony `dc=system-name`, `dc=domain-name`, což usnadňuje zahájení práce se serverem. Použití této přípony však není podmínkou. Můžete přidávat své vlastní přípony a předkonfigurovanou příponu vymazat.

Pro přípony existují dvě obvykle používané konvence pojmenování. Jedna je založena na doméně TCP/IP přidělené vaší organizaci. Ta druhá je založena na jménu a umístění organizace.

Předpokládejme například doménu TCP/IP se jménem `mycompany.com`, pro kterou si můžete zvolit příponu jako `dc=mycompany,dc=com`, kde atribut `dc` odkazuje na komponentu domény. V tomto případě by mohl záznam nejvyšší úrovně, který v adresáři vytvoříte, vypadat (s využitím LDIF, textového formátu souboru pro znázorňování záznamů LDAP) nějak takto:

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

Příslušná třída objektu `domain` má rovněž některé volitelné atributy, které budete pravděpodobně moci využít. Další použitelné atributy můžete zobrazit za pomoci webového administračního nástroje, který umožňuje rovněž prohlížet schéma nebo editovat záznam, který jste vytvořili. Další informace najdete v tématu “Jak provádět správu schématu” na stránce 154.

Jestliže je jméno vaší společnosti `My Company` a je-li tato společnost umístěna ve Spojených státech, mohli byste si zvolit podobnou příponu, jako je tato:

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

Kde `ou` je jméno pro třídu objektu `organizationalUnit`, `o` je jméno organizace pro třídu objektu organizace a `c` je standardní dvoupísmenná zkratka země používaná pro pojmenování třídy objektu země. V tomto případě by záznam nejvyšší úrovně, který vytvoříte, mohl vypadat takto:

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

Aplikace, které používáte, mohou vyžadovat, aby byly definovány určité přípony nebo aby byly použity konkrétní konvence pojmenování. Jestliže se například váš adresář používá pro správu digitálních podpisů, může být zapotřebí, abyste uspořádali část svého adresáře takovým způsobem, aby jména záznamů odpovídala jménům DN subjektů certifikátů, jejichž jsou držiteli.

Záznamy, které se mají přidat do adresáře, musí mít příponu, která odpovídá hodnotě DN, jako například `ou=Marketing,o=ibm,c=us`. Jestliže dotaz obsahuje příponu, která neodpovídá žádné příponě konfigurované pro místní databázi, je tento dotaz odkázan na server LDAP určený předvoleným odkazem. Pokud není zadán žádný předvolený odkaz LDAP, je vrácen výsledek `Object does not exist` (objekt neexistuje).

Další informace o způsobech přidávání nebo odstraňování přípon najdete v tématu “Jak přidávat a odstraňovat přípony serveru adresářů” na stránce 116.

Schéma

Schéma je sestava pravidel, která řídí, jakým způsobem je možné ukládat data v adresáři. Schéma definuje typ povolených záznamů, strukturu jejich atributů a syntaxi atributů.

Data jsou ukládána v adresáři pomocí záznamů adresáře. Záznam se skládá ze třídy objektu, která je povinná, a jejich atributů. Atributy mohou být buď povinné, nebo volitelné. Třída objektu určuje druh informací, které záznam popisuje, a definuje sadu atributů, které obsahuje. Každý atribut má jednu nebo více přiřazených hodnot. Více informací o způsobech správy záznamů najdete v tématu “Jak provádět správu záznamů adresáře” na stránce 165.

Další informace souvisejících se schématem najdete v těchto částech:

- “Schéma serveru adresářů IBM”
- “Podpora obecného schématu” na stránce 17
- “Třídy objektů” na stránce 18
- “Atributy” na stránce 19
- “Identifikátor objektu (OID)” na stránce 26
- “Záznamy podschématu” na stránce 27
- “Třída objektu IBMsubschema” na stránce 27
- “Dotazy na schéma” na stránce 27
- “Dynamické schéma” na stránce 27
- “Zakázané změny schématu” na stránce 28
- “Kontrola schématu” na stránce 31
- “Kompatibilita s iPlanet” na stránce 33
- “Zobecněný čas a UTC čas” na stránce 33

Schéma serveru adresářů IBM

Schéma pro server adresářů je předdefinované, pokud však máte další požadavky, můžete schéma změnit. Další informace o způsobu změny schématu najdete v tématu “Jak provádět správu schématu” na stránce 154.

Server adresářů obsahuje podporu dynamických schémat. Schéma je zveřejněno jako součást informací adresáře a je k dispozici v záznamu podschématu (DN="cn=schema"). Na schéma se můžete dotázat pomocí rozhraní API `ldap_search()` a modifikovat je pomocí `ldap_modify()`. Další informace o těchto rozhraních API najdete v tématu “Rozhraní API serveru adresářů”.

Schéma obsahuje více informací o konfiguraci než schéma začleněné v RFC (Request for Comments) LDAP Verze 3 nebo ve standardních specifikacích. Pro daný atribut můžete například stanovit, které indexy je nutno zachovávat. Tyto dodatečné informace o konfiguraci se podle potřeby uchovávají v záznamu podschématu. Další třída objektu je definována pro záznam podschématu IBMsubschema mající atributy typu “MAY”, které uchovávají přídatné informace schématu.

Server adresářů definuje pro celý server jediné schéma, které je přístupné prostřednictvím speciálního záznamu adresáře, “cn=schema”. Tento záznam obsahuje všechna schémata definovaná pro příslušný server. Chcete-li načíst informace o schématu, můžete provést `ldap_search` s využitím tohoto postupu:

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

Schéma poskytuje hodnoty pro tyto typy atributů:

- `objectClasses` (další informace o třídách objektů - `objectClasses` najdete v tématu “Třídy objektů” na stránce 18).
- `attributeTypes` (další informace o typech atributů - `attributeTypes` najdete v tématu “Atributy” na stránce 19).
- `IBMAttributeTypes` (další informace o typech `IBMAttributeTypes` najdete v tématu “Atribut `IBMAttributeTypes`” na stránce 21).
- Porovnávací pravidla (další informace o porovnávacích pravidlech najdete v tématu “Porovnávací pravidla” na stránce 22).
- Syntaxe `ldap` (další informace o syntaxích `ldap` najdete v tématu “Syntaxe atributu” na stránce 24).

Syntaxe těchto definicí schématu je založena na RFC Verze 3 LDAP.

Vzorový záznam schématu by mohl obsahovat:

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



```

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

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

ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.5 DESC 'binární' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.7 DESC 'booleovský' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.12 DESC 'DN' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.15 DESC 'adresářový řetězec' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.24 DESC 'zobecněný čas' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.26 DESC 'řetězec IA5' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.27 DESC 'celé číslo' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.50 DESC 'telefonní číslo' )
ldapSyntaxes=( 1.3.6.1.4.1.1466.115.121.1.53 DESC 'čas UTC' )

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




```

Informace schématu je možné modifikovat prostřednictvím rozhraní API `ldap_modify`. Chcete-li získat další informace, prostudujte si téma “Rozhraní API serveru adresářů”. Pomocí DN “`cn=schema`” můžete doplňovat, mazat nebo nahrazovat typ atributu nebo třídu objektu. Další informace najdete v tématech “Dynamické schéma” na stránce 27 a “Jak provádět správu schématu” na stránce 154. Je možné zadat i úplný popis. Záznamy schématu můžete přidávat nebo nahrazovat pomocí definice verze 3 LDAP či s využitím definice rozšíření atributu IBM nebo pomocí obou definic.

Podpora obecného schématu

Adresář IBM podporuje standardní schéma adresáře, jak je definováno těchto specifikacích:

- RFC verze 3 LDAP Internet Engineering Task Force (IETF) , jako například RFC 2252 a 2256.

- Directory Enabled Network (DEN) 
- Common Information Model (CIM) od Desktop Management Task Force (DMTF) 
- Lightweight Internet Person Schema (LIPS) od Network Application Consortium 

Tato verze LDAP zahrnuje v předvolené konfiguraci schématu definované schéma verze 3 LDAP. Obsahuje rovněž definice schématu DEN.

IBM také poskytuje sadu přidavných obecných definicí schémat, která sdílejí jiné produkty IBM při využití adresáře LDAP. Tato schémata zahrnují:

- Objekty pro aplikace "bílé stránky", jako jsou eperson, skupina, země, organizace, organizační jednotka a role, umístění, stát a tak dále.
- Objekty pro další podsystémy, jako jsou účty, služby a přístupové body, autorizace, autentizace, zabezpečení ochrany dat a tak dále.

Třídy objektů

Třída objektu specifikuje sestavu vlastností používaných k popisu objektu. Kdybyste například vytvořili třídu objektu **tempEmployee**, mohla by obsahovat atributy vztahující se k dočasnému zaměstnanci jako například **idNumber**, **dateOfHire** nebo **assignmentLength**. Je přirozeně možné přidávat takové uživatelské třídy objektu, které vyhovují potřebám vaší organizace. Schéma serveru adresářů IBM poskytuje některé základní typy třídy objektů, včetně typů:

- skupiny
- umístění
- organizace
- osoby

Poznámka: Třídy objektů, které jsou specifické pro server adresářů, mají předponu 'ibm-'.

Třídy objektů jsou definovány charakteristikami typu, dědičnosti a atributů.

Typ třídy objektu

Třída objektu může spadat pod jeden ze tří typů:

Strukturní:

Každý záznam musí příslušet do jedné a pouze jedné strukturní třídy objektu, která definuje základní obsah záznamu. Tato třída objektu představuje objekt, který na světě reálně existuje. Protože všechny záznamy musí příslušet do strukturní třídy objektu, jedná se o nejběžnější typ třídy objektu.

Abstraktní:

Tento typ se používá jako nadtřída neboli šablona pro jiné (strukturní) třídy objektů. Definuje sestavu atributů, které jsou společné pro množinu strukturních tříd objektů. Tyto třídy objektů, pokud jsou definovány jako podtřídy abstraktní třídy, dědí (přebírají) definované atributy. Atributy není nutno definovat pro každou z podřízených tříd objektů.

Pomocná:

Tento typ uvádí dodatečné atributy, které mohou být přiřazeny záznamu příslušejícímu do konkrétní strukturní třídy objektu. Ačkoli může záznam příslušet pouze do jediné strukturní třídy objektu, může příslušet do několika pomocných tříd objektů.

Dědičnost třídy objektu

Tato verze serveru adresářů podporuje dědičnost objektu pro definice třídy objektu a atributu. Nová třída objektu se může definovat pomocí nadřazených tříd (vícenásobná dědičnost) a dodatečných nebo změněných atributů.

Každý záznam je přiřazen jediné strukturní třídě objektu. Všechny třídy objektů dědí od abstraktní třídy objektu **top**. Mohou rovněž dědit i od jiných tříd objektů. Členění třídy objektu určuje seznam požadovaných a povolených atributů pro konkrétní záznam. Dědičnost třídy objektu závisí na pořadí definicí tříd objektů. Třída objektu může dědit pouze od tříd objektů, které jí předcházejí. Například struktura třídy objektu pro záznam osoby by mohla být definována v souboru LDIF jako:

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

Vteto strukturu dědí `organizationalPerson` od třídy objektů `person` a `top`, zatímco třída objektu `person` dědí pouze od třídy objektu `top`. Proto, když nějakému záznamu přiřadíte třídu objektu `organizationalPerson`, automaticky dědí povinné i povolené atributy od nadřazené třídy objektu (v tomto případě je to třída objektu `person`).

Před zpracováním a vykonáním operací aktualizace schématu se kontroluje jeho shodnost porovnáním s hierarchií tříd schématu.

Atributy

Každá třída objektu obsahuje mnoho povinných atributů a volitelných atributů. Povinné atributy jsou takové atributy, které musí být obsaženy v záznamech používajících tuto třídu objektu. Volitelné atributy jsou takové atributy, které smí být obsaženy v záznamech používajících tuto třídu objektu.

Atributy

Každý záznam adresáře obsahuje množinu atributů, která je k němu přiřazená prostřednictvím jeho třídy objektu. Zatímco třída objektu popisuje typ informací, které záznam obsahuje, skutečná data jsou obsažena v attributech. Atribut je představován jedním nebo více páry jméno-hodnota, které uchovávají specifické prvky dat, jako např. jméno, adresu nebo telefonní číslo. Server adresářů představuje data jako např. páry jméno-hodnota, popisný atribut jako `commonName (cn)` a specifické informace jako např. `John Doe`.

Například záznam pro osobu jménem `John Doe` by mohl obsahovat několik párů jméno-hodnota příslušného atributu.

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

I když standardní atributy jsou ve schématu již definovány, definice atributů je možné vytvářet, editovat, kopírovat nebo mazat tak, aby vyhovovaly potřebám vaší organizace.

Další informace najdete v těchto částech:

- “Obecné prvky podschématu”
- “Atribut `objectclass`” na stránce 20
- “Atribut `attributetypes`” na stránce 20
- “Atribut `IBMAttributeTypes`” na stránce 21
- “Porovnávací pravidla” na stránce 22
- “Pravidla indexování” na stránce 23
- “Syntaxe atributu” na stránce 24

Obecné prvky podschématu

Níže uvedené prvky se používají pro definování gramatiky hodnot atributů podschématu:

- `alpha = 'a' - 'z', 'A' - 'Z'`
- `number = '0' - '9'`

- `anh = alpha / number / '-' / ';`
- `anhstring = 1 * anh`
- `keystring = alpha [anhstring]`
- `numericstring = 1 * number`
- `oid = descr / numericoid`
- `descr = keystring`
- `numericoid = numericstring *("." numericstring)`
- `woid = whsp oid whsp ; sada několika oid jakékoli formy (numerická OID nebo jména)`
- `oids = woid / ("(" oidlist ")")`
- `oidlist = woid *("$" woid) ; deskriptory objektů používané jako jména prvků schématu`
- `qdescrs = qdescr / (whsp "(" qdescrlist ")" whsp)`
- `qdescrlist = [qdescr *(qdescr)]`
- `whsp "" descr "" whsp`

Atribut objectclass

Atribut `objectclasses` zobrazuje seznam tříd objektů podporovaných serverem. Každá hodnota tohoto atributu představuje samostatnou definici třídy objektu. Definice tříd objektů je možno přidávat, mazat nebo modifikovat pomocí příslušných modifikací atributu `objectclasses` záznamu `cn=schema`. Hodnoty atributu `objectclasses` se řídí touto gramatikou definovanou RFC 2252:

```
ObjectClassDescription = "(" whsp
    numericoid whsp ; Identifikátor atributu objectclass
    [ "NAME" qdescrs ]
    [ "DESC" qdstring ]
    [ "OBSOLETE" whsp ]
    [ "SUP" oids ] ; nadřazené objectclasses
    [ ( "ABSTRACT" / "STRUCTURAL" / "AUXILIARY" ) whsp ] ; předvolená hodnota je strukturní
    [ "MUST" oids ] ; AttributeTypes
    [ "MAY" oids ] ; AttributeTypes
    whsp ")"
```

Například definice třídy objektu (`objectclass`) osoby je:

```
( 2.5.6.6 NAME 'person' DESC 'Definuje záznamy, které v obecném použití představují osoby.'
STRUCTURAL SUP top MUST ( cn $ sn ) MAY ( userPassword $ telephoneNumber $ seeAlso $ description
) )
```

- OID pro tuto třídu je 2.5.6.6
- Jméno je "person"
- Jedná se o strukturní třídu objektu
- Dědí od třídy objektu "top"
- Povinné jsou tyto atributy: `cn`, `sn`
- Volitelné jsou tyto atributy: `userPassword`, `telephoneNumber`, `seeAlso`, `description`

Další informace o způsobech změny tříd objektů podporovaných serverem najdete v tématu "Jak provádět správu schématu" na stránce 154.

Atribut attributetypes

Atribut `attributetypes` zobrazuje seznam atributů podporovaných serverem. Každá hodnota tohoto atributu představuje samostatnou definici atributu. Definice atributů je možno přidávat, mazat nebo modifikovat pomocí příslušných modifikací atributu `attributetypes` záznamu `cn=schema`. Hodnoty atributu `attributetypes` se řídí následující gramatikou, jak je definována RFC 2252:

```
AttributeTypeDescription = "(" whsp
    numericoid whsp ; identifikátor AttributeType
    [ "NAME" qdescrs ] ; jméno používané v AttributeType
```

```

[ "DESC" qdstring ] ; popis
[ "OBSOLETE" whsp ]
[ "SUP" woid ] ; odvozeno od tohoto jiného AttributeType
[ "EQUALITY" woid ] ; jméno Matching Rule
[ "ORDERING" woid ] ; jméno Matching Rule
[ "SUBSTR" woid ] ; jméno Matching Rule
[ "SYNTAX" whsp noidlen whsp ]
[ "SINGLE-VALUE" whsp ] ; předvolená hodnota - s více hodnotami
[ "COLLECTIVE" whsp ] ; předvolená hodnota - není společně
[ "NO-USER-MODIFICATION" whsp ] ; předvolená hodnota - modifikovatelné uživatelem
[ "USAGE" whsp AttributeUsage ] ; předvolená hodnota - userApplications
whsp ")"

```

```

AttributeUsage =
  "userApplications" /
  "directoryOperation" /
  "distributedOperation" / ; DSA-sdíleno
  "dSAOperation" ; specifické pro DSA, hodnota závisí na serveru

```

Porovnávací pravidla a syntaxe hodnot musejí odpovídat jedné z hodnot definovaných podle následujících částí:

- “Porovnávací pravidla” na stránce 22
- “Syntaxe atributu” na stránce 24

Ve schématu je možné definovat nebo modifikovat pouze atributy "userApplications". Atributy "directoryOperation", "distributedOperation" a "dSAOperation" jsou definovány serverem a mají přesný význam pro činnost serveru.

Například atribut "description" (popis) má tuto definici:

```

( 2.5.4.13 NAME 'description' DESC 'Atribut společný pro schémata CIM a LDAP pro specifikaci
podrobného popisu záznamu objektu adresáře.' EQUALITY caseIgnoreMatch SUBSTR
caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications )

```

- Jeho OID je 2.5.4.13
- Jeho jméno je "description"
- Jeho syntaxe je 1.3.6.1.4.1.1466.115.121.1.15 (adresářový řetězec)

Další informace o způsobu změny typů atributů najdete v tématu “Jak provádět správu schématu” na stránce 154.

Atribut IBMAttributeTypes

Atribut IBMAttributeTypes je možné používat k definování informací o schématu neobsažených ve standardu LDAP verze 3 pro atributy. Hodnoty IBMAttributeTypes musí splňovat tato gramatická pravidla:

```

IBMAttributeTypesDescription = "(" whsp
  numericoid whsp
  [ "DBNAME" qdescrs ] ; maximálně 2 jména (tabulka, sloupec)
  [ "ACCESS-CLASS" whsp IBMAccessClass whsp ]
  [ "LENGTH" wlen whsp ] ; maximální délka atributu
  [ "EQUALITY" [ IBMwlen ] whsp ] ; tvorba indexu pro porovnávací pravidlo
  [ "ORDERING" [ IBMwlen ] whsp ] ; tvorba indexu pro porovnávací pravidlo
  [ "APPROX" [ IBMwlen ] whsp ] ; tvorba indexu pro porovnávací pravidlo
  [ "SUBSTR" [ IBMwlen ] whsp ] ; tvorba indexu pro porovnávací pravidlo
  [ "REVERSE" [ IBMwlen ] whsp ] ; převrácený index pro podřetězec
whsp ")"

```

```

IBMAccessClass =
  "NORMAL" / ; toto je předvolená hodnota
  "SENSITIVE" /
  "CRITICAL" /
  "RESTRICTED" /
  "SYSTEM" /
  "OBJECT" /

```

```

IBMwlen = whsp len

```

Numericoid

Používá se k uvedení hodnoty v atributu `attributetypes` v soulad s hodnotou v `IBMAttributeTypes`.

DBNAME

Je možné použít maximálně dvě jména, samozřejmě pokud jsou tato dvě jména stanovena. První je jméno tabulky používané pro tento atribut. Druhé je jméno sloupce používaného pro plně normalizovanou hodnotu atributu v tabulce. Pokud zadáte pouze jedno jméno, použije se jako jméno tabulky i jméno sloupce. Pokud nezadáte žádné jméno `DBNAME`, pak bude použito jméno na základě prvních 17 znaků jména atributu (které musí být jedinečné). Jména tabulky a sloupce databáze jsou omezena na 17 znaků.

ACCESS-CLASS

Klasifikace přístupu pro tento typ atributu. Je-li `ACCESS-CLASS` vynechán, je použita předvolená hodnota "normal".

LENGTH

Maximální délka tohoto atributu. Délka je vyjádřena jako počet bajtů. Server adresářů má opatření pro stanovení délky atributu. V hodnotě `attributetypes` může být řetězec:

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

použit k vyznačení, že `attributetype` s `oid attr-oid` má maximální délku.

EQUALITY, ORDERING, APPROX, SUBSTR, REVERSE

Jestliže je použit kterýkoli z těchto atributů, pro odpovídající porovnávací pravidlo se vytvoří index. Volitelná délka uvádí šířku indexovaného sloupce. Použije se jediný index, který využívá několika pravidel porovnávání. Není-li některé z nich určeno uživatelem, server adresářů přiřazuje délku 500. V odůvodněných případech může server rovněž použít kratší délku, než požaduje uživatel. Například, překročí-li délka indexu maximální délku atributu, délka indexu se ignoruje.

Porovnávací pravidla

Porovnávací pravidlo poskytuje vodítka pro porovnávání řetězců během operace vyhledávání. Tato pravidla jsou rozdělena do tří kategorií:

- rovnost
- řazení
- podřetězec

| Server adresářů podporuje porovnání rovnosti pro všechny syntaxe s výjimkou binární. Pro atributy definované pomocí binární syntaxe server podporuje pouze prohledávání existence, například "(jpegphoto=*)". Pro syntaxe řetězce IA5 String a syntaxe adresářového řetězce lze definici atributu dále definovat z hlediska rozlišování velkých a malých písmen (case exact nebo case ignore). Například atribut `cn` používá porovnávací pravidlo `caseIgnoreMatch`, takže hodnoty "John Doe" a "john doe" jsou ekvivalentní. U porovnávacích pravidel, která nerozlišují velká a malá písmena (case ignore), se porovnání provádí po převedení hodnot na velká písmena. Algoritmus převádění na velká písmena není přizpůsoben podle lokálního jazyka, takže nemusí u všech lokálních jazyků fungovat správně.

| Server adresářů podporuje porovnávání podřetězců pro atributy syntaxe adresářového řetězce, řetězce IA5 String a rozlišovacího jména. Prohledávací filtry pro porovnávání podřetězců používají znak "*", aby porovnali žádný nebo více znaků v řetězci. Například prohledávací filtr "(cn=*smith)" prohledá všechny hodnoty `cn` zakončené řetězcem "smith".

| Porovnávání řazení je podporováno pro syntaxe celočíselné proměnné (Integer), adresářového řetězce, řetězce IA5 a rozlišovacího jména. Pro syntaxe řetězců je řazení založeno na jednoduchém řazení bajtů hodnot řetězce UTF-8. Je-li atribut definován s porovnávacím pravidlem bez rozlišování malých a velkých písmen (case ignore), je řazení provedeno za použití hodnot řetězce převedených na velká písmena. Jak již bylo zmíněno výše, algoritmus převádění na velká písmena nemusí u všech lokálních jazyků fungovat správně.

| V serveru adresářů IBM je chování porovnávání řetězců a řazení odvozeno z porovnávacího pravidla: všechny syntaxe, které podporují porovnávání podřetězců, mají implicitní pravidlo porovnávání podřetězců a všechny syntaxe, které podporují řazení, mají implicitní pravidlo řazení. Pro atributy definované za použití porovnávacího pravidla bez rozlišování velkých a malých písmen (case ignore) jsou implicitní porovnávací pravidla podřetězců a řazení také bez

l rozlišování velkých a malých písmen.

Porovnávací pravidla rovnosti		
Porovnávací pravidlo	OID	Syntaxe
caseExactIA5Match	1.3.6.1.4.1.1466.109.114.1	Syntaxe adresářového řetězce
caseExactMatch	2.5.13.5 IA5	Syntaxe řetězce
caseIgnoreIA5Match	1.3.6.1.4.1.1466.109.114.2	Syntaxe řetězce IA5
caseIgnoreMatch	2.5.13.2	Syntaxe adresářového řetězce
distinguishedNameMatch	2.5.13.1	DN - rozlišovací jméno
generalizedTimeMatch	2.5.13.27	Syntaxe zobecněného času
ibm-entryUuidMatch	1.3.18.0.2.22.2	Syntaxe adresářového řetězce
integerFirstComponentMatch	2.5.13.29	Syntaxe celočíselné proměnné - celé číslo
integerMatch	2.5.13.14	Syntaxe celočíselné proměnné - celé číslo
objectIdentifierFirstComponentMatch	2.5.13.30	Řetězec pro zahrnutí OID. OID je řetězec obsahující číslice (0-9) a desetinné tečky (.).
objectIdentifierMatch	2.5.13.0	Řetězec pro zahrnutí OID. OID je řetězec obsahující číslice (0-9) a desetinné tečky (.).
octetStringMatch	2.5.13.17	Syntaxe adresářového řetězce
telephoneNumberMatch	2.5.13.20	Syntaxe telefonního čísla
uTCTimeMatch	2.5.13.25	Syntaxe času UTC

Porovnávací pravidla řazení		
Porovnávací pravidlo	OID	Syntaxe
caseExactOrderingMatch	2.5.13.6	Syntaxe adresářového řetězce
caseIgnoreOrderingMatch	2.5.13.3	Syntaxe adresářového řetězce
distinguishedNameOrderingMatch	1.3.18.0.2.4.405	DN - rozlišovací jméno
generalizedTimeOrderingMatch	2.5.13.28	Syntaxe zobecněného času

Porovnávací pravidla podřetězce		
Porovnávací pravidlo	OID	Syntaxe
caseExactSubstringsMatch	2.5.13.7	Syntaxe adresářového řetězce
caseIgnoreSubstringsMatch	2.5.13.4	Syntaxe adresářového řetězce
telephoneNumberSubstringsMatch	2.5.13.21	Syntaxe telefonního čísla

Poznámka: UTC-Time je formát časového řetězce definovaný podle standardů ASN.1. Viz normy ISO 8601 a X680. Tato syntaxe se používá pro ukládání časových hodnot ve formátu UTC-Time. Další informace najdete v tématu “Zobecněný čas a UTC čas” na stránce 33.

Pravidla indexování

Pravidla indexování připojená k atributům umožňují rychlejší načítání informací. Pokud je zadán pouze atribut, žádné indexy se neuchovávají. Server adresářů umožňuje tato pravidla indexování:

- rovnost

- řazení
- přibližně
- podřetězec
- opačné pořadí

Specifikace pravidel indexování pro atributy: Určení pravidla indexování pro určitý atribut řídí tvorbu a údržbu speciálních indexů pro hodnoty atributů. To výrazně zlepšuje dobu odezvy na hledání s filtry, které takové atributy obsahují. S činnostmi uplatněnými ve filtru vyhledávání souvisí těchto pět možných typů pravidel indexování.

Rovnost

Platí pro tyto činnosti při vyhledávání:

- equalityMatch '='

Například:

"cn = John Doe"

Řazení Platí pro tuto činnost při vyhledávání:

- greaterOrEqual '>='
- lessOrEqual '<='

Například:

"sn >= Doe"

Přibližně

Platí pro tuto činnost při vyhledávání:

- approxMatch '~='

Například:

"sn ~= doe"

Podřetězec

Platí pro operaci vyhledávání s použitím syntaxe podřetězce:

- substring '*'

Například:

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

Opačné pořadí

Platí pro tuto činnost při vyhledávání:

- '*' substring

Například:

"sn = *baugh"

Jako minimum se doporučuje, abyste určili indexování rovnosti jakýchkoli atributů, které se mají použít ve filtrech vyhledávání.

Syntaxe atributu

Syntaxe atributu definuje přípustné hodnoty daného atributu. Server používá definici syntaxe pro příslušný atribut k ověřování dat a určení způsobu, kterým se mají porovnávat hodnoty. Například "Booleovský" atribut může mít pouze hodnoty "TRUE" a "FALSE".

Atributy je možné definovat buď tak, že mají jedinou hodnotu, nebo několik hodnot. Hodnoty v attributech s více hodnotami nejsou uspořádány podle pořadí, takže by žádná aplikace neměla záviset na tom, zda bude skupina hodnot pro daný atribut vracena v konkrétním pořadí. V případě, že požadujete setříděnou množinu hodnot, máte možnost vložit seznam hodnot do jediné hodnoty atributu:

preferences: 1st-pref 2nd-pref 3rd-pref

Další možností je zahrnout informace o řazení přímo do dané hodnoty:

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

Atributy s více hodnotami jsou užitečné v případě, kdy je nějaký záznam označován několika jmény. Například `cn` (common name) má několik hodnot. Záznam by bylo možné definovat takto:

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

To umožňuje vyhledávání Johna Smithe i Jacka Smithe, přičemž se vrátí tytéž informace.

Binární atributy obsahují libovolný bajtový řetězec, například fotografii JPEG, a nelze je využívat k vyhledávání záznamů.

Booleovské atributy obsahují řetězec `TRUE` nebo `FALSE`.

Atributy DN obsahují rozlišovací jména LDAP. Hodnoty nemusí být jména DN existujících záznamů, ale musí mít platnou syntaxi DN.

Atributy s adresářovým řetězcem obsahují textový řetězec sestavený ze znaků UTF-8. Atribut může u hodnot používaných ve filtrech vyhledávání rozlišovat malá a velká písmena nebo může velikost písmen ignorovat (na základě porovnávacího pravidla definovaného pro daný atribut), hodnota je však vždy vrácena tak, jak byla původně zadána.

Atributy zobecněného času obsahují řetězec znázorňující datum a čas se zabezpečením přechodu přes rok 2000 s využitím času GMT s volitelným posunem časového pásma GMT. Další podrobnosti o syntaxi těchto hodnot najdete v tématu “Zobecněný čas a UTC čas” na stránce 33.

Atributy s řetězcem IA5 obsahují textový řetězec využívající znakovou sadu IA5 (7bitovou ASCII sadu používanou v USA). Atribut může u hodnot používaných ve filtrech vyhledávání rozlišovat malá a velká písmena nebo může velikost písmen ignorovat (na základě porovnávacího pravidla definovaného pro daný atribut), hodnota je však vždy vrácena tak, jak byla původně zadána. Řetězec IA5 rovněž umožňuje využití zástupných znaků pro vyhledávání podřetězců.

Celočíselné atributy obsahují znázornění hodnoty textovým řetězcem. Jako příklad může sloužit 0 nebo 1000. Hodnoty celočíselných atributů syntaxe musí být v rozmezí od -2147483648 do 2147483647.

Atributy telefonního čísla obsahují textové znázornění telefonního čísla. Server adresářů nevyžaduje u těchto hodnot žádnou konkrétní syntaxi. Následující hodnoty jsou všechny platné: (555)555-5555, 555.555.5555 i +1 43 555 555 5555.

Atributy času UTC používají starší formát řetězce pro znázornění data a času bez zabezpečení přechodu přes rok 2000. Chcete-li se dozvědět další podrobnosti, prostudujte si “Zobecněný čas a UTC čas” na stránce 33.

Ve schématu adresáře je syntaxe atributu specifikována pomocí identifikátoru objektu (OID) přiřazeného ke každé syntaxi. V následující tabulce jsou uvedeny syntaxe podporované serverem adresářů a jejich OID.

Syntaxe	OID
Syntaxe popisu typu atributu	1.3.6.1.4.1.1466.115.121.1.3
Binární - oktetový řetězec	1.3.6.1.4.1.1466.115.121.1.5
Booleovský - TRUE/FALSE	1.3.6.1.4.1.1466.115.121.1.7

Syntaxe	OID
Syntaxe adresářového řetězce	1.3.6.1.4.1.1466.115.121.1.15
Syntaxe popisu pravidla obsahu DIT	1.3.6.1.4.1.1466.115.121.1.16
Syntaxe popisu pravidla DITStructure	1.3.6.1.4.1.1466.115.121.1.17
DN - rozlišovací jméno	1.3.6.1.4.1.1466.115.121.1.12
Syntaxe zobecněného času	1.3.6.1.4.1.1466.115.121.1.24
Syntaxe řetězce IA5	1.3.6.1.4.1.1466.115.121.1.26
Popis typu atributu IBM	1.3.18.0.2.8.1
Syntaxe celočíselné proměnné - celé číslo	1.3.6.1.4.1.1466.115.121.1.27
Syntaxe popisu syntaxe LDAP	1.3.6.1.4.1.1466.115.121.1.54
Popis pravidla porovnávání	1.3.6.1.4.1.1466.115.121.1.30
Popis použití pravidla porovnávání	1.3.6.1.4.1.1466.115.121.1.31
Popis formy jména	1.3.6.1.4.1.1466.115.121.1.35
Syntaxe popisu třídy objektu	1.3.6.1.4.1.1466.115.121.1.37
Řetězec pro zahrnutí OID. OID je řetězec obsahující číslice (0-9) a desetinné tečky (.). Další informace najdete v tématu "Identifikátor objektu (OID)".	1.3.6.1.4.1.1466.115.121.1.38
Syntaxe telefonního čísla	1.3.6.1.4.1.1466.115.121.1.50
Syntaxe času UTC. UTC-Time je formát časového řetězce definovaný podle standardů ASN.1. Viz normy ISO 8601 a X680. Tato syntaxe se používá pro ukládání časových hodnot ve formátu UTC-Time. Další informace najdete v tématu "Zobecněný čas a UTC čas" na stránce 33.	1.3.6.1.4.1.1466.115.121.1.53


Identifikátor objektu (OID)

Identifikátor objektu (OID) je řetězec sestavený z dekadických čísel, který jednoznačně určuje příslušný objekt. Těmito objekty jsou typicky třída objektu nebo atribut.

Pokud nemáte OID, můžete zadat třídu objektu nebo jméno atributu s připojeným **-oid**. Například jestliže vytváříte atribut tempID, můžete zadat OID jako **tempID-oid**.


Zásadně důležité je to, aby soukromé OID vydávaly oprávněné orgány. Existují dvě základní strategie pro získávání legitimních OID:

- Zaregistrovat dané objekty u příslušného úřadu. Tato strategie může být například vhodná, jestliže potřebujete malý počet OID.
- Od úřadu získat arc (arc je samostatný podstrom stromu OID) a přidělit své vlastní OID podle potřeby. Tato strategie může být vhodnější, když je zapotřebí mnoho OID nebo když nejsou přiřazení OID stabilní.

Americký národní úřad pro normalizaci (ANSI) je registrační úřad pro jména organizací ve Spojených Státech v rámci globálního registračního procesu zavedeného organizacemi ISO (International Standards Organization) a ITU (International Telecommunication Union). Další informace o registraci jména organizace můžete nalézt na webových stránkách ANSI  (www.ansi.org). Arc OID úřadu ANSI pro organizace je 2.16.840.1. ANSI přiřadí číslo (NEWNUM) a vytvoří nový podstrom arc OID: 2.16.840.1.NEWNUM.

Ve většině zemí nebo regionů vede registr OID národní ústav pro normalizaci. Tak jako u podstromu arc úřadu ANSI se obvykle jedná o podstromy arc přiřazené pod OID 2.16. Je možné, že nalezení úřadu pro přidělování OID v některých zemích nebo regionech bude nutné věnovat určité úsilí. Národní úřad pro normalizaci ve vaší zemi nebo regionu může být členem ISO. Jména a kontaktní informace členů ISO je možné vyhledat na webových stránkách ISO

 (www.iso.ch).

Úřad IANA (Internet Assigned Numbers Authority) přiděluje soukromým podnikům čísla OID v podstromu arc 1.3.6.1.4.1. IANA přidělí číslo (NEWNUM) tak, aby nový arc OID byl 1.3.6.1.4.1.NEWNUM. Tato čísla je možné získat na webových stránkách IANA  (www.iana.org).

Jakmile byl vaší organizaci přidělen OID, můžete definovat své vlastní OID připojením vhodných čísel na konec přiděleného OID. Předpokládejme například, že vaší organizaci byl přidělen fiktivní OID 1.1.1. Žádné jiné organizaci nebyl přidělen OID, který začíná "1.1.1". Řadu pro LDAP můžete vytvořit připojením ".1", což vytvoří 1.1.1.1. Dále je možno dělit tuto řadu do řad pro třídy objektů (1.1.1.1.1), typy atributů (1.1.1.1.2) a tak dále, a přiřadit OID 1.1.1.1.2.34 atributu "foo".

Záznamy podschématu

Na každý server připadá jeden záznam podschématu. Všechny záznamy v adresáři mají implicitní typ atributu subschemaSubentry. Hodnotou typu atributu subschemaSubentry je DN záznamu podschématu, který odpovídá danému záznamu. Všechny záznamy pod stejným serverem sdílejí tentýž záznam podschématu a jejich typ atributu subschemaSubentry má tutěž hodnotu. Záznam podschématu má pevně naprogramováno DN 'cn=schema'.

Záznam podschématu náleží do třídy objektu 'top', 'subschema' a 'IBMsubschemata'. Třída objektu 'IBMsubschemata' nemá žádné atributy MUST a má jeden typ atributu MAY ('IBMattributeTypes').

Třída objektu IBMsubschemata

Třída objektu IBMsubschemata se používá pouze v záznamu podschématu, a to takto:

```
( 1.3.18.0.2.6.174
NAME 'ibmSubSchema'
DESC 'třída objektu specifická pro IBM, která uchovává všechny atributy třídy objektů pro daný server adresářů.'
SUP 'subschemata'
STRUCTURAL MAY ( IBMAttributeTypes ) )
```

Dotazy na schéma

Rozhraní API ldap_search() je možné využívat pro dotazování na záznam podschématu, jak je znázorněno v tomto příkladu:

```
DN          : "cn=schema"
rozsah vyhledávání : base
filtr       : objectclass=subschema nebo objectclass=*
```

Tento příklad načítá celé schéma. Chcete-li načíst všechny hodnoty vybraných typů atributů, použijte při hledání parametr attr v příkazu ldap_search. Není možné načíst pouze určitou hodnotu určitého typu atributu.

Další informace o rozhraní API pro ldap_search najdete v tématu "Rozhraní API serveru adresářů".

Dynamické schéma

K provádění změn dynamického schématu se používá rozhraní API pro ldap_modify se jménem DN "cn=schema". Současně je povoleno přidávat, mazat nebo nahrazovat pouze jeden subjekt schématu (například typ atributu nebo třídu objektu), nikoli více subjektů zároveň.

Chcete-li vymazat záznam schématu, určete atribut schématu, který definuje příslušný záznam schématu (objectclasses nebo attributetypes), a pro jeho hodnotu zadejte OID v závorkách. Například, chcete-li vymazat atribut s OID <attr-oid>:

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

Rovněž je možné zadat úplný popis. V každém případě porovnávacím pravidlem použitým při hledání subjektu schématu, který se má vymazat, je objectIdentifierFirstComponentMatch.

Při přidávání nebo nahrazování subjektu schématu MUSÍTE zadat definici LDAP Version 3 a SMÍTE zadat definici IBM. Ve všech případech musíte zadat pouze definici nebo definice subjektu schématu, které chcete postihnout.

Pokud chcete například vymazat typ atributu 'cn' (jeho OID je 2.5.4.3), použijte ldap_modify(s):

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

Chcete-li přidat nový typ atributu řádek (bar) s OID 20.20.20, který dědí od "jména" atributu a má délku 20 znaků:

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

Výše uvedený výraz ve verzi pro LDIF by byl:

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

Řízení přístupu

Změny dynamického schématu může provádět pouze dodavatel replikací nebo administrátor DN.

Replikace

Při provádění změny dynamického schématu se toto schéma replikuje.

Zakázané změny schématu

Přípustné jsou pouze některé změny schématu. Omezení změn zahrnují následující případy:

- Jakákoli změna schématu musí ponechat toto schéma v konzistentním stavu.
- Typ atributu, který je nadřazeným typem jiného typu atributu, se nesmí vymazat. Nesmí se vymazat ani typ atributu, který je typem atributu "MAY" nebo "MUST" některé třídy objektu.
- Nesmí se vymazat třída objektu, která je nadřazenou třídou jiné třídy.
- Není možné přidávat typy atributů nebo třídy objektů, které odkazují na neexistující subjekty (například syntaxe nebo třídy objektů).
- Typy atributů nebo třídy objektů není možné modifikovat takovým způsobem, aby nakonec odkazovaly na neexistující subjekty (například syntaxe nebo třídy objektů).
- Nové atributy nesmí používat existující databázové tabulky v jejich definici IBMattributeType.
- Atributy, které jsou použity v jakémkoliv existujícím záznamu adresáře, se nesmí vymazat.
- Délka a syntaxe atributů se nesmí měnit.

- Databázová tabulka nebo sloupec přidružený k atributu se nesmí měnit.
- Atributy používané v definicích existující třídy objektu se nesmí vymazat.
- Třídy objektu, které jsou použity v jakémkoliv existujícím záznamu adresáře, se nesmí vymazat.

Nejsou povoleny změny schématu, které ovlivňují činnost serveru. Níže uvedené definice schématu jsou vyžadovány serverem adresářů. Proto se nesmějí měnit.

Třídy objektů:

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

Atributy:

- aclEntry
- aclPropagate
- aclSource
- aliasedObjectName, aliasedentryName
- businessCategory
- cn, commonName
- createTimestamp
- creatorsName
- description
- dn, distinguishedName
- entryOwner
- hasSubordinates
- ibm-entryChecksum
- ibm-entryChecksumOp
- ibm-entryUuid
- member
- modifiersName
- modifyTimestamp
- name
- o, organizationName, organization
- objectClass
- os400-acgcde
- os400-astlvl
- os400-atnpgm
- os400-audlvl
- os400-aut
- os400-ccsid
- os400-chridctl
- os400-cntryid
- os400-curlib

- os400-dlvry
- os400-docpwd
- os400-dspsgninf
- os400-eimassoc
- os400-gid
- os400-groupmember
- os400-grpaut
- os400-grpauttyp
- os400-grpprf
- os400-homedir
- os400-IaspStorageInformation
- os400-inlmnu
- os400-inlpgm
- os400-invalidSignonCount
- os400-jobd
- os400-kbdbuf
- os400-langid
- os400-lclpwdmgt
- os400-lmtcpb
- os400-lmtdevssn
- os400-locale
- os400-maxstg
- os400-msgq
- os400-objaud
- os400-outq
- os400-owner
- os400-password
- os400-passwordExpirationDate
- os400-passwordLastChanged
- os400-previousSignon
- os400-profile
- os400-prtdev
- os400-ptylmt
- os400-pwdexp
- os400-pwdexpitv
- os400-setjobatr
- os400-sev
- os400-spcaut
- os400-spcenv
- os400-srtseq
- os400-status
- os400-storageUsed
- os400-storageUsedOnIasp
- os400-supgrpprf
- os400-sys os400-text

- os400-uid
- os400-usrcls
- os400-usropt
- ou, organizationalUnit, organizationalUnitName
- owner
- ownerPropagate
- ownerSource
- ref
- replicaBindDN
- replicaBindMethod
- replicaCredentials, replicaBindCredentials
- replicaHost
- replicaPort
- replicaUpdateTimeInterval
- replicaUseSSL
- seeAlso

Syntaxe:

Všechny

Porovnávací pravidla:

Všechna

Kontrola schématu

Když je server inicializován, přečtou se soubory schématu a zkontroluje se jejich konzistence a správnost. V případě, že této kontrole nevyhoví, server neprovede inicializaci a vyšle chybovou zprávu. Během jakékoli změny dynamického schématu se u výsledného schématu rovněž kontroluje konzistence a správnost. Pokud této kontrole nevyhoví, je vrácena chyba a změna se nezdaří. Některé kontroly jsou součástí gramatiky (například typ atributu může mít nanejvýš jeden nadřazený typ, ale třída objektu může mít jakýkoli počet nadřazených tříd).

U typů atributů se kontrolují tyto položky:

- Dva různé typy atributů nemohou mít stejné jméno nebo OID.
- Hierarchie dědičnosti typů atributů neobsahují cykly.
- Pro příslušný typ atributu je nutné definovat rovněž nadřazený typ, i když jeho definice může být zobrazena později nebo v samostatném souboru.
- Pokud je typ atributu podtyp jiného typu atributu, mají oba stejnou hodnotu USAGE.
- Syntaxe všech typů atributů může být buď přímo definovaná, nebo zděděná.
- Jako NO-USER-MODIFICATION mohou být označeny pouze operační atributy.

U tříd objektů se kontrolují následující položky:

- Dvě různé třídy objektů nemohou mít stejné jméno nebo OID.
- Hierarchie dědičnosti tříd objektů nemají cykly.
- Pro příslušnou třídu objektu je nutné definovat rovněž nadřazené třídy, i když se její definice může objevit později nebo v samostatném souboru.
- Pro příslušnou třídu objektu je nutné definovat rovněž typy atributu "MUST" a "MAY, i když se její definice může objevit později nebo v samostatném souboru.
- Každá strukturální třída objektu je přímou nebo nepřímou podtřídou nejvyšší třídy.
- Jestliže má abstraktní třída objektu nadřazené třídy, musí být tyto nadřazené třídy rovněž abstraktní.

Kontrola záznamu porovnáním se schématem

Když je prostřednictvím operace LDAP přidán nebo modifikován nějaký záznam, kontroluje se tento záznam porovnáním se schématem. Standardně se provádějí všechny kontroly uvedené v této kapitole. Je však možné výběrově některé z těchto kontrol schématu zakázat změnou úrovně kontroly schématu. To se provádí pomocí produktu iSeries Navigator změnou hodnoty pole **Kontrola schématu** na straně **Databáze/Přípony** vlastností serveru adresářů. Další informace o attributech konfigurace schématu najdete v tématu "Schéma konfigurace serveru adresářů" na stránce 219.

U záznamu, který má vyhovět schématu, se kontrolují tyto podmínky:

Pokud se týče tříd objektů:

- Musí mít alespoň jednu hodnotu typu atributu "objectClass" (třída objektu).
- Může mít jakýkoli počet pomocných tříd objektů včetně nuly. V tomto případě se nejedná o kontrolu, ale o objasnění. Není žádná možnost tuto funkci zakázat.
- Může mít jakýkoli počet abstraktních tříd objektů, ale pouze jako výsledek dědičnosti třídy. To znamená, že pro každou abstraktní třídu objektu, kterou tento záznam obsahuje, má rovněž strukturní nebo pomocnou třídu objektu, která dědí přímo nebo nepřímo od této abstraktní třídy objektu.
- Musí mít alespoň jednu strukturní třídu objektu.
- Musí mít přesně jednu aktuální nebo základní strukturní třídu objektu. To znamená, že ze všech strukturních tříd objektu přiřazených k záznamu musejí být všechny nadřazenými třídami přesně jedné z nich. Nejvíce odvozená třída objektu se nazývá "aktuální" nebo "základní strukturní" třída objektu záznamu nebo jednoduše "strukturní" třída objektu záznamu.
- Nemůže měnit svou aktuální strukturní třídu objektu (na ldap_modify).
- Pro každou třídu objektu patřící k záznamu se vypočítá množina všech jejích přímých i nepřímých nadřazených tříd; pokud žádná z těchto nadřazených tříd není k záznamu přiřazena, automaticky se přidá.
- Pokud je úroveň kontroly schématu nastavena na **Verze 3 (striktní)**, musejí být přiřazeny všechny strukturní nadřazené třídy. Chcete-li například vytvořit záznam s třídou objektu inetorgperson, je nutné určit tyto třídy objektu: person, organizationalperson a inetorgperson.

Platnost typů atributů pro daný záznam je určena takto:

- Množina typů atributů **MUST** pro příslušný záznam se spočítá jako sjednocení množin typů atributů **MUST** všech jeho tříd objektů, včetně implicitních zděděných tříd objektů. Pokud není množina typů atributů **MUST** pro příslušný záznam podmnožinou množiny typů atributů obsažených v záznamu, je tento záznam zamítnut.
- Množina typů atributů **MAY** pro příslušný záznam se spočítá jako sjednocení množin typů atributů **MAY** všech jeho tříd objektů, včetně implicitních zděděných tříd objektů. Pokud není množina typů atributů obsažených v příslušném záznamu podmnožinou sjednocení množin typů atributů **MUST** a **MAY** pro daný záznam, je tento záznam zamítnut.
- Jestliže je některý z typů atributů definovaných pro příslušný záznam označen jako **NO-USER-MODIFICATION**, je tento záznam zamítnut.

Platnost hodnot typů atributů pro daný záznam je stanovena takto:

- Pro každý typ atributu obsažený v záznamu platí, že pokud má daný typ atributu jedinou hodnotu a záznam má více než jednu hodnotu, je tento záznam zamítnut.
- Pro každou hodnotu typu atributu každého typu atributu obsaženého v záznamu platí, že pokud jeho syntaxe nevyhoví rutině kontroly syntaxe pro syntaxi tohoto atributu, je tento záznam zamítnut.
- Pro každou hodnotu typu atributu každého typu atributu obsaženého v záznamu platí, že pokud je jeho délka větší než maximální délka přiřazená k tomuto typu atributu, je tento záznam zamítnut.

Platnost DN se kontroluje takto:

- Provádí se kontrola, zda syntaxe dodržuje BNF pro rozlišovací jména. Pokud ji nedodržuje, je tento záznam zamítnut.
- Ověřuje se, zda je RDN sestaveno pouze z takových typů atributů, které jsou platné pro tento záznam.
- Ověřuje se, zda se v daném záznamu vyskytují hodnoty typů atributů použitých v RDN.

Kompatibilita s iPlanet

Kontrolní program používaný serverem adresářů umožňuje zadávání hodnot atributů pro typy atributů schématu (objectClasses a attributeTypes) s využitím gramatiky iPlanet. Například je možné zadávat hodnoty descr a numeric-oid uzavřené jednoduchými uvozovkami (jako kdyby to byly qdescr). Informace schématu jsou však vždy zpřístupňovány prostřednictvím ldap_search. Jakmile se (pomocí ldap_modify) provede jediná dynamická změna hodnoty některého atributu v souboru, je celý tento soubor nahrazen takovým souborem, ve kterém se všechny hodnoty atributů řídí specifikacemi serveru adresářů. Kontrolní program používaný pro soubory a pro požadavky ldap_modify je stejný, proto je ldap_modify, který pro hodnoty atributů používá gramatiku iPlanet, rovněž zpracován správně.

Když je proveden dotaz na záznam podschématu serveru iPlanet, může mít výsledný záznam pro daný OID více než jednu hodnotu. Jestliže má například určitý typ atributu dvě jména (jako např. 'cn' a 'commonName'), je popis tohoto typu atributu zadáván dvakrát, jednou pro každé jméno. Server adresářů může analyzovat schéma, ve kterém se popis jediného typu atributu nebo třídy objektu objeví několikrát se stejným popisem (s výjimkou NAME a DESCR). Pokud však server adresářů zveřejní dané schéma, uvede jediný popis takového typu atributu s vyjmenovanými všemi těmito jmény (krátké jméno je uvedeno první). Zde je uveden příklad, jakým způsobem iPlanet popisuje atribut obecného jména:

```
( 2.5.4.3 NAME 'cn'  
  DESC 'Standardní atribut'  
  SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )  
  
( 2.5.4.3 NAME 'commonName'  
  DESC 'Standardní atribut, alias pro cn'  
  SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

Toto je způsob, kterým je server adresářů popisuje:

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

Server adresářů podporuje podtypy. Jestliže nechcete, aby 'cn' bylo podtypem jména (které se odchyluje od standardu), můžete deklarovat toto:

```
( 2.5.4.3 NAME ( 'cn' 'commonName' )  
  DESC 'Standardní atribut'  
  SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

První jméno ('cn') je považováno za preferované neboli krátké jméno a všechna ostatní jména následující po 'cn' za alternativní jména. Od tohoto bodu dále mohou být řetězce '2.3.4.3', 'cn' a 'commonName' (ale také jejich ekvivalenty nerozlišující velká a malá písmena) v rámci schématu nebo pro záznamy přidávané do adresáře používány zaměnitelně.

Zobecněný čas a UTC čas

Pro vyznačení informací týkajících se data a času se používají různé notace. Například čtvrtý den února v roce 1999 může být zapsán takto:

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

is použitím mnoha dalších notací.

Server adresářů standardizuje znázornění časového označení tím, že vyžaduje od serverů LDAP podporu dvou syntaxí:

- Syntaxe zobecněného času, která má formu:
RRRRMMDDHHMMSS[. |, z1omek] [(+|-HHMM) |Z]

Vtomto zápise jsou čtyři číslice pro rok, dvě číslice pro měsíc, den, hodinu, minutu a sekundu a volitelný zlomek sekundy. Když nejsou doplněny žádné další přídavky, předpokládá se, že se jedná o datum a čas zapsaný pro místní

časové pásmo. Chcete-li vyznačit, že je čas měřen v koordinovaném univerzálním čase (Coordinated Universal Time), připojte k času nebo rozdílu místního času velké písmeno Z. Například:

```
"19991106210627.3"
```

je 6 minut, 27,3 sekund po 9. hodině odpoledne, 6. listopadu 1999, vyjádřeno v místním čase.

```
"19991106210627.3Z"
```

je koordinovaný univerzální čas.

```
"19991106210627.3-0500"
```

je místní čas jako v prvním příkladu s pětihodinovým rozdílem s ohledem na koordinovaný univerzální čas.

Pokud zadáváte volitelný zlomek sekundy, je vyžadována tečka nebo čárka. U rozdílu místního času musí hodnotu hodiny-minuty předcházet znak '+' nebo '-'

- Syntaxe univerzálního času, která má formu:

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

V tomto zápise jsou dvě číslice pro každé pole, tedy pro pole roku, měsíce, dne, hodiny, minuty a volitelně sekundy. Tak jako v zobecněném čase (GeneralizedTime) lze zadat volitelný časový rozdíl. Například, jestliže je místní čas dopoledne 2. ledna 1999 a koordinovaný univerzální čas je 12 hodin (poledne) 2. ledna 1999, hodnota času UTCTime je buď:

```
"9901021200Z"
```

nebo

```
"9901020700-0500"
```

Pokud je místní čas dopoledne 2. ledna 2001 a koordinovaný univerzální čas je 12 hodin (poledne) 2. ledna 2001, hodnota času UTCTime je buď:

```
"0101021200Z"
```

nebo

```
"0101020700-0500"
```

UTCTime umožňuje pouze zadávání dvou číslic pro hodnotu roku, proto se jeho použití nedoporučuje.

Podporovaná porovnávací pravidla jsou generalizedTimeMatch pro rovnost a generalizedTimeOrderingMatch pro nerovnost. Vyhledávání podřetězce není povoleno. Platné jsou například tyto filtry:

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

Platné nejsou tyto filtry:

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

Publikování

Operační systém i5/OS poskytuje prostřednictvím systému publikovat v adresáři LDAP určité druhy informací. To znamená, že systém vytvoří a aktualizuje záznamy LDAP představující různé typy dat.

Operační systém i5/OS má vestavěnou podporu publikování následujících informací na serveru LDAP:

Uživatelé

Když konfiguruje operační systém pro publikování informací typu uživatelé na serveru adresářů, automaticky se provede export záznamů z distribučního adresáře systému na server adresářů. K tomu slouží rozhraní API

QGLDSSDD. Toto nastavení také synchronizuje adresář LDAP se změnami prováděnými v systémovém distribučním adresáři. Informace o rozhraní API QGLDSSDD najdete v tématu “Rozhraní API serveru adresářů” v tématu Programování.

Publikování uživatelů je užitečné v případě, že chcete poskytnout serveru LDAP přístup k vyhledávání informací ze systémového distribučního adresáře (například poskytnout přístup k seznamu adres serveru LDAP klientům elektronické pošty typu POP3, jako např. Netscape Communicator nebo Microsoft Outlook Express, oprávněným k tomu serverem LDAP).

Publikování uživatelů je možné použít také k podpoře autentizace LDAP tehdy, když někteří uživatelé jsou publikováni ze systémového distribučního adresáře a jiní uživatelé jsou přidáváni do adresáře jinými prostředky. Publikovaný uživatel má atribut uid, který uvádí jméno uživatelského profilu, a nemá žádný atribut userPassword. Když se obdrží požadavek na spojení pro takovýto druh záznamu, server volá zabezpečení operačního systému, aby se ověřilo, že daný uid a heslo jsou platné pro tento profil. Chcete-li používat autentizaci LDAP a pokud byste chtěli umožnit stávajícím uživatelům provádět autentizaci s využitím jejich hesel operačního systému, zatímco osoby nevyužívající operační systém i5/OS by byly přidávány do adresáře manuálně, měli byste o této funkci uvažovat.

Další možností jak publikovat uživatele je převzít záznamy z existujícího ověřovacího seznamu HTTP a vytvořit odpovídající záznamy v serveru adresářů. K tomu slouží rozhraní API QGLDPUBVL. Toto API vytvoří záznamy adresáře s hesly, které jsou vázány na původní záznam ověřovacího seznamu. API lze spustit jednorázově, nebo lze naplánovat jeho pravidelné spuštění, aby se zkontrolovalo, zda existují nové záznamy a tyto se přidaly do serveru adresářů.

Poznámka: Toto API podporuje pouze záznamy ověřovacích seznamů vytvořené pro použití s HTTP serverem (na bázi Apache). Existující záznamy v serveru adresářů nebudou aktualizovány. Uživatelé, kteří jsou z ověřovacího seznamu vymazáni, se nezaznamenají.

Jakmile jsou uživatelé přidáni do adresáře, mohou se autentizovat do aplikací, které ověřování používají, a také do aplikací, které podporují autentizaci LDAP. Další informace o rozhraní API QGLDPUBVL najdete v tématu “Rozhraní API serveru adresářů” v tématu Programování.

Systémové informace

Když konfiguruje operační systém pro publikování informací systémového typu na server adresářů, budou publikovány tyto typy informací:

- Základní informace o tomto počítači a verzi operačního systému.
- Volitelně si můžete vybrat k publikování jednu nebo více tiskáren, v tom případě bude systém automaticky udržovat adresář LDAP synchronizovaný, pokud se týká změn, které jsou u těchto tiskáren v systému provedeny.

Informace o tiskárnách, které lze publikovat, zahrnují:

- Umístění
- Rychlost ve stránkách za minutu
- Podpora oboustranného tisku a barevného tisku
- Typ a model
- Popis

Tyto informace pocházejí z popisu zařízení v systému, který je publikován. V síťovém prostředí slouží tyto informace uživatelům při výběru tiskárny. Tyto informace se publikují poprvé od okamžiku, kdy je vybrána tiskárna k publikování, a aktualizují se tehdy, když je ukončen nebo spuštěn tiskový program nebo když se změní popis tiskového zařízení.

Sdílení tiskárny

Když konfigurujete operační systém pro publikování sdílení tiskárny, informace o sdílení vybrané tiskárny NetServer iSeries jsou publikovány na konfigurovaném aktivním serveru adresářů. Publikování sdílení tisku v aktivním adresáři umožňuje uživatelům pomocí průvodce v systému Windows 2000 přidat tiskárny systému iSeries na jejich pracovní plochu Windows 2000. K tomu je zapotřebí, abyste v průvodci pro přidání tiskárny zadali, že chcete tiskárnu vyhledat v aktivním adresáři Windows 2000. Sdílení tisku je nutné publikovat na takovém serveru adresářů, který podporuje schéma Microsoft Active Directory.

TCP/IP Quality of Service

Server TCP/IP Quality of Service (QOS) je možné konfigurovat pro použití sdílené zásady QOS definované v adresáři LDAP s využitím definovaného schématu IBM. Publikáčnı agent TCP/IP QOS je využíván serverem QOS ke čtenı informací zásady; definuje server, autentizační informace a umístění, kde jsou v adresáři informace o zásadě uloženy.

Pomocı tohoto vývojového prostředí můžete rovněž vytvořit aplikaci pro publikování nebo vyhledávání jiných druhů informací v adresáři LDAP, k tomu je nutno definovat další publikační agenty a využít rozhraní API pro publikování v adresáři. Další informace najdete v tématu “Publikování informací na server adresářů” na stránce 92 a Rozhraní API serveru adresářů v tématu Programování.

Replikace

Replikace je postup používaný servery adresářů ke zvýšení výkonu a spolehlivosti. Proces replikace udržuje data uložená ve více adresářích synchronizovaná.

Další informace o způsobech správy replikací najdete v tématu “Jak provádět správu replikací” na stránce 129. Chcete-li se o replikacích dozvědět více, prostudujte si tyto části:

- “Přehled replikací”
- “Terminologie replikace” na stránce 39
- “Ujednání o replikacích” na stránce 40
- “Způsob uložení informací replikace na serveru” na stránce 41
- “Hlediska zabezpečení ochrany dat pro informace replikace” na stránce 41
- “Replikace v prostředí s vysokou dostupností” na stránce 41

Přehled replikací

Replikace poskytuje dvě hlavní výhody:

- Zdvojení informací - repliky zálohují obsah svých dodavatelských serverů.
- Rychlejší vyhledávání - požadavky na hledání mohou být namísto uloženy na jediném serveru rozloženy mezi několik různých serverů, které uchovávají stejný obsah. To zlepšuje dobu odezvy pro splnění požadavku.

Specifické záznamy v adresáři jsou doplněním třídy objektu `ibm-replicationContext` označeny jako kořeny replikovaných podstromů. Každý podstrom je replikován samostatně. Podstrom pokračuje dolů podél informačního stromu adresáře DIT (directory information tree), až dosáhne listových záznamů nebo jiných replikovaných podstromů. Pod kořen replikovaného podstromu se přidávají záznamy, které budou obsahovat informace o topologii replikace. Tyto záznamy tvoří jednu nebo více replikačních skupin, pod nimiž se vytvářejí podzáznamy repliky. Ke každému replikačnímu podzáznamu jsou přiřazena ujednání o replikaci označující servery, které jsou každým serverem zabezpečovány (replikovány), ale také definice pověření a informace o časovém plánu.

Prostřednictvím replikace se změny provedené na jednom adresáři propagují (šíří) do jednoho nebo více dodatečných adresářů. Změna jednoho adresáře se ve skutečnosti projeví v několika různých adresářích. Adresář IBM podporuje rozšířený model replikace master-subordinate (hlavnı-podřízený). Topologie replikace se rozšřirují tak, aby zahrnovaly:

- Replikaci podstromů DIT (Directory Information Tree - informačního stromu adresáře) na určité servery.
- Vícevrstevnou topologii, která se označuje jako kaskádová replikace.
- Přiřazenı role serveru (hlavnı nebo replika) podstromem.

- Vícenásobné hlavní servery, což se označuje jako replikace peer to peer.
- Replikace přes brány v rámci sítí.

Výhodou replikace podle podstromů je to, že replika nemusí replikovat celý adresář. Je možné replikovat pouze část neboli podstrom adresáře.

Rozšířený model mění koncepci hlavního serveru a repliky. Tyto výrazy už nadále neplatí pro servery, ale spíše pro role, které má server plnit v souvislosti s konkrétním replikovaným podstromem. Server může pracovat pro některé podstromy jako hlavní server a pro jiné jako replika. Výraz hlavní server se používá pro server, který přijímá aktualizace klientů pro replikovaný podstrom. Výraz replika se používá pro server, který přijímá pouze aktualizace z jiných serverů určených za dodavatele replikovaného podstromu.

Typy serverů definované podle funkcí při replikaci jsou: *hlavní/peer*, *kaskádový*, *brána* a *replika*.

Tabulka 1. Role serverů

Adresář	Popis
Hlavní/peer	<p>Hlavní/peer server obsahuje informace o adresáři hlavního serveru, z něhož jsou šířeny aktualizace do replik. Všechny změny se provádějí a vyskytují na hlavním serveru a tento hlavní server je odpovědný za šíření těchto změn do replik.</p> <p>V systému může být několik serverů pracujících jako hlavní servery pro informace o adresáři, přičemž každý hlavní server je odpovědný za aktualizaci ostatních hlavních serverů a replikovaných serverů. To se označuje za peerovou replikaci. Peerová replikace může zvýšit výkon a spolehlivost. Zvýšení výkonu se dosahuje použitím místního serveru, který obsluhuje aktualizace v široce distribuované síti. Zvýšení spolehlivosti se dosahuje použitím záložního hlavního serveru připraveného okamžitě převzít roli hlavního serveru, pokud by primární hlavní server selhal.</p> <p>Poznámky:</p> <ol style="list-style-type: none"> 1. Hlavní servery replikují všechny klientské aktualizace, ale nereplikují aktualizace obdržené od ostatních hlavních serverů. 2. Aktualizace stejného záznamu provedené několika servery by mohly způsobit nekonzistence v datech adresáře, protože zde neexistuje řešení konfliktů.
Kaskádový (předávací)	Kaskádový server je replikovaný server, který replikuje všechny změny, které jsou na něj zaslány. Tím se liší od hlavního/peer serveru, neboť hlavní/peer server replikuje pouze změny, které jsou prováděny klienty připojenými k tomuto serveru. Kaskádový server může odlehčit replikační zatížení hlavních serverů v síti, která obsahuje mnoho velmi rozptýlených replik.
Brána	Replikace přes brány využívá servery bran k efektivnímu shromažďování a distribuci informací týkajících se replikace v síti, kde replikace probíhá. Hlavním přínosem replikace přes brány je snížení provozu v síti.
Replika (pouze pro čtení)	Replika je přídatný server, který obsahuje kopii informací adresáře. Repliky jsou kopie hlavního serveru (nebo podstromu, jehož je replikou). Replika zajišťuje zálohování replikovaného podstromu.

Pokud replikace selže, opakuje se i tehdy, když bude hlavní server restartován. Pro kontrolu nezdařených replikací je možné použít okno Manage Queues ve webovém nástroji administrace serveru.

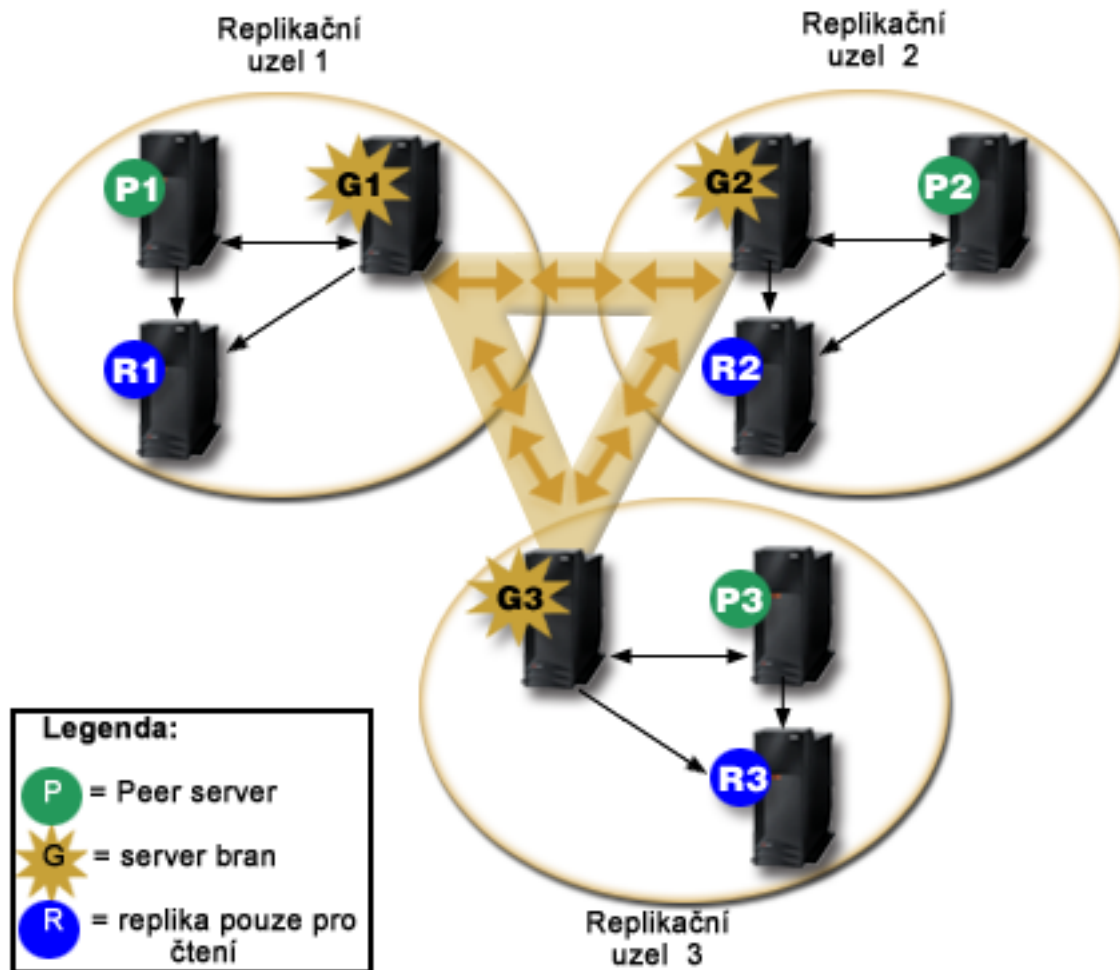
Všechny aktualizace je možno požadovat na replikovaném serveru, ale jednotlivé aktualizace se ve skutečnosti předávají na hlavní server vrácením odkazu klientovi. Jestliže je aktualizace úspěšná, hlavní server rozešle aktualizaci na jednotlivé repliky. Do doby, než hlavní server dokončí replikaci aktualizace, se změna neodrazí na replikovaném serveru, kde byla původně požadována. Změny se replikují v pořadí, ve kterém jsou prováděny na hlavním serveru.

Pokud už repliku nepoužíváte, musíte dodavateli odebrat souhlas s replikací. Ponechání definice způsobuje, že server řadí všechny aktualizace do fronty a užívá nepotřebný prostor adresáře. Kromě toho se dodavatel stále pokouší navazovat spojení s chybějícím odběratelem a znovu mu zasílat příslušná data.

Replikace přes brány

Replikace přes brány využívá servery bran k efektivnímu shromažďování a distribuci informací týkajících se replikace v síti, kde replikace probíhá. Hlavním přínosem replikace přes brány je snížení provozu v síti. Servery bran musí být hlavní (schopné zápisu).

Následující obrázek znázorňuje, jak replikace přes brány funguje:



Obrázek 2. Replikovaná síť se servery bran

Replikovaná síť na předcházejícím obrázku obsahuje tři replikační uzly, z nichž každý obsahuje server brány. Server brány shromažďuje replikační aktualizace z hlavních/peer serverů replikačního uzlu, ve kterém se nachází, a posílá aktualizace všem ostatním serverům bran v rámci replikované sítě. Shromažďuje také replikační aktualizace od ostatních serverů bran v replikované síti a posílá tyto aktualizace na hlavní/peer servery a replikované servery v replikačním uzlu, kde se nachází.

Servery bran používají ID serverů a ID odběratelů, aby určily, které aktualizace mají poslat ostatním serverům bran a které aktualizace mají poslat lokálním serverům v rámci replikačního uzlu.

Chcete-li nastavit replikaci přes brány, musíte vytvořit alespoň dva servery bran. Vytvořením serveru brány vytváříte replikační uzel. Pak musíte vytvořit ujednání o replikaci mezi bránou a veškerými hlavními/peer servery a replikovanými servery, které chcete zahrnout do replikačního uzlu dané brány.

Servery bran musí být hlavní (schopné zápisu). Budete-li se pokoušet přidat třídu objektu brány - `ibm-replicaGateway` - k podzápisu, který není hlavní, vrátí se vám chybová zpráva.

- | Existují dvě metody vytvoření serveru brány. Máte tyto možnosti:
 - | • Vytvořit nový server brány.
 - | • Převést existující peer server na server brány.
- | **Poznámka:** Je velmi důležité, abyste přiřadili pouze jeden server brány na replikační uzel.

Terminologie replikace

Některé výrazy používané při popisování replikace:

Kaskádová replikace

Topologie replikace, v níž existuje několik vrstev serverů. Peer/hlavní server replikuje na sadu serverů pouze pro čtení (předávacích), které na oplátku replikují na další servery. Taková topologie odnímá zatížení replikační práce z hlavních serverů.

Odběratelský server

Server, který přijímá změny prostřednictvím replikace z jiného (dodavatelského) serveru.

Pověření

Označuje metodu a potřebné informace, které dodavatel používá pro připojení k odběrateli. U jednoduchých připojení sestává toto pověření z DN a hesla. Pověření jsou uchovávána v záznamu, jehož DN je uvedeno v ujednání o replikaci.

Předávací server

Server pouze pro čtení, který replikuje všechny změny na něj zasílané z hlavního nebo peer serveru. Klientovy požadavky na aktualizaci se předávají na hlavní nebo peer server.

Server brány

- | Server, který přeposílá veškerý replikační provoz z lokálního replikačního uzlu, kde se nachází, dalším
- | serverům bran v replikované síti. Server brány přijímá replikační provoz z ostatních serverů bran v rámci
- | replikované sítě, který pak přeposílá všem serverům ve svém lokálním replikačním uzlu. Servery bran musí
- | být hlavní servery (schopné zápisu).

Hlavní server

Server, který je schopný zápisu (lze jej aktualizovat) pro daný podstrom.

Vnořený podstrom

Podstrom uvnitř replikovaného podstromu adresáře.

Peer server

Výraz používaný pro hlavní server v případě, že daný podstrom obsahuje několik hlavních serverů.

Skupina replik

První záznam vytvořený pod kontextem replikace má třídu objektu "ibm-replicaGroup" a představuje kolekci serverů účastnících se na replikaci. Poskytuje příhodné místo pro nastavení seznamů přístupových práv ACL tak, aby chránily informace o topologii replikace. Nástroje administrace v současnosti podporují jednu skupinu replik pod každým kontextem replikace, nazývanou **ibm-replicagroup=default**.

Podzáznam repliky

Pod záznamem skupiny replik je možno vytvořit jeden nebo více záznamů s třídou objektu "ibm-replicaSubentry"; jeden pro každý server účastnící se na replikaci jako dodavatel. Podzáznam repliky určuje roli, kterou tento server hraje v replikaci: hlavní server nebo pouze pro čtení. Server pouze pro čtení by mohl naopak obsahovat ujednání o replikaci pro podporu kaskádových replikací.

Replikovaný podstrom

Část DIT, která je replikována z jednoho serveru na druhý. Podle tohoto rozvržení může být daný podstrom replikován pouze na určité servery a nikoli na jiné. Určitý podstrom může být schopný zápisu na daném serveru, zatímco jiné podstromy mohou být pouze pro čtení.

Replikovaná síť

Síť, která obsahuje spojené replikační uzly.

Ujednání o replikaci

Informace obsažené v adresáři, které definují 'propojení' nebo 'replikační cestu' mezi dvěma servery. Jeden server je označován jako dodavatelský (server, který zasílá změny) a další je odběratelský (server, který přijímá změny). Ujednání obsahuje všechny informace potřebné pro vytvoření propojení od dodavatele k odběrateli a k naplánování replikace.

Kontext replikace

Označuje kořen replikovaného podstromu. Do záznamu může být přidána pomocná třída objektu `ibm-replicationContext`, která jej označuje jako kořen replikované oblasti. V sadě záznamů vytvořených pod kontextem replikace se uchovávají informace související s topologií replikace.

Replikační uzel

Server brány a veškeré další hlavní, peer nebo replikované servery konfigurované pro společnou replikaci.

Časový plán

U replikací je možné naplánovat, že budou prováděny v konkrétní dobu, přičemž změny u dodavatele se budou shromažďovat u dodavatele a posílat v dávce. Ujednání o replikaci obsahuje DN pro záznam, který takový časový plán zajišťuje.

Dodavatelský server

Server, který posílá změny na jiný (odběratelský) server.

Ujednání o replikacích

Ujednání o replikaci je záznam v adresáři s třídou objektu **ibm-replicationAgreement** vytvořený pod replikovaným podzáznamem s cílem definovat replikaci ze serveru reprezentovaného tímto podzáznamem na jiný server. Tyto objekty jsou podobné záznamům `replicaObject` používaným dřívějšími verzemi serveru adresářů. Ujednání o replikaci se skládá z těchto položek:

- Uživatelsky příjemné jméno, používané jako atribut pojmenování pro toto ujednání.
- URL LDAP určující server, číslo portu a instrukce o tom, zda by se mělo použít SSL.
- ID odběratelského serveru, pokud je znám. Servery adresářů ve verzích předcházejících V5R3 neměly ID serveru.
- DN objektu obsahujícího pověření používané dodavatelem pro připojení k odběrateli.
- Volitelný ukazatel DN na objekt obsahující informace o časovém plánu replikace. Pokud tento atribut není stanoven, změny se replikují okamžitě.

Uživatelsky příjemné jméno by mohlo být jméno odběratelského serveru nebo některý jiný popisný řetězec.

ID odběratelského serveru se používá v grafickém uživatelském rozhraní k překlenutí topologie. S daným ID odběratelského serveru může rozhraní GUI najít odpovídající podzáznam a jeho ujednání. Za tím účelem, aby mohl dodavatel vynutit správnost dat při připojování k odběrateli, načítá ID serveru z kořenového DSE a porovnává jej s hodnotou ujednání. Pokud ID serveru nesouhlasí, je zaprotokolováno varování.

Ujednání o replikaci může být replikováno, proto se používá DN objektů pověření. To umožňuje ukládat pověření v nereplikované oblasti adresáře. Replikace objektů pověření (z nichž musí být možné obdržet pověření s 'jasným textem') představuje potenciální bezpečnostní riziko. Vhodné předvolené umístění pro vytváření objektů pověření je přípona `cn=localhost`.

Pro každou z podporovaných metod autentizace jsou definovány třídy objektů:

- jednoduché připojení
- SASL
- mechanismus EXTERNAL s SSL
- autentizace Kerberos

Část replikovaného podstromu, která se nemá replikovat, je možné určit přidáním pomocné třídy `ibm-replicationContext` do kořene podstromu bez definování jakýchkoli podzáznamů repliky.

Poznámka: V souvislosti se sadou změn, které čekají na replikaci podle daného ujednání, označuje webový nástroj administrace tato ujednání také jako 'fronty'.

Způsob uložení informací replikace na serveru

Informace replikace jsou uloženy v adresáři na třech místech:


- Konfigurace serveru, která obsahuje informace o tom, jak se jiné servery mohou autentizovat na tomto serveru, aby mohly provést replikaci (například, komu tento server povolí jednat v úloze dodavatele).
- V adresáři v nejvyšší části replikovaného podstromu. Jestliže je nejvyšší částí replikovaného podstromu "o=my company", přímo pod ní bude vytvořen objekt pojmenovaný "ibm-replicagroup=default" (ibm-replicagroup=default,o=my company). Pod objektem "ibm-replicagroup=default" budou další objekty, které popisují servery uchováající repliky podstromu a ujednání mezi servery.
- Pro uchovávání informací o replikaci, které využívá pouze jeden server, se používá objekt pojmenovaný "cn=replication,cn=localhost". Například objekty obsahující pověření používaná dodavatelským serverem jsou vyžadovány pouze dodavatelským serverem. Pověření je možné umístit pod "cn=replication,cn=localhost", což je zpřístupňuje pouze pro tento server.
- Pro uchovávání informací o replikaci, které jsou replikovány na ostatní servery, se používá objekt pojmenovaný "cn=replication,cn=IBMpolicies".

Hlediska zabezpečení ochrany dat pro informace replikace

Proveďte posouzení hledisek zabezpečení ochrany dat pro tyto objekty:

- **ibm-replicagroup=default:** Řízení přístupu na tomto objektu určuje, kdo může prohlížet nebo měnit zde uložené informace o replikaci. Standardně tento objekt dědí řízení přístupu od svého nadřazeného objektu. Měli byste zvážit nastavení řízení přístupu na tomto objektu tak, aby se omezil přístup k informacím o replikaci. Mohli byste například definovat skupinu obsahující uživatele, kteří budou provádět správu replikací. Tato skupina by mohla být určena vlastníkem objektu "ibm-replicagroup=default" a jiní uživatelé nebudou mít k tomuto objektu přidělen přístup.
- **cn=replication,cn=localhost:** Pro tento objekt platí dvě hlediska týkající se zabezpečení ochrany dat:
 - Řízení přístupu na tomto objektu určuje, komu je povoleno prohlížet nebo aktualizovat zde uložené objekty. Předvolené řízení přístupu umožňuje anonymním uživatelům číst většinu informací s výjimkou hesel a vyžaduje administrátorské oprávnění pro přidávání, změny nebo mazání objektů.
 - Objekty uložené v "cn=localhost" se nikdy nereplikují na jiné servery. Do tohoto zásobníku můžete umísťovat pověření replikace na server, který pověření používá, a tato pověření nebudou přístupná pro jiné servery. Případně se můžete rozhodnout umístit pověření pod objekt "ibm-replicagroup=default", aby stejná pověření mohlo sdílet více serverů.
- **cn=IBMpolicies:** Pověření replikace můžete umístit do tohoto zásobníku, ale data v něm umístěná se replikují jakémukoliv odběrateli serveru. Umístění v cn=replication,cn=localhost je pro pověření považováno za bezpečnější.

Replikace v prostředí s vysokou dostupností

- Server adresářů se často využívá v řešeních pro jedno přihlašování (SSO), což může mít za následek vznik jednoho bodu selhání. Vysokou dostupnost serveru adresářů lze za použití replikace zajistit dvěma způsoby: použitím produktu IBM Load Balancer nebo přebíráním IP adres. Další informace k tomuto tématu najdete v kapitole 13.2 červené knihy IBM IBM WebSphere V5.1 Performance, Scalability, and High Availability. 

Sféry a uživatelské šablony

Objekty sfér a uživatelských šablon nalézající se ve webovém nástroji administrace se používají pro osvobození uživatele od nutnosti do podrobností znát některé ze základních otázek LDAP.

Sféra označuje kolekci uživatelů a skupin. V jasné adresářové struktuře uvádí např. informace o tom, kde jsou umístěni uživatelé a kde jsou umístěny skupiny. Sféra definuje umístění pro uživatele (např. "cn=users,o=acme,c=us") a vytváří uživatele jako přímé podřízené tohoto záznamu (například John Doe je vytvořen jako "cn=John

Doe,cn=users,o=acme,c=us"). Je možné definovat více sfér a dát jim známá jména (například Web Users). Znamé jméno mohou používat lidé, kteří vytvářejí uživatele a vykonávají jejich správu.

Šablona popisuje, jak uživatel vypadá. Uvádí třídy objektů, které se používají při tvorbě uživatelů (jak strukturní třídu objektu, tak jakékoli pomocné třídy, které pro objekt požadujete). Šablona rovněž určuje rozvržení panelů používaných pro tvorbu nebo editaci uživatelů (například jména karet, předvolené hodnoty a atributy, které se mají objevit na každé kartě).

Když přidáte novou sféru, vytvoříte v adresáři objekt `ibm-realm`. Objekt `ibm-realm` sleduje takové vlastnosti sféry, jako jsou například informace o tom, kde jsou definováni uživatelé a skupiny a která šablona se má použít. Objekt `ibm-realm` může ukazovat na existující záznam adresáře, který je nadřazeným záznamem uživatelů nebo může ukazovat sám na sebe (předvolená hodnota), což z něj činí zásobník pro nové uživatele. Například byste mohli mít existující `cn=users,o=acme,c=us` container a kdekoli v adresáři vytvořit sféru nazvanou `USERS` (případně také objekt zásobníku nazvaný `cn=realms,cn=admin stuff,o=acme,c=us`), který označuje `cn=users,o=acme,c=us` jako umístění pro uživatele a skupiny. To vytvoří objekt `ibm-realm`:

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

Nebo, pokud by neexistoval žádný objekt `cn=users,o=acme,c=us`, byste mohli vytvořit sféru `USERS` pod `o=acme,c=us` a nechat ji ukazovat na ni samotnou.

Administrátor adresáře je odpovědný za správu uživatelských šablon, sfér a administrátorských skupin sféry. Po vytvoření sféry jsou členové administrátorské skupiny této sféry odpovědní za správu uživatelů a skupin uvnitř této sféry.

Další informace o způsobu správy sfér a uživatelských šablon najdete v tématu “Jak provádět správu sfér a uživatelských šablon” na stránce 174.

Parametry prohledávání

Za účelem omezení množství zdrojů, které server používá, může administrátor nastavit parametry prohledávání tak, aby omezil prohledávací schopnosti uživatelů. Prohledávací schopnosti lze také pro určité uživatele rozšířit. Uživatelská hledání lze omezit nebo rozšířit pomocí těchto metod:

Omezit hledání

- Stránkované hledání
- Tříděné hledání
- Zablokování dereference aliasů

Rozšířit hledání

- Skupiny s limity hledání

Stránkované hledání

Výsledky stránkovaného hledání umožňují klientovi řídit objem dat vrácených z požadavku na hledání. Klient může požadovat zaslání podmnožiny záznamů (stránku) namísto obdržení všech výsledků ze serveru najednou. Následné požadavky na hledání zobrazují další stránky výsledků do té doby, než je operace zrušena nebo než je vrácen poslední výsledek. Administrátor může omezit použití tohoto typu hledání a povolit jeho použití jen administrátorům.

| Tříděné hledání

| Tříděné hledání umožňuje klientu získávat výsledky prohledávání seříděné podle seznamu kritérií, kde každé kritérium představuje třídící klíč. To přenáší odpovědnost za třídění z klientské aplikace na server. Administrátor může omezit použití tohoto typu hledání a povolit jeho použití jen administrátorům.

| Zablokování dereference aliasů

| Záznam adresáře s třídou objektu alias nebo aliasObject obsahuje atribut aliasedObjectName, který se používá pro odkazování na další záznam v adresáři. Pouze požadavky na hledání mohou specifikovat, zda u aliasů bude probíhat dereference. *Dereference* znamená sledování aliasu zpátky k původnímu záznamu. Doba odezvy serveru adresářů IBM u hledání, kde je volba dereference aliasů nastavena na hodnotu **always** nebo **search**, může být výrazně delší, než když je volba dereference aliasů nastavena na hodnotu **never**, a to i když v adresáři neexistují žádné záznamy aliasů. Chování serveru ohledně dereference aliasů určují dvě nastavení: volba dereference zadaná v klientově požadavku na hledání a volba dereference nakonfigurovaná na serveru administrátorem. Pokud je server takto nakonfigurovaný, může automaticky vynechávat dereferenci aliasů v případě, že v adresáři neexistují žádné objekty aliasů, a také může přepisovat volbu dereference zadanou v klientově požadavku na hledání. Níže uvedená tabulka popisuje, jak bude vypadat výsledná dereference aliasů při různých nastaveních na serveru a klientu.

| *Tabulka 2. Skutečná dereference aliasů na základě nastavení na serveru a klientu*

Server	Klient	Skutečnost
never	jakékoliv nastavení	never
always	jakékoliv nastavení	nastavení klienta
jakékoliv nastavení	always	nastavení serveru
search	find	never
find	search	never

| Skupiny s limity hledání

| Administrátor může vytvořit tzv. skupiny s limity hledání (search limit group), které mohou mít flexibilnější limity hledání než běžný uživatel. Jednotlivým členům nebo skupinám zahrnutým do skupiny s limity hledání jsou poskytnuty méně omezující limity hledání, než jsou limity uplatňované pro běžné uživatele.

| Když uživatel iniciuje prohledávání, nejprve se kontrolují omezení požadavku na hledání. Je-li uživatel členem skupiny s limity hledání, tato omezení se porovnají. Jsou-li omezení skupiny s limity hledání vyšší než omezení požadavku na hledání, použijí se omezení požadavku na hledání. Jsou-li omezení požadavku na hledání vyšší než omezení skupiny s limity hledání, použijí se omezení skupiny s limity hledání. Nejsou-li nalezeny žádné záznamy skupiny s limity hledání, provede se stejné porovnání vůči omezením hledání serveru. Pokud nebyla nastavena žádná omezení hledání serveru, provede se porovnání vůči předvolenému nastavení serveru. Použitá omezení jsou vždy ta nejnižší nastavení v provedeném porovnání.

| Patří-li uživatel do více skupin s limity hledání, poskytne se uživateli nejvyšší možná úroveň možností hledání. Například uživatel patří do skupiny vyhledávání 1, která uděluje limity pro rozsah vyhledávání ve výši 2000 záznamů a pro dobu vyhledávání ve výši 4000 vteřin, a zároveň patří do skupiny vyhledávání 2, která uděluje limity pro rozsah vyhledávání v neomezeném počtu záznamů a pro dobu vyhledávání ve výši 3000 vteřin. Tento uživatel má pak limity hledání následující: rozsah vyhledávání neomezený a doba vyhledávání 4000 vteřin.

| Skupiny s limity hledání mohou být uloženy buď pod localhost nebo IBMpolices. Skupiny s limity hledání pod IBMpolices jsou replikovány; skupiny pod localhost replikovány nejsou. Stejnou skupinu s limity hledání můžete uložit jak pod localhost tak pod IBMpolices. Není-li skupina s limity hledání uložena pod jedním z těchto DN, server ignoruje část s limity omezení skupiny a pracuje s ní jako s normální skupinou.

l Když uživatel iniciuje prohledávání, nejprve se kontrolují záznamy skupin s limity hledání pod localhost. Nenajde-li se pro daného uživatele žádný záznam, prohledají se dále záznamy skupin s limity hledání pod IBMpolicies. Jsou-li nalezeny pod localhost nějaké záznamy, záznamy skupin s limity hledání pod IBMpolicies se nekontrolují. Záznamy skupin s limity hledání pod localhost mají přednost před záznamy pod IBMpolicies.

l Další informace o parametrech prohledávání najdete v tématech:

- l • “Jak přizpůsobit nastavení vyhledávání” na stránce 124
- l • “Jak prohledávat záznamy adresáře” na stránce 169
- l • “Jak spravovat skupiny s limity hledání” na stránce 119

Pravidla pro podporu národního jazyka (NLS)

Je nutné mít na paměti tato hlediska NLS:

- Data mezi servery LDAP a klienty se přenášejí ve formátu UTF-8. Jsou povoleny všechny znaky ISO 10646.
- Server adresářů používá pro 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 (lokality).

Více informací o UCS-2 najdete v tématu “Globalizace” v tématu Plánování.

Jazykové příznaky

l Termín *jazykové příznaky* definuje mechanismus, který umožňuje adresáři asociovat kódy přirozeného jazyka s hodnotami uloženými v adresáři a umožňuje klientům dotazovat se v adresáři na hodnoty, které odpovídají požadavkům určitého přirozeného jazyka. Jazykový příznak je komponentou popisu atributu. Jazykový příznak je řetězec s předponou lang-, primární podpříznak tvoří abecední znaky a volitelné dodatečné podpříznaky jsou připojeny pomlčkou (-). Dodatečné podpříznaky mohou tvořit libovolné kombinace alfanumerických znaků; pouze primární podpříznak musí tvořit abecední znaky. Podpříznaky mohou být libovolně dlouhé; jediným omezením je, že celková délka příznaku nesmí přesáhnout 240 znaků. Jazykové příznaky nerozlišují malá a velká písmena; en-us a en-US a EN-US jsou identické. Jazykové příznaky nejsou povoleny v komponentách DN nebo RDN. Na jeden popis atributu je povolen pouze jeden jazykový příznak.

l **Poznámka:** Co se týče jednotlivých atributů, jazykové příznaky jsou u jedinečných atributů vzájemně exkluzivní. Pokud jste určitý atribut označili za jedinečný atribut, nemůže mít k sobě přiřazený jazykové příznaky.

l Jsou-li při přidávání dat do adresáře součástí jazykové příznaky, mohou se využít při operacích prohledávání pro selektivní získání hodnot atributu ve specifickém jazyku. Je-li v popisu atributu v rámci seznamu požadovaných atributů hledání uveden nějaký jazykový příznak, pak by se měly vrátit pouze ty hodnoty atributu v záznamu adresáře, které mají stejný jazykový příznak jako je uvedený příznak. Takže například pro hledání typu:

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

l server vrátí hodnoty atributu "description;lang-en", ale nevrátí hodnoty atributu "description" nebo "description;lang-fr".

l Pokud se zadá požadavek specifikující atribut bez uvedení jazykového příznaku, pak se vrátí všechny hodnoty atributu bez ohledu na jejich jazykový příznak.

l Typ atributu a jazykový příznak se oddělují znakem středníku (;).

l **Poznámka:** Znak středníku je možno používat v části jména typu atributu. Avšak protože se tento znak používá k oddělení typu atributu od jazykového příznaku, jeho použití v názvu typu atributu není povoleno.

l Například jestliže klient požaduje atribut "description" a odpovídající záznam obsahuje:

```
l objectclass: top  
l objectclass: organization  
l o: Software GmbH
```

```
| description: software
| description;lang-en: software products
| description;lang-de: Softwareprodukte
| postalAddress: Berlin 8001 Germany
| postalAddress;lang-de: Berlin 8001 Deutschland
```

| server vrátí:

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

| Pokud hledání požaduje atribut "description;lang-de", pak server vrátí:

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

| Použití jazykových příznaků umožňuje mít v adresáři vícejazyčná data, a tak podporovat klienty, kteří pracují v různých jazycích. S využitím jazykových příznaků lze napsat aplikaci tak, že německý klient vidí pouze data zadaná pro atribut lang-de a francouzský klient vidí pouze data zadaná pro atribut lang-fr.

| Chcete-li zjistit, zda je funkce jazykových příznaků povolena, zadejte prohledávání kořenového DSE specifikující atribut "ibm-enabledCapabilities".

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

| Vrátili-li se OID "1.3.6.1.4.1.4203.1.5.4", je tato funkce povolena.

| Pokud podpora jazykových příznaků není povolena, budou veškeré LDAP operace, které k atributu přiřazují nějaký jazykový příznak, zamítnuty s chybovou zprávou.

| Některé atributy k sobě mohou mít přiřazen jazykový příznak, jiné ho mít přiřazen nemohou. Chcete-li zjistit, zda lze k určitému atributu přiřadit jazykový příznak, použijte příkaz ldapexop:

- Pro atributy, které povolují jazykové příznaky: ldapexop -op getattributes -attrType language_tag -matches true
- Pro atributy, které nepovolují jazykové příznaky: ldapexop -op getattributes -attrType language_tag -matches false

| Další informace najdete v tématu "Jak přidat záznam obsahující atribut s jazykovým příznakem" na stránce 166.

Odkazy v adresáři LDAP

Odkazy umožňují serverům adresářů 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 Server adresářů umožňuje používat dva různé typy odkazů. Je možné určit předvolené referenční servery, na které bude server LDAP odkazovat klienty, kdykoli nebude požadované DN v jeho adresáři. Pomocí klienta LDAP můžete rovněž přidávat záznamy na server adresářů, který má odkaz objectClass. To umožňuje specifikovat odkazy na základě toho, jaké konkrétní DN klient požaduje.

Poznámka: V produktu Server adresářů smí referenční objekt obsahovat pouze rozlišovací jméno (dn), třídu objektu (objectClass) a atribut odkazu (ref). V části "ldapsearch" na stránce 202 najdete příklad, který ilustruje toto omezení.

Referenční servery blíže 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 můžete v systému konfigurovat tak, aby klientům umožnil používání transakcí (další informace o způsobech konfigurace nastavení transakcí najdete v tématu “Jak specifikovat nastavení transakcí” na stránce 115). Transakce je skupina operací adresáře LDAP, s nimiž 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 v uspořádaném stavu. 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 LDAP:

- 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.

Server adresářů - Zabezpečení ochrany dat

Jestliže potřebujete další informace o zabezpečení ochrany dat serveru adresářů, prostudujte si tyto části:

- “Monitorování”
- “SSL (Secure Sockets Layer) a TLS (Transport Layer Security) u serveru adresářů” na stránce 47
- “Autentizace Kerberos na serveru adresářů” na stránce 47
- “Skupiny a role” na stránce 48
- “Administrativní přístup” na stránce 54
- “Proxy autorizace” na stránce 55
- “Seznamy přístupových práv” na stránce 55
- “Vlastnictví objektů adresáře LDAP” na stránce 67
- “Zásada pro správu hesel” na stránce 67
- “Autentizace” na stránce 70
- “Odmítnutí služeb” na stránce 73

Související koncept

“Jak spravovat vlastnosti zabezpečení” na stránce 147

Monitorování

Server adresářů podporuje monitorování zabezpečení ochrany dat operačního systému i5/OS. Monitorovat můžete:

- připojení a odpojení od serveru adresářů
- změny povolení pro objekty adresáře LDAP
- změny vlastnictví objektů adresáře LDAP
- vytváření, odstraňování, vyhledávání a změny objektů adresáře LDAP
- změny hesla administrátora a aktualizace rozlišovacích jmen (DN)
- změny hesel uživatelů
- import a export souborů

Před zahájením monitorování záznamů adresáře budete možná muset změnit nastavení funkce monitorování. Je-li u systémové hodnoty QAUDCTL zadáno *OBJAUD, můžete aktivovat monitorování objektů prostřednictvím produktu iSeries Navigator. Další informace o monitorování najdete v publikaci *Zabezpečení ochrany dat - reference*



nebo v tématu “ Monitorování zabezpečení ochrany dat”.

SSL (Secure Sockets Layer) a TLS (Transport Layer Security) u serveru adresářů

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

SSL je standardem pro zabezpečení 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 nutné mít v systému nainstalován produkt DCM (Digital Certificate Manager), což je volba 34 operačního systému i5/OS. DCM poskytuje rozhraní, které slouží k vytváření a správě digitálních certifikátů a paměti certifikátů. Další informace o digitálních certifikátech a používání DCM najdete v tématu “ Digital Certificate Manager”. Pokud se chcete dozvědět další informace o použití SSL na serveru iSeries, prostudujte si téma “Secure Sockets Layer (SSL)”.

| TLS je navrženo jako následník protokolu SSL a používá stejné šifrovací metody, ale podporuje více šifrovacích
| algoritmů. Informace o TLS (Transport Layer Security) na serveru iSeries najdete v tématu Podporované protokoly
| SSL a TLS. TLS umožňuje serveru přijímat zabezpečené a nezabezpečené komunikace z klienta přes předvolený port
| 389. U zabezpečených komunikací musí klient používat přídatnou operaci StartTLS.

K tomu, aby mohl klient používat TLS:

1. Server adresářů musí být nakonfigurován pro použití TLS nebo SSLTLS. Další informace najdete v tématu “Jak aktivovat SSL a TSL (Transport Layer Security) na serveru adresářů” na stránce 151.
2. V obslužném programu příkazové řádky klienta musí být zadána volba -Y.

Poznámka: TLS a SSL nejsou interoperabilní. Vydání požadavku na zahájení TLS (volba -Y) přes port SSL způsobí operační chybu.

Klient se může připojit na zabezpečený port (636) buď za použití TLS nebo SSL. StartTLS je funkce LDAP, která vám umožní spustit zabezpečenou komunikaci přes existující nezabezpečené spojení (tj. port 389). Jako takovou můžete funkci StartTLS (nebo volbu -Y obslužného programu příkazové řádky) použít pouze se standardním nezabezpečeným portem (389); nemůžete použít StartTLS u zabezpečeného připojení.

Další informace najdete v tématu “Jak aktivovat SSL a TSL (Transport Layer Security) na serveru adresářů” na stránce 151.

Autentizace Kerberos na serveru adresářů

Produkt Server adresářů umožňuje používat autentizaci 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 nutno mít provedenou konfiguraci služby síťové autentizace.

Podpora produktu Server adresářů protokolem Kerberos obsahuje podporu mechanismu GSSAPI SASL. Ten umožňuje klientům LDAP serveru adresářů a Windows 2000 používat na serveru adresářů autentizaci Kerberos.

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

jméno-sluzby/jméno-hostitele@sfera

Jméno-slужby je "ldap" (ldap musí být zapsáno malými písmeny), jméno-hostitele je plně kvalifikované TCP/IP jméno systému a sféra je předvolená sféra zadaná v systémové konfiguraci Kerberos.

Například u systému pojmenovaného my-as400 v TCP/IP doméně acme.com a s předvolenou sférou Kerberos ACME.COM by bylo hlavní jméno serveru LDAP pro Kerberos ldap/my-as400.acme.com@ACME.COM . Předvolená sféra Kerberos je uvedena v konfiguračním souboru produktu Kerberos (standardně je to soubor /QIBM/UserData/OS400/NetworkAuthentication/krb5.conf) s direktivou "default_realm" (default_realm = ACME.COM). Server adresářů nelze pro použití autentizace Kerberos nakonfigurovat, není-li předtím nastavena předvolená sféra.

Při použití autentizace Kerberos přidruží server adresářů rozlišovací jméno (DN) k připojení, 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". Jméno ibm-kn= je ekvivalentem k ibm-kerberosName=.
- Server může v adresáři vyhledat rozlišovací jméno (DN), které obsahuje záznam o hlavním jménu a sféře Kerberos. Jestliže vyberete tuto volbu, bude server v adresáři hledat záznam, který udává tuto identitu Kerberos.

Je nezbytné, 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 v tématu Služby síťové autentizace pod heslem Zabezpečení. Část Konfigurace služby síťové autentizace popisuje, jak přidávat informace do souboru s tabulkou klíčů.

Skupiny a role

Skupina je seznam, kolekce jmen. Skupiny je možné používat v attributech **acentry**, **ibm-filterAclEntry** a **entryowner** při řízení přístupu, nebo se uplatňují ve využitích specifických pro určité aplikace, jako je např. poštovní seznam; viz "Seznamy přístupových práv" na stránce 55. Skupiny je možné definovat jako statické, dynamické nebo vnořené. Další informace o metodách práce se skupinami najdete v tématu "Jak provádět správu uživatelů a skupin" na stránce 172.

Role jsou podobné skupinám v tom, že jsou v adresáři znázorněny objektem. Role kromě toho obsahují skupinu jmen DN.

Další informace najdete v těchto částech:

- "Statické skupiny"
- "Dynamické skupiny" na stránce 49
- "Vnořené skupiny" na stránce 50
- "Hybridní skupiny" na stránce 50
- "Určení skupinového členství" na stránce 51
- "Třídy objektů skupiny pro vnořené a dynamické skupiny" na stránce 53
- "Typy atributů skupiny" na stránce 53
- "Role" na stránce 54

Statické skupiny

Statické skupiny definují každého člena individuálně pomocí strukturní třídy objektu **groupOfNames**, **groupOfUniqueNames**, **accessGroup** či **accessRole** nebo pomocnou třídou objektu **ibm-staticgroup**. Statická skupina využívající strukturní třídy objektů **groupOfNames** nebo **groupOfUniqueNames** musí mít alespoň jednoho člena. Skupina využívající strukturní třídy objektů **accessGroup** nebo **accessRole** může být prázdná. Statická skupina může být definována rovněž s využitím pomocné třídy objektu: **ibm-staticGroup**, která nevyžaduje atribut **member**, a proto může být prázdná.

Typický záznam skupiny je:


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

Každý objekt ve skupině obsahuje atribut s více hodnotami skládající se ze jmen DN jednotlivých členů.

Při vymazání přístupové skupiny je tato přístupová skupina vymazána rovněž ze všech ACL, na která byla uplatněna.

Dynamické skupiny

Dynamická skupina definuje své členy odlišně od statické skupiny. Namísto toho, aby je jednotlivě vyjmenovávala v seznamu, dynamická skupina definuje své členy s použitím hledání LDAP. Dynamická skupina používá strukturní třídu objektu **groupOfURLs** (nebo pomocnou třídu objektu **ibm-dynamicGroup**) a atribut **memberURL** k definování hledání pomocí zjednodušené syntaxe URL LDAP.

```
ldap:///<base DN of search> ? ? <scope of search> ? <searchfilter>
```

Poznámka: Jak příklad demonstruje, v syntaxi se nesmí vyskytovat jméno hostitele. Zbývající parametry se používají přesně jako v normální syntaxi URL ldap. Každé pole parametrů musí být odděleno otázkou (?), i když není zadán žádný parametr. Normálně by byl mezi základním DN a rozsahem hledání začleněn seznam atributů pro návrat. Tento parametr server při určování dynamického členství rovněž nepoužívá a může tedy být vynechán, oddělovač ? však vložen být musí.

Ve výše uvedeném příkladu:

base DN of search

Toto je bod, z něhož hledání v adresáři začíná. Může to být přípona nebo kořen adresáře jako např. **ou=Austin**. Tento parametr je povinný.

scope of search

Určuje šíři vyhledávání. Předvolený rozsah je "base".

base Vrací informace pouze o základním DN určeném v URL

one Vrací informace o záznamech jednu úroveň pod základním DN určeném v URL. Neobsahuje základní záznam.

sub Vrací informace o záznamech ve všech nižších úrovních a zahrnuje základní DN.

searchfilter

Toto je filtr, který chcete uplatnit pro záznamy v rozmezí rozsahu hledání. Informace o syntaxi searchfilter najdete v tématu "volba filtru ldapsearch" na stránce 206. Předvolená hodnota je objectclass=*

Hledání dynamických členů je vždy interní pro server, proto na rozdíl od úplného URL ldap nejsou nikdy uvedeny údaje o jménu hostitele a číslu portu a protokol je vždy **ldap** (nikdy **ldaps**). Atribut **memberURL** může obsahovat jakýkoli druh URL, ale server používá pro určení dynamického členství pouze **memberURL** začínající **ldap:///**.

Příklady

Jednotlivý záznam, v němž je předvolbou rozsahu základ a kde je předvolbou filtru objectclass=*

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

Všechny záznamy, které jsou jednu úroveň pod cn=Employees a filtr má předvolbu objectclass=*

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

Všechny záznamy, které jsou pod o=Acme s atributem objectclass=person:

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

V závislosti na třídách objektů, které používáte pro definování uživatelských záznamů, nemusí tyto záznamy obsahovat atributy, které jsou vhodné pro určení skupinového členství. Pokud chcete rozšířit uživatelské záznamy, aby obsahovaly atribut **ibm-group**, můžete použít pomocnou třídu objektu **ibm-dynamicMember**. Tento atribut umožňuje přidávat takové libovolné hodnoty do uživatelských záznamů, které by mohly sloužit jako cíle pro filtry dynamických skupin. Například:

Členy této dynamické skupiny jsou záznamy přímo pod záznamem `cn=users,ou=Austin`, které mají atribut `ibm-group` o hodnotě `GROUP1`:

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

Zde je příklad člena `cn=GROUP1,ou=Austin`:

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

Vnořené skupiny

Metoda vnořných skupin umožňuje tvorbu hierarchických vztahů, které je možné používat pro definování děděného skupinového členství. Vnořená skupina je definována jako podřízený skupinový záznam, na jehož DN se odkazuje pomocí atributu obsaženého uvnitř záznamu nadřazené skupiny. Nadřazená skupina je vytvořena rozšířením jedné ze strukturních tříd objektu skupiny (**groupOfNames**, **groupOfUniqueNames**, **accessGroup**, **accessRole** nebo **groupOfURLs**) s doplněním pomocné třídy objektu **ibm-nestedGroup**. Za příponu vnořené skupiny je možné přidat nulu nebo více atributů **ibm-memberGroup** s hodnotami nastavenými na jména DN vnořných podřízených skupin. Například:

```
dn: cn=Group 2, cn=Groups, o=IBM, c=US
objectclass: groupOfNames
objectclass: ibm-nestedGroup
objectclass: top
cn: Group 2
description: Skupina sestavená ze statických a vnořných členů.
member: cn=Person 2.1, cn=Dept 2, cn=Employees, o=IBM, c=US
member: cn=Person 2.2, cn=Dept 2, cn=Employees, o=IBM, c=US
ibm-memberGroup: cn=Group 8, cn=Nested Static, cn=Groups, o=IBM, c=US
```

Zavádění cyklů do hierarchie vnořných skupin není povoleno. Pokud je určeno, že operace tvorby vnořené skupiny má za následek cyklický odkaz, buď přímo, nebo prostřednictvím dědičnosti, považuje se to za narušení omezující podmínky a proto se aktualizace záznamu nezdaří.

Hybridní skupiny

Jakákoli ze strukturních tříd objektů skupiny může být rozšířena tak, že skupinové členství je popsáno kombinací statického, dynamického a vnořného typu člena. Například:

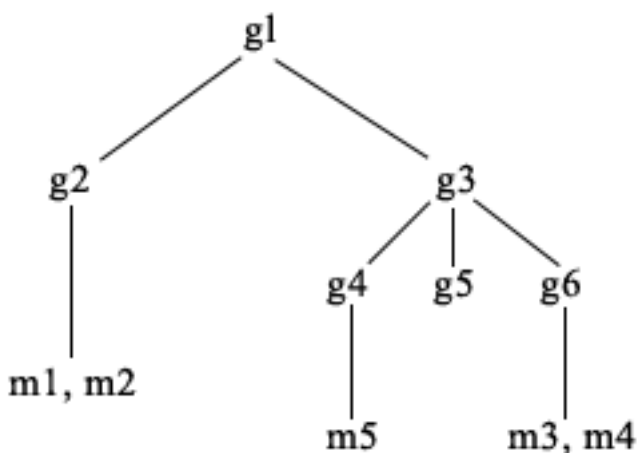
```
dn: cn=Group 10, cn=Groups, o=IBM,
c=US
objectclass: groupOfURLs
objectclass: ibm-nestedGroup
objectclass: ibm-staticGroup
objectclass: top
cn: Group 10
description: Skupina sestavená ze statických, dynamických a vnořných členů.
memberURL: ldap:///cn=Austin, cn=Employees, o=IBM, c=US??one?objectClass=person
ibm-memberGroup: cn=Group 9, cn=Nested Dynamic, cn=Groups, o=IBM, c=US
member: cn=Person 10.1, cn=Dept 2, cn=Employees, o=IBM, c=US
member: cn=Person 10.2, cn=Dept 2, cn=Employees, o=IBM, c=US
```

Určení skupinového členství

Pro dotaz na hromadné skupinové členství je možné použít dva operační atributy. Operační atribut **ibm-allMembers** uvádí pro daný skupinový záznam hromadnou sadu skupinového členství, včetně statických, dynamických a vnořených členů, popsanou v hierarchii vnořené skupiny. Operační atribut **ibm-allGroups** uvádí pro daný uživatelský záznam hromadnou sadu skupin, včetně nadřazených skupin, v nichž má tento uživatel členství.

Žadatel může obdržet pouze podmnožinu všech požadovaných dat, v závislosti na způsobu nastavení ACL pro data. Operační atributy **ibm-allMembers** a **ibm-allGroups** může vyžádat kdokoli, ale obdržená množina dat obsahuje pouze data pro záznamy a atributy LDAP, pro které má žadatel přístupová práva. Uživatel požadující atribut **ibm-allMembers** nebo **ibm-allGroups** musí mít přístup k hodnotám atributů **member** nebo **uniquemember** pro tuto skupinu a vnořené skupiny, aby mohl vidět statické členy, a musí být schopen provádět hledání uvedená v hodnotách atributu **memberURL**, aby mohl vidět dynamické členy. Například:

Příklady hierarchie



U tohoto příkladu jsou **m1** a **m2** v atributu člena záznamu **g2**. ACL pro **g2** umožňuje uživateli **user1** číst atribut člena, ale **user2** nemá přístup k atributu člena. Záznam LDIF pro záznam **g2** vypadá takto:

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

Záznam **g4** používá předvolené aclentry, což umožňuje jak uživateli **user1**, tak **user2** číst jeho atribut člena. LDIF pro záznam **g4** vypadá takto:

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

Záznam **g5** je dynamická skupina, která získává své dva členy z atributu **memberURL**. LDIF pro záznam **g5** vypadá takto:

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

Záznamy **m3** a **m4** jsou členy skupiny **g5**, protože odpovídají **memberURL**. Seznam ACL pro záznam **m3** umožňuje jak uživateli **user1**, tak **user2** v něm vyhledávat. Seznam ACL pro záznamy **m4** neumožňuje uživateli **user2** v něm vyhledávat. LDIF pro záznam **m4** vypadá takto:

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

Příklad 1:

Uživatel **user1** provádí hledání s cílem získat všechny členy skupiny **g1**. Uživatel **user1** má přístup ke všem členům, takže jsou vráceni všichni.

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

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

Příklad 2:

Uživatel **user2** provádí hledání s cílem získat všechny členy skupiny **g1**. Uživatel **user2** nemá přístup ke členům **m1** nebo **m2**, protože oni nemají přístup do atributu člena pro skupinu **g2**. Uživatel **user2** má přístup k atributu člena pro **g4** a proto má přístup k členovi **m5**. Uživatel **user2** může provádět hledání ve skupině **g5** **memberURL** záznamu **m3** tak, aby byl zobrazen seznam členů, ale nemůže provádět hledání **m4**.

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

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

Příklad 3:

Uživatel **user2** provádí hledání s cílem zjistit, jestli **m3** je členem skupiny **g1**. Uživatel **user2** má práva k provádění tohoto hledání, takže hledání ukáže, že **m3** je členem skupiny **g1**.

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

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

Příklad 4:

Uživatel **user2** provádí hledání s cílem zjistit, jestli **m1** je členem skupiny **g1**. Uživatel **user2** nemá přístup k atributu tohoto člena, takže hledání neukáže, že **m1** je členem skupiny **g1**.

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

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

Třídy objektů skupiny pro vnořené a dynamické skupiny

ibm-dynamicGroup

Tato pomocná třída umožňuje volitelný atribut **memberURL**. Používá se u strukturních tříd jako např. **groupOfNames** k tvorbě hybridní skupiny se statickými i dynamickými členy.

ibm-dynamicMember

Tato pomocná třída umožňuje volitelný atribut **ibm-group**. Používá se jako atribut filtru pro dynamické skupiny.

ibm-nestedGroup

Tato pomocná třída umožňuje volitelný atribut **ibm-memberGroup**. Používá se u strukturní třídy jako např. **groupOfNames** pro aktivaci vnoření podskupin do nadřazené skupiny.

ibm-staticGroup

Tato pomocná třída umožňuje volitelný atribut **member**. Používá se u strukturní třídy jako např. **groupOfURLs** k tvorbě hybridní skupiny se statickými i dynamickými členy.

Poznámka: **ibm-staticGroup** je jediná třída, pro kterou je **member** *volitelný*, všechny ostatní třídy používající atribut **member** vyžadují alespoň jednoho člena.

Typy atributů skupiny

ibm-allGroups

Zobrazí všechny skupiny, k nimž patří určitý záznam. Záznam může být členem přímo podle atributů **member**, **uniqueMember** nebo **memberURL** nebo nepřímo podle atributu **ibm-memberGroup**. Tento operační atribut **pouze pro čtení** není povolen ve filtru hledání. Atribut **ibm-allGroups** je možné používat pro požadavek na porovnání s cílem určit, zda je záznam členem dané skupiny. Chcete-li například určit, jestli je "cn=john smith,cn=users,o=my company" členem skupiny "cn=system administrators, o=my company":

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

ibm-allMembers

Zobrazuje všechny členy skupiny. Záznam může být členem přímo podle atributů **member**, **uniqueMember** nebo **memberURL** nebo nepřímo podle atributu **ibm-memberGroup**. Tento operační atribut **pouze pro čtení** není povolen ve filtru hledání. Atribut **ibm-allMembers** je možné používat pro požadavek na porovnání s cílem určit, zda je DN členem dané skupiny. Chcete-li například určit, jestli je "cn=john smith,cn=users,o=my company" členem skupiny "cn=system administrators, o=my company":

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

ibm-group

Toto je atribut využívaný pomocnou třídou **ibm-dynamicMember**. Používá se pro definování libovolných hodnot při kontrole členství záznamu v dynamických skupinách. Například je možné přidat hodnotu "Kušelkářské družstvo" a tím zahrnout záznam do jakékoli **memberURL**, která má filtr "ibm-group=Kušelkářské družstvo".

ibm-memberGroup

Toto je atribut využívaný pomocnou třídou **ibm-nestedGroup**. Označuje podskupiny záznamu nadřazené skupiny. Členové všech takových podskupin jsou při zpracovávání seznamů ACL nebo operačních atributů **ibm-allMembers** a **ibm-allGroups** považováni za členy nadřazené skupiny. Samotné záznamy podskupiny *nejsou* členy. Vnořené členství je rekurzivní.

member

Označuje rozlišovací jména pro každého člena skupiny. Například: member: cn=John Smith, dc=ibm, dc=com.

memberURL

Označuje URL přiřazené každému členovi skupiny. Je možné použít jakýkoli typ označené URL. Například: memberURL: ldap:///cn=jsmith,dc=ibm,dc=com.

uniquemember

Označuje skupinu jmen přiřazených záznamu, kde každému jménu byl přidělen jednoznačný identifikátor (uniqueIdentifier) zaručující jeho jednoznačnost. Hodnota pro atribut uniqueMember je DN s připojeným jednoznačným identifikátorem. Například: uniqueMember: cn=John Smith, dc=ibm, dc=com 17.

Role

Autorizace na základě rolí je pojmový doplněk k autorizaci na základě skupin, který je v určitých případech velmi prospěšný. Jako člen role máte oprávnění provádět potřebné úkony aby role mohla dokončit práci. Na rozdíl od skupiny doprovází roli implicitní sada povolení. Neexistuje předem daný předpoklad, která povolení budou udělena (nebo odebrána), když je někdo členem nějaké skupiny.

Role jsou podobné skupinám v tom, že jsou v adresáři znázorněny objektem. Role kromě toho obsahují skupinu jmen DN. Role, které se mají použít pro řízení přístupu, musí mít třídu objektu 'AccessRole'. Třída objektu 'Accessrole' je podtřídou třídy objektu 'GroupOfNames'.

Jestliže například existuje kolekce jmen DN jako 'sys admin', asi vás nejprve napadne, že to je 'skupina sys admin' (protože skupiny a uživatelé jsou nejznámější typy atributů práv). Protože však existuje sada povolení, jejichž udělení byste očekávali jako členové skupiny 'sys admin', kolekce jmen DN může být přesněji definována jako 'role sys admin'.

Administrativní přístup

Server adresářů IBM umožňuje tyto typy administrativního přístupu:

- **Projektovaný administrátor i5/OS:** Klient autentizovaný jako projektovaný uživatel (záznam LDAP reprezentující uživatelský profil operačního systému) se zvláštními oprávněními *ALLOBJ a *IOSYSCFG má oprávnění měnit konfiguraci adresáře pomocí rozhraní LDAP (cn=configuration subtree, nebo úlohy "Server administration" webového administrativního nástroje), a také fungovat jako administrátor LDAP pro ostatní záznamy adresáře (záznamy uložené v jedné z přípon DB2 nebo schématu). Pouze projektovaní administrátoři i5/OS mohou měnit konfiguraci serveru.
- **Administrátor LDAP:** Server adresářů IBM umožňuje, aby byl jeden ID uživatele (DN) primárním administrátorem LDAP serveru. Systém iSeries také umožňuje, aby projektované uživatelské profily operačního systému byly administrátory LDAP. Administrátoři serveru LDAP mohou vykonávat dlouhý seznam administrativních úloh jako je správa replikací, schématu a záznamů adresáře. Další informace najdete v tématu "Jak poskytnout administrátorský přístup projektovaným uživatelům" na stránce 117.
- **Skupina administrativních uživatelů:** Projektovaný administrátor i5/OS může ustanovit několik uživatelů, kteří budou v administrativní skupině. Členové této skupiny mohou vykonávat mnoho úloh, protože mají stejný administrativní přístup jako administrátor serveru LDAP.

Poznámka: Když se používá webová administrace, pak úlohy, které nebyly členům administrativní skupiny uděleny, jsou zneprístupněny.

Administrátor LDAP nebo člen administrativní skupiny může vykonávat tyto úlohy administrace serveru:

- Měnit své vlastní heslo.
- Ukončit připojení.
- Povolit a měnit zásadu hesel, s výjimkou šifrování hesel, které může měnit pouze projektovaný administrátor i5/OS.
- Spravovat jedinečné atributy.
- Spravovat schéma serveru.
- Spravovat replikace, s výjimkou úlohy vlastností replikace (zahrnuje připojovací DN hlavního serveru a předvolený odkaz), kterou může vykonávat pouze projektovaný administrátor i5/OS.

Informace o tom jak vytvořit administrativní skupinu najdete v tématu "Jak pracovat s administrativní skupinou" na stránce 118.

Proxy autorizace

- Proxy autorizace je speciální formou autentizace. Pomocí mechanismu proxy autorizace se může aplikace typu klient připojit k adresáři na základě své vlastní identity, ale je jí povoleno provádět operace i jménem jiného uživatele, aby měl přístup k cílovému adresáři. Sada důvěryhodných aplikací nebo uživatelů může přistupovat na server adresářů jménem více uživatelů.
- Členové skupiny s proxy autorizací mohou na sebe vzít libovolnou autentizovanou identitu s výjimkou identity administrátora nebo členů administrativní skupiny.
- Skupina s proxy autorizací může být uložena buď pod localhost nebo IBMpoliciies. Skupina s proxy autorizací pod IBMpoliciies se replikuje; skupina s proxy autorizací pod localhost se nereplikuje. Skupinu s proxy autorizací můžete uložit jak pod localhost tak pod IBMpoliciies. Není-li skupina s proxy autorizací uložena pod jedním z těchto DN, server ignoruje část s proxy autorizací v definici skupiny a pracuje s ní jako s normální skupinou.
- Uvedme si příklad: klientská aplikace - client1 - může přistupovat k serveru adresářů s vysokou úrovní přístupových oprávnění. Uživatel A s omezenými oprávněními odešle požadavek do klientské aplikace. Pokud je klient členem skupiny s proxy autorizací, pak namísto předání požadavku serveru adresářů jako client1 může požadavek předat jako uživatel A s použitím omezenější úrovně oprávnění. To v praxi znamená, že namísto zpracování požadavku jako client1 může aplikační server přistoupit pouze k těm informacím nebo provést pouze takové akce, ke kterým má oprávnění uživatel A. Zpracuje požadavek jménem neboli v zastoupení (proxy) uživatele A.
- Poznámka:** Člen atributu musí mít svoji hodnotu ve formě DN. Jinak se vrátí zpráva o neplatné syntaxi DN. Není povoleno, aby skupinové DN bylo členem skupiny s proxy autorizací.
- Není povoleno, aby administrátoři nebo členové administrativní skupiny byli členy skupiny s proxy autorizací. Protokol událostí zaznamenává jak připojovací DN tak proxy DN pro každou akci provedenou s využitím proxy autorizace.
- Další informace najdete v tématu “Jak spravovat skupiny s proxy autorizací” na stránce 121.

Seznamy přístupových práv

Seznamy přístupových práv (ACL) poskytují prostředky k ochraně informací uložených v adresáři LDAP. Administrátoři používají seznamy ACL k omezení přístupu k různým úsekům adresáře nebo určitým záznamům adresáře. Pomocí seznamu ACL je možné kontrolovat změny každého záznamu a atributu v adresáři. Seznam ACL pro daný záznam nebo atribut může být zděděný od nadřazeného záznamu nebo jej lze výslovně definovat.

Nejlepší je zahájit návrh své strategie řízení přístupu vytvořením skupin uživatelů, které budete používat při nastavování přístupových práv k objektům a atributům. Potom se nastaví vlastnictví a přístup k nejvyšší možné úrovni ve stromu a kontrola se nechá dědit na nižší úrovni stromu.

Operační atributy související s řízením přístupu, jako např. entryOwner, ownerSource, ownerPropagate, aclEntry, aclSource a aclPropagate jsou výjimečné v tom, že jsou logicky sdružené s každým objektem, ale mohou mít hodnoty, které závisí na jiných objektech na vyšších úrovních stromu. V závislosti na tom, jak jsou stanoveny, mohou být tyto hodnoty atributů výslovně přiřazené k nějakému objektu nebo zděděné od jeho předchůdce.

Model řízení přístupu definuje dvě sady atributů: informace o řízení přístupu (Access Control Information - ACI) a informace o vlastníku záznamu (entryOwner). ACI definuje přístupová práva udělená určenému subjektu s ohledem na činnosti, které mohou provádět na objektech, ke kterým se vztahují. K definici ACI se vztahují atributy aclEntry a aclPropagate. Informace entryOwner definují, které subjekty mohou definovat ACI pro přidružený objekt záznamu. K definici entryOwner se vztahují atributy entryOwner a ownerPropagate.

Můžete si vybrat ze dvou druhů seznamů přístupových práv: ACL na základě filtru a ACL bez filtru. Seznamy ACL bez filtru se vztahují výlučně na záznam adresáře, který je obsahuje, ale mohou být převedeny na žádný nebo všechny ze svých podřízených záznamů. Seznamy ACL na základě filtru se liší v tom, že uplatňují porovnávání založené na filtru, přičemž využívají zadaný filtr objektu k nalezení odpovídajících cílových objektů s účinným přístupem, který pro ně platí.

Pomocí ACL mohou administrátoři omezovat přístup k různým úsekům adresáře, určitým záznamům adresáře a na základě jména atributu nebo přístupové třídy atributu i k atributům obsaženým v záznamech. Každý záznam uvnitř adresáře LDAP má sadu přidružených ACI. Ve shodě s modelem LDAP jsou informace o ACI a entryOwner znázorněny jako páry atribut-hodnota. Kromě toho se ke správě těchto hodnot používá i syntaxe LDIF. Tyto atributy jsou:

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

Informace o možnostech při práci se seznamy ACL najdete v tomto tématu: “Jak provádět správu seznamů přístupových práv (ACL)” na stránce 181. Další informace najdete v těchto částech:

- “Filtrované seznamy ACL”
- “Syntaxe atributu řízení přístupu” na stránce 57
- “AclEntry a ibm-filterAclEntry” na stránce 57
- “Vlastník záznamu (EntryOwner)” na stránce 60
- “Propagace” na stránce 60
- “Vyhodnocování přístupu” na stránce 61
- “Definice ACI a vlastníků záznamu” na stránce 62
- “Změna ACI a hodnot vlastníka záznamu” na stránce 63
- “Vymazání hodnot ACI/vlastníka záznamu” na stránce 66
- “Načtení hodnot ACI/vlastníka záznamu” na stránce 66
- “Hlediska replikace podstromu” na stránce 66

Filtrované seznamy ACL

Seznamy ACL na základě filtru uplatňují porovnávání založené na filtru, přičemž využívají zadaný filtr objektu k nalezení odpovídajících cílových objektů s efektivním přístupem, který pro ně platí.

Seznamy ACL založené na filtru se ze své podstaty automaticky přenášejí na jakékoli odpovídající objekty nalezené srovnáváním v přidruženém podstromu. Z tohoto důvodu se na nové ACL založené na filtru nevztahuje atribut aclPropagate, který se používá k zastavení přenosu seznamů ACL bez filtru.

Standardním chováním seznamů ACL založených na filtru je akumulovat se od nejnižšího obsahujícího záznamu vzhůru podél řetězce nadřazených záznamů až po nejvyšší obsahující záznam v DIT. Efektivní přístup se počítá jako souhrn udělených nebo odepřených přístupových práv podle zúčastněných nadřazených záznamů. Z tohoto chování existuje výjimka. Z důvodu kompatibility s funkcí replikace podstromu a s cílem umožnit lepší řízení administrace se jako prostředku k zastavení akumulace v záznamu, v němž je obsažen, používá atribut dovoleného maxima.

Pro podporu seznamů ACL založených na filtru se používá nová specifická sada atributů řízení přístupu, která je výhodnější než začlenění charakteristik na základě filtru do stávajících seznamů ACL bez filtru. Tyto atributy jsou:

- ibm-filterAclEntry
- ibm-filterAclInherit

Atribut ibm-filterAclEntry má stejný formát jako aclEntry, s dodatkem komponenty filtru objektu. Přiřazený atribut povoleného maxima je ibm-filterAclInherit. Standardně je nastaven na hodnotu pravdivý (true). Když je nastaven na hodnotu nepravdivý (false), ukončuje akumulaci.

Syntaxe atributu řízení přístupu

Každý z těchto atributů je možné spravovat pomocí notace LDIF. Jako syntaxe pro nové atributy ACL na základě filtru se používá modifikovaných verzí současných atributů ACL bez filtru. Níže je uvedena syntaxe pro atributy ACI a entryOwner s využitím tvaru BNF (baccus naur form).

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

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

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

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

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

<subjectDnType> ::= "role" | "group" | "access-id"
<subjectDn> ::= <DN>
<DN> ::= rozlišovací jméno, jak je popsáno v RFC 2251, část 4.1.3.
<pseudoDn> ::= "group:cn=anybody" | "group:cn=authenticated" |
              "access-id:cn=this"
<object filter> ::= filtr hledání řetězce, jak je definován v RFC 2254, část 4
                  (rozšiřitelné porovnávání není podporováno).
<rights> ::= <accessList> [ ":" <rights> ]

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

<objectAccess> ::= "object:" [<action> ":"] <objectPermissions>
<action> ::= "grant" | "deny"
<objectPermissions> ::= <objectPermission> [ <objectPermissions> ]
<objectPermission> ::= "a" | "d" | ""

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

<attributeName> ::= jméno attributeType, jak je popsáno v RFC 2251, část 4.1.4.
                  (OID nebo alfanumerický řetězec s úvodním
                   písmenem, povoleno "-" a ";")

<attributePermissions> ::= <attributePermission>
                          [<attributePermissions>]
<attributePermission> ::= "r" | "w" | "s" | "c" | ""

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

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

AcIEntry a ibm-filterAcIEntry

Subjekt: Subjekt (entita požadující přístup k provedení operace na objektu) sestává z kombinace typu DN (rozlišovacího jména) a DN. Platné typy DN jsou: access-id, skupina a role.

DN určuje konkrétní access-id, roli nebo skupinu. Subjektem by mohlo být například access-id: cn=personA, o=IBM nebo skupina: cn=deptXYZ, o=IBM.

Protože oddělovačem polí je dvojtečka (:), DN obsahující dvojtečky musí být uzavřeno v dvojitéch uvozovkách (""). Jestliže DN již obsahuje znaky s dvojitými uvozovkami, musí být tyto znaky uvolněny pomocí zpětného lomítka (\).

Při řízení přístupu se mohou použít všechny skupiny adresáře.

Poznámka: Pro řízení přístupu je možno použít jakoukoli skupinu strukturních tříd objektů **AccessGroup**, **GroupOfNames**, **GroupOfUniqueNames** či **groupOfURLs** nebo pomocné třídy objektů **ibm-dynamicGroup** , **ibm-staticGroup**.

Dalším typem DN používaným v modelu řízení přístupu je role. Přestože jsou role a skupiny podobné, jsou koncepčně odlišné, pokud jde o implementaci. Když je uživatel přiřazen k určité roli, předem se předpokládá, že již byla stanovena potřebná pravomoc k provádění práce přiřčená k této roli. U skupinového členství neexistuje předem daný předpoklad, která povolení budou udělena (nebo odeprána), když je někdo členem této skupiny.

Role jsou podobné skupinám v tom, že jsou v adresáři znázorněny objektem. Role kromě toho obsahují skupinu jmen DN. Role, které se používají pro řízení přístupu, musí mít třídu objektu **AccessRole**.

Nepravá jména DN: Adresář LDAP obsahuje několik nepravých (pseudo) DN. Ta se používají k odkazování na velké počty DN, která ve spojovacím čase sdílejí společnou charakteristiku buď s ohledem na prováděnou činnost, nebo na cílový objekt, na němž se činnost provádí.

V současnosti jsou definována tři nepravá DN:

group:cn=anybody

Týká se všech subjektů, včetně těch, které nejsou autentizovány. Do této skupiny patří automaticky všichni uživatelé.

group:cn=authenticated

Týká se jakéhokoli jména DN, které bylo pro adresář autentizováno. Na metodu autentizace se nebere zřetel.

access-id:cn=this

Týká se přípojovacího Dn, které odpovídá DN cílového objektu, na němž se provádí daná operace.

Filtr objektu: Tento parametr se vztahuje pouze na filtrované seznamy ACL. Jako formát filtru objektu se používá filtr pro hledání řetězce podle definice v RFC 2254. Protože cílový objekt je již znám, k provádění skutečného hledání se nepoužívá řetězec. Namísto toho se provádí porovnávání dotyčného cílového objektu s filtrem a zjišťuje se, zda pro něj platí daná sada hodnot **ibm-filterAclEntry**.

Práva: Přístupová práva se mohou vztahovat na celý objekt nebo na atributy tohoto objektu. Přístupová práva LDAP jsou diskrétní. Z jednoho práva nevyplývá jiné právo. Práva se mohou spolu kombinovat tak, aby poskytovala seznam požadovaných práv, pokud se budou řídit soustavou pravidel projednávaných později. Práva mohou mít nespecifikovanou hodnotu, což znamená, že se neudělí žádná přístupová práva subjektu pro cílový objekt. Práva se skládají ze tří částí:

Akce: Definované hodnoty jsou **udělit** nebo **odepřít**. Pokud toto pole není v právu obsaženo, předvolená hodnota je nastavena na **udělit**.

Povolení:

Existuje šest základních operací, které je možno u objektu adresáře provádět. Z těchto operací se odvozuje základní sada povolení ACI. Jsou to: přidávání záznamu, mazání záznamu, čtení hodnoty atributu, zapisování hodnoty atributu, hledání atributu a porovnávání hodnoty atributu.

Možná povolení atributu jsou: čtení (r), zápis (w), hledání (s) a porovnávání (c). Kromě toho se na záznam jako celek vztahují povolení objektu. Tato povolení zahrnují přidávání podřízených záznamů (a) a mazání tohoto záznamu (d).

Následující tabulka shrnuje povolení potřebná k provádění každé z operací LDAP.

Operace	Potřebné povolení
ldapadd	přidávání (na nadřazený)
ldapdelete	mazání (na objekt)
ldapmodify	zápis (na modifikované atributy)
ldapsearch	<ul style="list-style-type: none"> • hledání, čtení (na atributy v RDN) • hledání (na atributy uvedené ve filtru hledání) • hledání (na atributy vrácené pouze se jmény) • hledání, čtení (na atributy vrácené s hodnotami)
ldapmodrdn	zápis (na atributy RDN)
ldapcompare	porovnávání (na porovnávaný atribut)

Poznámka: U vyhledávacích operací se vyžaduje, aby měl subjekt přístup k hledání pro všechny atributy ve filtru hledání, jinak nebudou vráceny žádné záznamy. U záznamů vrácených z hledání se vyžaduje, aby měl subjekt přístup k hledání (s) a čtení (r) pro všechny atributy v RDN vrácených záznamů, jinak tyto záznamy nebudou vráceny.

Cíl přístupu:

Tato povolení se mohou vztahovat na celý objekt (přidávání podřízeného záznamu, mazání záznamu), na jednotlivý atribut v rámci daného záznamu nebo se mohou vztahovat na skupiny atributů (přístupové třídy atributu), jak je popsáno níže.

Atributy vyžadující podobná povolení pro přístup jsou seskupeny ve třídách. Atributy se mapují na své třídy atributů v souboru schématu adresáře. Tyto třídy jsou diskrétní; přístup k jedné třídě neznamená přístup k jiné třídě. Povolení jsou stanovena s ohledem na přístupovou třídu atributu jako celek. Povolení stanovená na konkrétní třídu atributu platí pro všechny atributy uvnitř této přístupové třídy, pokud nejsou stanovena povolení přístupových tříd k jednotlivým atributům.

IBM definuje tři třídy atributů, které se používají při vyhodnocování přístupu k atributům uživatele: **normální**, **citlivá** a **kritická**. Například atribut **commonName** spadá do normální třídy a atribut **userpassword** patří do kritické třídy. Uživatelsky definované atributy patří do normální přístupové třídy, pokud není stanoveno jinak.

Definovány jsou rovněž dvě další přístupové třídy: systémová a vyhrazená. Atributy systémových tříd jsou tyto:

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

Toto jsou atributy uchovávané serverem LDAP a pro uživatele adresáře jsou pouze pro čtení. **OwnerSource** a **aclSource** jsou popsány v tématu Propagace (viz část “Propagace” na stránce 60).

Vyhrazená třída obsahuje tyto atributy, které definují řízení přístupu:

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

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

Ke čtení vyhrazených atributů mají přístup všichni uživatelé, ale vytvářet, modifikovat a mazat tyto atributy mohou pouze **vlastníci objektů** (entryOwners).

Poznámka: Atribut **ibm-effectiveAcl** je pouze pro čtení.

Vlastník záznamu (EntryOwner)

Vlastníci záznamů mají úplná povolení k provádění jakékoli operace na daném objektu bez ohledu na aclEntry. Kromě toho jsou vlastníci záznamů jediné osoby, kterým je povoleno vykonávat správu aclEntries pro tento objekt. EntryOwner je subjekt řízení přístupu, je možné jej definovat jako jednotlivce, skupiny nebo role.

Poznámka: Administrátor adresáře je standardně jeden z vlastníků záznamů (entryOwners) pro všechny objekty v adresáři a vlastnictví záznamu (entryOwnership) administrátora adresáře nelze z žádného objektu odstranit.

Propagace

Záznamy, v nichž byl umístěn aclEntry, jsou považovány za explicitní vlastníky **aclEntry**. Podobně, jestliže byl na konkrétní záznam nastaven **entryOwner**, má tento záznam explicitního vlastníka. Tyto dva případy se navzájem nemísí, záznam s explicitním vlastníkem může nebo nemusí mít explicitní **aclEntry** a záznam s explicitním **aclEntry** by mohl mít explicitního vlastníka. Pokud není některá z těchto hodnot v záznamu výslovně uvedena, chybějící hodnota je zděděna z nadřazeného uzlu v adresářovém stromu.

Každý explicitní **aclEntry** nebo **entryOwner** se vztahuje na záznam, pro nějž je nastaven. Navíc by hodnota mohla platit pro všechny podřízené záznamy, které nemají výslovně nastavenou hodnotu. Tyto hodnoty jsou považovány za šířené (propagované); jejich hodnoty se propagují adresářovým stromem. Propagace konkrétní hodnoty pokračuje do té doby, než je dosaženo jiné propagované hodnoty.

Poznámka: Seznamy ACL na základě filtru se nepropagují stejným způsobem jako ACL na filtru nezaložené. Propagují se do jakýchkoli objektů vyhovujících porovnání v přidruženém podstromu. Více informací o rozdílech najdete v tématu "Filtrované seznamy ACL" na stránce 56.

aclEntry a **entryOwner** mohou být nastaveny tak, aby se vztahovaly pouze na konkrétní záznam s hodnotou propagace na "false" nebo na záznam a jeho podstrom s hodnotou propagace nastavenou na "true". Ačkoli **aclEntry** i **entryOwner** se mohou propagovat, jejich propagace spolu nijak nesouvisí.

Atributy **aclEntry** a **entryOwner** umožňují vícenásobné hodnoty, atributy propagace (**aclPropagate** a **ownerPropagate**) však mohou mít v rámci stejného záznamu pouze jedinou hodnotu pro všechny hodnoty atributů **aclEntry** nebo **entryOwner**.

Systémové atributy **aclSource**, případně **ownerSource** obsahují DN efektivního uzlu, ze kterého jsou vyhodnocovány **aclEntry**, případně **entryOwner**. Pokud žádný takový uzel neexistuje, je přiřazena hodnota **default** (předvolená).

Definice efektivního řízení přístupu objektu je možné odvozovat podle této logiky:

- Pokud je v objektu sada explicitních atributů řízení přístupu, potom je tato sada definicí řízení přístupu tohoto objektu.
- Pokud neexistují výslovně definované atributy řízení přístupu, potom je potřeba postupovat podél stromu adresáře vzhůru, dokud se nedosáhne nadřazeného uzlu se sadou propagovaných atributů řízení přístupu.
- V případě, že se žádný takový nadřazený uzel nenalezne, je subjektu udělen předvolený přístup popsáný níže.

Vlastníkem záznamu je administrátor adresáře. Nepravé skupině cn=anybody (všichni uživatelé) je udělen přístup pro čtení, hledání a porovnávání atributů v normální přístupové třídě.

Vyhodnocování přístupu

Přístup pro konkrétní operaci je udělován nebo odepřen na základě přípojovacího DN objektu pro tuto operaci na cílovém objektu. Zpracování se zastavuje, jakmile je možné určit přístup.

Kontroly přístupu se provádějí nejprve hledáním definice efektivního **entryOwnership** a **ACI**, kontrolou vlastnictví záznamu a potom vyhodnocením hodnot ACI objektu.

Seznamy ACL na základě filtru se akumulují od nejnižšího obsahujícího záznamu vzhůru podél řetězce nadřazených záznamů až po nejvyšší obsahující záznam v DIT. Efektivní přístup se počítá jako souhrn udělených nebo odepřených přístupových práv podle zúčastněných nadřazených záznamů. K vyhodnocování efektivního přístupu u seznamů ACL na základě filtru se používá stávající sada pravidel specifičnosti a kombinačních pravidel.

Atributy založené na filtru a nezaložené na filtru se v rámci jediného obsahujícího záznamu adresáře vzájemně vylučují. Umísťování obou typů atributů do téhož záznamu není dovoleno a je považováno za narušení omezujících podmínek. Pokud je zjištěn tento stav, operace asociované s tvorbou nebo aktualizací záznamu adresáře selžou.

Při výpočtu efektivního přístupu první zjištěný typ ACL v řetězci záznamů nadřazených záznamu cílového objektu nastavuje režim výpočtu. V režimu na základě filtru se seznamy ACL nezaložené na filtru při výpočtu efektivního přístupu ignorují. Podobně se při výpočtu efektivního přístupu v režimu nezaloženém na filtru ignorují seznamy ACL na základě filtru.

Pokud chcete omezit akumulaci seznamů ACL na základě filtru ve výpočtu účinného přístupu, je možno do každého záznamu mezi nejvyšší a nejnižší výskyt **ibm-filterAclEntry** v daném podstromu umístit atribut **ibm-filterAclInherit** nastavený na hodnotu "false". To způsobí, že se bude ignorovat podmnožina výše položených atributů **ibm-filterAclEntry** v řetězci nadřazených záznamů cílového objektu.

Pokud se v režimu ACL na základě filtru neuplatní žádný seznam ACL na základě filtru, platí předvolený ACL (cn=anybody je udělen přístup pro čtení, hledání a porovnávání k atributům v normální přístupové třídě). K této situaci může dojít tehdy, když záznam, ke kterému je prováděn přístup, neodpovídá žádnému z filtrů uvedeným v hodnotách **ibm-filterAclEntry**. Pokud nechcete uplatnit toto předvolené řízení přístupu, můžete zadat jako předvolený filtr ACL například tento:

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

V tomto příkladu není udělen žádný přístup. Změňte jej tak, aby poskytoval přístup, který chcete uplatnit.

Administrátor adresáře a hlavní server nebo peer server (pro replikaci) mají standardně udělena plná přístupová práva ke všem objektům v adresáři s výjimkou přístupu pro zápis do systémových atributů. Ostatní **entryOwners** mají udělena plná přístupová práva k objektům pod jejich vlastnictvím s výjimkou přístupu pro zápis do systémových atributů. Všichni uživatelé mají přístupová práva pro čtení k systémovým a vyhrazeným atributům. Tato předdefinovaná práva není možno pozměňovat. Jestliže má žádající subjekt atribut **entryOwnership**, přístup je určen podle výše uvedených předvolených nastavení a zpracování přístupu se zastaví.

Pokud žádající objekt není entryOwner, kontrolují se hodnoty ACI pro záznamy objektu. Přístupová práva, jak jsou definována v ACI pro cílový objekt, se počítají podle specifičnosti a kombinačních pravidel.

Pravidlo specifičnosti

Nejspecifičtější definice aclEntry jsou definice použité při vyhodnocování povolení udělených/odepřených uživatelů. Úrovně specifičnosti jsou tyto:

- Access-id je specifičtější než skupina nebo role. Skupiny a role jsou na stejné úrovni.
- V rozmezí téže úrovně **dnType** jsou povolení úrovně individuálních atributů specifičtější než povolení úrovně třídy atributů.
- V rámci stejné úrovně atributu nebo třídy atributu je **odepření** specifičtější než **udělení**.

Kombinační pravidlo

Povolení udělená subjektům o stejné specifičnosti se kombinují. Pokud není možné v rámci stejné úrovně

specifičnosti určit přístup, použije se definici přístupu z nižší specifické úrovně. Jestliže není určen přístup ani po uplatnění všech definovaných ACI, přístup je odepřen.

Poznámka: Jakmile je při vyhodnocování přístupu nalezen záznam **aclEntry** o odpovídající úrovni access-id, záznamy **aclEntries** o úrovni skupiny nejsou zahrnuty do výpočtu přístupu. Výjimkou je případ, kdy jsou definovány všechny záznamy **aclEntries** s access-id odpovídající úrovni pod **cn=this**, potom jsou všechny záznamy **aclEntries** o odpovídající úrovni skupiny rovněž začleněny do vyhodnocování.

Jinými slovy, jestliže v rámci záznamu objektu záznam s definovanou ACI obsahuje DN subjektu s access-id, který odpovídá připojovacímu DN, potom jsou vyhodnocena povolení nejprve na základě tohoto **aclEntry**. Jestliže jsou pod stejným DN subjektu definována povolení odpovídající úrovni atributu, tato povolení přepíší jakákoli povolení definovaná pod třídami atributů. Jestliže pod stejnou definici úrovně atributu nebo třídy atributu existují vzájemně si odporující povolení, odepřená povolení převažují nad udělenými povoleními.

Poznámka: Definované povolení s hodnotou typu 'null' zamezuje zahrnutí méně specifických definicí povolení.

V případě, že stále není možné určit přístup a všechny odpovídající nalezené **aclEntries** jsou definovány pod "cn=this", je vyhodnoceno členství ve skupině. Pokud uživatel patří do více než jedné skupiny, obdrží tento uživatel kombinaci povolení z těchto skupin. Navíc, pokud tento uživatel uskutečnil autentizované spojení, patří automaticky do skupiny **cn=Anybody** a pravděpodobně do skupiny **cn=Authenticated**. Jestliže jsou pro tyto skupiny definována povolení, uživatel uvedená povolení obdrží.

Poznámka: Členství ve skupině a úloze je určeno v době spojení a trvá buď do té doby, než se uskuteční jiné spojení, nebo dokud není obdržen požadavek na odpojení. Vnořené skupiny a role, to znamená skupiny nebo role definované pro člena jiné skupiny nebo role, nejsou řešeny při určování členství ani při vyhodnocování přístupu.

Předpokládejme například, že **attribute1** je v citlivé třídě atributu a uživatel **cn=Person A, o=IBM** patří jak do skupiny **group1**, tak do **group2**, přičemž jsou definovány tyto záznamy **aclEntries**:

1. **aclEntry: access-id: cn=Person A, o=IBM: at.attribute1:grant:rsc:sensitive:deny:rsc**
2. **aclEntry: group: cn=group1,o=IBM:critical:deny:rwc**
3. **aclEntry: group: cn=group2,o=IBM:critical:grant:r:normal:grant:rsc**

Tento uživatel:

- obdrží přístup 'rsc' k **attribute1**, (od 1. Definice úrovně atributu přepíše definici úrovně třídy atributu)
- nemá žádný přístup k jiným atributům citlivé třídy v cílovém objektu (od 1)
- Nemá udělena žádná jiná práva (2 a 3 NEJSOU zahrnuta do vyhodnocení přístupu).

V jiném příkladu, s těmito záznamy **aclEntries**:

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

Uživatel:

- nemá žádný přístup k atributům citlivé třídy (od 1. Hodnota typu 'null' definovaná pod access-id zamezuje začlenění povolení do atributů citlivé třídy ze skupiny **group1**)
- má přístup 'rsc' k atributům normální třídy (od 2)

Definice ACI a vlastníků záznamu

Následující dva příklady uvádějí zavádění administrační poddomény. První příklad znázorňuje jediného uživatele, který je přiřazen jako **entryOwner** pro celou doménu. Druhý příklad znázorňuje skupinu přiřazenou jako **entryOwner**.

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

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

Další příklad znázorňuje způsob, kterým se záznamu `access-id "cn=Person 1, o=IBM"` udělují povolení pro čtení, hledání a porovnávání atributu `attribute1`. Povolení platí pro jakýkoli uzel v celém podstromu, od uzlu obsahujícího toto ACI, které odpovídá porovnávacímu filtru `"(objectclass=groupOfNames)"`, po nižší úrovni. Akumulace odpovídajících atributů `ibm-filteraclentry` v jakýchkoli nadřazených uzlech byla určena v tomto záznamu nastavením atributu `ibm-filteraclinherit` na `"false"`.

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

```
ibm-filterAclInherit: false
```

Následující příklad ukazuje způsob, kterým se skupině `"cn=Dept XYZ, o=IBM"` udělují povolení pro čtení, hledání a porovnávání atributu `attribute1`. Povolení platí pro celý podstrom pod uzlem obsahujícím toto ACI.

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

Následující příklad ukazuje způsob, kterým se úloze `"cn=System Admins, o=IBM"` udělují povolení pro přidávání objektů pod tento uzel a pro čtení, hledání a porovnávání atributu `attribute2` a kritické třídy atributů. Povolení platí pouze pro uzel obsahující toto ACI.

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

Změna ACI a hodnot vlastníka záznamu

Modifikace-nahrazení

Modifikace-nahrazení funguje stejným způsobem jako všechny ostatní atributy. Pokud hodnota atributu neexistuje, tato hodnota se vytvoří. Jestliže hodnota atributu existuje, tuto hodnotu nahradí.

Máte například následující ACI pro záznam:

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

provedeme tuto změnu:

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

Výsledné ACI je:

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

Hodnoty ACI pro Dept ABC jsou při nahrazování ztraceny.

Máte například následující ACI pro záznam:

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

provedeme tyto změny:

```
dn: cn=nějaký záznam
changetype: modify
replace: ibm-filterAclEntry
```



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

```
dn: cn=nějaký záznam
changetype: modify
replace: ibm-filterAclInherit
ibm-filterAclInherit: false
```

Výsledné ACI je:

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

Hodnoty ACI pro Dept ABC jsou při nahrazování ztraceny.

Modifikace-přidání

Pokud ACI nebo entryOwner neexistuje, jsou během ldapmodify-add vytvořeny ACI nebo entryOwner se specifickými hodnotami. Jestliže ACI nebo entryOwner existuje, potom se přidají uvedené hodnoty do daného ACI nebo entryOwner. Například ACI:

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

smodifikací:

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

by dalo toto aclEntry s více hodnotami:

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

Například ACI:

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

smodifikací:

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

by dalo toto aclEntry s více hodnotami:

```
Ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
                    :grant:rsc
ibm-filterAclEntry: group:cn=Dept ABC,o=IBM:(cn=Manager ABC):at.attribute1
                    :grant:rsc
```

Povolení pod stejným atributem nebo třídou atributu se považují za základní stavební bloky a akce se považují za kvalifikátory. Pokud se přidává stejná hodnota povolení více než jednou, ukládá se pouze jedna hodnota. Jestliže se přidává více než jednou stejná hodnota povolení s jinými hodnotami akce, použije se hodnota poslední akce. Pokud je pole výsledného povolení prázdné (""), je tato hodnota povolení nastavena na nulu a hodnota akce je nastavena na **udělit**.

Například ACI:

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

smodifikací:


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

dává záznam aclEntry:

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

Například ACI:

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

smodifikací:

```
dn: cn=nějaký záznam
changetype: modify
add: ibm-filterAclEntry
ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):normal
:deny:r:critical:deny::sensitive:grant:r
```

dává záznam aclEntry:

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

Modifikace-vymazání

Chcete-li vymazat konkrétní hodnotu ACI, použijte obvyklou syntaxi ldapmodify-delete.

Máte například ACI:

```
aclEntry: group:cn=Dept XYZ,o=IBM:object:grant:ad
aclEntry:
group:cn=Dept XYZ,o=IBM:normal:grant:rWSC
```

```
dn: cn =
nějaký záznam
changetype: modify
delete: aclEntry
aclEntry: group:cn=Dept XYZ,o=IBM:object:grant:ad
```

dává zbývající ACI na serveru:

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

Máte například ACI:

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

```
dn: cn =
nějaký záznam
changetype: modify
delete: ibm-filterAclEntry
ibm-filterAclEntry: group:cn=Dept XYZ,o=IBM:(cn=Manager XYZ):object
:grant:ad
```

dává zbývající ACI na serveru:

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

Vymazání hodnoty ACI nebo entryOwner, která neexistuje, má za následek nezměněné ACI nebo entryOwner a návratový kód uvádějící, že hodnota atributu neexistuje.

Vymazání hodnot ACI/vlastníka záznamu

Při operaci ldapmodify-delete je možné vymazat hodnotu entryOwner, a to tak, že se zadá

```
dn: cn =  
nějaký záznam  
changetype: modify  
delete: entryOwner
```

V tomto případě by záznam následně neměl žádného explicitního vlastníka záznamu (entryOwner). Hodnota ownerPropagate se rovněž vymaže automaticky. Tento záznam by zdědil svůj entryOwner od nadřazeného uzlu v adresářovém stromu podle pravidla propagace.

Totéž je možné provést, chceme-li úplně vymazat aclEntry:

```
dn: cn =  
nějaký záznam  
changetype: modify  
delete: aclEntry
```

Vymazání poslední hodnoty ACI nebo entryOwner ze záznamu není totéž jako vymazání ACI nebo entryOwner. Situace, kdy záznam obsahuje ACI nebo entryOwner bez jakýchkoli hodnot, je možná. V tomto případě, když klient provádí dotaz na ACI nebo entryOwner, se nevrátí nic a nastavení se propaguje na podřízené uzly, dokud není přepsáno. K tomu, aby mohl administrátor adresáře zamezit vzniku slepých záznamů, ke kterým nikdo nemůže získat přístup, má vždy úplný přístup k záznamu, i když má tento záznam nulovou hodnotu ACI nebo entryOwner.

Načtení hodnot ACI/vlastníka záznamu

Efektivní hodnoty ACI nebo entryOwner je možné načíst jednoduše zadáním požadovaného atributu ACL nebo entryOwner při hledání, například:

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

vrátí všechny informace o ACL nebo entryOwner, které se používají při vyhodnocování přístupu v objektu A. Povšimněte si, že návratové hodnoty nemusejí vypadat přesně stejně, jako když byly poprvé definovány. Hodnoty jsou rovnocenné původní formě.

Hledání samotného atributu ibm-filterAclEntry vrátí pouze hodnoty specifické pro obsahující záznam.

Operační atribut pouze pro čtení, ibm-effectiveAcl, se používá k zobrazení akumulovaného efektivního přístupu. Požadavek na hledání ibm-effectiveAcl vrátí efektivní přístup, který platí pro cílový objekt: ACL na základě filtru nebo nezaložené na filtru, v závislosti na tom, jak byly distribuovány v DIT.

Protože ACL na základě filtru mohou pocházet z několika nadřazených zdrojů, hledání atributu aclSource poskytne seznam přiřazených zdrojů.

Hlediska replikace podstromu

U přístupu na základě filtru, který se má začlenit do replikace podstromu, musí být všechny atributy ibm-filterAclEntry umístěny v přidruženém záznamu ibm-replicationContext nebo pod ním.

Protože efektivní přístup nemůže být akumulován z nadřazeného záznamu nad replikovaným podstromem, atribut ibm-filterAclInherit musí být nastaven na hodnotu **false** a umístěn v přidruženém záznamu ibm-replicationContext.

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 Server adresářů 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.

Další informace o metodách práce s vlastnostmi vlastnictví najdete v tématu “Jak provádět správu záznamů adresáře” na stránce 165.

Zásada pro správu hesel

Pro použití serverů LDAP autentizaci je důležité, aby server LDAP podporoval zásady týkající se vypršení hesel, neúspěšných pokusů o přihlášení a pravidel zacházení s hesly. Server adresářů poskytuje konfigurovatelnou podporu pro všechny tyto tři druhy zásad. Tato zásada se aplikuje na všechny záznamy adresáře, které mají atribut `userPassword`. Není možné definovat jednu zásadu pro jednu množinu uživatelů a jiné zásady pro ostatní množiny uživatelů. Server adresářů rovněž poskytuje mechanismus pro informování klientů o stavech souvisejících se zásadou správy hesel (heslo vyprší za tři dny) a sadu operačních atributů, které může administrátor používat při hledání takových subjektů, jako jsou uživatelé s vypršenými hesly nebo uzamčenými účty.

Další informace o způsobech práce s vlastnostmi zásady pro správu hesel najdete v tématu “Jak spravovat hesla” na stránce 147.

Konfigurace

Chování serveru, pokud se týká hesel, je možné konfigurovat v těchto oblastech:

- Globální přepínač “zapnutí/vypnutí” pro aktivaci nebo deaktivaci zásady správy hesel.
- Pravidla pro změnu hesel, včetně těchto:
 - Uživatelé mohou měnit svá vlastní hesla. Povšimněte si, že tato zásada platí jako doplněk k jakémukoli řízení přístupu. Jinými slovy, řízení přístupu musí uživateli poskytnout oprávnění měnit atribut `userPassword` i zásadu správy hesel umožňující uživatelům měnit svá vlastní hesla. Pokud je tato zásada vypnuta, uživatelé nemohou měnit svá vlastní hesla. Heslo pro určitý záznam může měnit pouze administrátor nebo jiný uživatel s oprávněním měnit atribut `userPassword`.
 - Hesla musí být měněna po obnovení původních hodnot. Pokud je tato zásada zapnuta a heslo je změněno kýmoli jiným než uživatelem, je heslo označeno za nastavené na původní hodnotu a uživatel je musí změnit, než může provádět jiné operace v adresáři. Požadavek na spojení s heslem nastaveným na původní hodnotu je úspěšné. K tomu, aby se aplikace mohla dozvědět, že je nutné heslo nastavit na původní hodnotu, musí být informovaná o zásadě správy hesel.
 - Uživatelé musejí při změně hesla zadávat stará hesla. Pokud je tato zásada zapnuta, heslo je možné změnit jen prostřednictvím požadavku na modifikaci, který obsahuje jak vymazání atributu `userPassword` (se starou hodnotou), tak přidání nové hodnoty `userPassword`. To zaručuje, že heslo může měnit pouze uživatel, který je zná. Administrátor nebo ostatní uživatelé s oprávněním měnit atribut `userPassword` mohou nastavit heslo vždy.
- Pravidla pro vypršení platnosti hesla, včetně těchto:
 - Platnost hesla nikdy nevyprší nebo jeho platnost vyprší po nastavitelné době od okamžiku, kdy byla naposledy změněna.
 - Nevarujte uživatele, kdy platnost hesla vyprší nebo varujte uživatele konfigurovatelnou dobu před koncem platnosti hesla. K tomu, aby bylo možno aplikaci varovat ohledně vypršení platnosti hesla, musí být informována o zásadě správy hesel.

- Umožněte provedení konfigurovatelného počtu dodatečných přihlášení po vypršení platnosti hesla uživatele. Aplikace informovaná o zásadě správy hesel bude uvědoměna o počtu zbývajících dodatečných přihlášení. Pokud nejsou povolena žádná dodatečná přihlášení, uživatel se nemůže autentizovat nebo změnit své vlastní heslo, jakmile jeho platnost vypršela.
- Pravidla pro ověření platnosti hesel, včetně těchto:
 - Konfigurovatelná velikost historie hesel, která určuje serveru, aby uchovával historii posledních N hesel a vyřazoval hesla, která byla použita dříve.
 - Kontrola syntaxe hesla, včetně nastavení způsobu, jakým by se měl server chovat při použití hesel s přepočtem klíče. Uvedené nastavení ovlivňuje to, zda by měl server ignorovat tuto zásadu za některých z těchto podmínek:
 - Server uchovává hesla s přepočtem klíče.
 - Klient nabídne serveru heslo s přepočtem klíče (to se může stát při přenosu záznamů mezi servery prostřednictvím souboru LDIF, když zdrojový server uchovává hesla s přepočtem klíče).

V kterémkoli z těchto případů nemusí být server schopen aplikovat všechna pravidla syntaxe. Jsou podporována tato pravidla syntaxe: minimální délka, minimální počet abecedních znaků, minimální počet číselných nebo speciálních znaků, počet opakovaných znaků a počet znaků, v nichž se heslo musí lišit od předchozího hesla.

- Pravidla pro neúspěšná přihlášení, včetně těchto:
 - Minimální povolená doba mezi změnami hesla, což zamezuje uživatelům rychle cyklicky střídát sadu hesel a dostat se zpět ke svým původním heslům.
 - Maximální počet neúspěšných pokusů o přihlášení předtím, než je účet uzamčen.
 - Konfigurovatelná doba trvání uzamčení hesla. Po uplynutí této doby je možné použít předchozí uzamčený účet. To může přispět k blokování hackera pokoušejícího se prolomit heslo a přitom pomoci uživateli, který zapomněl své heslo.
 - Konfigurovatelná doba, po kterou server sleduje neúspěšné pokusy o přihlášení. Pokud během této doby dojde k maximálnímu stanovenému počtu neúspěšných pokusů o přihlášení, účet je uzamčen. Jakmile tato doba vyprší, server vyřadí informace o předchozích neúspěšných pokusech o přihlášení k účtu.

Nastavení zásady správy hesel pro server adresářů se ukládají do objektu "cn=pwdpolicy", který vypadá takto:

```
cn=pwdpolicy
objectclass=container
objectclass=pwdPolicy
objectclass=ibm-pwdPolicyExt
objectclass=top
cn=pwdPolicy
pwdExpireWarning=0
pwdGraceLoginLimit=0
passwordMaxRepeatedChars=0
pwdSafeModify=false
pwdattribute=userpassword
pwdinhistory=0
pwdchecksyntax=0
passwordminotherchars=0
passwordminalphachars=0
pwdminlength=0
passwordmindiffchars=0
pwdminage=0
pwdmaxage=0
pwdallowuserchange=true
pwdlockoutduration=0
ibm-pwdpolicy=true
pwdlockout=true
pwdmaxfailure=2
pwdfailurecountinterval=0
pwdmustchange=false
```

Aplikace informované o zásadě správy hesel

Podpora zásady správy hesel serveru adresářů pro iSeries obsahuje sadu ovladačů LDAP, které může aplikace informovaná o zásadě správy hesel použít k získávání oznámení o dalších stavech týkajících se zásady správy hesel.

Aplikace může být informována o těchto varovných stavech:

- Zbývající doba do vypršení platnosti hesla.
- Počet dodatečných přihlášení po vypršení platnosti hesla.

Aplikace může být informována rovněž o těchto chybových stavech:

- Platnost hesla vypršela.
- Účet je uzamčen.
- Heslo bylo nastaveno na původní hodnotu a musí se změnit.
- Uživateli není povoleno změnit své heslo.
- Při změně hesla se musí zadat staré heslo.
- Nové heslo porušuje pravidla syntaxe.
- Nové heslo je příliš krátké.
- Heslo bylo změněno příliš nedávno.
- Nové heslo je obsaženo v historii.

Používají se dva ovladače. Ovladač požadavků zásady správy hesel se používá k informování serveru, že příslušná aplikace chce být informována o stavech souvisejících se zásadou správy hesel. Tento ovladač musí být specifikován aplikací u všech operací, se kterými souvisí, typicky u požadavku na výchozí spojení a u jakýchkoli požadavků na změnu hesla. Pokud existuje ovladač požadavků zásady správy hesel a když se vyskytne kterýkoli z výše uvedených chybových stavů, ze serveru se vrátí řízení odezvy zásady správy hesel.

Rozhraní API klienta serveru adresářů obsahují sadu rozhraní API, které mohou použít aplikace C k práci s těmito ovladači. Tato rozhraní API jsou:

- ldap_parse_pwdpolicy_response
- ldap_pwdpolicy_err2string

U aplikací nepoužívající tato rozhraní API jsou ovladače definovány níže. Je nutné aplikovat funkce poskytované rozhraními API klienta LDAP používané pro zpracování ovladačů. Například rozhraní JDNI (Naming and Directory Interface) prostředí Java má vestavěnou podporu pro některé známé ovladače a rovněž poskytuje rámec pro podporu ovladačů, které JNDI nerozpoznává.

Řízení požadavků zásady správy hesel

Jméno ovladače: 1.3.6.1.4.1.42.2.27.8.5.1

Kritický stav ovladače: FALSE

Hodnota ovladače: žádná

Řízení odezvy zásady správy hesel

Jméno ovladače: 1.3.6.1.4.1.42.2.27.8.5.1 (stejně jako u řízení požadavků)

Kritický stav ovladače: FALSE

Hodnota ovladače: kódovaná hodnota BER definovaná v ASN.1 takto:

```
PasswordPolicyResponseValue ::= SEQUENCE {
  warning [0] CHOICE OPTIONAL {
    timeBeforeExpiration [0] INTEGER (0 .. MaxInt),
    graceLoginsRemaining [1] INTEGER (0 .. maxInt) }
  error [1] ENUMERATED OPTIONAL {
    passwordExpired (0),
    accountLocked (1),
    changeAfterReset (2),
    passwordModNotAllowed (3),
    mustSupplyOldPassword (4),
```

```
invalidPasswordSyntax (5),
passwordTooShort      (6),
passwordTooYoung      (7),
passwordInHistory     (8) } }
```

Tak jako je tomu u jiných prvků protokolu LDAP, kódování BER používá implicitní značení.

Operační atributy zásady správy hesel

Server adresářů uchovává sadu operačních atributů pro každý záznam, který obsahuje atribut userPassword. Oprávnění uživatelé mohou tyto atributy vyhledávat a buď je použijí ve filtrech hledání, nebo jsou vráceny z požadavků na hledání. Tyto atributy jsou:

- pwdChangedTime - atribut GeneralizedTime obsahující čas, kdy bylo naposledy změněno heslo.
- pwdAccountLockedTime - atribut GeneralizedTime obsahující čas, kdy byl naposledy uzamčen účet. Pokud účet není uzamčen, tento atribut se neobjevuje.
- pwdExpirationWarned - atribut GeneralizedTime obsahující čas, kdy bylo poprvé klientovi zasláno varovné hlášení o vypršení hesla.
- pwdFailureTime - atribut GeneralizedTime s více hodnotami obsahující časy předchozích po sobě jdoucích neúspěšných přihlášení. Jestliže bylo poslední přihlášení úspěšné, tento atribut se neobjevuje.
- pwdGraceUseTime - atribut GeneralizedTime s více hodnotami obsahující časy předchozích dodatečných přihlášení.
- pwdReset - booleovský atribut obsahující hodnotu TRUE (pravdivý výrok), pokud bylo heslo nastaveno na původní hodnotu a uživatel je musí změnit.
- ibm-pwdAccountLocked - booleovský atribut indikující, že daný účet byl administračně uzamčen.

Replikace zásady správy hesel

Informace o zásadě správy hesel replikují dodavatelské servery na odběratele. Změny záznamu cn=pwdpolicy se replikují jakožto globální změny, stejně jako změny schématu. Informace o stavu zásady správy hesel pro jednotlivé záznamy se rovněž replikují, takže jestliže je například nějaký záznam uzamčen na dodavatelském serveru, bude tato akce replikována na jakékoli odběratele. Stav zásady správy hesel na replice pouze pro čtení se však nereplikuje na žádné jiné servery.

Autentizace

Řízení přístupu v rámci serveru adresářů je založeno na rozlišovacím jménu (DN) přidruženém k danému připojení. Toto DN je stanoveno jako výsledek připojení (přihlášení) k serveru adresářů.

Po prvním nakonfigurování serveru adresářů je možno k autentizaci na server použít tyto identity:

- Anonymous
- administrátor adresáře (standardně cn=administrator)
- projektovaný uživatelský profil i5/OS (viz téma “Procedura Backend projektovaná operačním systémem” na stránce 74)

Vhodné je vytvořit další uživatele, kterým je možné udělit oprávnění spravovat různé části adresáře, aniž by to od vás vyžadovalo sdílet identitu administrátora adresáře.

| Další informace najdete v tématu “Jak provádět správu uživatelů” na stránce 172.

Z hlediska LDAP existují dvě základní struktury pro autentizaci do LDAP:

- Jednoduché připojení, v němž aplikace poskytuje DN a čitelné textové heslo pro toto DN
- | • SASL (Simple Authentication and Security Layer), které poskytuje několik dalších autentizačních metod včetně
- | • CRAM-MD5, DIGEST-MD5, EXTERNAL, GSSAPI a OS400-PRFTKN.

Jednoduché připojení, DIGEST-MD5 a CRAM-MD5

K tomu, aby klient mohl používat jednoduché připojení, musí zadat DN existujícího záznamu LDAP a heslo, které odpovídá atributu userPassword pro tento záznam. Například by bylo možné vytvořit záznam pro osobu jménem John Smith takto:

```
sample.ldif:
dn: cn=John Smith,cn=users,o=acme,c=us
objectclass: inetorgperson
cn: John Smith
sn: smith
userPassword: mypassword
```

```
ldapadd -D cn=administrator -w secret -f sample.ldif
```

Při řízení přístupu nyní můžete použít DN "cn=John Smith,cn=users,o=acme,c=us" nebo z něj můžete učinit člena skupiny používané při řízení přístupu.

Zadávat userPassword umožňuje několik předdefinovaných tříd objektů, včetně (aniž by byl tento seznam úplný): person, organizationalperson, inetorgperson, organization, organizationalunit a dalších.

U hesel serveru adresářů se rozlišuje velikost písmen. Pokud vytvoříte záznam s hodnotou userPassword tajné, připojení, které zadává heslo TAJNÉ, bude neúspěšné.

Při použití jednoduchého připojení klient odesílá čitelné textové heslo do serveru jako součást požadavku na připojení. To zvyšuje riziko odhalení hesla na úrovni protokolu. K ochraně hesla by se mohlo používat připojení SSL (všechny informace zasílané přes připojení SSL jsou šifrovány). Další možností je použití metod SASL - DIGEST-MD5 nebo CRAM-MD5.

Metoda CRAM-MD5 vyžaduje, aby měl server přístup k čitelnému textovému heslu (ochrana hesla je nastavena na žádná, což ve skutečnosti znamená, že heslo je uloženo v dekódovatelné formě a vrací se při hledání jako čitelný text), a aby systémová hodnota QRETSVRSEC byla nastavena na 1. Klient odesílá DN na server. Server načte hodnotu userPassword pro daný záznam a vygeneruje náhodný řetězec. Tento náhodný řetězec se odešle ke klientovi. Jak klient, tak server přepočítávají náhodný řetězec s použitím hesla i klíče a klient odesílá výsledek do serveru. Jestliže se oba dva přepočítané řetězce shodují, požadavek na připojení je úspěšný, a přitom heslo nemuselo být nikdy odesláno na server.

Metoda DIGEST-MD5 je podobná metodě CRAM-MD5. Vyžaduje, aby měl server přístup k čitelnému textovému heslu (ochrana hesla je nastavena na žádná) a aby systémová hodnota QRETSVRSEC byla nastavena na 1. Namísto odeslání DN na server metoda DIGEST-MD5 vyžaduje, aby klient odeslal na server hodnotu username. Aby bylo možno použít metodu DIGEST-MD5 pro běžného uživatele (nikoliv administrátora), vyžaduje se, aby žádné další záznamy v adresáři neměly stejnou hodnotu pro atribut username. Další rozdíly u metody DIGEST-MD5 zahrnují více konfiguračních voleb: doména serveru, atribut username a heslo administrátora. Systém iSeries umožňuje uživatelům, aby se připojovali jako projektovaní nebo publikovaní uživatelé, přičemž server ověřuje dodané heslo proti heslu uživatelského profilu v systému. Vzhledem k tomu, že čitelné textové heslo pro uživatelské profily nemá server k dispozici, nelze metodu DIGEST-MD5 používat u projektovaných nebo publikovaných uživatelů.

Další informace najdete v tématu "Jak aktivovat autentizaci DIGEST-MD5 na serveru adresářů" na stránce 154.

Připojení jako publikovaný uživatel

Server adresářů poskytuje prostředky k tomu mít záznam LDAP, jehož heslo je shodné s heslem uživatelského profilu operačního systému na stejném systému. Aby to bylo možné, záznam:

- musí mít atribut UID, jehož hodnotou je jméno uživatelského profilu operačního systému
- nesmí mít atribut userPassword

Když server obdrží požadavek na připojení záznamu, který má hodnotu UID, ale žádný userPassword, server volá zabezpečení operačního systému, aby se ověřilo, že příslušný UID je platné jméno uživatelského profilu a že toto zadané heslo je správné heslo pro tento uživatelský profil. Takový záznam je označován jako publikovaný uživatel v souvislosti s publikováním systémového distribučního adresáře (SDD) v LDAP, které takové záznamy vytváří.

Připojení jako projektovaný uživatel

Záznam LDAP představující uživatelský profil operačního systému je označován jako projektovaný uživatel. DN projektovaného uživatele je možné použít spolu se správným heslem pro tento uživatelský profil v jednoduchém připojení. Například DN pro uživatele JSMITH v systému my-system.acme.com by bylo:

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

Připojení SASL EXTERNAL

Pokud se pro autentizaci klienta používá SSL nebo TLS (klient má například soukromý certifikát), je možné využívat metodu SASL EXTERNAL. Tato metoda přikazuje serveru, aby získal klientovu identitu z vnějšího zdroje, v tomto případě z připojení SSL. Server získá veřejnou část klientova certifikátu (zaslanou na server jako součást vytvoření připojení SSL) a extrahuje DN subjektu. Toto DN server LDAP přiřadí k příslušnému připojení.

Máte například certifikát přiřazený k:

```
obecné jméno: John Smith
organizační jednotka: Engineering
organizace: ACME
místo: Minneapolis
stát: MN
země: US
```

DN subjektu by bylo:

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

Povšimněte si, že při generování DN subjektu se prvky cn, ou, o, l, st a c používají v uvedeném pořadí.

Připojení SASL GSSAPI

Mechanismus připojení SASL GSSAPI se používá pro autentizaci k serveru s využitím tiketu Kerberos. To je užitečné, když klient uskutečnil KINIT nebo jinou formu autentizace Kerberos (například přihlášení do domény Windows 2000). V tomto případě server ověřuje klientův tiket a potom získává hlavní jméno a jméno sféry Kerberos; například hlavní jméno jsmith ve sféře acme.com, normálně vyjádřeno jako jsmith@acme.com. Server může být konfigurován tak, aby mapoval tuto identitu k DN jedním z těchto dvou způsobů:

- Vytvoření nepravého DN s tvarem ibm-kn=jsmith@acme.com.
- Hledání záznamu, který má pomocnou třídu ibm-securityidentities a hodnotu altsecurityidentities tvaru KERBEROS:<hlavní>@<sféra>.

Záznam, který by se mohl použít pro jsmith@acme.com, by mohl vypadat takto:

```
dn: cn=John Smith,cn=users,o=acme,c=us
objectclass: inetorgperson
objectclass: ibm-securityidentities
cn: John Smith
sn: Smith
altsecurityidentities: kerberos:jsmith@acme.com
```

Informace o způsobu aktivace autentizace Kerberos najdete v tématu “Jak aktivovat autentizaci Kerberos na serveru adresářů” na stránce 153.

Připojení OS400-PRFTKN

Mechanismus připojení OS400-PRFTKN SASL se používá pro autentizaci k serveru s využitím tokenu profilu (viz část Tvorba tokenu profilu rozhraní API). Při použití tohoto mechanismu server ověřuje platnost tokenu profilu a přiřadí k připojení DN projektovaného uživatele (například os400-profile=JSMITH,cn=accounts,os400-system=my-as400.mycompany.com). Pokud již aplikace má token profilu, tento mechanismus odstraňuje nutnost získávat jméno uživatelského profilu a uživatelského hesla při uskutečňování jednoduchého připojení. Jestliže chcete mechanismus využívat, prostřednictvím rozhraní API ldap_sasl_bind s zadejte pro mechanismus nulové jméno DN OS400-PRFTKN a berval (binární data, která jsou zakódována pomocí zjednodušených kódovacích pravidel) obsahující 32bajtový token profilu pro příslušná pověření. Když se pro přístup na lokální server adresářů používají LDAP API v operačním systému i5/OS nebo příkazové utility QSH (jako např. ldapsearch), můžete heslo vynechat a API klienta provedou autentizaci na server jako aktuální uživatelský profil pro tuto úlohu. Například:

```
> ldapsearch -m OS400-PRFTKN -b "o=ibm,c=us" "(uid=johndoe)"
```

provede vyhledávání pod oprávněním aktuálního uživatelského profilu, jako kdybyste použili:

```
> ldapsearch -D os400-profile=myprofile,cn=accounts,os400-sys=mysystem -w mypassword -b "o=ibm,c=us" "(uid=johndoe)"
```

LDAP jako autentizační služba

LDAP běžně poskytuje autentizační službu. Webový server je možné konfigurovat tak, aby prováděl autentizaci pro LDAP. Nastavením několika webových serverů (nebo jiných aplikací) na provádění autentizace pro LDAP můžete vytvořit jediný uživatelský registr pro tyto aplikace namísto nutnosti definovat uživatele znovu a znovu pro každou aplikaci nebo instanci webového serveru.

Jak to funguje? Stručně řečeno, webový server vyzve uživatele k zadání jména uživatele a hesla. Webový server tyto informace převezme a potom v adresáři LDAP provede hledání záznamu s tímto jménem uživatele (například by bylo možné konfigurovat webový server tak, aby mapoval jméno uživatele na atributy LDAP 'uid' nebo 'mail'). Jestliže webový server najde přesně jeden záznam, vyšle na server požadavek na připojení s použitím DN záznamu, který právě našel, spolu s heslem, které uživatel zadal. Je-li připojení úspěšné, uživatel je nyní autentizován. Připojení SSL je možné používat k ochraně údajů hesla před odhalením na úrovni protokolu.

Webový server může rovněž sledovat použité DN, aby daná aplikace mohla toto DN využívat, například uložením údajů o uživatelském přizpůsobení v tomto záznamu, jiném záznamu k němu přidruženém nebo v samostatné databázi s využitím DN jako klíče pro hledání těchto informací.

Běžná alternativa k použití požadavku na připojení je použití porovnávací operace LDAP, například `ldap_compare(ldap_session, dn, "userPassword", enteredPassword)`. To umožňuje, aby příslušná aplikace použila jedinou relaci LDAP namísto spouštění a ukončování relací pro každý požadavek na autentizaci.

Odmítnutí služeb

- | Server adresářů chrání proti těmto typům útoků zaměřených na odmítnutí služeb (denial of service):
 - | • Klienti, kteří odesílají data pomalu, odesílají částečná data nebo neposílají žádná data.
 - | • Klienti, kteří nečtou výsledky dat nebo čtou výsledky pomalu.
 - | • Klienti, kteří se neodpojí.
 - | • Klienti, kteří posílají požadavky, jež produkují dlouhotrvající databázové požadavky.
 - | • Klienti, kteří se připojují anonymně.
 - | • Stáhnutí na server, která zabraňují administrátorům provádět administraci serveru.
- | Server adresářů poskytuje administrátorům několik metod jak zabránit útokům zaměřeným na odmítnutí služeb.
- | Administrátor má stále přístup na server prostřednictvím nouzového vlákna, a to dokonce i tehdy, když je server zaneprázdněný dlouhotrvajícími operacemi. Kromě toho má administrátor kontrolu nad přístupem na server včetně

| schopnosti odpojit klienty s konkrétním připojovacím DN nebo IP adresou a nakonfigurovat server tak, aby
| nepovoloval anonymní přístupy. Lze aktivovat i další konfigurační volby, které serveru umožní aktivně předcházet
| útokům zaměřeným na odmítnutí služeb.

| Další informace najdete v těchto tématech:

- | • “Jak spravovat připojení serveru” na stránce 111
- | • “Jak spravovat vlastnosti připojení” na stránce 112

Procedura Backend projektovaná operačním systémem

Procedura Backend projektovaná systémem má schopnost mapovat objekty operačního systému i5/OS jako záznamy v rámci adresářového stromu přístupného z LDAP. Projektované objekty jsou LDAP reprezentacemi objektů v operačním systému namísto skutečných záznamů uložených v databázi serveru LDAP. Uživatelské profily jsou jedinými objekty, které jsou mapovány nebo projektovány jako záznamy v adresářovém stromu. Mapování objektů uživatelských profilů se nazývá procedura Backend projektovaná uživatelem operačního systému.

Operace LDAP jsou mapovány do objektů operačního systému a operace LDAP provádějí funkce operačního systému, aby tak mohly přistupovat k těmto objektům. Všechny operace LDAP prováděné v uživatelských profilech jsou uskutečňovány s oprávněním uživatelského profilu asociovaným s připojením klienta.

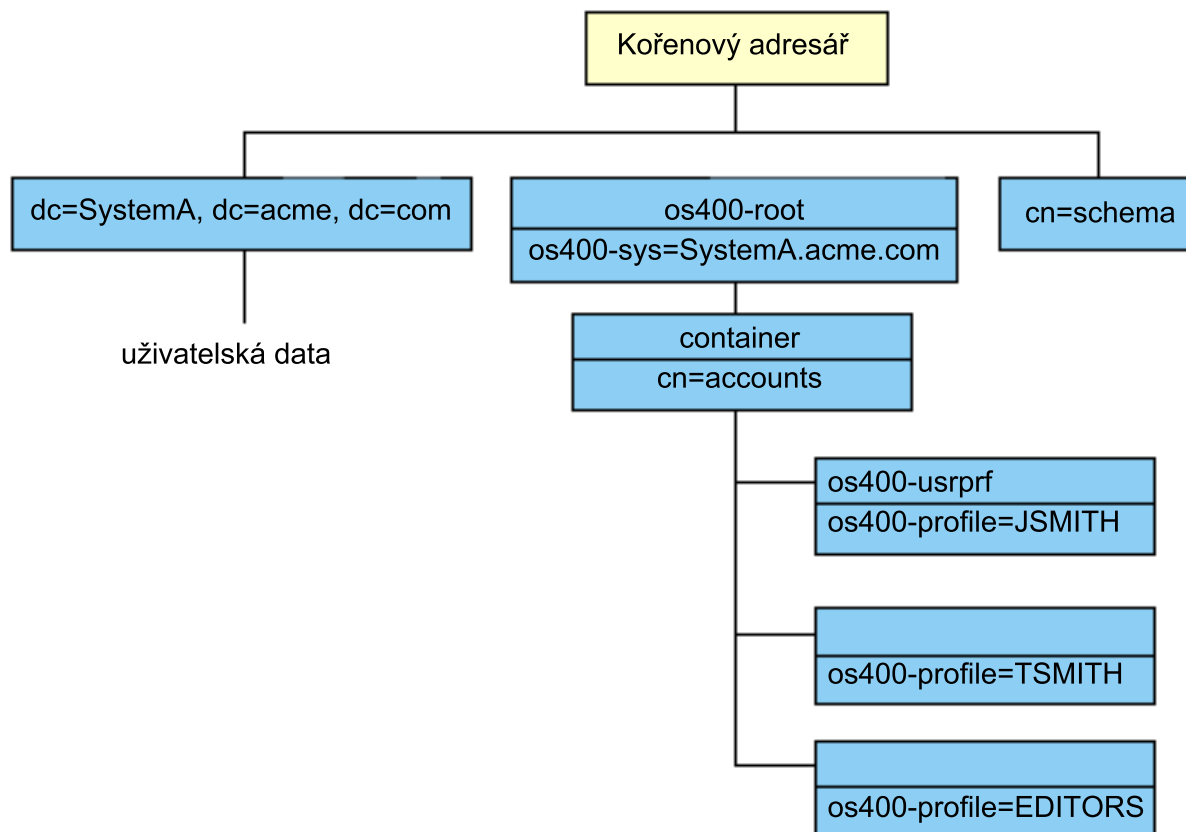
Podrobnější informace o proceduře Backend projektované operačním systémem najdete v těchto částech:

- “Stromová struktura adresáře projektovaná uživatelem”
- “Operace LDAP” na stránce 75
- “Připojovací DN administrátora a repliky” na stránce 79
- “Schéma projektované uživatelem” na stránce 79

Stromová struktura adresáře projektovaná uživatelem

Níže uvedený obrázek ukazuje příklad adresářového stromu, neboli DIT (directory information tree) pro 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.

Pro ilustraci je na obrázku uvedena přípona dc=SystemA, dc=acme, dc=com. Tato přípona představuje proceduru typu “Backend” aktuální databáze, která spravuje ostatní záznamy LDAP. Přípona cn=schema reprezentuje aktuální používané schéma pro celý server.



Kořenem stromu je přípona, která má předem stanovenou hodnotu `os400-sys=SystemA.acme.com`, kde *SystemA.acme.com* je jméno vašeho systému. Atribut objectclass je `os400-root`. Ačkoli strom DIT nemůže být modifikován nebo vymazán, je možné konfigurovat příponu systémových objektů. Je však nutné zabezpečit, aby aktuální přípona nebyla používána v seznamech ACL nebo někde jinde v systému, kde je potřeba modifikovat záznamy v případě, že by se přípona změnila.

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

Operace LDAP

Toto jsou operace LDAP, které mohou být prováděny pomocí projektovaných uživatelských profilů.

Připojení

Klient LDAP může být připojen (autentizován) na server LDAP pomocí projektovaného uživatelského profilu. To se provádí zadáním rozlišovacího jména (DN) projektovaného uživatelského profilu pro připojovací DN spolu se správným heslem uživatelského profilu 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.

Pro autentizaci k serveru adresářů jako projektovaný uživatel lze použít dva další mechanismy:

- Připojení GSSAPI SASL. Jestliže je operační systém konfigurován tak, aby mohl využívat EIM (Enterprise Identity Mapping), server adresářů se dotáže EIM na to, zda existuje přidružení z výchozí identity Kerberos k lokálnímu uživatelskému profilu. Pokud takové přidružení existuje, server k uživatelskému profilu přiřadí připojení, které je možné použít k získání přístupu k proceduře Backend projektované systémem. Další informace o EIM najdete v tématu EIM.
- Připojení OS400-PRFTKN SASL. Token profilu je možné použít pro autentizaci pro server adresářů. V tomto případě přiřazuje server připojení k uživatelskému profilu s tokenem profilu.

Server provádí všechny operace pomocí oprávnění tohoto uživatelského profilu. DN projektovaného uživatelského profilu může být použito také v LDAP ACL, stejně jako DN ostatních záznamů LDAP. Metoda jednoduchého připojení je jedinou povolenou metodou připojení v případě, když je v požadavku na připojení specifikován projektovaný uživatelský profil.

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. Systém umožňuje vyhledávat všechny atributy uživatelského profilu kromě hesla a podobných atributů.

U některých filtrů se vrátí pouze hodnoty DN objectclass a os400-profile. Podrobnější informace je však možné získat provedením několika po sobě jdoucích vyhledávání.

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

Tabulka 3. Chování procedury Backend projektované systémem při operacích vyhledávání

Požadované vyhledávání	Výchozí bod vyhledávání	Rozsah vyhledávání	Filtr vyhledávání	Poznámky
Vrácení informací pro os400-sys=SystemA, (volitelně) pro zásobníky pod ním a (volitelně) pro objekty v těchto zásobnicích.	os400-sys=SystemA.acme.com	base, sub nebo one	objectclass=* objectclass=os400-root objectclass=container objectclass=os400-usrprf	Vrácení odpovídajících atributů a jejich hodnot podle zadaného rozsahu a filtru. Pro systémovou příponu objektů a zásobník pod ní se vrátí pevně naprogramované atributy a jejich hodnoty.
Vrácení všech uživatelských profilů.	cn=accounts, os400-sys=SystemA.acme.com	one nebo sub	os400-gid=0	Pro projektované uživatelské profily se vrátí pouze hodnoty rozlišovacího jména (DN), třídy objektu a atributu os400-profile. Pokud je zadán jakýkoli jiný filtr, vrátí se LDAP_UNWILLING_. Vrábí se TO_PERFORM.

Tabulka 3. Chování procedury Backend projektované systémem při operacích vyhledávání (pokračování)

Požadované vyhledávání	Výchozí bod vyhledávání	Rozsah vyhledávání	Filtr vyhledávání	Poznámky
Vrácení všech skupinových profilů.	cn=accounts, os400- sys=SystemA.acme.com	one nebo sub	(!(os400-gid=0))	Pro projektované uživatelské profily se vrátí pouze hodnoty rozlišovacího jména (DN), třídy objektu a atributu os400-profile. Pokud je zadán jakýkoli jiný filtr, vrátí se LDAP_UNWILLING_Vrátí se TO_PERFORM.
Vrácení všech uživatelských a skupinových profilů.	cn=accounts, os400- sys=SystemA.acme.com	one nebo sub	os400-profile=*	Pro projektované uživatelské profily se vrátí pouze hodnoty rozlišovacího jména (DN), třídy objektu a atributu os400-profile. Pokud je zadán jakýkoli jiný filtr, vrátí se LDAP_UNWILLING_Vrátí se TO_PERFORM.
Vrácení informací 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.
Vrácení informací 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 i rozsah jedné úrovně, výsledek vyhledávání by nevrátil žádné hodnoty, protože v DIT pod uživatelským profilem JSMITH se nenachází nic.
Vrácení všech uživatelských a skupinových profilů, 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 rozlišovacího jména (DN), třídy objektu a atributu os400-profile. Pokud je zadán jakýkoli jiný filtr, vrátí se LDAP_UNWILLING_Vrátí se TO_PERFORM.

Tabulka 3. Chování procedury Backend projektované systémem při operacích vyhledávání (pokračování)

Požadované vyhledávání	Výchozí bod vyhledávání	Rozsah vyhledávání	Filtr vyhledávání	Poznámky
Vrácení všech skupinových profilů, 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 rozlišovacího jména (DN), třídy objektu a atributu os400-profile. Pokud je zadán jakýkoli jiný filtr, vrátí se LDAP_UNWILLING_Vrátí se TO_PERFORM.
Vrácení všech uživatelských profilů, 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 rozlišovacího jména (DN), třídy objektu a atributu os400-profile. Pokud je zadán jakýkoli jiný filtr, vrátí se LDAP_UNWILLING_Vrátí se TO_PERFORM.

Porovnávání

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

Přidání a změna

Uživatelské profily můžete vytvořit pomocí operace LDAP přidání nebo je můžete změnit pomocí operace LDAP modifikace.

Výmaz

Pomocí operace LDAP výmaz je možné mazat uživatelské profily. K tomu, aby bylo možné specifikovat chování parametrů DLTUSRPRF OWNBJOPT a PGPOPT, jsou nyní k dispozici dva ovladače serveru LDAP. Tyto ovladače mohou být zadány v operaci LDAP výmaz. Více informací o chování těchto parametrů najdete v tématu popisující příkaz DLTUSRPRF (Výmaz uživatelského profilu).

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

- os400-dltusrprf-ownbjopt 1.3.18.0.2.10.8

Hodnota ovladače je řetězec tohoto tvaru:

- 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 jako řetězec tohoto tvaru:

```
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 mazán 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 v operaci výmazu zadán, 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 import a export dat v rámci procedury Backend projektované systémem nepodporují.

Připojovací DN administrátora a repliky

Projektovaný uživatelský profil můžete zadat jako připojovací DN konfigurovaného administrátora nebo repliky. Použijte 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.

Další informace najdete v tématu “Administrativní přístup” na stránce 54.

Schéma projektované uživatelem

Třídy objektů a atributy z projektované procedury Backend je možné najít ve schématu pro celý server. Jména atributů LDAP jsou ve formátu os400-*nnn*, kde *nnn* > je obvykle klíčové slovo atributu v příkazech uživatelského profilu. Například atribut os400-usrcls odpovídá parametru USRCLS příkazu CRTUSRPRF. Hodnoty atributů odpovídají hodnotám parametrů přijatých příkazy CRTUSRPRF a CHGUSRPRF nebo zobrazeným hodnotám při zobrazování uživatelského profilu. Chcete-li prohlížet definice tříd objektů os400-usrprf a přiřazené atributy os400-xxx, použijte webový nástroj administrace nebo jinou aplikaci.

Server adresářů a podpora žurnálování i5/OS

Server adresářů používá k uchování informací adresáře databázovou podporu operačního systému i5/OS. Server adresářů používá k ukládání záznamů adresáře v databázi vázané zpracování. To vyžaduje podporu žurnálování i5/OS.

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 budou možná vyžadovat změnu nastavení předvolených hodnot, včetně způsobu správy objektů a velikosti prahových hodnot. V případě potřeby můžete uvedené parametry příkazu pro žurnálování změnit. Žurnálování LDAP je standardně nastaveno tak, aby vymazalo staré zásobníky. Je-li nakonfigurován protokol změn a vy si chcete ponechat staré zásobníky, zadejte z příkazového řádku tento příkaz:

```
CHGJRN 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 žurnálování najdete v odstavci “Programy OS/400” v tématu Programování.

Jedinečné atributy

Funkce jedinečných atributů zajišťuje, aby specifikované atributy měly v rámci adresáře vždy jedinečnou hodnotu. Tyto atributy lze specifikovat pouze ve dvou záznamech: `cn=uniqueattribute,cn=localhost` a `cn=uniqueattribute,cn=IBMpolices`. Výsledky hledání pro jedinečné atributy jsou jedinečné pouze pro databázi daného serveru. Výsledky hledání, které obsahují výsledky z odkazovaných databází, nemusí být jedinečné.

Poznámka: Binární atributy, operační atributy, konfigurační atributy a atribut `objectclass` nelze označit jako jedinečné.

Ne všechny atributy lze specifikovat jako jedinečné. Chcete-li zjistit, zda nějaký atribut může být specifikován jako jedinečný, použijte příkaz `ldapexop`:

- Pro atributy, které mohou být jedinečné: `ldapexop -op getattributes -attrType unique -matches true`
- Pro atributy, které nemohou být jedinečné: `ldapexop -op getattributes -attrType unique -matches false`

Další informace o jedinečných attributech najdete v tématu “Jak spravovat jedinečné atributy” na stránce 122.

Operační atributy

Existuje několik atributů, které mají pro server adresářů speciální význam; označují se jako operační atributy. Jsou to atributy, které se uchovávají na serveru a buď odrážejí takové informace o záznamech, které spravuje příslušný server, nebo které ovlivňují činnost serveru. Tyto atributy mají speciální vlastnosti:

- Tyto atributy nejsou vráceny z operace vyhledávání, pokud to není specificky (podle jména) vyžadováno v požadavku na hledání
- Atributy nejsou součástí žádné třídy objektu. Server určuje, které záznamy tyto atributy budou mít.

Server adresářů podporuje tyto sady operačních atributů:

- creatorsName, createTimestamp, modifiersName, modifyTimestamp existují u každého záznamu. Tyto atributy uvádějí připojovací DN a čas, kdy byl záznam poprvé vytvořen nebo naposledy modifikován. Tyto atributy je možné použít pro filtry vyhledávání, například pro vyhledání všech záznamů modifikovaných po uvedeném čase. Tyto atributy nemůže modifikovat každý uživatel. Tyto atributy se replikují na spotřebitelské servery a jsou importovány a exportovány do souborů LDIF.
- ibm-entryuuid. Existuje u každého záznamu, který je vytvořen v době, kdy je server spuštěn ve verzi V5R3 nebo později. Tento atribut je všeobecně jednoznačný řetězcový identifikátor, který server přiřazuje ke každému záznamu v okamžiku vytvoření tohoto záznamu. Je užitečný pro aplikace, které potřebují rozlišovat mezi identicky pojmenovanými záznamy na různých serverech. Atribut s využitím označení času, adresy adaptéru a dalších informací používá algoritmus DCE UUID pro vytvoření ID, který je jedinečný mezi všemi záznamy na všech serverech.
- entryowner, ownersource, ownerpropagate, aclentry, aclsource, aclpropagate, ibm-filteracl, ibm-filteraclinherit, ibm-effectiveAcl. Další informace najdete v tématu “Seznamy přístupových práv” na stránce 55.
- hasSubordinates. Existuje v každém záznamu a má hodnotu TRUE (pravdivý výrok), pokud má záznam podřízené záznamy.
- numSubordinates. Existuje v každém záznamu a obsahuje takový počet záznamů, kolik je v tomto záznamu podřízených záznamů.
- pwdChangedTime, pwdAccountLockedTime, pwdExpirationWarned, pwdFailureTime, pwdGraceUseTime, pwdReset, pwdHistory. Další informace najdete v tématu “Zásada pro správu hesel” na stránce 67.
- subschemasubentry. Existuje v každém záznamu a určuje umístění schématu pro tuto část stromu. To je užitečné u serverů s několika schématy, pokud chcete najít schéma, které můžete použít v této části stromu.

Úplný seznam operačních atributů získáte pomocí této rozšířené operace: `ldapexop -op getattributes -attrType operational -matches true`.

Serverové paměti cache

- Paměti cache LDAP jsou rychlé vyrovnávací paměti používané k ukládání informací LDAP jako jsou dotazy, odpovědi nebo autentizace uživatele pro budoucí použití. Vyladění paměti cache LDAP je kritické pro zdokonalení výkonu.
- Hledání LDAP, které využívá paměť cache LDAP, může být rychlejší než hledání, které vyžaduje připojení do DB2, a to i když jsou informace uloženy v paměti cache DB2. Z toho důvodu může vyladění paměti cache LDAP zdokonalit výkon, neboť eliminuje nutnost volání do databáze. Paměti cache LDAP jsou obzvlášť užitečné pro aplikace, které často načítají opakované informace ukládané do paměti cache.
- V následujících částech jsou popsány jednotlivé paměti cache LDAP a jejich optimální nastavení pro váš systém.
 - “Paměť cache atributů”
 - “Paměť cache filtrů” na stránce 82
 - “Paměť cache záznamů” na stránce 82
 - “Paměť cache seznamů ACL” na stránce 82
- Další informace o konfigurování paměti cache najdete v tématu “Jak přizpůsobit nastavení výkonu” na stránce 125.

Paměť cache atributů

- Paměť cache atributů má výhodu, že je schopna řešit filtry spíše v paměti než v databázi. Její výhodou je také to, že je aktualizována pokaždé, když se provede operace LDAP přidání, vymazání, modifikace nebo modRDN.
- Při rozhodování, které atributy chcete v této paměti ukládat, byste měli zvážit:
 - Množství paměti dostupné serveru.
 - Velikost adresáře.
 - Typy filtrů pro hledání, které aplikace obvykle používá.

Poznámka: Správce paměti cache atributů umí řešit tyto typy jednoduchých filtrů: filtry pro přesnou shodu (exact match) a filtry pro přítomnost. Dále umí řešit složité filtry, které jsou konjunktivní (spojovací) nebo disjunktivní (vylučovací), přičemž podfiltry musí být typu přesná shoda (exact match), přítomnost, konjunktivní nebo disjunktivní.

Ne všechny atributy lze přidávat do paměti cache atributů. Chcete-li zjistit, zda lze určitý atribut přidat do paměti cache atributů nebo ne, použijte příkaz ldapexop:

- Pro atributy, které mohou být přidány: ldapexop -op getattributes -attrType attribute -matches true
- Pro atributy, které nemohou být přidány: ldapexop -op getattributes -attrType attribute -matches false

Ukládání atributů do paměti cache lze nakonfigurovat dvěma způsoby: manuálně nebo automaticky. Chcete-li nakonfigurovat ukládání atributů do paměti cache manuálně, měl by administrátor provést hledání cn=monitor, aby zjistil, jak docílit co nejefektivnějšího ukládání atributů do paměti cache. Tato hledání vrátí aktuální seznam atributů, které jsou ukládány do paměti cache, množství paměti používané každou pamětí cache atributu, celkové množství paměti používané na ukládání atributů do paměti cache a seznam atributů nejčastěji používaných ve filtrech pro hledání. S využitím těchto informací může administrátor změnit množství paměti, které je povoleno používat pro ukládání atributů do paměti cache, a také který atribut má být ukládán do paměti cache, kdykoliv je to nutné, na základě nových hledání cn=monitor.

Anebo může administrátor nakonfigurovat automatické ukládání atributů do paměti cache. Když je aktivováno automatické ukládání atributů do paměti cache, server adresářů sleduje kombinace atributů, které by bylo nejužitečnější ukládat do paměti cache v rámci limitů paměti definovaných administrátorem. Pak aktualizuje ukládání atributů do paměti cache v době a časovém intervalu nakonfigurovaném administrátorem.

Paměť cache filtrů

Když klient vydá dotaz na data a dotaz nelze řešit v paměti pomocí správce paměti cache atributu, přejde dotaz do paměti cache filtru. Tato paměť cache obsahuje ID záznamů uložená do paměti cache. Když dotaz dorazí do paměti cache filtru, mohou nastat dvě alternativy:

- **ID, které odpovídají nastavením filtru použitým v dotazu, se nacházejí v této paměti cache filtru.** Jde-li o tento případ, odešle se do paměti cache záznamu seznam odpovídajících ID záznamů.
- **Odpovídající ID záznamů se nenacházejí v paměti cache filtru.** V tomto případě musí dotaz přistoupit na DB2 a hledat požadovaná data tam.

Chcete-li stanovit, jak velká by měla být paměť cache filtrů, spusťte pracovní zatížení s pamětí cache filtru nastavenou na odlišné hodnoty a měřte rozdíly v operacích za vteřinu.

Počet záznamů, které lze přidat do paměti cache filtru, omezuje konfigurační proměnná FilterCacheBypassLimit. Například pokud je tato proměnná nastavena na 1000, pak filtry pro hledání, kterým vyhovuje více než 1000 záznamů, nejsou do paměti cache filtru přidány. Tak je zabráněno tomu, aby velká neobvyklá hledání přepsala užitečné záznamy paměti cache. Chcete-li stanovit optimální limitní počet záznamů pro paměť cache, spusťte opakovaně pracovní zatížení a měřte průchodnost.

Paměť cache záznamů

Paměť cache záznamů obsahuje data záznamů. Do paměti cache záznamu se posílají ID záznamu. Pokud záznamy, které odpovídají ID záznamu, jsou v této paměti cache, pak se výsledky vrátí klientovi. Pokud tato paměť cache neobsahuje záznamy, které odpovídají ID záznamu, dotaz přejde do příslušné DB2 odpovídajících záznamů.

Chcete-li stanovit, jak velká by měla být paměť cache záznamů, spusťte pracovní zatížení s pamětí cache záznamů nastavenou na odlišné velikosti a měřte rozdíly v operacích za vteřinu.

Paměť cache seznamů ACL

Paměť cache seznamů ACL obsahuje informace týkající se řízení přístupu, jako je vlastník záznamu nebo povolení záznamu pro záznamy, na které se nedávno přistupovalo. Tato paměť cache se používá ke zlepšení výkonu hodnocení

- | přístupu k přidání, vymazání, modifikaci nebo hledání záznamů. Pokud daný záznam není v paměti cache seznamů
- | ACL nalezen, načte se informace týkající se řízení přístupu z databáze. Chcete-li stanovit vhodnou velikost paměti
- | cache seznamů ACL, měřte výkon serveru při použití typického pracovního zatížení a různých velikostech paměti
- | cache seznamů ACL.

Ovladače a přídatné operace

Ovladače

Ovladače poskytují serveru přídatné informace, které umožňují řídit způsob, jimiž má interpretovat daný požadavek. Například v požadavku LDAP pro výmaz je možné zadat ovladač **výmaz podstromu**, který stanoví, že server by měl vymazat záznam a všechny jeho podřízené záznamy namísto vymazání pouze určeného záznamu. Ovladač se skládá ze tří částí:

- Typ ovladače, což je OID určující tento ovladač.
- Indikátor kritičnosti, který určuje způsob, který by se měl server chovat v případě, že ovladač nepodporuje. Tento indikátor má booleovskou hodnotu. FALSE označuje, že ovladač není kritický a server by jej měl ignorovat, pokud jej nepodporuje. TRUE označuje, že ovladač je kritický a celý požadavek by měl být neúspěšný (s chybou nepodporované kritické přípony), pokud server nemůže ovladač rozpoznat.
- Volitelná hodnota ovladače, která obsahuje další informace specifické pro daný ovladač. Obsah hodnoty ovladače se zadává s využitím notace ASN.1. Samotná hodnota jsou data ovladače v kódování BER.

Přídatné operace

Přídatné operace se používají pro spouštění dodatečných operací nad rámec základních operací LDAP. Přídatné operace byly například definovány pro seskupení sady operací do jediné transakce. Přídatná operace se skládá z těchto položek:

- Jméno požadavku, OID, který identifikuje specifickou operaci.
- Volitelná hodnota požadavku, která obsahuje další informace specifické pro danou operaci. Obsah hodnoty požadavku se zadává s využitím notace ASN.1. Samotná hodnota jsou data požadavku v kódování BER.

Přídatné operace obvykle mají rozšířenou odezvu. Odezva se skládá z těchto položek:

- Komponenty standardního výsledku LDAP (chybový kód, odpovídající DN a chybová zpráva).
- Jméno odezvy, OID, který identifikuje typ odezvy.
- Volitelná hodnota, která obsahuje další informace specifické pro danou odezvu. Obsah hodnoty odezvy se zadává s využitím notace ASN.1. Samotná hodnota jsou data odezvy v kódování BER.

Úplný seznam ovladačů a přídatných operací, včetně jejich příslušných identifikátorů OID a popisů, najdete v tématu “Identifikátory objektů (OID)” na stránce 259.

Kapitola 5. Začínáme s produktem Server adresářů

Server adresářů se instaluje automaticky při instalaci operačního systému i5/OS. Server adresářů se nainstaluje s předvolenou konfigurací. Chcete-li zahájit práci se serverem adresářů, postupujte takto:

1. Pokud instalujete vydání V5R4 a předtím jste používali server adresářů na předchozím vydání, prostudujte si pokyny pro migraci. Další informace najdete v tématu “Pokyny pro migraci”.
2. Rozvrhněte si plán svého serveru adresářů. Další informace najdete v tématu “Plánování serveru adresářů” na stránce 89.
3. Chcete-li uživatelsky přizpůsobit nastavení serveru adresářů, spusťte průvodce konfigurací serveru adresářů. Další informace najdete v tématu “Konfigurace serveru adresářů” na stránce 90.
4. Spusťte server. Další informace najdete v tématu “Jak spustit/zastavit server adresářů” na stránce 110.
5. Při tvorbě nebo editaci adresářů LDAP můžete použít webový nástroj administrace. Další informace najdete v tématu “Webová administrace” na stránce 97.
6. Více informací o způsobech provádění různých úkolů při práci se serverem adresářů získáte, když si prostudujete část Kapitola 7, “Jak provádět správu serveru adresářů”, na stránce 109.

Pokyny pro migraci

Server adresářů se instaluje automaticky při instalaci operačního systému i5/OS. Při svém prvním spuštění server automaticky provede migraci veškeré stávající konfigurace a všech dat. To může způsobit dlouhou prodlevu před prvním náběhem serveru.

Poznámka: Migrace konfigurace a souborů schématu se provádí během instalace a prvního spuštění serveru. Když se toto první spuštění serveru dokončí, pak pokud se soubory konfigurace a schématu v `/qibm/userdata/os400/dirsrv` obnoví ze zálohy předchozího vydání, budou schéma a konfigurace pro nové vydání přepsány soubory z předchozího vydání, které již nebudou znovu migrovány. Pokud se provádí obnova schématu a konfigurace z předchozího vydání po migraci, může to způsobit, že se server nespustí nebo jiné nepředvídatelné omyly. Pokud je zálohování konfigurace serveru a schématu žádoucí, měla by se tato data po úspěšném spuštění serveru uložit.

Máte-li server adresářů spuštěn pod V5R3 nebo V5R2, prostudujte si část “Provedení migrace z V5R3 nebo V5R2 na verzi V5R4”.

Máte-li server adresářů spuštěn pod V4R4, V4R5 nebo V5R1, můžete provést migraci svých dat na V5R4. Další informace najdete v tématu “Provedení migrace dat z verzi V4R4, V4R5 nebo V5R1 na verzi V5R4” na stránce 86.

Pokud máte síť replikačních serverů, další informace získáte v tématu “Provedení migrace sítě replikačních serverů” na stránce 87.

Jestliže používáte Kerberos, prostudujte si část “Změna jména služby Kerberos” na stránce 89.

Provedení migrace z V5R3 nebo V5R2 na verzi V5R4

Ve verzi V5R4 operačního systému i5/OS byly do produktu Server adresářů přidány 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 nezbytné 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 nainstalovány nižší verzi produktu iSeries Navigator, měli byste přejít na verzi V5R4.

i5/OS V5R4 podporuje přímý přechod z verze V5R2 na verzi V5R3. Přejíte-li na verzi V5R4 operačního systému i5/OS, automaticky se provede migrace dat adresáře LDAP i souborů schémat adresáře tak, aby odpovídaly formátům verze V5R4.

Když přecházíte na verzi V5R4 operačního systému i5/OS, mějte na paměti několik skutečností spojených s migrací:

- Při přechodu na verzi V5R4 produkt Server adresářů automaticky provede migraci souborů schémat na verzi V5R4 a staré soubory schémat vymaže. Pokud jste však původní soubory schémat odstranili nebo přejmenovali, produkt Server adresářů nemůže provést jejich migraci. Buď se zobrazí chyba nebo produkt Server adresářů usoudí, že tyto soubory již byly migrovány.
- Po přechodu na verzi V5R4 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. Produkt Server adresářů migruje data adresáře na formát V5R4 v okamžiku prvního spuštění serveru nebo prvního importu souboru LDIF. Při plánování vyhradte určitý čas, aby se migrace dat mohla dokončit.
- 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.

Provedení migrace dat z verzí V4R4, V4R5 nebo V5R1 na verzi V5R4

Verze V5R4 operačního systému i5/OS nepodporuje přímý přechod z verze V4R4, V4R5 nebo V5R1. Chcete-li provést migraci z těchto vydání na verzi V5R4, můžete použít jeden z těchto postupů:

- “Přechod z verze V4R4, V4R5 nebo V5R1 na prozatímní vydání”
- “Uložení databázové knihovny a instalace verze V5R4” na stránce 87

Při přechodu z verze V4R4 na jakoukoli vyšší verzi byste si měli uvědomit tyto skutečnosti:


- Verze V4R4 a nižší verze produktu Server adresářů 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 vyšší verzi z verze V4R4 nebo nižší, přizpůsobí produkt Server adresářů 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.
- Přecházíte-li na vyšší verzi z verze V4R4 nebo nižší, uvědomte si, že data adresáře budou potřebovat přibližně dvakrát více prostoru než potřebovaly dříve. Důvodem je to, že ve verzi V4R4 nebo v nižších verzích produkt Server adresářů podporoval pouze znakovou sadu IA5 a data ukládal ve formátu ccsid 37 (jednobajtový formát). Produkt Server adresářů podporuje plnou znakovou sadu ISO 10646. Po přechodu 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.

Přechod z verze V4R4, V4R5 nebo V5R1 na prozatímní vydání

Přímé přechody z verzí V4R4, V4R5 a V5R1 na verzi V5R4 sice nejsou podporovány, jsou však podporovány tyto přechody:

- Přechod z verze V4R4 a V4R5 na verzi V5R1.
- Přechod z verze V4R5 a V5R1 na verzi V5R2.
- Přechod z verze V5R1 a V5R2 na verzi V5R3.
- Přechod z verze V5R2 a V5R3 na verzi V5R4.

Jedním ze způsobů, jak migrovat server Server adresářů, je přejít na prozatímní verzi (V5R2 nebo V5R3) a potom na verzi V5R4. Podrobné informace o činnostech při instalaci operačního systému i5/OS najdete v publikaci *Instalace*


softwaru . Při migraci postupujte podle níže uvedených kroků. Migrace změn schématu se provádí automaticky. Po každé instalaci ověřte, že jsou změny schématu stále přítomny.

1. U verze V4R4 proveďte instalaci verze V5R1. Pak proveďte instalaci verze V5R3.
2. U verze V4R5 proveďte instalaci verze V5R1 nebo V5R2. Pokud nainstalujete verzi V5R1, musíte následně provést instalaci verze V5R2 nebo V5R3.
3. U verze V5R1 proveďte instalaci verze V5R3.
4. Když jste úspěšně přešli na verzi V5R2 nebo V5R3, proveďte instalaci verze V5R4.

5. Spusťte server adresářů, není-li již spuštěn.

Uložení databázové knihovny a instalace verze V5R4

Migraci produktu Server adresářů můžete provést uložením databázové knihovny, kterou produkt Server adresářů používá ve verzi V4R4 nebo V4R5, a potom jejím obnovením po instalaci verze V5R4. To vám ušetří jeden krok - instalaci prozatímní verze. Neprovede se však migrace nastavení serveru, a proto je ho nezbytné znovu nakonfigurovat.

Podrobné informace o činnostech při instalaci operačního systému i5/OS najdete v publikaci *Instalace softwaru* . 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. Pokud byly aktualizace schémat provedeny s využitím souborů LDIF spolu s obslužným programem ldapmodify, vyhledejte tyto soubory, abyste je mohli použít po převedení serveru na novou verzi. Pro zobrazení definic jednotlivých typů atributů a tříd objektů můžete použít nástroj Directory Management Tool nebo webovou administraci. Pokud vaše změny spočívají pouze v přidání nových typů atributů a tříd objektů, udělejte kopii souboru /qibm/userdata/os400/dirsrv/v3.modifiedschema. Tento soubor můžete použít ke konstrukci souboru LDIF obsahujícího aktualizace schématů. Další informace najdete v tématu “Schéma” na stránce 15.
2. Poznamenejte si různá konfigurační nastavení ve vlastnostech serverů Server adresářů, včetně jména databázové knihovny.
3. Uložte databázovou knihovnu, která je uvedena v konfiguraci produktu Server adresářů. Pokud jste konfigurovali protokol změn, bude muset uložit rovněž knihovnu QUSRDIRCL.
4. Poznamenejte si konfiguraci publikování. Konfiguraci publikování, s výjimkou informací o heslu, lze zobrazit pomocí produktu iSeries Navigator, když zvolíte **Vlastnosti** systému a klepnete na kartu **Adresářové služby**.
5. Nainstalujte na systém operační systém i5/OS verzi V5R4.
6. Pomocí produktu EZ-Setup proveďte konfiguraci serveru adresářů.
7. Obnovte databázovou knihovnu, kterou jste uložili v kroku 3. Pokud jste v bodě 3 uložili knihovnu QUSRDIRCL, obnovte ji nyní.
8. Pomocí produktu iSeries Navigator znovu proveďte konfiguraci serveru adresářů. Určete databázovou knihovnu, která byla dříve nakonfigurována a která byla uložena a obnovena v předchozích fázích postupu.
9. Pomocí produktu iSeries Navigator znovu proveďte konfiguraci publikování.
10. Restartujte server adresářů.
11. Pomocí webového administračního nástroje změňte soubory schémat podle uživatelských změn, které jste si poznamenali v kroku 1.

Provedení migrace sítě replikačních serverů

Při prvním spuštění hlavního serveru provede tento server migraci informací v adresáři, který řídí replikaci. Záznamy s třídou objektu replicaObject pod cn=localhost jsou nahrazeny záznamy používanými novým replikačním modelem (více informací najdete v tématu “Replikace” na stránce 36). Hlavní server je konfigurován tak, aby replikoval všechny přípony v adresáři. Záznamy ujednání se vytvoří s atributem ibm-replicationOnHold nastaveným na hodnotu true (pravdivý výrok). To umožňuje akumulaci aktualizací provedených na hlavním serveru pro repliku do té doby, než je replika dokončena.

Tyto záznamy se označují jako replikační topologie. Nový hlavní server je možné použít s replikami spuštěnými v nižších verzích; data související s novými funkcemi nebudou replikována na servery s nižší úrovní. Po provedení migrace replikovaného serveru je nezbytné provést export záznamů replikační topologie z hlavního serveru a přidat je do každé repliky. Chcete-li tyto záznamy exportovat, použijte nástroj pro příkazový řádek Qshell “ldapsearch” na stránce 202 a uložte výstup do souboru. Příkaz pro vyhledávání se zadává například takto:

```
ldapsearch -h master-server-host-name -p master-server-port \  
-D master-server-admin-DN -w master-server-admin-password \  
-b ibm-replicagroup=default,suffix-entry-DN \  
-L "(|(objectclass=ibm-replicaSubEntry)(objectclass=ibm-replicationAgreement))" \  
> replication.topology.ldif
```

Tento příkaz vytvoří v aktuálním pracovním adresáři výstupní soubor LDIF nazvaný replication.topology.ldif. Tento soubor obsahuje pouze nové záznamy.

Poznámka: Nezačleňujte tyto přípony:

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

Začleňte pouze uživatelsky vytvořené přípony.

Opakujte tento příkaz pro každý záznam přípony na hlavním serveru, ale při přidávání dat do výstupního souboru u následujících hledání nahraďte symbol ">" symbolem ">>". Až bude soubor úplný, zkopírujte jej na replikované servery.

Soubor přidávejte na replikované servery až po jejich úspěšné migraci; nepřidávejte jej na servery spuštěné pod nižšími verzemi serveru adresářů. Před přidáním souboru je nutné server spustit a opět zastavit.

Server se spouští pomocí volby **Spustit** v produktu iSeries Navigator. Další informace najdete v tématu "Jak spustit/zastavit server adresářů" na stránce 110.

Server se zastavuje pomocí volby **Zastavit** v produktu iSeries Navigator. Další informace najdete v tématu "Jak spustit/zastavit server adresářů" na stránce 110.

Když přidáváte soubor na replikovaný server, ujistěte se, že replikovaný server není spuštěn. K přidávání dat používejte volbu **Importovat soubor** v produktu iSeries Navigator.

Po zavedení záznamů replikační topologie spusťte replikovaný server a pokračujte v replikaci. Replikaci je možné znovu spustit jedním z těchto způsobů:

- Na hlavním serveru použijte volbu **Manage Queues in Replication Management** webového administračního nástroje.
- Použijte obslužný program pro příkazový řádek **ldapexop**. Například:

```
ldapexop -h master-server-host-name -p master-server-port \  
-D master-server-admin-DN -w master-server-admin-password \  
-op controlrepl -action resume -ra replica-agreement-DN
```

Tento příkaz znovu spustí replikaci pro server definovaný v záznamu se zadaným DN.

Chcete-li určit, které DN ujednání o replikaci odpovídá replikovanému serveru, podívejte se do souboru replication.topology.ldif. Hlavní server zaprotokoluje zprávu, že replikace byla pro tuto repliku spuštěna, a varování, že ID replikovaného serveru v ujednání neodpovídá ID příslušného replikovaného serveru. K tomu, aby ujednání o replikaci používalo správný ID serveru, je nutné je aktualizovat, což je možné provést s použitím volby **Správa replikace** ve webovém nástroji administrace nebo pomocí nástroje pro příkazový řádek **ldapmodify**. Například:

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

Tyto příkazy je možné zadat přímo na příkazový řádek nebo můžete tyto příkazy uložit do souboru LDIF a vložit je do příkazu pomocí volby **-i soubor**. Příkaz můžete ukončit pomocí volby **Ukončit předchozí požadavek**.

Migrace pro tuto repliku je dokončena.

I v případě, že chcete nadále spouštět repliku pod nižší verzí, je nezbytné znovu spustit replikaci s použitím nástroje pro příkazový řádek **ldapexop** nebo volby **Replication Management** ve webovém nástroji administrace pro tuto repliku. Pokud je migrace repliky spuštěná pod nižší verzí provedena později, synchronizujte data adresáře s použitím nástroje pro příkazový řádek **ldapdiff**. To zajistí na replice aktualizaci záznamů nebo atributů, které nebyly replikovány.

Změna jména služby Kerberos

Počínaje verzí V5R3 se změnila jména služeb používaná serverem adresářů a klientskými rozhraními API pro autentizaci GSSAPI (Kerberos). Tato změna je nekompatibilní se jménem služby používaným před verzí V5R3 (V5R2M0 PTF 5722SS1-SI08487 obsahuje stejnou změnu).

Před verzí V5R3 server adresářů a klientská rozhraní API používaly pro autentizaci pomocí mechanismu GSSAPI (Kerberos) jméno služby ve tvaru LDAP/dns-host-name@Kerberos-realm. Toto jméno nevyhovuje standardům, které v definici autentizace GSSAPI stanovují, že hlavní jméno by mělo začínat údajem "ldap" zapsaným malými písmeny. To má za následek, že ani server adresářů ani klientská rozhraní API nejspíše nebudou spolupracovat s produkty ostatních prodejců. To platí zejména v případě, že KDC (key distribution center) služby Kerberos používá hlavní jména s rozlišováním velkých a malých písmen. Příkladem klienta obsaženého v operačním systému, který používá správné jméno služby, je poskytovatel služeb LDAP pro JNDI protokolu LDAP systému Java.

Verze V5R3M0 změnila jméno služby tak, aby těmto standardům vyhovovalo. To však přináší problémy s vlastní kompatibilitou.

- Server adresářů konfigurovaný pro použití autentizace GSSAPI nespustí instalaci tohoto vydání. To se děje z toho důvodu, že soubor klíčů (keytab) využívaný serverem obsahuje pověření používající staré jméno služby (LDAP/mysys.ibm.com@IBM.COM), zatímco server očekává pověření používající nové jméno služby (ldap/mysys.ibm.com@IBM.COM).
- Server adresářů nebo aplikace LDAP používající rozhraní API LDAP ve verzi V5R3M0 možná nebudou schopny provést autentizaci pro starší servery nebo klienty operačního systému OS/400. Tento problém můžete napravit pomocí tohoto postupu:
 1. Jestliže KDC používá hlavní jména s rozlišováním velkých a malých písmen, vytvořte účet s využitím správného jména služby (ldap/mysys.ibm.com@IBM.COM).
 2. Aktualizujte soubor klíčů používaný serverem adresářů tak, aby obsahoval pověření pro nové jméno služby. Můžete rovněž vymazat stará pověření. K aktualizaci souboru klíčů je možné použít obslužný program Qshell pro správu klíčů. Server adresářů standardně používá soubor klíčů /QIBM/UserData/OS400/NetworkAuthentication/keytab/krb5.keytab. Průvodce síťové autentizační služby (Network Authentication Service) Kerberos verze V5R3M0 v produktu iSeries Navigator rovněž vytváří záznamy klíčů s využitím nového jména služby.
 3. Pomocí PTF 5722SS1-SI08487 aktualizujte systémy OS/400 verze V5R2M0, ve kterých se používá GSSAPI.

Případně je možné nechat server adresářů a klientská rozhraní API i nadále používat staré jméno služby. To by mohlo být vhodné v případě, že používáte autentizaci Kerberos ve smíšené síti systémů spuštěných s PTF i bez nich. Pokud chcete využít tuto možnost, nastavte proměnnou prostředí LDAP_KRB_SERVICE_NAME. Tuto proměnnou můžete nastavit pro celý systém (vyžadováno nastavení jména služby pro server) pomocí tohoto příkazu:

```
ADDENVVAR ENVVAR(LDAP_KRB_SERVICE_NAME)
```

nebo v QSH (ovlivní obslužné programy LDAP spuštěné z této relace QSH):

```
export LDAP_KRB_SERVICE_NAME=1
```

Plánování serveru adresářů

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

- **Uspořádejte adresář.** Naplánujte strukturu adresáře a určete, jaké přípony a atributy bude server vyžadovat. Další informace najdete v tématech "Doporučené postupy pro strukturu adresáře" na stránce 96, "Adresáře" na stránce 7, "Přípona (kontext pojmenování)" na stránce 14 a "Atributy" na stránce 19.

- **Rozhodněte se, 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 Server adresářů 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 attributech. Jeho velikost též rapidně vzroste v případě, že adresář obsahuje velké objekty, jako například obrázky.

- **Rozhodněte se, jaká bezpečnostní opatření použijete.**

Server adresářů umožňuje využívat zásadu správy hesel a tak zabezpečit, aby uživatelé měnili svá hesla periodicky a aby tato hesla vyhovovala požadavkům organizace na syntaxi hesel.

Produkt Server adresářů podporuje použití SSL (Secure Sockets Layer) i digitálních certifikátů a TLS (Translation Layer Security), které zajišťují bezpečnost komunikací. Podporována je rovněž autentizace Kerberos.

Produkt Server adresářů umožňuje řídit přístup k objektům adresáře pomocí seznamů přístupových práv (ACL). K zabezpečení adresáře můžete použít i funkci monitorování zabezpečení poskytovanou operačním systémem.

Kromě toho rozhodněte, jakou zásadu správy hesel budete využívat.

- **Zvolte DN a heslo administrátora.** Předvolené DN administrátora je `cn=admin`. To je jediná identita, která má oprávnění vytvářet nebo modifikovat záznamy adresáře při výchozí konfiguraci serveru. Je možné použít předvolené DN administrátora nebo vybrat odlišné DN. Pro DN administrátora také musíte vytvořit heslo.
- **Nainstalujte nezbytný předchozí software pro webový nástroj administrace serveru adresářů.** K tomu, aby bylo možné používat webový nástroj administrace serveru adresářů, je nutné na server nainstalovat tyto nezbytné předchozí produkty:
 - IBM HTTP Server for iSeries (5722-DG1)
 - Aplikační server IBM WebSphere - Express (5722-IWE Base a volba 2)

Další informace o IBM HTTP serveru pro iSeries a aplikačním serveru IBM WebSphere - Express najdete v tématu IBM HTTP Server.

Konfigurace serveru adresářů

1. 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 Server adresářů automaticky s omezenou předvolenou konfigurací. Další informace najdete v tématu "Předvolená konfigurace produktu Server adresářů" na stránce 91. Produkt Server adresářů obsahuje průvodce, který vám pomůže nakonfigurovat server adresářů 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 výchozí konfiguraci serveru adresářů. Průvodce můžete 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 vymazat, 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, musíte mít i zvláštní oprávnění *AUDIT.

2. Ke spuštění průvodce konfigurací produktu Server adresářů použijte tento postup:
 - a. V prostředí produktu iSeries Navigator rozbalte položku **Sít**.

- b. Rozbalte položku **Servery**.
- c. Klepněte na **TCP/IP**.
- d. Pravým tlačítkem myši klepněte na **Server adresářů IBM** a vyberte volbu **Konfigurovat**.

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

3. Proveďte konfiguraci serveru adresářů podle instrukcí, které zobrazuje průvodce konfigurací serveru adresářů.

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 v nezávislé ASP, selžou.

4. Po ukončení průvodce bude server adresářů nastaven podle základní konfigurace. 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. Je nutné provést jeden z následujících kroků:
 - Změnit port, který používá produkt Lotus Domino. Další informace najdete v části “Hostování LDAP produktu Domino a serveru adresářů na stejném systému iSeries” v tématu E-mail.
 - Změnit port, který používá produkt Server adresářů. Další informace najdete v tématu “Jak změnit port nebo IP adresu” na stránce 115.
 - Použít specifické IP adresy. Další informace najdete v tématu “Jak změnit port nebo IP adresu” na stránce 115.
5. Vytvořte záznamy odpovídající příponě nebo příponám, které jste konfigurovali. Další informace najdete v tématu “Jak přidávat a odstraňovat přípony serveru adresářů” na stránce 116.

Dříve, než budete pokračovat, je dále možné provést některé nebo všechny z těchto činností:

- Importovat data na server, viz “Import a export souboru LDIF” na stránce 93.
- Aktivovat zabezpečení pomocí SSL (Secure Sockets Layer), viz “Jak aktivovat SSL a TSL (Transport Layer Security) na serveru adresářů” na stránce 151.
- Aktivovat autentizaci Kerberos, viz “Jak aktivovat autentizaci Kerberos na serveru adresářů” na stránce 153.
- Nastavit odkazy, viz “Jak specifikovat server pro adresářové odkazy” na stránce 116.

Předvolená konfigurace produktu Server adresářů

Server adresářů se instaluje automaticky při instalaci operačního systému i5/OS. Tato instalace zahrnuje předvolenou konfiguraci. Server adresářů používá předvolenou konfiguraci za těchto okolností:

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

Používá-li server adresářů předvolenou konfiguraci, dojde k této situaci:

- Server adresářů 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 Server adresářů.
- Vytvoří se předvolená přípona založená na jménu IP 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 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.

Naplnění adresáře

Existuje řada způsobů jak adresář naplnit. Další informace najdete v těchto částech:

- “Publikování informací na server adresářů”
- “Import a export souboru LDIF” na stránce 93
- “Kopírování uživatelů z ověřovacího seznamu HTTP serveru do serveru adresářů” na stránce 94

Publikování informací na server adresářů

Systém můžete konfigurovat tak, aby publikoval určité informace na server adresářů v témže nebo jiném systému, a to včetně uživatelsky definovaných informací. Operační systém automaticky publikuje tyto informace na server adresářů vždy, když pomocí produktu iSeries Navigator změňte údaje v operačním systému i5/OS. Publikovatelné informace zahrnují systém (systémy a tiskárny), sdílení tisku, informace uživatele a zásady QoS (Quality of Service) TCP/IP (další informace najdete v tématu “Publikování” na stránce 34).

Pokud nadřazené DN, na kterém mají být data publikována, neexistuje, produkt Server adresářů je automaticky vytvoří. I jiné nainstalované aplikace i5/OS mohou publikovat informace v adresáři LDAP. Kromě toho můžete z vlastních programů volat rozhraní API pro publikování dalších typů informací v adresáři LDAP.

Poznámka: Informace operačního systému i5/OS lze publikovat i na serveru adresářů, který není spuštěný pod operačním systémem i5/OS, je-li tento server nakonfigurován tak, aby používal schéma IBM.

Chcete-li nakonfigurovat systém tak, aby mohl publikovat informace systému i5/OS na serveru adresářů, postupujte takto:

1. V prostředí produktu iSeries Navigator klepněte pravým tlačítkem myši na požadovaný systém a vyberte volbu **Vlastnosti**.
2. Klepněte na kartu **Server adresářů**.
3. Vyberte 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 zaškrtačací 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 zobrazí, zadejte jméno serveru adresářů, na kterém chcete publikovat informace systému i5/OS, a klepněte na **OK**.
8. V poli **Pod DN** zadejte nadřazené rozlišovací jméno (DN), pod které chcete na serveru adresářů přidávat informace.
9. V rámečku **Připojení na server** vyplňte pole, která odpovídají vaší konfiguraci.

Poznámka: Chcete-li publikovat informace systému i5/OS na serveru adresářů s využitím SSL nebo Kerberos, je nezbytné nejprve nakonfigurovat daný server adresářů tak, aby používal odpovídající protokol. Více informací o produktech SSL a Kerberos najdete v tématu “Autentizace Kerberos na serveru adresářů” na stránce 47.

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, zobrazí se výzva k jejímu vytvoření.

Poznámka: Jestliže nadřazené DN neexistuje a vy je nevytvoříte, publikování nebude úspěšné.

12. Klepněte na **OK**.

Poznámka: Informace operačního systému i5/OS lze publikovat i na serveru adresářů, který je postaven na jiné platformě. Uživatelské a systémové informace můžete však publikovat pouze na serveru adresářů, který

l používá schéma kompatibilní se schématem produktu IBM Server adresářů. Další informace o schématu
l adresářů IBM najdete v tématu “Schéma serveru adresářů IBM” na stránce 16.

l **Rozhraní API pro publikování informací systému i5/OS na serveru adresářů**

l Produkt Server adresářů poskytuje vestavěnou podporu pro publikování informací o uživateli a systému. Seznam
l těchto položek je uveden na stránce **Server adresářů** systémového dialogu **Vlastnosti**. Pomocí konfigurace serveru
l LDAP a rozhraní API pro publikování můžete umožnit i publikování jiných typů informací prostřednictvím vlastních
l uživatelských programů i5/OS. Tyto typy informací se potom zobrazují i na stránce **Server adresářů**. Stejně jako je
l tomu u uživatelů a systémů, tyto typy nejsou zpočátku povoleny a je nezbytné je nakonfigurovat pomocí stejného
l postupu. Program, který přidává data do adresáře LDAP, se nazývá Publishing Agent. Typ informací, které jsou
l publikovány tak, jak se zobrazují na stránce **Server adresářů**, se nazývá jméno agenta.

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

l **QgldChgDirSvrA**

l Aplikace používá formát CSV0500 pro první přidání jména agenta, které je označeno jako nepovolený
l záznam. Pokyny pro uživatele této aplikace doporučují použít produkt iSeries Navigator k přechodu na
l stránku vlastností Serveru adresářů, kde je možné konfigurovat program Publishing Agent. Jako příklad jmen
l agentů slouží jména agentů pro systémy a uživatele, která se automaticky zobrazují na stránce **Server**
l **adresářů**.

l **QgldLstDirSvrA**

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

l **QgldPubDirObj**

l Toto rozhraní API použijte ke skutečnému publikování informací.

l Podrobné informace o rozhraní API najdete v tématu LDAP (Lightweight Directory Access Protocol) pod heslem
l Programování v rámci aplikace iSeries Information Center.

l **Import a export souboru LDIF**

l **Jak importovat soubor LDIF**

l Informace je možné přenášet mezi různými servery adresářů pomocí souborů LDIF (LDAP Data Interchange Format).
l Další informace najdete v tématu “LDAP data interchange format (LDIF)” na stránce 216. Než spustíte tuto
l proceduru, přesuňte soubor LDIF na server iSeries jako proudový soubor.

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

- l 1. Je-li spuštěn server adresářů, zastavte jej. Informace o zastavení serveru adresářů najdete v tématu “Jak
l spustit/zastavit server adresářů” na stránce 110.
- l 2. V prostředí produktu iSeries Navigator rozbalte položku **Sítě**.
- l 3. Rozbalte položku **Servery**.
- l 4. Klepněte na **TCP/IP**.
- l 5. Pravým tlačítkem myši klepněte na **Server adresářů IBM**, vyberte volbu **Nástroje** a potom volbu **Importovat**
l **soubor**.

l Volitelně je možné nechat server replikovat nově importovaná data při dalším spuštění, a to výběrem **Replikovat**
l **importovaná data**. To je užitečné v případě, že chcete přidávat nové záznamy do existujícího adresářového
l stromu na hlavním serveru. Jestliže importujete data s cílem inicializovat replikovaný (nebo peer) server, obvykle
l nebudete chtít nechat replikovat data, protože na serverech, pro které tento server slouží jako dodavatelský, již
l mohou existovat.

l **Poznámka:** K importu souborů LDIF můžete také použít obslužný program ldapadd (viz “ldapmodify a ldapadd”
l na stránce 187).

l **Jak exportovat soubor LDIF**

Informace lze přenášet mezi různými servery adresářů pomocí souborů LDIF (LDAP Data Interchange Format), viz část “LDAP data interchange format (LDIF)” na stránce 216. 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 **Server adresářů IBM**, vyberte volbu **Nástroje** a potom volbu **Exportovat soubor**.

Poznámka: Nezádáte-li úplnou cestu, kam mají být data souboru LDIF exportována, soubor bude vytvořen v domovském adresáři, který je uveden v uživatelském profilu operačního systému.

5. Zadejte, zda chcete **Exportovat celý adresář** nebo **Exportovat vybraný podstrom**, a také zda chcete **Exportovat operační atributy**. Operační atributy, které se exportují, jsou creatorsName, createTimeStamp, modifiersName a modifyTimeStamp.

Poznámky:

1. Při exportu dat za účelem jejich importu do serveru adresářů verze V5R3 nebo dřívější nevybírejte volbu **Exportovat operační atributy**. Tyto operační atributy nelze do serverů adresářů verze V5R3 nebo dřívějších naimportovat.
2. K vytvoření úplného nebo částečného souboru LDIF můžete použít také obslužný program ldapsearch, jehož popis najdete v tématu “ldapsearch” na stránce 202. Použijte volbu -L a přesměrujte výstup na soubor.
3. 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**.

Kopírování uživatelů z ověřovacího seznamu HTTP serveru do serveru adresářů

Pokud aktuálně používáte nebo jste v minulosti používali HTTP server, asi máte vytvořen ověřovací seznam, ve kterém jsou uloženi internetoví uživatelé a jejich hesla. Když přecházíte na WebSphere Application Server, Portal Server a další aplikace, které podporují autentizaci LDAP, budete zřejmě chtít i nadále používat tyto současné internetové uživatele a jejich hesla. Toto lze provést pomocí rozhraní API QGLDCPYVL (Copy Validation List to Directory).

API QGLDCPYVL přečte záznamy z ověřovacího seznamu a vytvoří odpovídající objekty LDAP v lokálním serveru adresářů. Objekty budou skeletové záznamy inetOrgPerson s atributem userPassword, který obsahuje kopii informace o hesle ze záznamu ověřovacího seznamu. Můžete rozhodnout, jak a kdy bude toto API voláno. Můžete ho použít jako jednorázovou operaci pro ověřovací seznam, který se nebude měnit, nebo jako plánovanou úlohu pro aktualizaci serveru adresářů, která bude reflektovat nové záznamy ověřovacího seznamu.

Podrobnější informace o rozhraní API QGLDCPYVL najdete v tématu API serveru adresářů. Příklad použití tohoto API najdete v tématu “Scénář: Kopírování uživatelů z ověřovacího seznamu HTTP serveru do serveru adresářů”.

Scénář: Kopírování uživatelů z ověřovacího seznamu HTTP serveru do serveru adresářů

Situace a přehled

V současné době provozujete aplikaci na HTTP serveru (na bázi Apache), která používá internetové uživatele v ověřovacím seznamu MYLIB/HTTPVLDL. Stejně internetové uživatele byste chtěli používat i u aplikačního serveru WebSphere Application Server (WAS) s autentizací LDAP. Abyste se vyhnuli duplicitní údržbě uživatelských informací v ověřovacím seznamu a LDAP, nakonfigurujete aplikaci HTTP serveru tak, aby také používala autentizaci LDAP.

Chcete-li toho docílit, postupujte takto:

- | 1. Zkopírujte uživatele existujícího ověřovacího seznamu do lokálního serveru adresářů.
- | 2. Nakonfigurujte server WAS pro použití autentizace LDAP.
- | 3. Překonfigurujte HTTP server tak, aby místo ověřovacího seznamu používal autentizaci LDAP.

| **Krok 1: Zkopírujte uživatele existujícího ověřovacího seznamu do lokálního serveru adresářů**

| Předpokládejme, že server adresářů byl dříve nakonfigurován s příponou "o=my company" a že je spuštěný. Uživatelé LDAP by měli být uloženi v podstromu adresáře "cn=users,o=my company". Jméno DN administrátora serveru adresářů je "cn=administrator" a heslo administrátora je "secret".

| Rozhraní API volejte z příkazového řádku následovně:

```
| CALL PGM(QSYS/QGLDCPYVL) PARM('HTTPVLDL MYLIB      ' 'cn=administrator' X'00000000' 'secret'  
| X'00000000' 'cn=users,o=my company' X'00000000' ' X'00000000' X'00000000')
```

| Po dokončení procedury bude server adresářů obsahovat záznamy inetorgperson na základě záznamů ověřovacího seznamu. Například uživatel z ověřovacího seznamu:

```
| User name: jsmith  
| Description: John Smith  
| Password: *****
```

| bude mít ve výsledku tuto podobu záznamu adresáře:

```
| dn: uid=jsmith,cn=users,o=my company  
| objectclass: top  
| objectclass: person  
| objectclass: organizationalperson  
| objectclass: inetorgperson  
| uid: jsmith  
| sn: jsmith  
| cn: jsmith  
| description: John Smith  
| userpassword: *****
```

| Tento záznam je nyní možné použít pro autentizaci do serveru adresářů. Například při provedení tohoto hledání QSH ldapsearch se přečte kořenový záznam DSE serveru:

```
| > ldapsearch -D "uid=jsmith,cn=users,o=my company" -w ***** -s base "(objectclass=*)"
```


| Když je záznam adresáře vytvořen, můžete ho editovat, aby obsahoval další informace. Například můžete chtít změnit hodnoty cn nebo sn, abyste zadali správně celé jméno uživatele resp. jeho příjmení, nebo přidat telefonní číslo a e-mailovou adresu.

| **Krok 2: Nakonfigurujte server WAS pro použití autentizace LDAP**

| Zabezpečení LDAP serveru WAS je nutno nakonfigurovat tak, aby hledalo záznamy pod dn "cn=users,o=my company" za použití filtru pro hledání, který mapuje zadané jméno uživatele do záznamů inetOrgPerson obsahujících tuto hodnotu atributu uid. Například autentizace do WAS používající jméno uživatele jsmith vyvolá hledání záznamů vyhovujících filtru "(uid=jsmith)". Další informace najdete v tématu Configure LDAP search filters v rámci aplikace Websphere Application Server for iSeries Information Center.

| **Krok 3: Překonfigurujte HTTP server tak, aby místo ověřovacího seznamu používal autentizaci LDAP**

| **Poznámka:** Procedura popsána níže má za cíl ilustrovat příklad v tomto scénáři a prezentuje pouze základní přehled konfigurace HTTP serveru pro použití autentizace LDAP. Podrobnější informace obsahuje červená kniha

| IBM Implementation and Practical Use of LDAP on the IBM eServer iSeries Server, SG24-6193 
| Section 6.3.2 "Setting up LDAP authentication for the powered by Apache server", a také téma Set up password protection on HTTP Server (powered by Apache).

1. Klepněte na volbu **Basic Authentication** na kartě **Configuration** vašeho HTTP serveru v nástroji HTTP Administration.
2. U položky **User authentication method** změňte volbu **Use Internet users in validation lists** na **Use user entries in LDAP server** a klepněte na **OK**.
3. Vraťte se na kartu **Configuration** a klepněte na volbu **Control Access**. Proveďte konfiguraci tak, jak je popsáno v červené knize, na kterou je odkaz výše, a klepněte na **OK**.
4. Na kartě **Configuration** klepněte na volbu **LDAP Authentication**.
 - a. Zadejte port a hostitelské jméno serveru LDAP. Pro **User search base DN** zadejte `cn=users,o=my company`.
 - b. U položky **Create a unique LDAP DN for user authentication** zadejte filtr `(&objectclass=person)(uid=%v1)`.
 - c. Zadejte informace skupiny a klepněte na **OK**.
5. Proveďte konfiguraci tak, jak je popsáno v červené knize, na kterou je odkaz výše.

Doporučené postupy pro strukturu adresáře

Server adresářů se často používá jako úložiště pro uživatele a skupiny. V této části je popsáno několik doporučených postupů pro nastavení takové struktury adresáře, která je optimální pro správu uživatelů a skupin. Tuto strukturu a související model zabezpečení lze aplikovat i na další použití adresáře.

Uživatelé jsou obvykle uloženi v jednom nebo několika místech. Můžete mít jediný zásobník, `cn=users`, který je nadřazeným záznamem pro všechny uživatele, nebo samostatné zásobníky pro různé sady uživatelů, které jsou spravovány samostatně. Tak lze mít například zaměstnance, prodejce a uživatele registrující se přes Internet uloženy odděleně v objektech nazvaných `cn=employees`, `cn=vendors` a `cn=internet users`. Někdy existuje tendence ukládat lidi podle organizace, do které patří; to však může dělat problémy, když se daná osoba přesune do jiné organizace, protože záznam adresáře pak je také potřeba přesunout a rovněž je potřeba aktualizovat skupiny a další datové zdroje (jak interní tak externí vzhledem k adresáři), aby reflektovaly nové DN. Vztah uživatelů k organizační struktuře lze vyjádřit v rámci záznamu uživatele použitím atributů adresáře, jako je "o" (organization name), "ou" (organizational unit name) nebo departmentNumber, které jsou součástí standardního schématu pro `organizationalPerson` a `inetOrgPerson`.

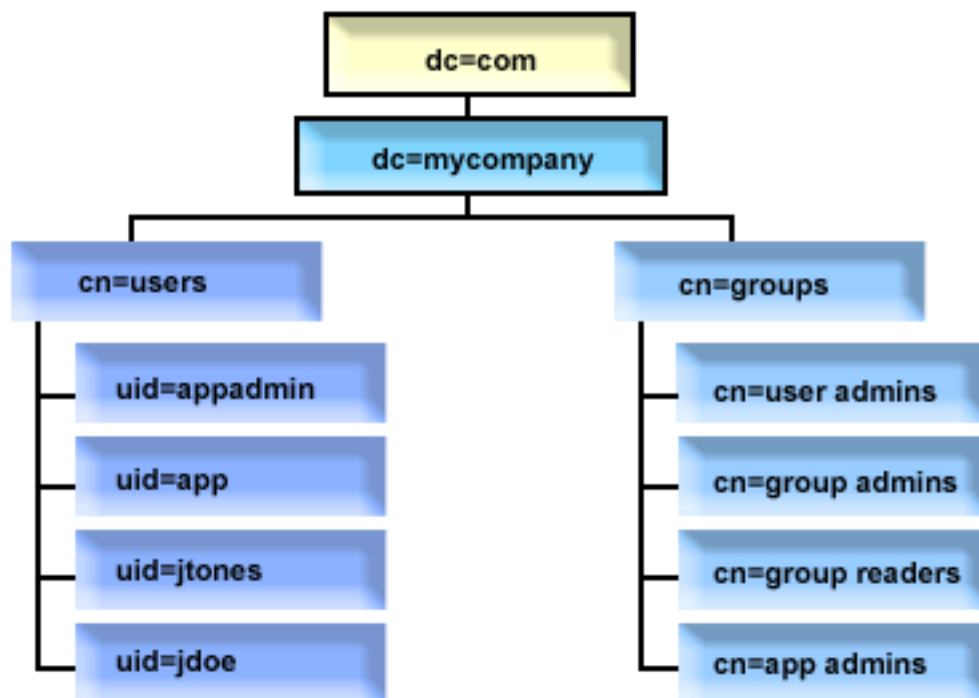
Obdobně se často do samostatných zásobníků umísťují skupiny, například do zásobníku jménem "cn=groups".

Pokud se uživatelé a skupiny organizují tímto způsobem, pak existuje jen několik míst, kde je potřeba nastavit přístupové seznamy (ACL).

Podle způsobu použití serveru adresářů a podle způsobu správy uživatelů a skupin lze použít jeden z uvedených modelů přístupové kontroly:

- Pokud se adresář používá pro aplikace jako seznam adres, můžete vytvořit zvláštní skupinu `cn=anybody`, které udělíte oprávnění ke čtení a hledání "normálních" atributů v zásobníku `cn=users` a jeho nadřazených objektech.
- Přístup k zásobníku `cn=groups` často potřebují pouze jména DN používaná specifickými aplikacemi a administrátoři skupin. Můžete tedy vytvořit skupinu obsahující DN administrátorů skupin a udělat z této skupiny vlastníka zásobníku `cn=groups` a jeho podřazených objektů. A můžete vytvořit další skupinu obsahující DN používaná aplikacemi pro čtení skupinových informací a udělit této skupině povolení ke čtení a hledání pro `cn=groups`.
- Pokud jsou uživatelské objekty aktualizovány přímo uživateli, budete chtít udělit speciálnímu přístupovému `cn=this appropriate` oprávnění ke čtení, zapisování a hledání.
- Pokud jsou uživatelé aktualizováni prostřednictvím aplikací, tyto aplikace jsou často spuštěny pod svou vlastní identitou, a oprávnění aktualizovat uživatelské objekty potřebují pouze tyto aplikace. Opět platí, že je vhodné dát tyto DN do jedné skupiny, např. `cn=user administrators`, a udělit této skupině nezbytná povolení pro `cn=users`.

Použijete-li tento typ struktury a kontroly přístupu, mohl by váš počáteční adresář vypadat takto:



Obrázek 3. Příklad struktury adresáře

- `dc=mycompany, dc=com` je vlastněným administrátorem adresáře nebo jiným uživatelem či skupinou s oprávněním spravovat nejvyšší úroveň adresáře. Další záznamy ACL udělují přístup ke čtení pro normální atributy pro jeden z `cn=anybody` nebo `cn=authenticated`, nebo případně nějakou jinou skupinu, pokud je zapotřebí restriktivnější ACL.
- `cn=users` má záznamy ACL mimo záznamy popsané níže, aby se umožnil příslušný přístup k uživatelům. Seznamy ACL mohou obsahovat:
 - přístup ke čtení a hledání pro normální atributy pro `cn=anybody` nebo `cn=authenticated`
 - přístup ke čtení a hledání pro normální a citlivé atributy pro správce
 - další záznamy ACL podle potřeby, například povolující přístup k zapisování pro jednotlivce k jejich vlastním záznamům

Poznámka:

- Pro zlepšení čitelnosti byly namísto plného DN použity RDN záznamů. Například skupina "user admins" by měla jako člen plné jméno DN `uid=app,cn=users,dc=mycompany,dc=com`, ne pouze kratší `uid=app`.
- Některé uživatele a skupiny by bylo možno kombinovat. Například pokud by administrátor aplikace měl oprávnění spravovat uživatele, mohla by aplikace být spuštěna pod DN administrátora aplikace. To by však mohlo přinést jistá omezení, např. schopnost změnit heslo administrátora pro aplikaci, aniž by se také nenakonfigurovalo nové heslo v aplikaci.
- Vzhledem k tomu, že výše uvedené postupy jsou optimální pro adresáře používané pouze jednou aplikací, mohlo by být účelnější nechat všechny aktualizace dělat s autentizací administrátora adresáře. Proti tomuto postupu hovoří důvody zmiňované v předchozím textu.

Webová administrace

Pomocí webové administrací konzole je možné provádět administraci jednoho nebo více serverů adresářů. Webová administrací konzole umožňuje:

- Přidávat nebo měnit seznam serverů adresářů, jejichž administraci je možné provádět.
- Provádět administraci serveru adresářů pomocí webového administracího nástroje.

- Měnit atributy webové administrační konzole.

Chcete-li použít webovou administrační konzoli, postupujte takto:

1. Jestliže se jedná o první použití webové administrace serveru adresářů, musíte nejprve nastavit webovou administraci (viz “První nastavení webové administrace”) a teprve potom přikročit k dalšímu bodu.
2. Přihlaste se do webové administrace serveru adresářů pomocí jednoho z těchto úkonů:
 - Z prostředí produktu iSeries Navigator vyberte příslušný server a klepněte na **Síť > Servery > TCP/IP**, klepněte pravým tlačítkem myši na **Adresář** a klepněte na **Administrace serveru**.
 - Ze stránky iSeries Tasks (http://your_server:2001) klepněte na **IBM Directory Server**.
3. Chcete-li zahájit správu serveru adresářů, postupujte takto:
 - a. V poli **LDAP Hostname** vyberte server adresářů, jehož správu chcete provádět.
 - b. Zadejte DN administrátora, které používáte k připojení k serveru adresářů.
 - c. Zadejte heslo administrátora.
 - d. Klepněte na **Login**. Zobrazí se webový nástroj administrace serveru adresářů IBM. Další informace o stránce webového administračního nástroje serveru adresářů IBM najdete v tématu “Webový nástroj administrace” na stránce 99.
4. Chcete-li přidávat nebo měnit seznam serverů adresářů, jejichž správu je možné provádět, nebo pokud chcete měnit atributy webové administrační konzole, postupujte takto:
 - a. V poli **LDAP Hostname** vyberte **Console Admin**.
 - b. Zadejte přihlašovací údaje administrátora konzole.
 - c. Zadejte heslo administrátora konzole.
 - d. Klepněte na **Login**. Zobrazí se webový nástroj administrace serveru adresářů IBM. Další informace o stránce webového administračního nástroje serveru adresářů IBM najdete v tématu “Webový nástroj administrace” na stránce 99.
 - e. Klepněte na **Console administration** a potom vyberte jednu z těchto položek:
 - **Change console administrator login**, pokud chcete změnit jméno přihlášení administrátora konzole.
 - **Change console administrator password**, pokud chcete změnit heslo administrátora konzole.
 - **Manage console servers**, chcete-li určit, u kterých serverů adresářů lze provádět administraci pomocí webové administrační konzole.
 - **Manage console properties**, chcete-li měnit vlastnosti webové administrační konzole.

První nastavení webové administrace

Při prvním nastavování webové administrace serveru adresářů postupujte takto:

1. Nainstalujte aplikační server IBM WebSphere - Express 5.1 (5722E51 Base a volba 2) a související nezbytný software, pokud nebyly nainstalovány dříve.
2. Aktivujte instanci systémového aplikačního serveru na serveru HTTP ADMIN. Další informace najdete v tématu IBM HTTP Server.
 - a. Instanci serveru HTTP ADMIN je možné spustit pomocí jednoho z těchto postupů:
 - V prostředí produktu iSeries Navigator klepněte na **Síť -> Servery -> TCP/IP** a klepněte pravým tlačítkem myši na **Administrace HTTP**. Potom klepněte na **Start**.
 - Do příkazového řádku napište `STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)`.
 - b. Přihlaste se do webové administrace IBM pro systém iSeries. Pomocí uživatelského profilu a hesla operačního systému se přihlaste na stránku iSeries Tasks (http://your_server:2001) a klepněte na **IBM Web Administration for iSeries**.
 - c. Na stránce HTTP Server Administration *your_server* klepněte na kartu **Manage** a potom klepněte na kartu **HTTP Servers**. Ujistěte se, že v rozbalovacím seznamu **Server** je vybrána položka **ADMIN – Apache** a v rozbalovacím seznamu **Server Area** je vybrána položka **Include /QIBM/UserData/HTTPPA/admin/conf/admin-cust.conf**.
 - d. Ve volbách v levém podokně této stránky klepněte na **General Server Configuration**.

Poznámka: Možná budete potřebovat rozbalit část **Server Properties**, abyste si mohli prohlédnout možnosti konfigurace serverů ve volbě **General Server Configuration**.

- e. Nastavte **Start the system application server instance when the 'Admin' server is started** na **Yes**.
- f. Klepněte na **OK**.
- g. Restartujte instanci serveru HTTP ADMIN tím, že klepnete na restartovací tlačítko (druhé tlačítko pod kartou **HTTP Servers**). Instanci serveru HTTP ADMIN můžete rovněž zastavit a spustit pomocí produktu iSeries Navigator nebo příkazového řádku.

Instanci serveru HTTP ADMIN je možné zastavit pomocí jednoho z těchto postupů:

- V prostředí produktu iSeries Navigator klepněte na **Síť -> Servery -> TCP/IP** a klepněte pravým tlačítkem myši na **Administrace HTTP**. Potom klepněte na **Stop**.
- Do příkazového řádku napište `ENDTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)`.

Instanci serveru HTTP ADMIN je možné spustit pomocí jednoho z těchto postupů:

- V prostředí produktu iSeries Navigator klepněte na **Síť -> Servery -> TCP/IP** a klepněte pravým tlačítkem myši na **Administrace HTTP**. Potom klepněte na **Start**.
- Do příkazového řádku napište `STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)`.

Další informace najdete v tématu IBM HTTP Server.

3. Přihlaste se do webového nástroje pro administraci adresářových serverů.
 - a. Jedním z níže uvedených postupů vyvolejte **přihlašovací stránku**.
 - Z prostředí produktu iSeries Navigator vyberte váš server a klepněte na **Síť -> Servery -> TCP/IP**, klepněte pravým tlačítkem myši na **IBM Directory Server** a klepněte na **Server Administration**.
 - Ze stránky iSeries Tasks (http://your_server:2001) klepněte na **IBM Directory Server for iSeries**.
 - b. Vyberte **Console Admin** v poli **LDAP Hostname**.
 - c. V poli **Username** napište `superadmin`.
 - d. Do pole **Password** napište `secret`.
 - e. Klepněte na **Login**. Zobrazí se webový nástroj administrace serveru adresářů IBM.
4. Změňte přihlašovací údaje administrátora konzole.
 - a. Klepněte na **Console administration** v levém podokně. Tím rozbalíte sekci a potom klepněte na **Change console administrator login**.
 - b. V poli **Console administrator login** napište nové přihlašovací jméno administrátora konzole.
 - c. V poli **Current password** napište současné heslo (`secret`).
 - d. Klepněte na **OK**.
5. Změňte heslo administrátora konzole. V levém podokně klepněte na **Change console administrator password**.
6. Přidejte server adresářů, jehož správu chcete provádět. V levém podokně klepněte na **Manage console servers**.

Poznámka: Při přidávání serveru adresářů se nepoužívá **Administration port**, který se v tomto případě ignoruje.

7. Pokud chcete změnit vlastnosti konzole, postupujte takto: V levém podokně klepněte na **Manage console properties**.
8. Klepněte na **Logout**. Jestliže se objeví obrazovka úspěšného odhlášení (Logout successful), klepněte na odkaz **HERE**, abyste se vrátili na přihlašovací obrazovku webové administrace.

Po prvním nakonfigurování konzole se můžete kdykoli vrátit do konzole a provádět tyto činnosti:

- Změna přihlášení a hesla administrátora konzole.
- Změna seznamu serverů adresářů, jejichž správu je možné provádět pomocí webového administrátora nástroje.
- Změna vlastností konzole.

Webový nástroj administrace

Po přihlášení na webový nástroj administrace se zobrazí okno aplikace sestávající z pěti částí:

Oblast banneru

Oblast banneru je umístěna ve vrchní části dialogového okna a obsahuje jméno aplikace a logo IBM.

Navigační oblast

Navigační oblast, umístěná na levé straně dialogového okna, zobrazuje rozbalovací nabídku kategorií pro různé úlohy obsahu serveru, jako například:

User properties

Tato úloha umožňuje měnit heslo aktuálního uživatele.

Schema management

Tato úloha umožňuje pracovat s třídami objektů, atributy, porovnávacími pravidly a syntaxemi.

Directory management

Tato úloha umožňuje pracovat se záznamy adresáře.

Replication management

Tato úloha umožňuje pracovat s pověřeními, topologií, časovými plány a frontami.

Realms and templates

Tato úloha umožňuje pracovat s uživatelskými šablonami a sférami.

Users and groups

Tato úloha umožňuje pracovat s uživateli a skupinami v definovaných sférah. Jestliže například chcete vytvořit nového webového uživatele, úloha **Users and groups** pracuje s atributy `objectclass` a `groupOfNames` pro jednotlivé skupiny. Skupinovou podporu není možné přizpůsobovat.

Server administration

Tato úloha umožňuje měnit konfiguraci serveru a bezpečnostní nastavení.

Pracovní oblast

Pracovní oblast zobrazí úlohy spojené s úlohou vybranou v navigační oblasti. Jestliže je například v navigační oblasti vybrána *Managing server security*, pracovní oblast zobrazí stranu *Server Security* a karty obsahující úlohy týkající se nastavení zabezpečení serveru.

Stavová oblast serveru

Stavová oblast serveru, umístěná ve vrchní části pracovní oblasti. Ikona na levé straně stavové oblasti serveru udává aktuální stav serveru. Vedle ikony je jméno serveru, jehož správu právě provádíte. Ikona na pravé straně stavové oblasti serveru poskytuje propojení na online nápovědu.

Stavová oblast úlohy

Oblast úlohy, umístěná pod pracovní oblastí, zobrazuje stav aktuální úlohy.

Kapitola 6. Scénář: Nastavení serveru adresářů

Situace

Jakožto administrátor počítačových systémů vaší společnosti byste rád umístil informace o zaměstnancích vaší organizace, jako například telefonní čísla a adresy elektronické pošty, do centrální schránky LDAP.

Cíle

V tomto scénáři chce MyCo, Inc. konfigurovat server adresářů a vytvořit adresářovou databázi, která bude obsahovat informace o zaměstnancích, jako jméno, adresu elektronické pošty a telefonní číslo.

Cíle tohoto scénáře jsou tyto:

- Zpřístupnit informace o zaměstnancích kdekoli v síti společnosti pro zaměstnance používající poštovního klienta Lotus Notes nebo Microsoft Outlook Express.
- Umožnit správcům měnit data zaměstnanců v adresářové databázi a přitom zabránit jiným osobám měnit tato data.
- Umožnit serveru iSeries publikovat data zaměstnanců do adresářové databáze.

Podrobnosti

Server adresářů bude spuštěn na serveru iSeries pojmenovaném myiSeries.

Následující příklad znázorňuje informace, které chce MyCo, Inc. pro každého zaměstnance zařadit do své adresářové databáze.

Jméno: Jose Alvirez
Oddělení: DEPTA
Telefonní číslo: 999 999 9999
Adresa elektronické pošty: jalvirez@my_co.com

Členění adresáře pro tento scénář bychom si mohli představit asi nějak takto:

```
/
|
+- my_co.com
  |
  +- zaměstnanci
    |
    +- Jose Alvirez
      |
      DEPTA
      999-555-1234
      jalvirez@my_co.com
    +- John Smith
      |
      DEPTA
      999-555-1235
      jsmith@my_co.com
    + Skupina správců
      Jose Alvirez
      myiSeries.my_co.com
  .
  .
  .
```

Všichni zaměstnanci (správci i ostatní osoby) jsou obsaženi v adresářovém stromu zaměstnanců. Správci náležejí kromě toho i do skupiny správců. Členové skupiny správců mají oprávnění měnit data zaměstnanců.

Server iSeries (myiSeries) rovněž musí mít oprávnění měnit data zaměstnanců. V tomto scénáři je server iSeries umístěn v adresářovém stromu a je zařazen mezi členy skupiny správců.

Pokud chcete uchovávat záznamy zaměstnanců oddělené od záznamu serveru iSeries, můžete vytvořit další adresářový strom (například: počítače) a přidat sem server iSeries. Server iSeries bude muset mít stejné oprávnění, jako mají správci.

Nutné předpoklady a podmínky

Webový nástroj administrace je správně konfigurován a spuštěn. Další informace najdete v tématu “Webová administrace” na stránce 97.

Kroky nastavení

Proveďte tyto úkony:

1. “Podrobnosti scénáře: Nastavení serveru adresářů”.
2. “Podrobnosti scénáře: Vytvoření adresářové databáze” na stránce 103.
3. “Podrobnosti scénáře: Publikace dat iSeries do adresářové databáze” na stránce 105.
4. “Podrobnosti scénáře: Zadávání informací do adresářové databáze” na stránce 106.
5. “Podrobnosti scénáře: Testování adresářové databáze” na stránce 107.

Podrobnosti scénáře: Nastavení serveru adresářů

Krok 1: Konfigurace serveru adresářů

Poznámka: Ke konfiguraci serveru adresářů musíte mít zvláštní oprávnění *ALLOBJ a *IOSYSCFG.

1. V prostředí produktu iSeries Navigator klepněte na **Network** → **Servers** → **TCP/IP**.
2. V okně **Úkoly konfigurace serveru** v pravé spodní části produktu iSeries Navigator klepněte na **Konfigurovat systém jako server adresářů**.
3. Objeví se **Průvodce konfigurací serveru adresářů**.
4. V okně **Průvodce konfigurací serveru adresářů IBM - Vítejte!** klepněte na **Konfigurovat lokální server adresářů LDAP**.
5. V okně **Průvodce konfigurací serveru adresářů IBM - Vítejte!** klepněte na **Další**.
6. V okně **Průvodce konfigurací serveru adresářů IBM - Zadat nastavení** vyberte **Ne**. To umožní konfigurovat server LDAP bez použití předvolených nastavení.
7. V okně **Průvodce konfigurací serveru adresářů IBM - Zadat nastavení** klepněte na **Další**.
8. Zrušte výběr **Generováno systémem** v okně **Průvodce konfigurací serveru adresářů IBM - Zadat DN administrátora** a zadejte toto:

DN administrátora	cn=administrator
Heslo	secret
Potvrdit heslo	secret

Poznámka: Všechna hesla uvedená v tomto scénáři slouží pouze pro účely tohoto příkladu. Pokud chcete zabránit ohrožení vašeho systému nebo zabezpečení sítě, neměli byste nikdy tato hesla používat jako součást své vlastní konfigurace.

9. V okně **Průvodce konfigurací serveru adresářů IBM - Zadat DN administrátora** klepněte na **Další**.
10. V poli **Přípona** okna **Průvodce konfigurací serveru adresářů IBM - Zadat přípony** napište dc=my_co,dc=com.
11. V okně **Průvodce konfigurací serveru adresářů IBM - Zadat přípony** klepněte na **Přidat**.
12. V okně **Průvodce konfigurací serveru adresářů IBM - Zadat přípony** klepněte na **Další**.

13. V okně **Průvodce konfigurací serveru adresářů IBM - Vybrat IP adresy** vyberte **Ano, použít všechny IP adresy**.
14. V okně **Průvodce konfigurací serveru adresářů IBM - Vybrat IP adresy** klepněte na **Další**.
15. V okně **Průvodce konfigurací serveru adresářů IBM - Zadat preference TCP/IP** vyberte **Ano**.
16. V okně **Průvodce konfigurací serveru adresářů IBM - Zadat preference TCP/IP** klepněte na **Další**.
17. V okně **Průvodce konfigurací serveru adresářů IBM - Přehled** klepněte na **Dokončit**.
18. Pravým tlačítkem myši klepněte na **Server adresářů IBM** a klepněte na **Spustit**.

Krok 2: Konfigurace webového administračního nástroje serveru adresářů

1. Naveďte svůj prohlížeč na stránku http://myiSeries.my_co.com:9080/IDSWebApp/IDSjsp/Login.jsp, kde *myiSeries.my_co.com* je váš server iSeries.
2. Měla by se objevit přihlašovací stránka. Klepněte na seznam **LDAP Hostname** vyberte **Console Admin**. Jako jméno uživatele zadejte **superadmin** a jako heslo **secret**. Klepněte na **Logon**.
3. Nakonfigurujte webový nástroj administrace pro připojení k serveru LDAP na systému iSeries. V navigační oblasti na levé straně vyberte **Console administration** → **Manage console servers**.
4. Klepněte na tlačítko **Add**.
5. V poli **Add server** napište *myiSeries.my_co.com*.
6. Klepněte na **Ok**. Nový server se objeví v seznamu pod **Manage console servers**.
7. V navigační oblasti na levé straně klepněte na **logout**.
8. Na přihlašovací stránce webového administračního nástroje klepněte na seznam **LDAP Hostname** a vyberte server, který jste právě konfigurovali (**myiSeries.my_co.com**).
9. V poli **Username** napište **cn=admin** a v poli **Password** napište **secret**. Klepněte na **Login**. Měla by se objevit hlavní stránka webového administračního nástroje serveru adresářů IBM.

Podrobnosti scénáře: Vytvoření adresářové databáze

Dříve, než můžete zahájit zadávání dat, musíte vytvořit místo, kde se budou data uchovávat.

Krok 1: Vytvoření objektu základního DN

1. Ve webovém nástroji administrace klepněte na **Directory management** → **Manage entries**. Spatříte seznam objektů v základní úrovni adresáře. Protože je server nový, uvidíte pouze strukturální objekty, které obsahují informace o konfiguraci.
2. Chcete přidat nový objekt, který by obsahoval data MyCo, Inc. Nejprve klepněte na **Add...** na pravé straně okna. V dalším okně posouvejte seznam **Object class** až na položku **domain** a potom klepněte na **Next**.
3. Nyní nechcete přidávat žádné pomocné třídy objektů, proto opět klepněte na **Next**.
4. V okně **Zadání atributů** zadejte data, která odpovídají příponě, kterou jste vytvořili dříve v průvodci. Ponechte rozbalovací seznam **Object class** na položce **domain**. V poli **Relative DN** napište **dc=my_co**. V poli **Parent DN** napište **dc=com**. V poli **dc** napište **my_co**.
5. Ve spodní části okna klepněte na **Finish**. Na základní úrovni byste měli vidět nové základní DN.

Krok 2: Vytvoření uživatelské šablony

Nyní vytvoříte uživatelskou šablonu, která pomáhá při přidávání dat zaměstnanců MyCo, Inc.

1. Ve webovém nástroji administrace klepněte na **Realms and templates** → **Add user**.
2. V poli **User template name** zadejte **Employee**.
3. Klepněte na tlačítko **Browse...** vedle pole **Parent DN**. Klepněte na základní DN, které jste vytvořili v předchozí kapitole (**dc=my_co,dc=com**) a klepněte na **Select** na pravé straně okna.
4. Klepněte na **Next**.
5. V rozbalovacím seznamu **Structural object class**
6. vyberte **inetOrgPerson** a klepněte na **Next**.

7. V rozbalovacím seznamu **Naming attribute** vyberte **cn**.
8. V seznamu **Tabs** vyberte **Required** a klepněte na **Edit**.
9. Okno **karty Edit** je místo, kde se vybírají pole, která se mají začlenit do uživatelské šablony. Atributy **sn** a **cn** jsou povinné.
10. V seznamu **Attributes** vyberte **departmentNumber** a klepněte na **Add >>>**.
11. Vyberte **telephoneNumber** a klepněte na **Add >>>**.
12. Vyberte **mail** a klepněte na **Add >>>**.
13. Vyberte **userPassword** a klepněte na **Add >>>**.
14. Klepnutím na **OK** a potom na **Finish** vytvoříte uživatelskou šablonu.

Krok 3: Vytvoření sféry

1. Ve webovém nástroji administrace klepněte na **Realms and templates** —> **Add realm**.
2. V poli **Realm name** zadejte **employees**.
3. Klepněte na **Browse...** vpravo od pole **Parent DN**.
4. Vyberte nadřazené DN, které jste vytvořili (**dc=my_co,dc=com**) a klepněte na **Select** na pravé straně okna.
5. Klepněte na **Next**.
6. V dalším okně musíte pouze změnit položku v rozbalovacím seznamu **User template**. Vyberte uživatelskou šablonu, kterou jste vytvořili (**cn=employees,dc=my_co,dc=com**).
7. Klepněte na **Finish**.

Krok 4: Vytvoření skupiny správců

1. Vytvořte skupinu správců.
 - a. Ve webovém nástroji administrace klepněte na **Users and groups** —> **Add group**.
 - b. V poli **Group name** napište **managers**.
 - c. Zkontrolujte, že je ve stahovacím seznamu **Realm** vybráno **employees**.
 - d. Klepněte na **Finish**.
2. Proveďte konfiguraci administrátora skupiny správců pro sféru **employees**.
 - a. Klepněte na **Realms and templates** —> **Manage realms**.
 - b. Vyberte sféru, kterou jste vytvořili (**cn=employees,dc=my_co,dc=com**) a klepněte na **Edit**.
 - c. Vpravo vedle pole **Administrator group** klepněte na **Browse...**
 - d. Vyberte **dc=my_co,dc=com** a klepněte na **Expand**.
 - e. Vyberte **cn=employees** a klepněte na **Expand**.
 - f. Vyberte **cn=managers** a klepněte na **Select**.
 - g. V okně **Edit realm** klepněte na **OK**.
3. Přidejte skupině správců oprávnění pro příponu **dc=my_co,dc=com**.
 - a. Klepněte na **Directory management** —> **Manage entries**.
 - b. Vyberte **dc=my_co,dc=com** a klepněte na **Edit ACL...**
 - c. V okně **Edit ACL** klepněte na kartu **Owners**.
 - d. Vyberte zaškrtnávací okénko **Propagate owner**. Každý, kdo je členem skupiny správců, se stává vlastníkem datového stromu **dc=my_co,dc=com**.
 - e. Ve stahovacím seznamu **Type** vyberte **Group**.
 - f. V poli **DN (Distinguished name)** napište **cn=managers,cn=employees,dc=my_co,dc=com**.
 - g. Klepněte na tlačítko **Add**.
 - h. Klepněte na **Ok**.

Krok 5: Přidání uživatele jakožto správce

1. Ve webovém nástroji administrace klepněte na **Users and groups** —> **Add user**.

2. V rozbalovacím menu **Realm** vyberte sféru, kterou jste vytvořili (**employees**), a klepněte na **Next**.
3. V poli **cn** napište Jose Alvarez.
4. V poli ***sn** (příjmení) napište Alvarez.
5. V poli ***cn** (úplné jméno) napište Jose Alvarez. Atribut cn se používá pro tvorbu DN záznamu. Atribut *cn je atributem objektu.
6. V poli **telephoneNumber** napište 999 555 1234.
7. V poli **departmentNumber** napište DEPTA.
8. V poli **mail** napište jalvarez@my_co.com.
9. V poli **userPassword** napište secret.
10. Klepněte na kartu **User groups**.
11. V seznamu **Available groups** vyberte **managers** a klepněte na **Add** —>.
12. Ve spodní části okna klepněte na **Finish**.
13. Klepnutím na **Log out** v levé navigační oblasti se odhláste z webového administračního nástroje.

Podrobnosti scénáře: Publikace dat iSeries do adresářové databáze

Publikace se nastavuje tak, aby umožňovala serveru iSeries automaticky vkládat uživatelské informace do adresáře LDAP. Uživatelské informace ze systémového distribučního adresáře se publikují do adresáře LDAP.

Poznámka: Uživatelům vytvořeným pomocí produktu iSeries Navigator je přidělen jednak uživatelský profil, jednak uživatelský záznam v systémovém distribučním adresáři. Pokud pro tvorbu uživatelů používáte příkazy spuštěné z příkazového řádku, musíte vytvořit jak uživatelský profil (**CRTUSRPRF**) tak uživatelský záznam v systémovém distribučním adresáři (**WRKDIRE**). Jestliže vaši uživatelé existují pouze jako uživatelské profily a vy je chcete publikovat v adresáři LDAP, musíte pro ně vytvořit uživatelské záznamy v systémovém distribučním adresáři.

Krok:1 Vytvoření serveru iSeries jako uživatele serveru adresářů

1. Přihlaste se do webového administračního nástroje (http://myiSeries.my_co.com:9080/IDSWebApp/IDSjsp/Login.jsp) jako administrátor.
 - a. V seznamu **LDAP Hostname** vyberte **myiSeries.my_co.com**.
 - b. V poli **Username** napište cn=administrator.
 - c. V poli **Password** zadejte secret.
 - d. Klepněte na **Login**.
2. Vyberte **Users and groups** —> **Add user**.
3. V seznamu **Realm** vyberte **employees**.
4. Klepněte na **Next**.
5. V poli **cn** napište myiSeries.my_co.com.
6. V poli ***sn** napište myiSeries.my_co.com.
7. V poli ***cn** napište myiSeries.my_co.com.
8. V poli **userPassword** napište secret.
9. Klepněte na kartu **User groups**.
10. Vyberte skupinu **managers**.
11. Klepněte na **Add** —>.
12. Klepněte na **Finish**.

Krok:2 Konfigurace serveru iSeries pro publikování dat

1. V prostředí produktu iSeries Navigator klepněte v levé navigační oblasti pravým tlačítkem myši na příslušný server iSeries a vyberte **Properties**.
2. V dialogovém okně **Properties** zvolte kartu **Directory Server**.

3. Vyberte **Users** a klepněte na **Details**.
4. Vyberte zaškrťovací políčko **Publish user information**.
5. V sekci **Where to publish** klepněte na tlačítko **Edit**. Objeví se okno.
6. Napište `myiSeries.my_co.com`.
7. V poli **Under DN** zadejte `cn=employees,dc=my_co,dc=com`.
8. V sekci **Server connection** zkontrolujte, že je v poli **Port** zadáno předvolené číslo portu **389**. V rozbalovacím seznamu **Authentication method** zvolte **Distinguished name** a v poli **Distinguished name** zadejte `cn=myiSeries,cn=employees,dc=my_co,dc=com`.
9. Klepněte na **Password**.
10. V poli **Password** napište `secret`.
11. V poli **Confirm Password** napište `secret`.
12. Klepněte na **OK**.
13. Klepněte na tlačítko **Verify**. To provede kontrolu, že jste zadali všechny informace správně a že se systém iSeries může připojit k adresáři LDAP.
14. Klepněte na **OK**.
15. Klepněte na **OK**.

Podrobnosti scénáře: Zadávání informací do adresářové databáze

Jakožto správce nyní Jose Alvirez přidává a aktualizuje data pro jednotlivé osoby ve svém oddělení. Potřebuje přidat některé další informace o Jane Doe. Jane Doe je uživatelkou na serveru iSeries a její informace byly publikovány. Jose Alvirez také potřebuje přidat informace o osobě jménem John Smith. John Smith není uživatelem na serveru iSeries. Jose Alvirez bude postupovat takto:

Krok 1: Přihlášení do webového administračního nástroje

Přihlaste se do webového administračního nástroje (http://myiSeries.my_co.com:9080/IDSWebApp/IDSjsp/Login.) pomocí tohoto postupu:

1. V seznamu **LDAP Hostname** vyberte **myiSeries.my_co.com**.
2. V poli **Username** zadejte `cn=Jose Alvirez,cn=myco employees,dc=my_co,dc=com`.
3. V poli **password** napište `secret`.
4. Klepněte na **Logon**.

Krok 2: Modifikace dat zaměstnance

1. Klepněte na **Users and groups** → **Manage users**.
2. V seznamu **Realm** vyberte **employees** a klepněte na **View users**.
3. V seznamu uživatelů vyberte **Jane Doe** a klepněte na **Edit**.
4. V poli **departmentNumber** zadejte `DEPTA`.
5. Klepněte na **OK**.
6. Klepněte na **Close**.

Krok 3: Přidávání dat zaměstnance

1. Klepněte na **Users and groups** → **Add user**.
2. Ve stahovacím menu **Realm** vyberte **employees** a klepněte na **Next**.
3. V poli **cn** napište `John Smith`.
4. V poli ***sn** napište `Smith`.
5. V poli ***cn** napište `John Smith`.
6. V poli **telephoneNumber** napište `999 555 1235`.
7. V poli **departmentNumber** napište `DEPTA`.

8. V poli **mail** napište `jsmith@my_co.com`.
9. Ve spodní části okna klepněte na **Finish**.

Podrobnosti scénáře: Testování adresářové databáze

Po zadání dat zaměstnance do adresářové databáze je vhodné tuto adresářovou databázi a server adresářů otestovat s využitím jednoho z těchto postupů:

Prohledání adresářové databáze pomocí seznamu adres elektronické pošty

Informace v adresáři LDAP je možné snadno prohledávat prostřednictvím programů povolených pro LDAP. Mnoho klientů elektronické pošty má do svého seznamu adres zabudovanou funkci, s jejíž pomocí dokáže prohledávat adresář LDAP. Následující příklad uvádí postup pro konfiguraci produktu Lotus Notes 6 a Microsoft Outlook Express 6. Postup pro většinu ostatních klientů elektronické pošty bude podobný.

Lotus Notes

1. Otevřete seznam adres.
2. Klepněte na **Akce** → **Nový** → **Účet**.
3. V poli **Jméno účtu** napište `myiSeries`.
4. V poli **Jméno serveru účtu** napište `myiSeries.my_co.com`.
5. V poli **Protokol** vyberte **LDAP**.
6. Klepněte na na kartu **Konfigurace protokolu**.
7. V poli **Výchozí bod hledání** napište `dc=my_co,dc=com`.
8. Klepněte na **Uložit a zavřít**.
9. Klepněte na **Vytvořit** → **Pošta** → **Poznámka**.
10. Klepněte na **Adresa...**
11. V poli **Vybrat seznam adres** vyberte `myiSeries`.
12. V poli **Hledat** napište `Alvirez`.
13. Klepněte na **Hledat**. Objeví se data pro Jose Alvireze

Microsoft Outlook Express

1. Klepněte na **Nástroje** → **Účty**.
2. Klepněte na **Přidat** → **Adresářová služba**.
3. V poli **Adresářový server Internetu (LDAP)** zadejte webovou adresu systému `iSeries (myiSeries.my_co.com)`.
4. Zrušte zaškrtnutí zaškrťovacího políčka **Server LDAP požaduje přihlášení**.
5. Klepněte na **Next**.
6. Klepněte na **Next**.
7. Klepněte na **Finish**.
8. Vyberte `myiSeries.my_co.com` (adresářovou službu, kterou jste právě konfigurovali) a klepněte na **Vlastnosti**.
9. Klepněte na **Upřesnit**.
10. V poli **Výchozí bod hledání** zadejte `dc=my_co,dc=com`.
11. Klepněte na **Ok**.
12. Klepněte na **Close**.
13. Pomocí klávesové zkratky `Ctrl+E` otevřete okno **Najít osoby**.
14. Ze seznamu **Oblast hledání** vyberte `myiSeries.my_co.com`.
15. V poli **Jméno** zadejte `Alvirez`.

16. Klepněte na **Najít**. Objeví se data pro Jose Alvireze.

Prohledání adresářové databáze pomocí příkazu `ldapsearch` spuštěného z příkazového řádku

1. V textově orientovaném rozhraní zadejte na příkazovém řádku příkaz **QSH**, který otevře relaci Qshell.
2. Seznam všech záznamů LDAP v dané databázi získáte zadáním tohoto příkazu:

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

kde:

-h je jméno hostitelského systému, na kterém je spuštěn server LDAP.

-b je základní DN, pod kterým se má hledat.

objectclass=*

vrací všechny záznamy v adresáři.

Tento příkaz vrátí data podobná těmto:

```
dc=my_co,dc=com  
dc=my_co  
objectclass=domain  
objectclass=top
```

```
cn=MyCo employee,dc=my_co,dc=com
```

```
.  
.  
.
```

```
cn=Jose Alvarez,cn=MyCo Employees,dc=my_co,dc=com
```

```
sn=Alvarez  
departmentNumber=DEPTA  
mail=jalvarez@my_co.com  
telephoneNumber=999 999 9999  
objectclass=top  
objectclass=inetOrgPerson  
objectclass=organizationalPerson  
objectclass=person  
cn=Jose Alvarez
```

```
.  
.  
.
```

První řádek každého záznamu se označuje jako rozlišovací jméno (DN - distinguished name). DN slouží jako úplné jméno souboru každého záznamu. Některé ze záznamů neobsahují data a jsou pouze strukturní. Jména DN s řádkem **objectclass=inetOrgPerson** odpovídají záznamům, které jste vytvořili pro příslušné osoby. DN osoby jménem Jose Alvarez je **cn=Jose Alvarez,cn=MyCo Employees,dc=my_co,dc=com**.

Kapitola 7. Jak provádět správu serveru adresářů

Ke správě serveru adresářů musí mít uživatelský profil, který používáte, tato 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 seznamů přístupových práv, vlastnictví objektů a replik), připojte se k adresáři s administrátorským DN nebo jiným DN, které má odpovídající oprávnění LDAP. Jestliže používáte integraci oprávnění, může být administrátorem také projektovaný uživatel (viz “Procedura Backend projektovaná operačním systémem” na stránce 74), který má oprávnění k ID funkce Directory Server Administrator. Většinu administračních úloh mohou také provádět uživatelé ve skupině administrátorů (viz “Administrační přístup” na stránce 54).

Obecné úlohy administrace

- “Jak spustit/zastavit server adresářů” na stránce 110
- “Jak kontrolovat stav serveru adresářů” na stránce 111
- “Jak kontrolovat úlohy na serveru adresářů” na stránce 111
- “Jak spravovat připojení serveru” na stránce 111
- “Jak spravovat vlastnosti připojení” na stránce 112
- “Jak aktivovat oznámení o události” na stránce 114
- “Jak specifikovat nastavení transakcí” na stránce 115
- “Jak změnit port nebo IP adresu” na stránce 115
- “Import a export souboru LDIF” na stránce 93
- “Jak specifikovat server pro adresářové odkazy” na stránce 116
- “Jak přidávat a odstraňovat přípony serveru adresářů” na stránce 116
- “Jak uložit a obnovit informace o produktu Server adresářů” na stránce 117
- “Jak poskytnout administrátorský přístup projektovaným uživatelům” na stránce 117
- “Jak pracovat s administrační skupinou” na stránce 118
- “Jak spravovat skupiny s limity hledání” na stránce 119
- “Jak spravovat skupiny s proxy autorizací” na stránce 121
- “Jak spravovat jedinečné atributy” na stránce 122
- “Jak sledovat přístup a změny u adresáře LDAP” na stránce 123
- “Jak aktivovat monitorování objektů pro server adresářů” na stránce 124
- “Jak přizpůsobit nastavení vyhledávání” na stránce 124
- “Jak přizpůsobit nastavení výkonu” na stránce 125
- “Jak provádět správu replikací” na stránce 129

Úlohy týkající se zabezpečení

- “Jak spravovat hesla” na stránce 147
- “Jak aktivovat SSL a TSL (Transport Layer Security) na serveru adresářů” na stránce 151
- “Jak aktivovat autentizaci Kerberos na serveru adresářů” na stránce 153

- “Jak aktivovat autentizaci DIGEST-MD5 na serveru adresářů” na stránce 154

Úlohy týkající se obsahu adresáře

- “Jak provádět správu schématu” na stránce 154
- “Jak provádět správu záznamů adresáře” na stránce 165
- “Jak provádět správu uživatelů a skupin” na stránce 172
- “Jak provádět správu sfér a uživatelských šablon” na stránce 174
- “Jak provádět správu seznamů přístupových práv (ACL)” na stránce 181

Úlohy týkající se publikace

- “Publikování informací na server adresářů” na stránce 92

Jak spustit/zastavit server adresářů

Chcete-li spustit server adresářů, postupujte takto:

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

Může trvat několik minut, než se server adresářů spustí. Závísí 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 přechodu serveru z nižší verze produktu Server adresářů může trvat jeho první spuštění o několik minut déle než obvykle, protože server musí migrovat soubory. Stav serveru je možné čas od času kontrolovat (viz “Jak kontrolovat stav serveru adresářů” na stránce 111) a zjišťovat, jestli je již spuštěn.

Server adresářů lze spustit i z textově orientovaného rozhraní 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`.

Režim pouze pro konfiguraci

Server adresářů lze spustit v režimu pouze pro konfiguraci ze znakově orientovaného rozhraní zadáním příkazu `TRCTCPAPP APP(*DIRSRV) ARGLIST(SAFEMODE)`.

Režim pouze pro konfiguraci spouští server, který má aktivní pouze příponu `cn=configuration` a nezávisí na úspěšné inicializaci databázových procedur typu Backend.

Chcete-li server adresářů zastavit, postupujte takto:

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 pokoušely o připojení k serveru.

Chcete-li zastavit server adresářů, postupujte takto:

1. V prostředí produktu iSeries Navigator rozbalte položku **Sítě**.
2. Rozbalte položku **Servery**.
3. Klepněte na **TCP/IP**.
4. Pravým tlačítkem myši klepněte na **Server adresářů IBM** a vyberte volbu **Zastavit**.

Může trvat několik minut, než se server adresářů zastaví. Závísí to na rychlosti systému, na rozsahu aktivity serveru a na velikosti dostupné paměti. Stav serveru je možné čas od času kontrolovat (viz “Jak kontrolovat stav serveru adresářů” na stránce 111) a zjišťovat, jestli je již spuštěn.

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 kontrolovat stav serveru adresářů

Základní informace o stavu můžete najít v prostředí produktu iSeries Navigator. Podrobnější a úplné informace o stavu najdete pomocí webového administračního nástroje.

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

Chcete-li zjistit stav serveru adresářů v prostředí produktu iSeries Navigator, postupujte takto:

1. Rozbalte položku **Sít**.
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 **Server adresářů IBM** a vyberte volbu **Stav**. Zobrazí se počet aktivních připojení a další informace, jako jsou např. minulá a aktuální úroveň 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.

Chcete-li zjistit stav serveru adresářů pomocí webového administračního nástroje, postupujte takto:

1. V navigační oblasti rozbalte kategorii **Server administration**.

Poznámka: Chcete-li měnit konfigurační nastavení serveru pomocí úloh v kategorii Server administration, musíte se na server autentizovat jako uživatelský profil i5/OS, který má speciální oprávnění *ALLOBJ a IOSYSCFG. Toho lze docílit tak, že se budete autentizovat jako projektovaný uživatel s heslem pro tento profil. Chcete-li se přihlásit z webového administračního nástroje jako projektovaný uživatel, zadejte uživatelské jméno ve formě `os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM`, kde řetězce MYUSERNAME a MYSYSTEM.COM nahradíte vašim jménem uživatelského profilu a konfigurovanou systémovou projektovanou příponou.

2. Klepněte na **View server status**.
3. Na panelu **View server status** vyberte některou z karet, které zobrazují informace o stavu.

Jak kontrolovat úlohy na serveru adresářů

Občas je zapotřebí na serveru adresářů monitorovat určité úlohy. Chcete-li zkontrolovat úlohy serveru v prostředí produktu iSeries Navigator, postupujte takto:

1. V prostředí produktu iSeries Navigator rozbalte položku **Sít**.
2. Rozbalte položku **Servery**.
3. Klepněte na **TCP/IP**.
4. Pravým tlačítkem myši klepněte na **Server adresářů IBM** a vyberte volbu **Úlohy serveru**.

Jak spravovat připojení serveru

Administrátor si často potřebuje zobrazit připojení k serveru a operace, které tato připojení provádějí. Na základě těchto informací se pak administrátor může rozhodnout řídit přístup a zabránit útokům zaměřeným na odmítnutí služeb. Toto se provádí prostřednictvím webového administračního nástroje.

V navigační oblasti rozbalte kategorii **Server administration**. Klepněte na volbu **Manage server connections**. Zobrazí se tabulka s těmito informacemi pro každé připojení:

Poznámka: Chcete-li měnit konfigurační nastavení serveru pomocí úloh v kategorii Server administration, musíte se na server autentizovat jako uživatelský profil i5/OS, který má speciální oprávnění *ALLOBJ a IOSYSCFG. Toho lze docílit tak, že se budete autentizovat jako projektovaný uživatel s heslem pro tento profil. Chcete-li se přihlásit z webového administračního nástroje jako projektovaný uživatel,

zadejte uživatelské jméno ve formě `os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM`, kde řetězce `MYUSERNAME` a `MYSYSTEM.COM` nahradíte vaším jménem uživatelského profilu a konfigurovanou systémovou projektovanou příponou.

DN Uvádí DN klientských připojení k serveru.

IP address

Uvádí IP adresu klienta, který má připojení k serveru.

Start time

Uvádí datum a čas (v lokálním čase serveru), kdy bylo připojení zahájeno.

Status Uvádí, zda je připojení aktivní nebo nečinné. Připojení se považuje za aktivní, pokud v rámci něj probíhá nějaká operace.

Ops initiated

Uvádí počet operací požadovaných od počátku navázání připojení.

Ops completed

Uvádí počet operací, které byly u každého připojení dokončeny.

Type Uvádí, zda bylo připojení zabezpečeno pomocí SSL nebo TLS. Jinak je pole prázdné.

Poznámka: Tato tabulka zobrazuje až 20 připojení v daném okamžiku.

Můžete zadat, zda chcete tabulku zobrazit podle DN nebo podle IP adresy. To provedete tak, že rozbalíte menu v horní části panelu a provedete příslušný výběr. Předvolený výběr je podle DN. Obdobně můžete také zadat, zda chcete tabulku zobrazit ve vzestupném nebo sestupném pořadí.

Klepnutím na **Refresh** provedete aktualizaci současných informací o připojení.

Pokud jste přihlášení jako administrátor nebo jako člen administrační skupiny, máte na panelu k dispozici další volby pro odpojování připojení k serveru. Schopnost odpojit připojení k serveru vám umožňuje zastavit útoky zaměřené na odmítnutí služeb a řídit přístup k serveru. Jednotlivá připojení odpojíte tak, že rozbalíte rozbalovací menu, vyberete DN, IP adresu nebo obojí, a klepnete na **Disconnect**.

Chcete-li odpojit všechna připojení k serveru kromě toho, které provádí daný požadavek, klepněte na **Disconnect all**. Zobrazí se potvrzující zpráva s varováním. Klepněte na **OK**, chcete-li pokračovat v procesu odpojení, nebo klepněte na **Cancel**, čímž akci odpojení zastavíte a vrátíte se na panel **Manage server connections**.

Další informace o zabránění útokům zaměřeným na odmítnutí služeb (denial of service) najdete v tématu “Jak spravovat vlastnosti připojení”.

Jak spravovat vlastnosti připojení

Schopnost spravovat vlastnosti připojení vám umožní, abyste zabránili klientům zablokovat server. Zajišťuje také, aby měl administrátor vždy přístup k serveru v případech, že je procedura typu backend přetížená dlouhotrvajícími úlohami. Správa vlastností připojení se provádí prostřednictvím webového administračního nástroje.

Poznámka: Tyto volby se zobrazí pouze tehdy, pokud jste přihlášení jako administrátor nebo člen administrační skupiny na serveru, který podporuje tuto funkci.

Chcete-li nastavit vlastnosti připojení, postupujte takto:

1. V navigační oblasti rozbalte kategorii **Server administration** a klepněte na **Manage connection properties**.

Poznámka: Chcete-li měnit konfigurační nastavení serveru pomocí úloh v kategorii **Server administration**, musíte se na server autentizovat jako uživatelský profil `i5/OS`, který má speciální oprávnění `*ALLOBJ` a `IOSYSCFG`. Toho lze docílit tak, že se budete autentizovat jako projektovaný uživatel s heslem pro tento profil. Chcete-li se přihlásit z webového administračního nástroje jako

projektovaný uživatel, zadejte uživatelské jméno ve formě `os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM`, kde řetězce `MYUSERNAME` a `MYSYSTEM.COM` nahradíte vaším jménem uživatelského profilu a konfigurovanou systémovou projektovanou příponou.

2. Vyberte kartu **General**.

3. Zadejte nastavení pro anonymní připojení. Zaškrťovací okénko **Allow anonymous connections** je již označeno, takže anonymní připojení jsou povolena. Toto je předvolené nastavení. Na zaškrťovací okénko můžete klepnout a zrušit výběr funkce **Allow anonymous connections**. Tento úkon způsobí, že server bude odpojovat všechna anonymní připojení.

Poznámka: Některé aplikace mohou selhat, pokud zrušíte povolení anonymních připojení.

4. V poli **Cleanup threshold for anonymous connections** nastavte prahovou hodnotu pro inicializaci odpojování anonymních připojení. Můžete zadat číslo v rozmezí 0 až 65535.

Poznámka: Skutečná maximální hodnota je omezena počtem souborů povolených na proces. V systémech UNIX můžete pro stanovení těchto omezení použít příkaz **ulimit -a**. V systémech Windows je to pevně stanovený počet.

Předvolené nastavení je 0. Když se tento počet anonymních připojení překročí, připojení jsou vyčištěna na základě časového limitu v nečinnosti, který nastavíte v poli **Idle time out**.

5. V poli **Cleanup threshold for authenticated connections** nastavte prahovou hodnotu pro inicializaci odpojování autentizovaných připojení. Můžete zadat číslo v rozmezí 0 až 65535.

Poznámka: Skutečná maximální hodnota je omezena počtem souborů povolených na proces. V systémech UNIX můžete pro stanovení těchto omezení použít příkaz **ulimit -a**. V systémech Windows je to pevně stanovený počet.

Předvolené nastavení je 1100. Když se tento počet autentizovaných připojení překročí, připojení jsou vyčištěna na základě časového limitu v nečinnosti, který nastavíte v poli **Idle time out**.

6. V poli **Cleanup threshold for all connections** nastavte prahovou hodnotu pro inicializaci odpojování všech připojení. Můžete zadat číslo v rozmezí 0 až 65535.

Poznámka: Skutečná maximální hodnota je omezena počtem souborů povolených na proces. V systémech UNIX můžete pro stanovení těchto omezení použít příkaz **ulimit -a**. V systémech Windows je to pevně stanovený počet.

Předvolené nastavení je 1200. Když se tento celkový počet připojení překročí, připojení jsou vyčištěna na základě časového limitu v nečinnosti, který nastavíte v poli **Idle time out**.

7. V poli **Idle timeout limit** nastavte počet vteřin, během kterých může být připojení v nečinnosti, než je uzavřeno procesem čištění. Můžete zadat číslo v rozmezí 0 až 65535.

Poznámka: Skutečná maximální hodnota je omezena počtem souborů povolených na proces. V systémech UNIX můžete pro stanovení těchto omezení použít příkaz **ulimit -a**. V systémech Windows je to pevně stanovený počet.

Předvolené nastavení je 300. Když se zahájí proces čištění, veškerá připojení, kterých se tento proces týká a která překročí stanovený limit, budou uzavřena.

8. V poli **Result timeout limit** nastavte počet vteřin povolený mezi jednotlivými pokusy o zapisování. Můžete zadat číslo v rozmezí 0 až 65535. Předvolené nastavení je 120. Veškerá připojení, která překročí tento limit, budou ukončena.

Poznámka: Toto se týká pouze systémů Windows. Připojení, které překročí 30 vteřin, je operačním systémem automaticky uvolněno. Toto nastavení parametru **Result timeout limit** je tudíž po 30 vteřinách potlačeno operačním systémem.

9. Klepněte na kartu **Emergency thread**.

10. Zadejte nastavení pro vlákno stavu nouze. Zaškrťovací okénko **Enable emergency thread** je již označeno, takže vlákno stavu nouze lze aktivovat. Toto je předvolené nastavení. Na zaškrťovací okénko můžete klepnout a zrušit výběr funkce **Enable emergency thread**. To způsobí, že vlákno stavu nouze nebude moci být aktivováno.

11. V poli **Pending request threshold** nastavte početní limit pro pracovní požadavky, který aktivuje vlákno stavu nouze. Zadejte číslo v rozmezí 0 až 65535, které určuje limit pracovních požadavků, které mohou být ve frontě, než se aktivuje vlákno stavu nouze. Předvolená hodnota je 50. Když se překročí zadaný limit, aktivuje se vlákno stavu nouze.
 12. V poli **Time threshold** nastavte počet minut, který může uplynout od doby, kdy byl z fronty odstraněna poslední pracovní položka. Pokud jsou ve frontě nějaké pracovní položky a tento časový limit je překročen, aktivuje se vlákno stavu nouze. Můžete zadat číslo v rozmezí 0 až 240. Předvolené nastavení je 5.
 13. Vyberte z rozbalovacího menu kritéria, která se budou používat pro aktivaci vlákna stavu nouze. Můžete vybrat:
 - **Size only:** Vlákno stavu nouze se aktivuje pouze tehdy, když fronta překročí zadaný počet nevyřízených pracovních položek.
 - **Time only:** Vlákno stavu nouze se aktivuje pouze tehdy, když časový limit mezi odstraněnými pracovními položkami překročí stanovenou dobu.
 - **Size or time:** Vlákno stavu nouze se aktivuje tehdy, když velikost fronty nebo časový limit překročí stanovené limity.
 - **Size and time:** Vlákno stavu nouze se aktivuje tehdy, když jak velikost fronty tak časový limit překročí stanovené limity.

Předvoleně je nastaveno kritérium Size and time.
 14. Klepněte na **OK**.
- Další informace najdete v tématu “Jak spravovat připojení serveru” na stránce 111.


Jak aktivovat oznámení o události

Server adresářů podporuje oznámení o události, které umožňuje klientům registrovat se na 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 navigační oblasti webového administračního nástroje rozbalte kategorii **Manage server properties** a vyberte kartu **Event notification**.
2. Zaškrtněte okénko **Enable event notification**, abyste aktivovali oznamování o událostech. Je-li funkce **Enable event notification** deaktivována, server ignoruje všechny ostatní volby na tomto panelu.
3. Nastavte parametr **Maximum registrations per connection**. Klepněte buď na tlačítko **Registrations** nebo **Unlimited**. Pokud vyberete **Registrations**, musíte v poli zadat maximální počet registrací povolených pro jednotlivá připojení. Maximální počet transakcí je 2.147.483.647. Předvolené nastavení je 100 registrací.
4. Nastavte parametr **Maximum registrations total**. Tento výběr nastavuje, kolik registrací může server mít v jednom okamžiku současně. Klepněte buď na tlačítko **Registrations** nebo **Unlimited**. Pokud vyberete **Registrations**, musíte v poli zadat maximální počet registrací povolených pro jednotlivá připojení. Maximální počet transakcí je 2.147.483.647. Předvolená hodnota pro počet registrací je **Unlimited**.
5. Když skončíte, klepněte buď na tlačítko **Apply**, abyste změny uložili a pokračovali, nebo klepněte na tlačítko **OK**, abyste změny uložili a odešli z tohoto panelu, nebo klepněte na tlačítko **Cancel**, abyste z tohoto panelu odešli bez provedení jakýchkoliv změn.
6. Pokud jste aktivovali oznamování o událostech, je nutné restartovat server, aby změny vstoupily v platnost. Pokud jste pouze modifikovali nastavení, není nutno server restartovat.

Poznámka: Chcete-li deaktivovat oznamování o událostech, zrušte označení zaškrtačovacího okénka **Enable event notifications** a restartujte server.

- Další informace o oznamování událostí najdete v tématu Oznamování událostí v publikaci IBM Directory Server Version 5.2 Programming Reference .

Jak specifikovat nastavení transakcí

Produkt Server adresářů podporuje transakce, které umožňují pracovat se skupinou operací adresáře LDAP jako s jedinou jednotkou. Další informace najdete v tématu “Transakce” na stránce 46.

Ke konfiguraci nastavení transakcí na serveru použijte tento postup:

1. V navigační oblasti webového administračního nástroje rozbalte kategorii **Manage server properties** a vyberte kartu **Transactions**.
2. Zaškrtněte okénko **Enable transaction processing**, abyste aktivovali zpracování transakcí. Je-li funkce **Enable transaction processing** deaktivována, všechny ostatní volby na tomto panelu, jako je např. **Maximum number of operations per transaction** nebo **Pending time limit**, bude server ignorovat.
3. Nastavte parametr **Maximum number of transactions**. Klepněte buď na tlačítko **Transactions** nebo **Unlimited**. Pokud vyberete **Transactions**, musíte v poli zadat maximální počet transakcí. Maximální počet transakcí je 2.147.483.647. Předvolené nastavení je 20 transakcí.
4. Nastavte parametr **Maximum number of operations per transaction**. Klepněte buď na tlačítko **Operations** nebo **Unlimited**. Pokud vyberete **Operations**, musíte v poli zadat maximální počet operací povolených pro jednotlivé transakce. Maximální počet operací je 2.147.483.647. Čím nižší je počet, tím lepší bude výkon. Předvolená hodnota je 5 operací.
5. Nastavte parametr **Pending time limit**. Tato volba určuje maximální hodnotu časového limitu nevyřízených transakcí ve vteřinách. Klepněte buď na tlačítko **Seconds** nebo **Unlimited**. Pokud vyberete **Seconds**, musíte v poli zadat maximální počet vteřin povolený pro jednotlivé transakce. Maximální počet vteřin je 2.147.483.647. Transakce, které zůstanou nedokončeny po delší dobu, než je tato, budou zrušeny (odstraněny). Předvolená hodnota je 300 vteřin.
6. Když skončíte, klepněte buď na tlačítko **Apply**, abyste změny uložili a pokračovali, nebo klepněte na tlačítko **OK**, abyste změny uložili a odešli z tohoto panelu, nebo klepněte na tlačítko **Cancel**, abyste z tohoto panelu odešli bez provedení jakýchkoliv změn.
7. Pokud jste aktivovali podporu pro transakce, je nutné restartovat server, aby změny vstoupily v platnost. Pokud jste pouze modifikovali nastavení, není nutno server restartovat.

Poznámka: Chcete-li deaktivovat zpracování transakcí, zrušte označení zaškrťovacího okénka **Enable transaction processing** a restartujte server.

Jak změnit port nebo IP adresu

Server adresářů používá tyto předvolené porty:

- 389 pro nezabezpečená připojení.
- 636 pro zabezpečená připojení (jestliže jste pomocí produktu Digital Certificate Manager povolili Server adresářů jako aplikaci, která může používat zabezpečený port).

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

Používáte-li již tyto porty pro jiné aplikace, můžete buď přiřadit produktu Server adresářů jiný port, nebo můžete použít pro tyto dva servery různé IP adresy, pokud aplikace podporují připojení ke specifické IP adrese.

Příklad konfliktu serveru Domino LDAP se serverem adresářů najdete v tématu Host Domino LDAP a server adresářů na stejném serveru iSeries.

Ke změně portů, které používá server adresářů, použijte tento postup:

1. V prostředí produktu iSeries Navigator rozbalte položku **Sítě**.
2. Rozbalte položku **Servery**.
3. Klepněte na **TCP/IP**.
4. Pravým tlačítkem myši klepněte na **Server adresářů IBM** a vyberte volbu **Vlastnosti**.
5. Klepněte na kartu **Sítě**.
6. Zadejte příslušná čísla portů a klepněte na **OK**.

Chcete-li změnit IP adresu, na které server adresářů přijímá připojení, postupujte takto:

1. V prostředí produktu iSeries Navigator rozbalte položku **Síť**.
2. Rozbalte položku **Servery**.
3. Klepněte na **TCP/IP**.
4. Pravým tlačítkem myši klepněte na **Server adresářů IBM** a vyberte volbu **Vlastnosti**.
5. Klepněte na kartu **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 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 **Server adresářů IBM** a vyberte volbu **Vlastnosti**.
5. Vyberte stránku vlastností **Obecné**.
6. V poli **Nový odkaz** zadejte URL referenčního serveru.
7. Do názvu 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.

8. Klepněte na tlačítko **Přidat**.
9. Klepněte na **OK**.

Jak přidávat a odstraňovat přípony serveru adresářů

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

Poznámka: Není možné 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 **Server adresářů IBM** a vyberte volbu **Vlastnosti**.
5. Klepněte na kartu **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 nezbytné jej vytvořit stejným způsobem jako jiný objekt.

K odstranění přípony 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 **Server adresářů IBM** a vyberte volbu **Vlastnosti**.
5. Klepněte na kartu **Databáze/Přípony**.

6. Klepnutím vyberte příponu, kterou chcete odstranit.
7. Klepněte na tlačítko **Odstranit**.

Poznámka: Je možné rovněž 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 o produktu Server adresářů

Produkt Server adresářů uchovává informace v těchto místech:

- Databázová knihovna (standardně QUSRDIRDB) - obsahuje obsah serveru adresářů.


Poznámka: To, kterou databázovou knihovnu používáte, můžete vidět na kartě **Databáze/Přípony** panelu Vlastnosti serveru adresářů IBM v prostředí produktu iSeries Navigator.

- 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 kdykoli použijete PTF.

Informace o ukládání a obnově dat najdete v tématu Zálohování a obnova, SC41-5304 .

Jak poskytnout administrátorský přístup projektovaným uživatelům

Produkt umožňuje udělit administrátorský přístup uživatelským profilům, které dostaly přístup k ID funkce QIBM_DIRSRV_ADMIN (Directory Server Administrator).

Pokud například dostane uživatelský profil JOHNSMITH přístup k ID funkce Directory Server Administrator a v dialogu Vlastnictví adresáře je vybrána volba Udělení administrátorského přístupu oprávněným uživatelům, profil JOHNSMITH získá 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 tématu “Procedura Backend projektovaná operačním systémem” na stránce 74.

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. Na kartě **Obecné** pod položkou **Informace pro administrátora** vyberte volbu **Udělení administrátorského přístupu oprávněným uživatelům**.

Při nastavení ID funkce s oprávněním Directory Server Administrator v uživatelském profilu postupujte takto:

1. V prostředí produktu iSeries Navigator klepněte pravým tlačítkem myši na jméno systému a vyberte volbu **Administrace aplikací**.
2. Klepněte na kartu **Hostitelské aplikace**.
3. Rozbalte položku **Operating System/400**.

4. Klepnutím zvýrazněte volbu **Administrátor serveru adresářů**.
5. Klepněte na tlačítko **Přizpůsobit**.
6. Rozbalte položky **Uživatelé**, **Skupiny** nebo **Uživatelé, kteří nejsou ve skupině** podle toho, co je pro uživatele vhodné.
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 **Administrace aplikací**.

Jak pracovat s administrační skupinou

Administrační skupina umožňuje poskytovat administrátorské schopnosti, aniž by bylo nutno mezi administrátory sdílet jeden ID a jedno heslo. Členové administrační skupiny mají své vlastní jedinečné ID a hesla. DN jednotlivých členů administrační skupiny se nesmí shodovat a také se nesmí shodovat s DN administrátora serveru adresářů IBM. Naopak také DN administrátora serveru adresářů IBM se nesmí shodovat s DN kteréhokoliv člena administrační skupiny.

Toto pravidlo se týká rovněž ID administrátora serveru adresářů IBM a ID členů administrační skupiny pro Kerberos nebo Digest-MD5. Tato DN se nesmí shodovat s kterýmkoliv z DN dodavatelů replikací serveru adresářů IBM. To také znamená, že DN dodavatelů replikací serveru adresářů IBM se nesmí shodovat s DN kteréhokoliv člena administrační skupiny nebo s DN administrátora serveru adresářů IBM.

Poznámka: DN dodavatelů replikací serveru adresářů IBM se navzájem mohou shodovat.

Další informace najdete v těchto tématech:

- “Jak povolit administrační skupinu”
- “Jak přidávat, upravovat a odstraňovat členy administrační skupiny” na stránce 119

Související informace

“Administrační přístup” na stránce 54

Jak povolit administrační skupinu

K provedení této operace musíte být administrátor serveru adresářů IBM.

1. V navigační oblasti webového administračního nástroje rozbalte kategorii **Server administration** a klepněte na **Manage administrative group**.

Poznámka: Chcete-li měnit konfigurační nastavení serveru pomocí úloh v kategorii Server administration, musíte se na server autentizovat jako uživatelský profil i5/OS, který má speciální oprávnění *ALLOBJ a IOSYSCFG. Toho lze docílit tak, že se budete autentizovat jako projektovaný uživatel s heslem pro tento profil. Chcete-li se přihlásit z webového administračního nástroje jako projektovaný uživatel, zadejte uživatelské jméno ve formě `os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM`, kde řetězce MYUSERNAME a MYSYSTEM.COM nahradíte vašim jménem uživatelského profilu a konfigurovanou systémovou projektovanou příponou.

2. Chcete-li povolit nebo zakázat administrační skupinu, klepněte na zaškrťovací okénko vedle položky **Enable administrative group**. Je-li okénko zaškrtnuté, administrační skupina je povolena.

3. Klepněte na **OK**.

Poznámka: Pokud administrační skupinu zakážete, kterýkoliv člen, který je přihlášený, může pokračovat v administračních operacích, dokud není nutno, aby se znovu připojil.

Jak přidávat, upravovat a odstraňovat členy administrační skupiny

Nezbytný předpoklad: K provedení této operace musíte být administrátor serveru adresářů IBM.

1. V navigační oblasti webového administračního nástroje rozbalte kategorii **Server administration** a klepněte na **Manage administrative group**.

Poznámka: Chcete-li měnit konfigurační nastavení serveru pomocí úloh v kategorii Server administration, musíte se na server autentizovat jako uživatelský profil i5/OS, který má speciální oprávnění *ALLOBJ a IOSYSCFG. Toho lze docílit tak, že se budete autentizovat jako projektovaný uživatel s heslem pro tento profil. Chcete-li se přihlásit z webového administračního nástroje jako projektovaný uživatel, zadejte uživatelské jméno ve formě `os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM`, kde řetězce MYUSERNAME a MYSYSTEM.COM nahradíte vaším jménem uživatelského profilu a konfigurovanou systémovou projektovanou příponou.

2. Na panelu **Manage administrative group** klepněte na tlačítko **Add**.
3. Na panelu **Add administrative group member** proveďte následující:
 - a. Zadejte administrátorské DN člena (musí to být platná syntaxe DN).
 - b. Zadejte heslo člena.
 - c. Pro potvrzení znovu zadejte heslo člena.
 - d. Volitelně: Zadejte Kerberos ID člena. Kerberos ID musí být buď ve formátu `ibm-kn` nebo `ibm-KerberosName`. Hodnoty nejsou citlivé na velikost písmen, např. `ibm-kn=root@TEST.ROCHESTER.IBM.COM` je ekvivalentní hodnotě `ibm-kn=ROOT@TEST.ROCHESTER.IBM.COM`.
4. Volitelně: zadejte **uživatelské jméno Digest-MD5** člena.

Poznámka: Uživatelské jméno Digest-MD5 není citlivé na velikost písmen.

5. Klepněte na **OK**.
6. Tento postup opakujte pro každého člena, kterého chcete přidat do administrační skupiny.

Administrátorské DN člena, uživatelské jméno Digest-MD5 username, je-li zadáno, a Kerberos ID, je-li zadán, jsou zobrazeny v okně se seznamem členů administrační skupiny.

Chcete-li změnit nebo odstranit člena administrační skupiny, postupujte podle stejného postupu jako výše, ale na panelu **Manage administrative group** použijte tlačítka **Edit** a **Delete**.

Jak spravovat skupiny s limity hledání

K tomu, aby se zabránilo vyhledávacím požadavkům nějakého uživatele spotřebovat příliš mnoho zdrojů a následně narušit výkon serveru, lze využít limitů hledání, které se uplatní na tyto požadavky pro jakéhokoliv daného uživatele. Administrátor tyto limity hledání, kterými se omezuje velikost a doba hledání, nastavuje při konfiguraci serveru.

Z těchto limitů hledání, které se uplatňují na všechny uživatele, jsou vyjmuti pouze administrátor a členové administrační skupiny. Administrátor však může podle potřeby vytvořit tzv. skupiny s limity hledání (search limit group), které mohou mít flexibilnější limity hledání než běžný uživatel. Tímto způsobem může administrátor poskytnout skupině uživatelů speciální vyhledávací oprávnění.

Další informace najdete v těchto tématech:

- “Jak vytvořit skupinu s limity hledání” na stránce 120
- “Jak měnit skupinu s limity hledání” na stránce 120
- “Jak kopírovat skupinu s limity hledání” na stránce 121
- “Jak odstranit skupinu s limity hledání” na stránce 121

Ke správě skupin s limity hledání se používá webový administrační nástroj.

Související koncept

| “Parametry prohledávání” na stránce 42

| Jak vytvořit skupinu s limity hledání

| Chcete-li vytvořit skupiny s limity hledání, je nutno vytvořit pomocí webového administračního nástroje skupinový záznam.

- | 1. V navigační oblasti rozbalte kategorii **Directory management** a klepněte na **Add an entry**. Anebo klepněte na **Manage entries**, vyberte umístění (cn=IBMpolicies nebo cn=localhost) a klepněte na **Add**. Záznamy pod cn=IBMpolicies se budou replikovat, záznamy pod cn=localhost nikoliv.
- | 2. Vyberte jednu z tříd objektu skupiny z menu **Structural object class**.
- | 3. Klepněte na **Next**.
- | 4. Vyberte pomocnou třídu objektu **ibm-searchLimits** z menu **Available** a klepněte na **Add**. Tento postup opakujte pro každou pomocnou třídu objektu, která se má přidat. Pomocnou třídu objektu můžete také z menu **Selected** odstranit tak, že ji vyberete a klepnete na **Remove**.
- | 5. Klepněte na **Next**.
- | 6. V poli **Relative DN** zadejte relativní rozlišovací jméno (RDN) skupiny, která se má přidat. Například cn=Search Group1.
- | 7. V poli **Parent DN** zadejte rozlišovací jméno stromového záznamu, který jste vybrali. Například cn=localhost. Můžete také klepnout na **Browse** a vybrat nadřazené DN (Parent DN) ze seznamu. Proveďte volbu a klepněte na **Select**, abyste zadali nadřazené DN. Záznam vybraný v daném stromu se stane předvolenou hodnotou pro **Parent DN**.

| **Poznámka:** Pokud jste zahájili tuto úlohu z panelu **Manage entries**, je toto pole automaticky vyplněno. **Parent DN** bylo vybráno předtím, než jste klepnuli na **Add** a zahájili proces přidání záznamu.

- | 8. Na kartě **Required attributes** zadejte hodnoty pro povinné atributy.
 - | • **cn** je relativní DN, které jste zadali dříve.
 - | • V poli **ibm-searchSizeLimit** zadejte počet záznamů, kterým budete omezovat velikost hledání. Tento počet může být v rozmezí 0 až 2 147 483 647. Nastavení počtu 0 je totéž jako **Unlimited**.
 - | • V poli **ibm-searchTimeLimit** zadejte počet vteřin, kterým budete omezovat dobu hledání. Tento počet může být v rozmezí 0 až 2 147 483 647. Nastavení počtu 0 je totéž jako **Unlimited**.
 - | • V závislosti na třídě objektu, kterou jste vybrali, se vám může zobrazit pole **Member** nebo **uniqueMember**. To jsou členové skupiny, kterou tvoříte. Tento záznam je ve formátu DN, například cn=Bob Garcia,ou=austin,o=ibm,c=us.
- | 9. Jestliže chcete pro příslušný atribut přidat více než jednu hodnotu, klepněte na **Multiple values** a potom hodnoty přidávejte postupně jednu po druhé. Když dokončíte přidávání dalších hodnot, klepněte na **OK**. Hodnoty se přidají do rozbalovacího menu zobrazeného u atributu.
- | 10. Pokud má váš server aktivovány jazykové příznaky, klepněte na **Language tag value** a přidejte nebo odstraňte popisovače jazykových příznaků.
- | 11. Klepněte na **Other attributes**.
- | 12. Na kartě **Other attributes** zadejte příslušné hodnoty pro atributy. Další informace najdete v tématu “Jak změnit binární atributy” na stránce 171.
- | 13. Klepnutím na **Finish** vytvoříte záznam.

| Jak měnit skupinu s limity hledání

| U skupiny s limity hledání můžete měnit atributy limitů velikosti nebo doby hledání. Do skupiny je také možno přidávat členy nebo je z ní odstraňovat. Ke změně skupiny s limity hledání použijte webový administrační nástroj.

| Chcete-li změnit skupinu s limity hledání, vyhledejte si téma “Jak editovat záznam” na stránce 167.

Jak kopírovat skupinu s limity hledání

Kopírování skupiny s limity hledání je užitečné tehdy, když chcete mít stejnou skupinu s limity hledání jak pod localhost tak pod IBMpolicies. Je také užitečné, pokud chcete vytvořit novou skupinu, která má podobné parametry jako existující skupina, jen s menšími rozdíly.

Chcete-li kopírovat skupinu s limity hledání, vyhledejte si téma “Jak kopírovat záznam” na stránce 167.

Jak odstranit skupinu s limity hledání

Chcete-li odstranit skupinu s limity hledání, vyhledejte si téma “Jak vymazat záznam” na stránce 167.

Jak spravovat skupiny s proxy autorizací

Členové skupiny s proxy autorizací mohou přistupovat na server adresářů a provádět mnoho úloh jménem více uživatelů, aniž by se museli za každého uživatele opětovně přihlašovat. Členové skupiny s proxy autorizací mohou na sebe vzít libovolnou autentizovanou identitu s výjimkou identity administrátora nebo členů administrační skupiny. Další informace najdete v tématu “Proxy autorizace” na stránce 55.

Ke správě skupin s proxy autorizací se používá webový administrační nástroj.

Další informace najdete v těchto tématech:

- “Jak vytvořit skupinu s proxy autorizací”
- “Jak měnit skupinu s proxy autorizací” na stránce 122
- “Jak kopírovat skupinu s proxy autorizací” na stránce 122
- “Jak odstranit skupinu s proxy autorizací” na stránce 122

Jak vytvořit skupinu s proxy autorizací

1. V navigační oblasti rozbalte kategorii **Directory management** a klepněte na **Add an entry**. Anebo klepněte na **Manage entries**, vyberte umístění (cn=ibmPolicies nebo cn=localhost) a klepněte na **Add**.
2. Vyberte třídy objektu **groupof Names object** z menu **Structural object class**.
3. Klepněte na **Next**.
4. Vyberte pomocnou třídu objektu **ibm-proxyGroup** z menu **Available** a klepněte na **Add**. Tento postup opakujte pro každou další pomocnou třídu objektu, kterou chcete přidat.
5. Klepněte na **Next**.
6. V poli **Relative DN** napište cn=proxyGroup.
7. V poli **Parent DN** zadejte rozlišovací jméno stromového záznamu, který jste vybrali, například cn=localhost. Můžete také klepnout na **Browse** a vybrat **Parent DN** ze seznamu. Vyberte svou volbu a klepnutím na **Select** určete požadované Parent DN. Předvolenou hodnotou pro Parent DN je záznam vybraný v daném stromu.

Poznámka: Pokud jste zahájili tuto úlohu z panelu Manage entries, je toto pole automaticky vyplněno. Parent DN bylo vybráno předtím, než jste klepnuli na Add a zahájili proces přidání záznamu.

8. Na kartě **Required attributes** zadejte hodnoty pro povinné atributy.
 - **cn** je proxyGroup.
 - **Member** (člen) je ve formátu DN, například cn=Bob Garcia,ou=austin,o=ibm,c=us.Další informace o přidávání binárních hodnot najdete v tématu “Jak změnit binární atributy” na stránce 171.
9. Jestliže chcete pro příslušný atribut přidat více než jednu hodnotu, klepněte na **Multiple values** a potom hodnoty přidávejte postupně jednu po druhé.

Poznámka: Nevytvářejte vícenásobné hodnoty pro hodnotu cn. Skupina s proxy autorizací musí mít dobře známé jméno, proxyGroup.

Když dokončíte přidávání dalších hodnot, klepněte na **OK**. Hodnoty se přidají do rozbalovacího menu zobrazeného u atributu.

10. Pokud má váš server aktivovány jazykové příznaky, klepněte na **Language tag value** a přidejte nebo odstraňte popisovače jazykových příznaků.
11. Klepněte na **Other attributes**.
12. Na kartě **Other attributes** zadejte příslušné hodnoty pro atributy. Další informace o přidávání binárních hodnot najdete v tématu “Jak změnit binární atributy” na stránce 171.
13. Jestliže chcete pro příslušný atribut přidat více než jednu hodnotu, klepněte na **Multiple values** a potom hodnoty přidávejte postupně jednu po druhé. Když dokončíte přidávání dalších hodnot, klepněte na **OK**. Hodnoty se přidají do rozbalovacího menu zobrazeného u atributu.
14. Pokud má váš server aktivovány jazykové příznaky, klepněte na **Language tag value** a přidejte nebo odstraňte popisovače jazykových příznaků.
15. Klepnutím na **Finish** vytvoříte záznam.

Jak měnit skupinu s proxy autorizací

Změny skupin s proxy autorizací, jako přidávání nebo vymazání členů skupiny, můžete provádět pomocí webového administračního nástroje.

Chcete-li změnit skupinu s proxy autorizací, vyhledejte si téma “Jak editovat záznam” na stránce 167.

Jak kopírovat skupinu s proxy autorizací

Kopírování skupiny s proxy autorizací je užitečné tehdy, když chcete mít stejnou skupinu s proxy autorizací jak pod localhost tak pod IBMpolicies.

Chcete-li kopírovat skupinu s proxy autorizací, vyhledejte si téma “Jak kopírovat záznam” na stránce 167.

Jak odstranit skupinu s proxy autorizací

Chcete-li odstranit člena ze skupiny s proxy autorizací pomocí webového administračního nástroje, vyhledejte si téma “Jak vymazat záznam” na stránce 167.

Jak spravovat jedinečné atributy

Správa jedinečných atributů se provádí v rámci kategorie **Server administration** webového administračního nástroje. Další informace najdete v těchto částech:

- “Jak vytvořit seznam jedinečných atributů”
- “Jak odstranit záznam ze seznamu jedinečných atributů” na stránce 123

Poznámka: Co se týče jednotlivých atributů, jazykové příznaky jsou u jedinečných atributů vzájemně exkluzivní. Pokud jste určitý atribut označili za jedinečný atribut, nemůže mít k sobě přiřazený jazykové příznaky.

Poznámka: Chcete-li měnit konfigurační nastavení serveru pomocí úloh v kategorii Server administration, musíte se na server autentizovat jako uživatelský profil i5/OS, který má speciální oprávnění *ALLOBJ a IOSYSCFG. Toho lze docílit tak, že se budete autentizovat jako projektovaný uživatel s heslem pro tento profil. Chcete-li se přihlásit z webového administračního nástroje jako projektovaný uživatel, zadejte uživatelské jméno ve formě os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM, kde řetězce MYUSERNAME a MYSYSTEM.COM nahradíte vaším jménem uživatelského profilu a konfigurovanou systémovou projektovanou příponou.

Jak vytvořit seznam jedinečných atributů

1. V navigační oblasti rozbalte kategorii **Server administration**. Klepněte na volbu **Manage unique attributes**.
2. Z menu **Available attributes** vyberte atribut, který chcete přidat jako jedinečný atribut. Atributy uvedené v seznamu jsou ty, které lze označit jako jedinečné; například sn.

3. Klepněte buď na **Add to cn=localhost** nebo na **Add to cn=IBMpolicies**. Rozdíl mezi těmito dvěma zásobníky spočívá v tom, že záznamy v `cn=IBMpolicies` se replikují, zatímco záznamy v `cn=localhost` se nereplikují. Atribut se zobrazí v příslušném okně se seznamem. Stejný atribut můžete mít v seznamu v obou zásobnících.

Poznámka: Pokud se záznam vytvoří jak pod `cn=localhost` tak pod `cn=IBMpolicies`, bude výsledným spojením těchto dvou záznamů seznam jedinečných atributů. Například pokud atributy `cn` a `employeeNumber` jsou označeny jako unikátní v `cn=localhost` a atributy `cn` a `telephoneNumber` jsou označeny jako unikátní v `cn=IBMpolicies`, server jako jedinečné atributy bere atributy `cn`, `employeeNumber` a `telephoneNumber`.

4. Tento postup opakujte pro každý atribut, který se má přidat jako jedinečný atribut.
5. Klepněte na **OK** a uložte změny.

Když se přidává nebo modifikuje záznam jedinečného atributu a nastavení jedinečnosti pro některý z typů jedinečných atributů uvedených v seznamu skončí chybou, záznam nebude přidán ani se v adresáři nevytvoří. Předtím, než lze záznam vytvořit nebo modifikovat, musí být problém vyřešen a příkaz pro přidání nebo modifikaci se musí vydat znovu. Například když budete přidávat do adresáře záznam jedinečného atributu a nastavení jedinečnosti pro tabulku jednoho z typů jedinečných atributů uvedených v seznamu selže, (tj. protože v databázi existují duplikované hodnoty), záznam jedinečného atributu nebude do adresáře přidán. Bude vydána chyba.

Když se aplikace pokouší přidat do adresáře záznam s hodnotou atributu, která je duplicitní s existujícím záznamem adresáře, LDAP server vyšle chybu s výsledkovým kódem 20 (LDAP: error code 20 - Attribute or Value Exists).

Při spuštění server kontroluje seznam jedinečných atributů a určuje, zda pro každý z nich existuje omezení DB2. Pokud pro atribut neexistuje omezení, protože bylo odstraněno obslužným programem typu `bulkload` nebo protože bylo odstraněno manuálně uživatelem, je atribut odstraněn ze seznamu jedinečných atributů a do protokolu chyb (`ibmslapd.log`) se zaznamená chybová zpráva. Například pokud atribut `cn` je označen jako jedinečný v `cn=uniqueattributes,cn=localhost` a neexistuje pro něj omezení DB2, zaznamená se do protokolu tato zpráva:

```
Values for the attribute CN are not unique.  
The attribute CN was removed from the unique attribute  
entry: CN=UNIQUEATTRIBUTES,CN=LOCALHOST
```

Jak odstranit záznam ze seznamu jedinečných atributů

Pokud jedinečný atribut existuje jak v `cn=uniqueattribute,cn=localhost` tak v `cn=uniqueattribute,cn=IBMpolicies` a je odstraněn pouze z jednoho záznamu, server i nadále pracuje s tímto atributem jako s jedinečným. Atribut přestává být jedinečným teprve tehdy, až je odstraněn z obou záznamů.

1. V navigační oblasti rozbalte kategorii **Server administration** a klepněte na **Manage unique attributes**.
2. Vyberte atribut, který chcete odstranit ze seznamu jedinečných atributů tak, že klepnete na tento atribut v příslušném okně se seznamem.
3. Klepněte na tlačítko **Remove**.
4. Tento postup opakujte pro každý atribut, který chcete odstranit ze seznamu.
5. Klepněte na **OK** a uložte změny.

Poznámka: Pokud odstraníte poslední jedinečný atribut z okénka se seznamem pro `cn=localhost` nebo `cn=IBMpolicies`, záznam zásobníku pro toto okénko se seznamem (`cn=uniqueattribute,cn=localhost` nebo `cn=uniqueattribute,cn=IBMpolicies`) se automaticky vymaže.

Jak sledovat přístup a změny u adresáře LDAP

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

Chcete-li aktivovat protokol změn, použijte tento postup:

1. V prostředí produktu iSeries Navigator rozbalte položku **Sít**.

- | 2. Rozbalte položku **Servery**.
- | 3. Klepněte na **TCP/IP**.
- | 4. Pravým tlačítkem myši klepněte na **Server adresářů IBM** a vyberte volbu **Vlastnosti**.
- | 5. Klepněte na kartu **Protokol změn**.
- | 6. Vyberte volbu **Protokolovat změny adresáře**.
- | 7. Volitelné: Do pole **Maximum záznamů** zadejte maximální počet záznamů, které může protokol uchovávat. Do pole **Maximální stáří** zadejte, jak dlouho jsou uchovávány záznamy v protokolu změn.

| **Poznámka:** I když jsou tyto parametry nepovinné, rozhodně se doporučuje zadat buď maximální počet záznamů, nebo jejich maximální stáří. Jestliže ani jedno z nich nezadáte, protokol změn bude uchovávat všechny záznamy a jeho velikost bude značně narůstat.

| Třída objektů `changeLogEntry` slouží k znázornění změn provedených na serveru adresářů. Sada změn je dána sadou všech záznamů uspořádanou v rámci zásobníku protokolu změn podle definice v atributu `changeNumber`. Informace v protokolu změn jsou určeny "pouze pro čtení".

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

| **Příklad:**

| Tento příklad ukazuje, jak lze pomocí obslužného programu příkazového řádku **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**

| Server adresářů podporuje monitorování zabezpečení ochrany dat operačního systému i5/OS. Je-li u systémové hodnoty QAUDCTL zadáno *OBJAUD, můžete aktivovat monitorování objektů prostřednictvím produktu iSeries Navigator.

| Chcete-li aktivovat monitorování objektů pro produkt 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 **Server adresářů IBM** a vyberte volbu **Vlastnosti**.
- | 5. Klepněte na kartu **Monitorování**.
- | 6. Vyberte požadované nastavení monitorování pro váš server.
- | 7. Klepněte na **OK**.

| Změny v nastavení monitorování se projeví, jakmile klepnete na tlačítko **OK**. Není nutné restartovat server adresářů. Další informace najdete v tématu "Server adresářů - Zabezpečení ochrany dat" na stránce 46.

| **Jak přizpůsobit nastavení vyhledávání**

| Můžete nastavit parametry vyhledávání, které řídí prohledávací možnosti uživatele, jako např. stránkované a tříděné vyhledávání, limity velikosti a doby prohledávání nebo volby dereference aliasů, a to pomocí webového administračního nástroje.

| Výsledky stránkovaného hledání umožňují klientovi řídit objem dat vrácených z požadavku na hledání. Klient může požadovat zaslání podmnožiny záznamů (stránku) namísto obdržení všech výsledků ze serveru najednou. Následné požadavky na vyhledávání zobrazují další stránky výsledků do té doby, než je operace zrušena nebo než je vrácen poslední výsledek.

| Tříděné hledání umožňuje klientu získávat výsledky prohledávání setříděné podle seznamu kritérií, kde každé kritérium představuje třídící klíč. To přenáší odpovědnost za třídění z klientské aplikace na server.

| Chcete-li přizpůsobit nastavení vyhledávání v serveru adresářů, postupujte takto:

| 1. V navigační oblasti rozbalte kategorii **Server administration** a vyberte **Manage server properties**.

| **Poznámka:** Chcete-li měnit konfigurační nastavení serveru pomocí úloh v kategorii Server administration, musíte se na server autentizovat jako uživatelský profil i5/OS, který má speciální oprávnění *ALLOBJ a IOSYSCFG. Toho lze docílit tak, že se budete autentizovat jako projektovaný uživatel s heslem pro tento profil. Chcete-li se přihlásit z webového administračního nástroje jako projektovaný uživatel, zadejte uživatelské jméno ve formě `os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM`, kde řetězce MYUSERNAME a MYSYSTEM.COM nahradíte vašim jménem uživatelského profilu a konfigurovanou systémovou projektovanou příponou.

| 2. Vyberte kartu **Search settings**.

| 3. Nastavte parametr **Search size limit**. Klepněte buď na tlačítko **Entries** nebo **Unlimited**. Pokud vyberete **Entries**, musíte do pole zadat maximální počet záznamů, které může hledání vrátit. Předvolené nastavení je 500. Pokud vyhledávacímu kritériu vyhovuje více záznamů, tyto se nevrátí. Tento limit se netýká administrátorů nebo členů skupin s limity hledání, kterým byly uděleny větší limity pro velikost hledání.

| 4. Nastavte parametr **Search time limit**. Klepněte buď na tlačítko **Seconds** nebo **Unlimited**. Pokud vyberete **Seconds**, musíte do pole zadat maximální dobu ve vteřinách, po kterou server může zpracovávat požadavek. Předvolené nastavení je 900. Tento limit se netýká administrátorů nebo členů skupin s limity hledání, kterým byly uděleny větší limity pro dobu hledání.

| 5. Chcete-li omezit schopnosti tříděného vyhledávání pouze na administrátory, označte zaškrtačkové okénko **Only allow administrators to sort searches**.

| 6. Chcete-li omezit schopnosti stránkového vyhledávání pouze na administrátory, označte zaškrtačkové okénko **Only allow administrators to page searches**.

| 7. Rozbalte rozbalovací menu u parametru **Alias dereferencing** a vyberte jednu z následujících možností. Předvolené nastavení je **Always**.

| **Never** Dereference aliasů se neprovádí nikdy.

| **Find** Dereference aliasů se provádí při hledání počátečního bodu pro prohledávání, ale ne při prohledávání pod tímto počátečním záznamem.

| **Search** Dereference aliasů se provádí při prohledávání záznamů pod počátečním bodem hledání, ale ne při hledání tohoto počátečního záznamu.

| **Always**

| Dereference aliasů se provádí vždy, jak při hledání počátečního bodu prohledávání, tak při prohledávání záznamů pod tímto počátečním záznamem. Toto je předvolené nastavení.

| Další informace najdete v tématech “Parametry prohledávání” na stránce 42 a “Jak prohledávat záznamy adresáře” na stránce 169.

| Jak přizpůsobit nastavení výkonu

| Nastavení výkonu serveru adresářů můžete přizpůsobit změnou některé z těchto položek:

- | • Velikost paměti cache ACL, velikost paměti cache záznamu, maximální počet vyhledávání, který se má uchovávat v paměti cache filtru a nejzrozsáhlejší vyhledávání, které se má uchovávat v paměti cache filtru.
- | • Počet databázových připojení a vláken na serveru.
- | • Nastavení paměti cache atributů.
- | • Nastavení transakcí serveru.

| Další informace najdete v těchto tématech:

- | • “Jak nastavit databázová připojení a nastavení paměti cache” na stránce 126
- | • “Jak konfigurovat paměť cache atributu” na stránce 126

- “Jak konfigurovat nastavení transakcí” na stránce 128

Jak nastavit databázová připojení a nastavení paměti cache

Chcete-li nastavit databázová připojení a nastavení paměti cache, postupujte takto:

1. V navigační oblasti webového administračního nástroje rozbalte kategorii **Manage server properties** a klepněte na kartu **Performance** v pravém podokně.
2. Zadejte **Number of database connections**. Tím nastavíte počet připojení DB2 používaných serverem. Minimální počet, který musíte zadat, je 4. Předvolené nastavení je 15. Pokud váš LDAP server přijímá vysoký objem klientských požadavků nebo klienti dostávají chybové hlášky "connection refused", možná dosáhnete lepších výsledků, když zvýšíte nastavení počtu připojení, které server provádí do DB2. Maximální počet připojení je určen nastavením databáze DB2. I když ohledně zadaného počtu připojení neexistuje nějaké omezení, je třeba si uvědomit, že každé připojení spotřebovává zdroje.
3. Zadejte **Number of database connections**. Tím nastavíte počet připojení DB2 používaných serverem pro replikaci. Minimální počet, který musíte zadat, je 1. Předvolené nastavení je 4.

Poznámka: Celkový počet připojení zadaných pro databázová připojení, včetně databázových připojení pro replikaci, nesmí přesáhnout počet připojení nastavených v databázi DB2.

4. Vyberte položku **Cache ACL information**, ve které zadáte níže uvedená nastavení paměti cache ACL.
5. V parametru **Maximum number of elements in ACL cache** zadejte maximální počet prvků v paměti cache ACL. Předvolená hodnota je 25 000.
6. V parametru **Maximum number of elements in entry cache** zadejte maximální počet prvků v paměti cache záznamu. Předvolená hodnota je 25 000.
7. V parametru **Maximum number of elements in search cache** zadejte maximální počet prvků v paměti cache vyhledávacího filtru. Předvolená hodnota je 25 000. Paměť cache vyhledávacího filtru obsahuje aktuální dotazy na požadované filtry atributů a výsledné identifikátory záznamů, které odpovídaly. Při operaci aktualizace jsou všechny záznamy paměti cache filtru zrušeny.
8. V parametru **Maximum number of elements from a single search added to search filter cache** zadejte maximální počet prvků přidávaných do paměti cache vyhledávacího filtru z jednotlivých hledání. Pokud vyberete **Elements**, musíte zadat konkrétní číslo. Předvolená hodnota je "100". Jinak vyberte **Unlimited**. Záznamy vyhledávání, které odpovídají více záznamům než je počet zadaný zde, nebudou přidány do paměti cache vyhledávacího filtru.
9. Po dokončení klepněte na **OK**.
10. Pokud jste nastavovali počet databázových připojení, restartujte server, aby změny vstoupily v platnost. Pokud jste pouze modifikovali nastavení paměti cache, není nutno server restartovat.

Jak konfigurovat paměť cache atributu

Nastavení pro paměť cache atributu se konfiguruje jak ve webovém administračním nástroji tak v prostředí produktu iSeries Navigator.

Chcete-li manuálně upravit nastavení paměti cache atributu pomocí webového administračního nástroje, postupujte takto:

1. V navigační oblasti webového administračního nástroje rozbalte kategorii **Server administration** a klepněte na kartu **Attribute cache** v pravém podokně.

Poznámka: Chcete-li měnit konfigurační nastavení serveru pomocí úloh v kategorii Server administration, musíte se na server autentizovat jako uživatelský profil i5/OS, který má speciální oprávnění *ALLOBJ a IOSYSCFG. Toho lze docílit tak, že se budete autentizovat jako projektovaný uživatel s heslem pro tento profil. Chcete-li se přihlásit z webového administračního nástroje jako projektovaný uživatel, zadejte uživatelské jméno ve formě `os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM`, kde řetězce MYUSERNAME a MYSYSTEM.COM nahradíte vašim jménem uživatelského profilu a konfigurovanou systémovou projektovanou příponou.

2. Změňte objem paměti v kilobytech, který je k dispozici pro paměť cache adresáře. Předvolené nastavení je 16 384 kilobytů (16 MB).
3. Změňte objem paměti v kilobytech, který je k dispozici pro paměť cache protokolu změn. Předvolené nastavení je 16 384 kilobytů (16 MB).

Poznámka: Pokud není protokol změn nakonfigurován, je tato volba deaktivovaná. Ukládání do paměti cache atributu pro protokol změn by mělo být nastaveno na 0 a neměly by být konfigurovány žádné atributy, pokud neprovádíte v rámci protokolu změn častá vyhledávání a výkon těchto hledání není kritickým faktorem.

4. Z menu **Available attributes** vyberte atribut, který chcete ukládat do paměti cache. Zobrazeny jsou pouze ty atributy, které lze ukládat do paměti cache; například sn.

Poznámka: Atribut zůstává v seznamu dostupných atributů, dokud nebude umístěn jak v zásobníku cn=directory tak v zásobníku cn=changelog.

5. Klepněte buď na **Add to cn=directory** nebo na **Add to cn=changelog**. Atribut se zobrazí v příslušném okně se seznamem. Stejný atribut můžete mít v seznamu v obou zásobnících.

Poznámka: Pokud není protokol změn nakonfigurován, je volba **Add to cn=changelog** deaktivována. Ukládání do paměti cache atributu pro protokol změn by mělo být nastaveno na 0 a neměly by být konfigurovány žádné atributy, pokud neprovádíte v rámci protokolu změn častá vyhledávání a výkon těchto hledání není kritickým faktorem.

6. Tento postup opakujte pro každý atribut, který chcete přidat do paměti cache atributů.
7. Po dokončení klepněte na **OK**.

Chcete-li aktivovat automatické ukládání do paměti cache atributů v prostředí produktu iSeries Navigator, postupujte takto:

1. V prostředí produktu iSeries Navigator rozbalte položku **Sítě**.
2. Rozbalte položku **Servery**.
3. Klepněte na **TCP/IP**.
4. Pravým tlačítkem myši klepněte na **Server adresářů IBM** a vyberte volbu **Vlastnosti**.
5. Klepněte na kartu **Výkon**.
6. Vyberte **Povolit automatické ukládání do paměti cache atributů** buď pro **Databáze** nebo pro **Protokol změn**, nebo obojí. Automatické ukládání do paměti cache atributu pro protokol změn by se nemělo aktivovat, pokud neprovádíte v rámci protokolu změn častá vyhledávání a výkon těchto hledání není kritickým faktorem.
7. Zadejte **Čas spuštění** (v lokálním čase serveru) a **Interval** pro každý typ ukládání do paměti cache, který jste se rozhodli aktivovat. Například pokud aktivujete ukládání do paměti cache pro databázi a nastavíte čas spuštění na 6.00 a interval na 6 hodin, bude se paměť cache automaticky upravovat v 6.00, ve 12.00, v 18.00 a ve 24.00 hod., bez ohledu na to, kdy byl spuštěn server nebo kdy bylo automatické upravování nakonfigurováno.

Poznámka: Automatické ukládání do paměti cache atributů bude atributy ukládat až do maxima objemu paměti pro ukládání do paměti cache, které bylo zadáno v rámci webového administračního nástroje, jak je popsáno výše.

Tabulka 4. Vzájemné vazby mezi nastaveními paměti cache atributů

Aktivita	Co se stane
Spuštění serveru	Je-li aktuálně povoleno ukládání do paměti cache atributu a automatické ukládání do paměti cache bylo povoleno, když byl server naposledy ukončen, pak stejné atributy, které byly ukládány do paměti cache, když byl server ukončen, budou vytvořeny, když se server restartuje. Je-li ještě k dispozici pro ukládání do paměti cache další paměť, atributy, které byly konfigurovány manuálně, se budou rovněž ukládat do paměti cache. Je-li aktuálně povoleno ukládání do paměti cache a při posledním ukončení serveru nebylo povoleno, atributy, které jsou manuálně konfigurovány pro ukládání do paměti cache, se budou do paměti cache ukládat. V obou případech pak server automaticky upraví paměti cache atributů na základě zadaného času spuštění a časového intervalu. Pokud automatické ukládání do paměti cache není povoleno, budou platit manuálně upravená nastavení paměti cache.
Povolení automatického ukládání do paměti cache atributů po spuštění serveru	Automatické ukládání do paměti cache atributů bude fungovat tak, jak je popsáno u spuštění serveru. Veškeré manuálně nakonfigurované paměti cache atributů, které neodpovídají objemu paměti nakonfigurované pro ukládání do paměti cache atributů, budou vymazány.
Deaktivace automatického ukládání do paměti cache atributů po spuštění serveru	Do paměti cache se budou ukládat pouze atributy, které byly nakonfigurovány manuálně.
Modifikace manuálně ukládaných atributů do paměti cache, přičemž automatické ukládání do paměti cache bylo povoleno po spuštění serveru	Nestane se nic. Manuální konfigurace začne platit v okamžiku, kdy bude automatické ukládání do paměti cache deaktivováno.
Modifikace objemu paměti dostupné pro ukládání do paměti cache po spuštění serveru	Pokud je povoleno automatické ukládání do paměti cache, server okamžitě znovu provede uložení do paměti cache na základě nové velikosti. Pokud je automatické ukládání do paměti cache deaktivováno, server bude ukládat do paměti cache manuálně nakonfigurované atributy až do nové velikosti paměti.
Modifikace času spuštění a intervalu ukládání do paměti cache po spuštění serveru	Pokud je povoleno automatické ukládání do paměti cache, začnou nová nastavení účinkovat v zadaném čase spuštění nebo intervalu. Pokud je automatické ukládání do paměti cache deaktivováno, nastavení se uloží a začnou účinkovat v okamžiku, kdy bude automatické ukládání do paměti cache povoleno.

Jak konfigurovat nastavení transakcí

Chcete-li nastavit nastavení transakcí, postupujte takto:

1. V navigační oblasti webového administračního nástroje rozbalte kategorii **Manage server properties** a vyberte kartu **Transactions** v pravém podokně.
2. Zaškrtněte okénko **Enable transaction processing**, abyste aktivovali zpracování transakcí. Je-li funkce **Enable transaction processing** deaktivována, všechny ostatní volby na tomto panelu bude server ignorovat.
3. Nastavte parametr **Maximum number of transactions**. Klepněte buď na tlačítko **Transactions** nebo **Unlimited**. Pokud vyberete **Transactions**, zadejte maximální počet transakcí. Maximální možný počet transakcí je 2 147 483 647. Předvolené nastavení je 20 transakcí.
4. Nastavte parametr **Maximum number of operations per transaction**. Klepněte buď na tlačítko **Operations** nebo **Unlimited**. Pokud vyberete **Operations**, zadejte maximální počet operací povolených pro jednotlivé transakce. Maximální možný počet operací je 2 147 483 647. Čím nižší je počet, tím lepší bude výkon. Předvolená hodnota je 5 operací.
5. Nastavte parametr **Pending time limit**. Tato volba určuje maximální hodnotu časového limitu nevyřízených transakcí ve vteřinách. Klepněte buď na tlačítko **Seconds** nebo **Unlimited**. Pokud vyberete **Seconds**, zadejte maximální počet vteřin povolený pro jednotlivé transakce. Maximální možný počet vteřin je 2 147 483 647. Transakce, které zůstanou nedokončeny po delší dobu, než je tato, budou zrušeny (odstraněny). Předvolená hodnota je 300 vteřin.
6. Po dokončení klepněte na **OK**.

- 7. Pokud jste aktivovali podporu pro transakce, restartujte server, aby změny vstoupily v platnost. Pokud jste pouze modifikovali nastavení, není nutno server restartovat.

Jak provádět správu replikací

Chcete-li provádět správu replikací, rozbalte kategorii **Replication management** webového administračního nástroje. Více informací o koncepcích replikací najdete v tématu “Replikace” na stránce 36.

Další informace najdete v těchto částech:

- “Jak vytvořit topologii hlavní server-replika”
- “Jak vytvořit topologii hlavní server-předávací server-replika” na stránce 134
- “Přehled tvorby úplné replikační topologie” na stránce 136
- “Jak vytvořit úplnou topologii s peerovou replikací” na stránce 136
- “Jak nastavit topologii brány” na stránce 139
- “Jak provádět správu topologií” na stránce 140
- “Jak měnit vlastnosti replikace” na stránce 143
- “Jak vytvářet časové plány replikací” na stránce 144
- “Jak provádět správu front” na stránce 146
- “Jak nastavit replikaci přes zabezpečené spojení” na stránce 146

Jak vytvořit topologii hlavní server-replika

Pokud chcete definovat základní topologii hlavní server-replika, musíte:

1. Vytvořit hlavní server a definovat, co obsahuje. Vyberte podstrom, který chcete replikovat, a určete tento server jako hlavní. Další informace najdete v tématu “Jak vytvořit hlavní server (replikovaný podstrom)” na stránce 130.
2. Vytvořit pověření, které má používat dodavatel. Další informace najdete v tématu “Jak vytvořit pověření” na stránce 130.
3. Vytvořit replikovaný server. Další informace najdete v tématu “Jak vytvořit replikovaný server” na stránce 132.
4. Exportovat topologii z hlavního serveru na repliku. Další informace najdete v tématu “Jak kopírovat data do repliky” na stránce 133.
5. Změnit konfiguraci repliky tak, aby se určilo, kdo je oprávněn replikovat její změny, a přidat odkaz na hlavní server. Další informace najdete v tématu “Jak přidávat informace dodavatele na repliku” na stránce 133.

Poznámka:

Pokud záznam v kořeni podstromu, který chcete replikovat, není příponou na serveru, musíte před použitím funkce **Add subtree** zajistit, aby byly seznamy ACL definovány takto:

Pro nefiltrované ACL:

```
ownersource: <stejně jako DN záznamu>  
ownerpropagate: TRUE
```

```
aclsource: <stejně jako DN záznamu>  
aclpropagate: TRUE
```

Pro filtrované ACL:

```
ibm-filteraclinherit: FALSE
```

Mají-li se uspokojit požadavky ACL a pokud příslušný záznam není přípona na serveru, editujte seznam ACL pro tento záznam v dialogovém okně **Manage entries**. Vyberte příslušný záznam a klepněte na **Edit ACL**. Jestliže chcete přidat nefiltrované seznamy ACL, vyberte tuto kartu a výběrem zaškrtnávacího políčka určete, zda jsou seznamy ACL explicitní jak pro seznamy ACL, tak pro vlastníky. Zkontrolujte, zda jsou zaškrtnuta políčka **Propagate ACLs** a **Propagate owner**. Jestliže chcete přidat filtrované seznamy ACL, vyberte tuto kartu a přidejte záznam **cn=this** s úlohou **access-id** pro seznamy ACL i

vlastníky. Zkontrolujte, že zaškrtnutí políčka **Accumulate filtered ACLs** je zrušeno a že políčko **Propagate owner** je zaškrtnuté. Podrobnější informace najdete v tématu “Jak provádět správu seznamů přístupových práv (ACL)” na stránce 181.

Na začátku objekt **ibm-replicagroup** vytvořený tímto procesem dědí seznam ACL kořenového záznamu pro replikovaný podstrom. Tyto seznamy ACL by nemusely být vhodné pro řízení přístupu k informacím o replikaci v adresáři.

Jak vytvořit hlavní server (replikovaný podstrom)

Poznámka: K tomu, aby bylo možné tuto úlohu uskutečnit, musí být server spuštěn.

Tato úloha označí určitý záznam jako kořen nezávisle replikovaného podstromu a vytvoří **ibm-replicasubentry** představující tento server jako jediný hlavní server pro tento podstrom. Chcete-li vytvořit replikovaný podstrom, musíte označit podstrom, který má server replikovat.

V navigační oblasti rozbalte kategorii Replication management a klepněte na **Manage topology**.

1. Klepněte na **Add subtree**.
2. Zadejte DN kořenového záznamu podstromu, který chcete replikovat, případně klepnutím na **Browse** rozbalte záznamy a vyberte záznam, který se má stát kořenem podstromu.
3. URL odkazu na hlavní server se zobrazuje ve formě LDAP URL, například:
`ldap://<myservername>.<mylocation>.<mycompany>.com`

Poznámka: URL odkazu na hlavní server je volitelné. Používá se pouze:

- Pokud server obsahuje (nebo bude obsahovat) jakékoli podstromy pouze pro čtení.
- K definování URL odkazu, který se vrací k aktualizacím do jakéhokoli podstromu pouze pro čtení na serveru.

4. Klepněte na **OK**.
5. Nový server se zobrazuje v dialogovém okně Manage topology pod záhlavím **Replicated subtrees**.

Jak vytvořit pověření

V navigační oblasti webového administračního nástroje rozbalte kategorii Replication management a klepněte na **Manage credentials**

1. Ze seznamu podstromů vyberte umístění, které chcete používat pro uchování pověření. Webový nástroj administrace umožňuje definovat pověření v těchto místech:
 - **cn=replication,cn=localhost**, v tom případě se pověření uchovávají pouze pro aktuální server.

Poznámka: Ve většině případů replikací se dává přednost umístování pověření v **cn=replication,cn=localhost**, protože to poskytuje lepší zabezpečení než replikovaná pověření umístěná v podstromu. Mohou však nastat některé situace, v nichž pověření umístěná v **cn=replication,cn=localhost** nejsou dostupná.

Jestliže se pokoušíte přidat repliku pod nějaký server, například pod "serverA", a jste prostřednictvím webového administračního nástroje připojeni k jinému serveru, např. k serveru "serverB", pole **Select credentials** nezobrazuje volbu **cn=replication,cn=localhost**. Důvodem této situace je to, že není možné číst informace nebo aktualizovat žádné informace pod **cn=localhost** serveru "serverA", když jste připojeni k serveru "serverB".

Volba **cn=replication, cn=localhost** je dostupná pouze tehdy, když server, do kterého chcete přidat repliku, je stejný jako server, k němuž jste připojeni prostřednictvím webového administračního nástroje.

- Uvnitř replikovaného podstromu. V takovém případě jsou pověření replikována se zbytkem podstromu. Pověření umístěná v replikovaném podstromu jsou vytvořena pod záznamem **ibm-replicagroup=default** pro tento podstrom.

Poznámka: V případě, že nejsou zobrazeny žádné podstromy, prostudujte si pokyny v tématu “Jak vytvořit hlavní server (replikovaný podstrom)” na stránce 130 o tvorbě podstromu, který chcete replikovat.

2. Klepněte na tlačítko **Add**.
3. Pro pověření, které vytváříte, zadejte jméno, například **mycreds**, v poli je předem automaticky vyplněno **cn=**.
4. Vyberte typ metody autentizace, kterou chcete použít, a klepněte na **Next**.
 - Pokud jste zvolili autentizaci jednoduchého připojení:
 - a. Zadejte DN, které server používá k připojení k replice, například **cn=any**.
 - b. Zadejte heslo, které server používá, když se připojuje k replice, například **secret**.
 - c. Znovu zadejte heslo, aby se potvrdilo, že jste se nedopustili překlepu.
 - d. Chcete-li, zadejte stručný popis pověření.
 - e. Klepněte na **Finish**.

Poznámka: V tomto okamžiku je vhodné zapsat si pro budoucí použití připojovací DN a heslo pověření. Toto heslo budete potřebovat při tvorbě ujednání o replikaci.

- Pokud jste vybrali autentizaci Kerberos:
 - a. Zadejte své připojovací DN pro Kerberos.
 - b. Zadejte jméno souboru s tabulkou klíčů.
 - c. Chcete-li, zadejte stručný popis pověření. Žádné další informace nejsou zapotřebí. Další informace najdete v tématu “Jak aktivovat autentizaci Kerberos na serveru adresářů” na stránce 153.
 - d. Klepněte na **Finish**.

Panel **Add Kerberos Credentials** bere volitelné připojovací DN formy **ibm-kn=user@realm** a volitelný soubor s tabulkou klíčů (nazývá se klíčový soubor). Je-li zadáno připojovací DN, server používá zadané hlavní jméno k autentizaci na odběratelský server. Jinak se použije jméno služby Kerberos serveru (**ldap/host-name@realm**). Pokud se používá soubor s tabulkou klíčů, server ho použije k získání pověření pro zadané hlavní jméno. Pokud není zadán soubor s tabulkou klíčů, server použije soubor s tabulkou klíčů zadaný v konfiguraci Kerberos serveru. Pokud existuje více než jeden dodavatel, musíte určit, které hlavní jméno a soubor s tabulkou klíčů mají všichni dodavatelé používat.

Na serveru, kde jste vytvořili příslušná pověření:

- a. Rozbalte **Directory management** a klepněte na **Manage entries**.
- b. Vyberte podstrom, kde jste uložili pověření, například **cn=localhost**, a klepněte na **Expand**.
- c. Vyberte **cn=replication** a klepněte na **Expand**.
- d. Vyberte pověření pro kerberos (**ibm-replicationCredentialsKerberos**) a klepněte na **Edit attributes**.
- e. Klepněte na kartu **Other attributes**.
- f. Zadejte jméno **replicaBindDN**, například **ibm-kn=myprincipal@SOME.REALM**.
- g. Zadejte **replicaCredentials**. To je soubor s tabulkou klíčů použitý pro **myprincipal**.

Poznámka: Toto hlavní jméno a heslo by mělo být stejné jako jméno a heslo, které používáte pro spuštění **kinit** z příkazového řádku.

Na replice

- a. V navigační oblasti klepněte na **Manage replication properties**.
- b. Z rozbalovacího menu **Supplier information** vyberte dodavatele nebo zadejte jméno replikovaného podstromu, pro který chcete konfigurovat dodavatelská pověření.
- c. Klepněte na **Edit**.
- d. Zadejte jméno připojení **bindDN** replikace. V tomto příkladě to je **ibm-kn=myprincipal@SOME.REALM**.
- e. Zadejte a potvrďte heslo pro připojení k replikaci **Replication bind password**. To je heslo KDC použité pro **myprincipal**.

- Pokud jste vybrali SSL s autentizací pomocí certifikátu a používáte certifikát serveru, nemusíte poskytovat žádné další informace. Pokud jste zvolili použití jiného certifikátu než je certifikát serveru:
 - a. Zadejte jméno klíčového souboru.
 - b. Zadejte heslo klíčového souboru.
 - c. Pro potvrzení znovu zadejte heslo klíčového souboru.
 - d. Zadejte označení klíče.
 - e. Chcete-li, zadejte stručný popis.
 - f. Klepněte na **Finish**.

Další informace najdete v tématu “Jak aktivovat SSL a TSL (Transport Layer Security) na serveru adresářů” na stránce 151.

5. Na serveru, kde jste vytvořili příslušná pověření, nastavte hodnotu QRETSVRSEC (Allow server security information to be retained) na 1 (uchovávat data). Protože jsou pověření replikace uložena v ověřovacím seznamu, tato volba umožňuje serveru během připojování k replice načítat pověření z ověřovacího seznamu.

Jak vytvořit replikovaný server

Poznámka: K tomu, aby bylo možné tuto úlohu uskutečnit, musí být server spuštěn.

V navigační oblasti rozbalte kategorii **Replication management** a klepněte na **Manage topology**.

1. Vyberte podstrom, který chcete replikovat, a klepněte na **Show topology**.
2. Klepnutím na šipku vedle výběru **Replication topology** rozbalte seznam dodavatelských serverů.
3. Vyberte dodavatelský server a klepněte na **Add replica**.

Na kartě **Server** okna **Add replica**:

- Zadejte jméno hostitele a číslo portu pro repliku, kterou vytváříte. Předvolený port bez SSL je 389 a s použitím SSL je 636. Tato pole jsou povinná.
- Vyberte, zda se má povolit komunikace s použitím SSL.
- Zadejte jméno repliky nebo nechte toto pole prázdné, pokud se má použít jméno hostitele.
- Zadejte ID repliky. Pokud je server, na kterém vytváříte repliku, spuštěn, klepnutím na **Get replica ID** se toto pole automaticky vyplní. V případě, že server, který přidáváte, má sloužit jako peer server nebo předávací server, je toto pole povinné. Doporučuje se, aby všechny servery byly stejné verze.
- Zadejte popis replikovaného serveru.

Na kartě **Additional**:

1. Uveďte pověření, která používá příslušná replika pro komunikaci s hlavním serverem.

Poznámka: Webový nástroj administrace umožňuje definovat pověření v těchto umístěních:

- **cn=replication,cn=localhost**, v tom případě se pověření uchovávají pouze na serveru, který je používá.
- Uvnitř replikovaného podstromu. V takovém případě jsou pověření replikována se zbytkem podstromu. Pověření umístěná v replikovaném podstromu jsou vytvořena pod záznamem **ibm-replicagroup=default** pro tento podstrom.

Umístění v **cn=replication,cn=localhost** je pro pověření považováno za bezpečnější.

- a. Klepněte na **Select**.
- b. Vyberte umístění, které chcete pro pověření používat. Nejvhodnější je pro ně **cn=replication,cn=localhost**.
- c. Klepněte na **Show credentials**.
- d. Rozbalte seznam pověření a vyberte to, které chcete používat.
- e. Klepněte na **OK**.

Více informací o pověřeních pro ujednání najdete v tématu “Jak vytvořit pověření” na stránce 130.

2. Z rozbalovacího seznamu vyberte časový plán replikace nebo po klepnutí na **Add** můžete vytvořit další. Další informace najdete v tématu “Jak vytvářet časové plány replikací” na stránce 144
3. V seznamu schopností dodavatele můžete zrušit označení jakýchkoli schopností, které nechcete replikovat pro zákazníka.

Jestliže vaše síť obsahuje směs serverů různých verzí, jsou u novějších verzí dostupné schopnosti, které nejsou k dispozici na starších verzích. Některé schopnosti, jako například filtrování seznamů ACL a zásada správy hesel, používají operační atributy, které se replikují s ostatními změnami. Pokud se tyto funkce využívají, je ve většině případů vhodné, aby je podporovaly všechny servery. Pokud některé ze serverů příslušnou schopnost nepodporují, není vhodné ji používat. Například byste neměli používat na jednotlivých serverech různé seznamy ACL. Mohou však nastat situace, kdy byste mohli chtít využít některou schopnost na serverech, které ji podporují, a nenechat replikovat změny související s touto schopností na servery, které ji nepodporují. V takových případech můžete využít seznam schopností pro označení určitých schopností, které se nemají replikovat.

4. Klepnutím na **OK** vytvoříte repliku.
5. Zobrazí se zpráva upozorňující na skutečnost, že je zapotřebí provést další úkony. Klepněte na **OK**.

Poznámka: Jestliže přidáváte více serverů jako dodatečné repliky nebo vytváříte úplnou topologii, neměli byste zahajovat činnosti z částí “Jak kopírovat data do repliky” nebo “Jak přidávat informace dodavatele na repliku”, dokud jste nedokončili definování topologie na hlavním serveru. Jestliže po dokončení tvorby topologie vytvoříte soubor *masterfile.ldif*, tento soubor obsahuje záznamy adresáře hlavního serveru a úplnou kopii ujednání o topologii. Když na každý ze serverů tento soubor zavedete, každý server bude mít stejné informace.

Jak kopírovat data do repliky

Po vytvoření repliky musíte exportovat topologii z hlavního serveru na repliku.

1. Na hlavním serveru vytvořte pro příslušná data soubor LDIF. Všechna data obsažená na hlavním serveru můžete kopírovat pomocí tohoto postupu:
 - a. V prostředí produktu iSeries Navigator rozbalte položku **Síť**.
 - b. Rozbalte položku **Servery**.
 - c. Klepněte na **TCP/IP**.
 - d. Pravým tlačítkem myši klepněte na **Server adresářů IBM**, vyberte volbu **Nástroje** a potom volbu **Exportovat soubor**.
 - e. Zadejte jméno výstupního souboru LDIF (například *masterfile.ldif*), volitelně můžete určit podstrom pro export (například *subtreeDN*), a klepněte na **OK**.
2. Na počítači, kde vytváříte repliku, proveďte tyto činnosti:
 - a. Zkontrolujte, že jsou v konfiguraci replikovaného serveru definovány replikované přípony.
 - b. Zastavte replikovaný server.
 - c. Zkopírujte soubor LDIF do repliky a proveďte tyto činnosti:
 - 1) V prostředí produktu iSeries Navigator rozbalte položku **Síť**.
 - 2) Rozbalte položku **Servery**.
 - 3) Klepněte na **TCP/IP**.
 - 4) Pravým tlačítkem myši klepněte na **Server adresářů IBM**, vyberte volbu **Nástroje** a potom volbu **Importovat soubor**.
 - 5) Zadejte jméno vstupního souboru LDIF (například *masterfile.ldif*), volitelně můžete určit, jestli chcete replikovat data, a klepněte na **OK**.

Na repliku jsou zavedena ujednání o replikaci, časové plány, pověření (pokud jsou uloženy v replikovaném podstromu) a data záznamu.

- d. Spusťte server.

Jak přidávat informace dodavatele na repliku

Je nutné změnit konfiguraci repliky tak, aby se určilo, kdo je oprávněn replikovat její změny, a přidat odkaz na hlavní server.

Na počítači, kde vytváříte repliku:

1. V navigační oblasti rozbalte **Replication management** a klepněte na **Manage replication properties**.

Poznámka: K tomu, abyste mohli měnit nastavení na panelu **Manage replication properties**, musíte se do webového administračního nástroje přihlásit jako projektovaný uživatel OS/400 se zvláštními oprávněními *ALLOBJ a *IOSYSCFG.

2. Klepněte na tlačítko **Add**.
3. Z rozbalovacího menu **Replicated subtree** vyberte dodavatele nebo zadejte jméno replikovaného podstromu, pro který chcete konfigurovat dodavatelství pověření. Jestliže editujete dodavatelství pověření, toto pole není přístupné pro editaci.
4. Zadejte jméno připojení bindDN replikace. V tomto příkladě to je cn=any.

Poznámka: Použit můžete kteroukoli z těchto dvou voleb, podle situace.

- Nastavte připojovací DN (a heslo) replikace a předvolený odkaz pro všechny podstromy replikované na server s využitím 'předvolených pověření a odkazu'. To se může využít v případě, že se všechny podstromy replikují ze stejného dodavatele.
 - Nezávisle pro každý replikovaný podstrom nastavte připojovací DN a heslo replikace doplněním informací dodavatele pro každý podstrom. To se může využít v případě, že má každý podstrom jiného dodavatele (tzn. jiný hlavní server pro každý podstrom).
5. V závislosti na typu pověření zadejte a potvrďte heslo pověření (to jste si dříve poznamenali pro budoucí použití).
 - **Jednoduché připojení** - Zadejte DN a heslo.
 - **Kerberos** - Pokud pověření na dodavateli neurčují hlavní jméno a heslo, tzn. má se použít vlastní hlavní jméno serveru, potom připojovací DN je `ibm-kn=ldap/<yourservername@yourrealm>`. Jestliže pověření obsahuje hlavní jméno, jako např. `<myprincipal@myrealm>`, použijte je jako DN. V obou případech není zapotřebí zadávat heslo.
 - **SSL s připojením EXTERNAL** - Zadejte DN subjektu pro certifikát, heslo se nezadává.

Další informace najdete v tématu "Jak vytvořit pověření" na stránce 130.

6. Klepněte na **OK**.
7. K tomu, aby mohly změny vstoupit v platnost, je nutné znovu spustit repliku.

Další informace najdete v tématu "Jak měnit vlastnosti replikace" na stránce 143.

Replika je v pozastaveném stavu a nezačíná žádná replikace. Po dokončení nastavování replikační topologie musíte klepnout na **Manage queues**, vybrat příslušnou repliku a klepnutím na **Suspend/resume** spustit replikaci. Podrobnější informace najdete v tématu "Jak provádět správu front" na stránce 146. Replika nyní přijímá aktualizace z hlavního serveru.

Jak vytvořit topologii hlavní server-předávací server-replika

Chcete-li definovat topologii hlavní server-předávací server-replika, musíte:

1. Mít vytvořený hlavní server a replikovaný server. Další informace najdete v tématu "Jak vytvořit topologii hlavní server-replika" na stránce 129.
2. Vytvořit nový replikovaný server pro původní repliku. Další informace najdete v tématu "Jak vytvořit nový replikovaný server".
3. Zkopírovat data do replik. Další informace najdete v tématu "Jak kopírovat data do repliky" na stránce 133.

Jak vytvořit nový replikovaný server

Jestliže jste nastavili replikační topologii (viz část "Jak vytvořit hlavní server (replikovaný podstrom)" na stránce 130) s hlavním serverem (server1) a replikou (server2), můžete změnit úlohu serveru "server2" na úlohu předávacího serveru. K tomu potřebujete vytvořit novou repliku (server3) pod serverem "server2".

1. Připojte webovou administraci k hlavnímu serveru (server1).
2. V navigační oblasti rozbalte kategorii Replication management a klepněte na **Manage topology**.
3. Vyberte podstrom, který chcete replikovat, a klepněte na **Show topology**.

4. Klepnutím na šipku vedle výběru **Replication topology** rozbalte seznam dodavatelských serverů.
5. Klepnutím na šipku vedle výběru **server1** rozbalte seznam serverů.
6. Vyberte server2 a klepněte na **Add replica**.
7. Na kartě **Server** okna **Add replica**:
 - Zadejte jméno hostitele a číslo portu pro repliku (server3), kterou vytváříte. Předvolený port bez SSL je 389 a s použitím SSL je 636. Tato pole jsou povinná.
 - Vyberte, zda se má povolit komunikace s použitím SSL.
 - Zadejte jméno repliky nebo nechte toto pole prázdné, pokud se má použít jméno hostitele.
 - Zadejte ID repliky. Pokud je server, na kterém vytváříte repliku, spuštěn, klepnutím na **Get replica ID** se toto pole automaticky vyplní. V případě, že server, který přidáváte, má sloužit jako peer server nebo předávací server, je toto pole povinné. Doporučuje se, aby všechny servery byly stejné verze.
 - Zadejte popis replikovaného serveru.

Na kartě **Additional**:

- a. Uveďte pověření, která používá příslušná replika pro komunikaci s hlavním serverem.

Poznámka: Webový nástroj administrace umožňuje definovat pověření ve dvou umístěních:

- **cn=replication,cn=localhost**, v tom případě se pověření uchovávají pouze na serveru, který je používá.
- Uvnitř replikovaného podstromu. V takovém případě jsou pověření replikována se zbytkem podstromu.

Umístění v **cn=replication,cn=localhost** je pro pověření považováno za bezpečnější. Pověření umístěná v replikovaném podstromu jsou vytvořena pod záznamem **ibm-replicagroup=default** pro tento podstrom.

- 1) Klepněte na **Select**.
- 2) Vyberte umístění, které chcete pro pověření používat. Nejvhodnější je pro ně **cn=replication,cn=localhost**.
- 3) Klepněte na **Show credentials**.
- 4) Rozbalte seznam pověření a vyberte to, které chcete používat.
- 5) Klepněte na **OK**.

Více informací o pověřeních pro ujednání najdete v tématu “Jak vytvořit pověření” na stránce 130.

- b. Z rozbalovacího seznamu vyberte časový plán replikace nebo po klepnutí na **Add** můžete vytvořit další. Další informace najdete v tématu “Jak vytvářet časové plány replikací” na stránce 144.
- c. V seznamu schopností dodavatele můžete zrušit označení jakýchkoli schopností, které nechcete replikovat pro zákazníka.

Jestliže vaše síť obsahuje směs serverů různých verzí, jsou u novějších verzí dostupné schopnosti, které nejsou k dispozici na starších verzích. Některé schopnosti, jako například filtrování seznamů ACL a zásada správy hesel, používají operační atributy, které se replikují s ostatními změnami. Pokud se tyto funkce využívají, je ve většině případů vhodné, aby je podporovaly všechny servery. Pokud některé ze serverů příslušnou schopnost nepodporují, není vhodné ji používat. Například byste neměli používat na jednotlivých serverech různé seznamy ACL. Mohou však nastat situace, kdy byste mohli chtít využít některou schopnost na serverech, které ji podporují, a nenechat replikovat změny související s touto schopností na servery, které ji nepodporují. V takových případech můžete využít seznam schopností pro označení určitých schopností, které se nemají replikovat.

- d. Klepnutím na **OK** vytvoříte repliku.

8. Zkopírujte data ze serveru “server2” na nový replikovaný server “server3”. Informace o tom, jak postupovat, najdete v tématu “Jak kopírovat data do repliky” na stránce 133.
9. Do serveru “server3” přidejte dodavatelské ujednání, které činí server2 dodavatelem pro server 3 a server 3 odběratelem pro server2. Informace o tom, jak postupovat, najdete v tématu “Jak přidávat informace dodavatele na repliku” na stránce 133.

Úlohy serverů jsou ve webovém nástroji administrace znázorňovány ikonami. Vaše topologie je nyní tato:

- server1 (hlavní)
 - server2 (předávací)
 - server3 (replika)

Přehled tvorby úplné replikační topologie

Tento přehled vysoké úrovně je možné využít jako návod pro nastavení úplné replikační topologie.

1. Spusťte všechny peer servery nebo budoucí repliky. To je nutné z toho důvodu, aby webový nástroj administrace mohl shromáždit informace ze serverů.
2. Spusťte 'první' hlavní server a nakonfigurujte jej jako hlavní server pro kontext.
3. Pokud tato data již nejsou zavedena, zaveďte data pro podstrom, který se má replikovat na 'první' hlavní server.
4. Vyberte podstrom, který se má replikovat.
5. Přidejte všechny potenciální hlavní peer servery jako repliky 'prvního' hlavního serveru.
6. Přidejte všechny ostatní repliky.
7. Přesuňte ostatní hlavní peer servery do vyšší úrovně.
8. Do každého z hlavních peer serverů přidejte ujednání o replikaci pro repliky.

Poznámka: Pokud se mají vytvořit pověření v `cn=replication,cn=localhost`, musí se tato pověření vytvořit na každém serveru, avšak až po jejich novém spuštění. Replikace provedená peer servery se nezdaří do doby, než se vytvoří objekty pověření.

9. Do každého z hlavních peer serverů přidejte ujednání o replikaci pro ostatní hlavní servery. 'První' hlavní server již tyto informace obsahuje.
10. Uveďte do klidu replikovaný podstrom. To zamezí provádění aktualizací během kopírování dat na ostatní servery.
11. Pomocí Queue management u každé fronty přeskočíte vše.
12. Exportujte data pro replikovaný podstrom z 'prvního' hlavního serveru.
13. Vybuďte podstrom.
14. Zastavte replikované servery a importujte data pro replikovaný podstrom na každou repliku a hlavní peer server. Potom restartujte servery.
15. Proveďte nastavení vlastností replikace na každé replice a hlavním peer serveru a určete, která pověření mají dodavatelé používat.

Jak vytvořit úplnou topologii s peerovou replikací

Peerová replikace je replikační topologie, v níž je několik serverů hlavními servery. Na rozdíl od prostředí s několika hlavními servery neprobíhá mezi peer servery řešení konfliktů. Servery LDAP přijímají aktualizace poskytované peer servery a aktualizují své vlastní kopie dat. Nepřihlíží se na pořadí, ve kterém se přijímají aktualizace, ani na to, zda se jednotlivé aktualizace nedostávají do rozporu.

Další hlavní servery (peer) se přidávají tak, že nejprve přidáte server jako repliku (pouze pro čtení) existujících hlavních serverů (viz část "Jak vytvořit replikovaný server" na stránce 132), inicializujete data adresáře a potom zvýšíte úroveň serveru do pozice hlavního serveru (viz část "Jak přesunout server nebo zvýšit jeho úroveň" na stránce 141).

Na začátku objekt **ibm-replicagroup** vytvořený tímto procesem dědí seznam ACL kořenového záznamu pro replikovaný podstrom. Tyto seznamy ACL by nemusely být vhodné pro řízení přístupu k informacím o replikaci v adresáři.

Má-li být operace Add subtree úspěšná, musí mít DN záznamu, který přidáváte, správné seznamy ACL, pokud nejde o příponu v serveru.

Pro nefiltrované ACL:

- ownersource : <DN záznamu>
- ownerpropagate : TRUE

- aclsource : <DN záznamu>
- aclpropagate: TRUE

Filtrované ACL:

- ownersource : <DN záznamu>
- ownerpropagate : TRUE
- ibm-filteraclinherit : FALSE
- ibm-filteraclentry : <jakákoli hodnota>

Funkce **Edit ACLs** webového administračního nástroje se používá k nastavování seznamů ACL pro informace replikace přiřazované k nově vytvořenému replikovanému podstromu (viz část “Jak editovat seznamy přístupových práv” na stránce 143).

Replika je v pozastaveném stavu a nezahájí se žádná replikace. Po dokončení nastavování replikační topologie musíte klepnout na **Manage queues**, vybrat příslušnou repliku a klepnutím na **Suspend/resume** spustit replikaci. Podrobnější informace najdete v tématu “Jak provádět správu front” na stránce 146. Replika nyní přijímá aktualizace z hlavního serveru.

Peerová replikace se používá pouze v prostředích, kde je dobře znám vzor aktualizací adresáře. Aktualizace konkrétních objektů uvnitř adresáře musí provádět pouze jeden peer server. Účelem této zásady je zamezit takovému scénáři, kdy by jeden server vymazal nějaký objekt a následně by jiný server tento objekt modifikoval. Tento scénář představuje možnost, že peer server obdrží příkaz výmazu následovaný příkazem modifikace, což vytváří konflikt.

Chcete-li definovat topologii peer-předávací server-replika, sestávající ze dvou peer-hlavních serverů, dvou předávacích serverů a čtyř replik, musíte:

1. Mít vytvořený hlavní server a replikovaný server. Další informace najdete v tématu “Jak vytvořit topologii hlavní server-replika” na stránce 129.
2. Vytvořit dva další replikované servery pro hlavní server. Další informace najdete v tématu “Jak vytvořit replikovaný server” na stránce 132.
3. Vytvořit dvě repliky pod každým ze dvou nově vytvořených replikovaných serverů.
4. Zvýšit úroveň původní repliky na hlavní server. Další informace najdete v tématu “Jak zvýšit úroveň serveru do pozice peer serveru”.

Poznámka: Server, jehož úroveň chcete zvýšit na hlavní server, musí být koncová replika bez jakýchkoli podřízených replik.

5. Zkopírujte data z hlavního serveru na nový hlavní server a repliky. Další informace najdete v tématu “Jak kopírovat data do repliky” na stránce 133.

Jak zvýšit úroveň serveru do pozice peer serveru

Pomocí předávací topologie vytvořené podle části “Jak vytvořit topologii hlavní server-předávací server-replika” na stránce 134 je možné zvýšit úroveň serveru do pozice peer serveru. V tomto příkladě zvýšíte úroveň repliky (server3) do pozice peer serveru vůči hlavnímu serveru (server1).

1. Připojte webovou administraci k hlavnímu serveru (server1).
2. V navigační oblasti rozbalte kategorii Replication management a klepněte na **Manage topology**.
3. Vyberte podstrom, který chcete replikovat, a klepněte na **Show topology**.
4. Klepnutím na šipku vedle výběru **Replication topology** rozbalte seznam serverů.
5. Klepnutím na šipku vedle výběru **server1** rozbalte seznam serverů.
6. Klepnutím na šipku vedle výběru **server2** rozbalte seznam serverů.
7. Klepněte na **server1** a klepněte na **Add replica**. Vytvořte server4. Další informace najdete v tématu “Jak vytvořit replikovaný server” na stránce 132. Stejným postupem vytvořte server5. Úlohy serverů jsou ve webovém nástroji administrace znázorňovány ikonami. Vaše topologie je nyní tato:
 - server1 (hlavní)

- server2 (předávací)
 - server3 (replika)
 - server4 (replika)
 - server5 (replika)
8. Klepnutím na **server2** a potom na **Add replica** vytvořte server6.
 9. Klepnutím na **server4** a potom na **Add replica** vytvořte server7. Stejným postupem vytvořte server8. Vaše topologie je nyní tato:
 - server1 (hlavní)
 - server2 (předávací)
 - server3 (replika)
 - server6 (replika)
 - server4 (předávací)
 - server7 (replika)
 - server8 (replika)
 - server5 (replika)
 10. Vyberte **server5** a klepněte na **Move**.

Poznámka: Server, který chcete přesunout, musí být koncová replika bez jakýchkoli podrízených replik.

11. Výběrem **Replication topology** zvýšíte úroveň repliky na hlavní server. Klepněte na **Move**.
12. Zobrazí se **Create additional supplier agreements panel**. Peerová replikace vyžaduje, aby každý hlavní server byl dodavatelem i odběratelem pro každý z ostatních hlavních serverů v topologii a pro každou z replik první úrovně, server2 a server4. Server5 již je odběratelem serveru "server1", nyní se musí stát dodavatelem pro server1, server2 a server4. Zkontrolujte, zda jsou zaškrtnuta políčka dodavatelského ujednání pro:

Tabulka 5.

	Dodavatel	Odběratel
✓	server5	server1
✓	server5	server2
✓	server5	server4

Klepněte na **Continue**.

Poznámka: V některých případech se zobrazí dialogové okno Select credentials s dotazem na pověření, které je uloženo v jiném místě než cn=replication,cn=localhost. V takových situacích musíte poskytnout objekt pověření, který je uložen v jiném místě než cn=replication,cn=localhost. Pověření, které má podstrom používat, vyberte z existujících sad pověření nebo vytvořte nová pověření. Další informace najdete v tématu "Jak vytvořit pověření" na stránce 130

13. Klepněte na **OK**. Vaše topologie je nyní tato:
 - server1 (hlavní)
 - server2 (předávací)
 - server3 (replika)
 - server6 (replika)
 - server4 (předávací)
 - server7 (replika)
 - server8 (replika)
 - server5 (hlavní)
 - server5 (hlavní)

- server1 (hlavní)
- server2 (předávací)
- server4 (předávací)

14. Zkopírujte data ze serveru "server1" na všechny servery. Informace o tom, jak postupovat, najdete v tématu "Jak kopírovat data do repliky" na stránce 133.

Jak nastavit topologii brány

Dříve než budete nastavovat topologii replikace, udělejte si záložní kopii originálního souboru `ibmslapd.conf`. Pokud později nastanou při replikaci potíže, budete moci pomocí této záložní kopie obnovit původní konfiguraci.

Chcete-li nastavit bránu využívající úplné topologie s peer replikací z procedury v tématu "Jak zvýšit úroveň serveru do pozice peer serveru" na stránce 137, musíte provést tyto kroky:

- Přeměnit existující peer server (peer 1) na server brány a vytvořit replikační uzel 1.
- Vytvořit nový server brány pro replikační uzel 2 a ujednání se serverem peer 1.
- Vytvořit topologii pro replikační uzel 2 (v tomto příkladu není ilustrováno).
- Zkopírovat data z hlavního serveru na všechny stroje v topologii.

Převedení existujícího peer serveru na server brány

1. Pomocí webového administračního nástroje se přihlaste na hlavní server (server1).
2. V navigační oblasti rozbalte kategorii **Replication management** a klepněte na **Manage topology**.
3. Vyberte podstrom, který chcete replikovat, a klepněte na **Show topology**.
4. Klepnutím na šipku vedle výběru **Replication topology** rozbalte seznam serverů.
5. Chcete-li převést existující server na server brány, vyberte **server1** nebo jeho peer **server5**. V tomto příkladě použijeme **server1**.
6. Klepněte na **Edit server**.
7. Ověřte, že je zaškrtnuto **Server is a master**, a pak vyberte **Server is a gateway**.
8. Klepněte na **OK**.

Poznámka: Pokud server, který chcete používat jako bránu, není hlavní server, musí to být koncová replika, bez jakýchkoliv podřízených replik, kterou nejprve převeďte na vyšší úroveň hlavního serveru a pak označíte jako bránu.

Vytvoření serveru brány a zkopírování dat z hlavního serveru na všechny stroje v topologii

1. Vyberte **server1** a klepněte na **Add replica**.
2. Vytvořte novou repliku **server9**. V tématu "Jak vytvořit replikovaný server" na stránce 132 najdete informace o tvorbě replik, přidávání pověření a informací o dodavatelích.
3. Vyberte **server9** a klepněte na **Move**.
4. Výběrem **Replication topology** zvýšíte úroveň repliky na hlavní server. Klepněte na **Move**.
5. Zobrazí se panel **Create additional supplier agreements**. Na tomto panelu zkontrolujte, zda jsou zaškrtnuta políčka dodavatelského ujednání pouze pro server1.

	Dodavatel	Odběratel
✓	server9	server1
	server9	server2
	server9	server4
	server9	server5

Klepněte na **Continue**.

- l **Poznámka:** V některých případech se zobrazí dialogové okno **Select credentials** s dotazem na pověření, které
l je uloženo v jiném místě než `cn=replication,cn=localhost`. V takových situacích musíte poskytnout
l objekt pověření, který je uložen v jiném místě než `cn=replication,cn=localhost`. Vyberte pověření,
l které má podstrom používat, z existujících sad pověření, nebo vytvořte nová pověření. Další
l informace najdete v tématu “Jak vytvořit pověření” na stránce 130.
- l 6. Klepněte na **OK**.
 - l 7. Vyberte **server9** a klepněte na **Edit server**.
 - l 8. Ověřte, že je zaškrtnuto **Server is a master**, a pak vyberte **Server is a gateway**.
 - l 9. Klepněte na **OK**. Úlohy serverů jsou ve webovém nástroji administrace znázorňovány ikonami. Vaše topologie je
l nyní tato:
 - l • server1 (hlavní-brána pro replikační uzel 1)
 - l – server2 (předávací)
 - l - server3 (replika)
 - l - server6 (replika)
 - l – server4 (předávací)
 - l - server7 (replika)
 - l - server8 (replika)
 - l – server5 (hlavní)
 - l – server9 (hlavní-brána pro replikační uzel 2)
 - l • server5 (hlavní)
 - l – server1 (hlavní)
 - l – server2 (předávací)
 - l – server4 (předávací)
 - l • server9 (hlavní-brána)
 - l – server1 (hlavní-brána)
 - l 10. Přidejte k **server9** replikované servery a vytvořte topologii pro replikační uzel 2.
 - l 11. Opakováním tohoto postupu vytvořte další replikační uzly. Nezapomeňte, že je možno vytvořit vždy pouze jeden
l server brány na replikační uzel.
 - l 12. Po dokončení vytvoření topologie zkopírujte data ze serveru server1 na všechny nové servery ve všech
l replikačních uzlech a přidejte do všech nových serverů informace o dodavateli. Informace o tom jak postupovat
l najdete v tématech “Jak kopírovat data do repliky” na stránce 133 a “Jak přidávat informace dodavatele na
l repliku” na stránce 133.

Jak provádět správu topologií

Topologie jsou specifické pro replikované podstromy.

- “Jak prohlížet topologii” na stránce 141
- “Jak přidat repliku” na stránce 141
- “Jak editovat ujednání” na stránce 141
- “Jak přesunout server nebo zvýšit jeho úroveň” na stránce 141
- “Jak snížit úroveň hlavního serveru” na stránce 142
- “Jak replikovat podstrom” na stránce 142
- “Jak editovat podstrom” na stránce 142
- “Jak odstranit podstrom” na stránce 142
- “Jak uvést podstrom do klidu” na stránce 143
- “Jak editovat seznamy přístupových práv” na stránce 143

Jak prohlížet topologii

Poznámka: K tomu, aby bylo možné tuto úlohu uskutečnit, musí být server spuštěn.

V navigační oblasti rozbalte kategorii **Replication management** a klepněte na **Manage topology**.

1. Vyberte podstrom, který chcete prohlížet, a klepněte na **Show topology**.

Topologie je zobrazena v seznamu Replication topology. Rozbalte topologie klepnutím na modré trojúhelníky. Z tohoto seznamu je možné:

- Přidat repliku.
- Editovat informace o existující replice.
- Přejít na jiný dodavatelský server pro příslušnou repliku nebo zvýšit úroveň repliky na úroveň hlavního serveru.
- Vymazat repliku.

Jak přidat repliku

Další informace najdete v tématu “Jak vytvořit replikovaný server” na stránce 132.

Jak editovat ujednání

Produkt umožňuje změnit tyto informace pro repliku:

Na kartě **Server** můžete pouze:

- měnit jméno hostitele
- měnit port
- aktivovat SSL
- Popis

Na kartě **Additional** můžete:

- Měnit pověření - viz část “Jak vytvořit pověření” na stránce 130.
- Měnit časové plány replikací - viz část “Jak vytvářet časové plány replikací” na stránce 144.
- Měnit schopnosti replikované na odběratelskou repliku. V seznamu schopností dodavatele můžete zrušit označení jakýchkoli schopností, které nechcete replikovat pro zákazníka.
- Po dokončení klepněte na **OK**.

Jak přesunout server nebo zvýšit jeho úroveň

1. Vyberte požadovaný server a klepněte na **Move**.
2. Úroveň repliky můžete zvýšit na úroveň hlavního serveru výběrem serveru, na který chcete přesunout repliku nebo výběrem **Replication topology**. Klepněte na **Move**.
3. V některých případech se zobrazí dialogové okno Select credentials s dotazem na pověření, které je uloženo v jiném místě než cn=replication,cn=localhost. V takových situacích musíte poskytnout objekt pověření, který je uložen v jiném místě než cn=replication,cn=localhost. Pověření, které má podstrom používat, vyberte z existujících sad pověření nebo vytvořte nová pověření. Další informace najdete v tématu “Jak vytvořit pověření” na stránce 130.
4. Zobrazí se **Create additional supplier agreements**. Vyberte dodavatelská ujednání vhodná pro úlohu serveru. Jestliže je například úroveň replikačního serveru zvýšena na úroveň peer serveru, musíte zvolit tvorbu dodavatelského ujednání se všemi ostatními servery a jejich replikami první úrovně. Tato ujednání umožňují serveru se zvýšenou úrovní působit jako dodavatel pro ostatní servery a jejich repliky. Stávající dodavatelská ujednání z ostatních serverů vůči serveru s nově zvýšenou úrovní jsou stále platná a není nutné je znovu vytvářet.
5. Klepněte na **OK**.

Změna stromu topologie odráží přesun serveru.

Další informace najdete v tématu “Jak vytvořit úplnou topologii s peerovou replikací” na stránce 136.

Jak snížit úroveň hlavního serveru

Změnit úlohu serveru z hlavního serveru na repliku můžete takto:

1. Připojte webový nástroj administrace k serveru, jehož úroveň chcete snížit.
2. Klepněte na **Manage topology**.
3. Vyberte podstrom a klepněte na **Show topology**.
4. Vymažte všechna ujednání pro server, jehož úroveň chcete snížit.
5. Vyberte server, jehož úroveň snižujete, a klepněte na **Move**.
6. Vyberte server, pod nímž chcete umístit server se sníženou úrovní, a klepněte na **Move**.
7. Stejným způsobem jako u nové repliky vytvořte nová dodavatelská ujednání mezi serverem se sníženou úrovní a jeho dodavatelem. Pokyny k tomu najdete v tématu “Jak vytvořit replikovaný server” na stránce 132.

Jak replikovat podstrom

Poznámka: K tomu, aby bylo možné tuto úlohu uskutečnit, musí být server spuštěn.

V navigační oblasti rozbalte kategorii **Replication management** a klepněte na **Manage topology**.

- Klepněte na **Add subtree**.
- Zadejte DN podstromu, který chcete replikovat, případně klepnutím na **Browse** rozbalte záznamy a vyberte záznam, který se má stát kořenem podstromu.
- Zadejte URL odkazu hlavního serveru. Ten musí být uveden ve tvaru URL pro LDAP, například:
`ldap://<myservername>.<mylocation>.<mycompany>.com`
- Klepněte na **OK**.
- Nový server se zobrazuje v dialogovém okně Manage topology pod záhlavím **Replicated subtrees**.

Jak editovat podstrom

Tato volba se používá ke změně URL hlavního serveru, na který tento podstrom a jeho repliky posílají aktualizace. To je nutné učinit tehdy, když měníte číslo portu či hostitelské jméno hlavního serveru nebo když měníte hlavní server na jiný server.

1. Vyberte podstrom, který chcete editovat.
2. Klepněte na **Edit subtree**.
3. Zadejte URL odkazu hlavního serveru. Ten musí být uveden ve tvaru URL pro LDAP, například:
`ldap://<mynewservername>.<mylocation>.<mycompany>.com`

V závislosti na úloze, kterou bude server plnit na tomto podstromu (zda bude působit jako hlavní server, replika nebo předávací server), se na panelu objeví různá označení a tlačítka.

- Když je úlohou podstromu replika, zobrazí se označení znázorňující, že server působí jako replika nebo předávací server, spolu s tlačítkem **Make server a master**. Po klepnutí na toto tlačítko se server, ke kterému je webový nástroj administrace připojen, stane hlavním serverem.
- Když je podstrom pomocí přidání pomocné třídy konfigurován pouze pro replikace (není určena předvolená skupina a podzáznam), zobrazí se označení **This subtree is not replicated** spolu s tlačítkem **Replicate subtree**. Po klepnutí na toto tlačítko je doplněna předvolená skupina a podzáznam, aby se server, ke kterému je webový nástroj administrace připojen, stal hlavním serverem.
- Pokud se nenajdou žádné podzáznamy pro hlavní server, zobrazí se označení **No master server is defined for this subtree** spolu s tlačítkem s titulkem **Make server a master**. Po klepnutí na toto tlačítko je doplněn takový chybějící podzáznam, aby se server, ke kterému je webový nástroj administrace připojen, stal hlavním serverem.

Jak odstranit podstrom

1. Vyberte podstrom, který chcete odstranit.
2. Klepněte na **Delete subtree**.
3. Když budete vyzváni k potvrzení vymazání, klepněte na **OK**.

Podstrom je odstraněn ze seznamu **Replicated subtree**.

Poznámka: Tato operace je úspěšná pouze tehdy, když je záznam `ibm-replicaGroup=default` prázdný.

Jak uvést podstrom do klidu

Tato funkce je užitečná v případě, že chcete vykonávat údržbu nebo provádět změny topologie. Uvedení do klidu minimalizuje počet aktualizací, které mohou být na serveru provedeny. Server uvedený do klidu nepřijímá klientské požadavky. Přijímá požadavky pouze od administrátora používajícího řízení administrace serveru.

Tato funkce má booleovskou hodnotu.

1. Podstrom uvedete do klidu klepnutím na **Quiesce/Unquiesce**.
2. Když budete vyzváni k potvrzení akce, klepněte na **OK**.
3. Klepnutím na **Quiesce/Unquiesce** podstrom vybudíte (zrušíte uvedení do klidu).
4. Když budete vyzváni k potvrzení akce, klepněte na **OK**.

Jak editovat seznamy přístupových práv

Informace o replikaci (podzáznamy replikace, ujednání o replikaci, časové plány, eventuálně pověření) jsou uloženy pod speciálním objektem **ibm-replicagroup=default**. Objekt `ibm-replicagroup` je umístěn bezprostředně pod kořenovým záznamem replikovaného podstromu. Standardně tento podstrom dědí seznam ACL od kořenového záznamu replikovaného podstromu. Tento seznam ACL nemusí být vhodný pro řízení přístupu k informacím replikace.

Povinná oprávnění:

- Řízení replikace - musíte mít přístup k zápisu do objektu `ibm-replicagroup=default` (nebo být vlastník/administrátor).
- Replikace kaskádového řízení - musíte mít přístup k zápisu do objektu `ibm-replicagroup=default` (nebo být vlastník/administrátor).
- Fronta řízení - musíte mít přístup k ujednání o replikaci.

Informace o prohlížení vlastností seznamů ACL pomocí webového administračního nástroje a o práci s těmito seznamy najdete v tématu “Jak provádět správu seznamů přístupových práv (ACL)” na stránce 181.

Další informace najdete v tématu “Seznamy přístupových práv” na stránce 55.

Jak měnit vlastnosti replikace

V navigační oblasti rozbalte kategorii **Replication management** a klepněte na **Manage replication properties**. K tomu, abyste mohli měnit nastavení na panelu **Manage replication properties**, musíte se do webového administračního nástroje přihlásit jako projektovaný uživatel se zvláštními oprávněními `*ALLOBJ` a `*IOSYSCFG`.

Na tomto panelu můžete:

- Měnit maximální počet nevyřízených změn, které se mají vracet z dotazů na stav replikace. Předvolená hodnota je 200.
- Přidávat, editovat nebo mazat informace dodavatele.

Poznámka: DN dodavatele může odpovídat DN uživatelského profilu projektovaného uživatele i5/OS. Uživatelský profil projektovaného uživatele i5/OS nesmí mít oprávnění k administraci LDAP. Uživatel nemůže být uživatelem se zvláštními oprávněními `*ALLOBJ` a `*IOSYSCFG` a nemůže mu být uděleno oprávnění k administraci prostřednictvím aplikačního ID administrátora serveru adresářů.

Další informace najdete v těchto částech:

- “Jak přidávat informace dodavatele” na stránce 144
- “Jak editovat informace dodavatele” na stránce 144
- “Jak odstranit informace dodavatele” na stránce 144

Jak přidávat informace dodavatele

1. Klepněte na tlačítko **Add**.
2. Z rozbalovacího menu vyberte dodavatele nebo zadejte jméno replikovaného podstromu, který chcete přidat jako dodavatele.
3. Zadejte připojovací DN replikace pro příslušná pověření.

Poznámka: Použit můžete kteroukoli z těchto dvou voleb, podle situace.

- Nastavte připojovací DN (a heslo) replikace a předvolený odkaz pro všechny podstromy replikované na server s využitím 'předvolených pověření a odkazu'. To se může využít v případě, že se všechny podstromy replikují ze stejného dodavatele.
 - Nezávisle pro každý replikovaný podstrom nastavte připojovací DN a heslo replikace doplněním informací dodavatele pro každý podstrom. To se může využít v případě, že má každý podstrom jiného dodavatele (tzn. jiný hlavní server pro každý podstrom).
4. V závislosti na typu pověření zadejte a potvrďte heslo pověření (to jste si dříve poznamenali pro budoucí použití).
 - **Jednoduché připojení** - Zadejte DN a heslo.
 - **Kerberos** - zadejte nepravé DN ve tvaru 'ibm-kn=LDAP-service-name@realm' bez hesla.
 - **SSL s připojením EXTERNAL** - Zadejte DN subjektu pro certifikát, heslo se nezadá.

Další informace najdete v tématu "Jak vytvořit pověření" na stránce 130.

5. Klepněte na **OK**.

Podstrom dodavatele je přidán do seznamu informací dodavatele.

Jak editovat informace dodavatele

1. Vyberte podstrom dodavatele, který chcete editovat.
2. Klepněte na **Edit**.
3. Pokud editujete **Předvolená pověření a odkaz**, které se používají pro tvorbu záznamu cn=Master Server pod cn=configuration, v poli Default supplier's LDAP URL zadejte URL serveru, ze kterého si přeje klient přijímat aktualizace repliky. Tento odkaz musí být platný URL pro LDAP (ldap://). Jinak přejděte k bodu 4.
4. Zadejte připojovací DN replikace pro nová pověření, která chcete použít.
5. Zadejte a potvrďte heslo pro pověření.
6. Klepněte na **OK**.

Jak odstranit informace dodavatele

1. Vyberte podstrom dodavatele, který chcete odstranit.
2. Klepněte na **Delete**.
3. Když budete vyzváni k potvrzení vymazání, klepněte na **OK**.

Podstrom je odstraněn ze seznamu informací dodavatele.

Jak vytvářet časové plány replikací

Volitelně můžete definovat časové plány replikací a tak naplánovat provedení replikací na určité časy nebo naopak provádění replikací během určitých časů zakázat. Pokud nepoužíváte časový plán, server provede replikace, kdykoli dojde ke změně. To je rovnocenné časovému plánu, ve kterém je určena okamžitá replikace počínající každý den ve 12:00 (v poledne).

V navigační oblasti rozbalte kategorii **Replication management** a klepněte na **Manage schedules**.

Na kartě **Weekly schedule** vyberte podstrom, pro který chcete vytvořit časový plán, a klepněte na **Show schedules**. Pokud existují nějaké časové plány, budou zobrazeny v okénku **Weekly schedules**. Nový časový plán vytvoříte nebo přidáte takto:

1. Klepněte na tlačítko **Add**.
2. Zadejte jméno pro časový plán, například **schedule1**.
3. Pro každý den od neděle do soboty je denní časový plán uveden jako **None**. To znamená, že nejsou naplánovány žádné události aktualizace replikace. Poslední replikační událost, pokud vůbec existovala, je stále v platnosti. Protože zde jde o novou repliku, žádné předchozí replikační události se neuskutečnily, proto je předvolenou hodnotou časového plánu okamžitá replikace.
4. Nyní můžete vybrat den a klepnutím na **Add a daily schedule** pro něj vytvořit denní časový plán replikací. Pokud vytvoříte denní časový plán, stane se předvoleným časovým plánem pro každý den týdne. Máte tyto možnosti:
 - Tento denní časový plán můžete ponechat jako předvolený pro každý den nebo vybrat určitý den a změnit časový plán na none (žádný). Nezapomínejte, že pro den, který nemá naplánované žádné replikační události, je stále v platnosti poslední replikační událost, ke které došlo.
 - Výběrem dne a klepnutím na **Edit a daily schedule** modifikujete denní časový plán. Nezapomínejte na to, že změny denního časového plánu ovlivňují všechny dny využívající tento časový plán, nikoli pouze den, který jste vybrali.
 - Výběrem dne a klepnutím na **Add a daily schedule** vytvoříte další denní časový plán. Po svém vytvoření se tento časový plán přidá do rozbalovacího menu **Daily schedule**. Chcete-li tento časový plán používat, musíte jej vybrat pro každý den, kdy má být v platnosti.

Více informací o nastavování denních časových plánů najdete v tématu “Jak vytvořit denní časový plán”.

5. Po dokončení klepněte na **OK**.

Jak vytvořit denní časový plán

V navigační oblasti rozbalte kategorii **Replication management** a klepněte na **Manage schedules**.

Na kartě **Daily schedule** vyberte podstrom, pro který chcete vytvořit časový plán, a klepněte na **Show schedules**. Pokud existují nějaké časové plány, budou zobrazeny v okénku **Daily schedules**. Nový časový plán vytvoříte nebo přidáte takto:

1. Klepněte na tlačítko **Add**.
2. Zadejte jméno pro časový plán, například **monday1**.
3. Vyberte nastavení časového pásma, buď UTC, nebo místní.
4. Z rozbalovacího menu vyberte typ replikace:

Immediate

Provádí všechny nevyřízené aktualizace záznamů od poslední replikační události a potom aktualizuje záznamy nepřetržitě do té doby, než je dosaženo další naplánované události aktualizace.

Once Provede všechny aktualizace nevyřízené před časem spuštění. Jakékoli aktualizace provedené po času spuštění čekají do doby další naplánované replikační události.

5. Vyberte čas spuštění (v lokálním čase serveru) pro replikační události.
6. Klepněte na tlačítko **Add**. Zobrazí se typ a čas replikační události.
7. Časový plán upravte přidáním nebo odstraněním události. Seznam událostí se aktualizuje v chronologickém pořadí.
8. Po dokončení klepněte na **OK**.

Například:

Tabulka 6.

Typ replikace	Čas spuštění
Immediate	00:00 (půlnoc)
Once	10:00 dopoledne
Once	14:00 odpoledne
Immediate	16:00 odpoledne

Tabulka 6. (pokračování)

Typ replikace	Čas spuštění
Once	20:00 večer

V tomto časovém plánu se první replikační událost uskuteční o půlnoci a aktualizuje všechny nevyřízené změny před tímto časem. Aktualizace replikace se stále provádějí okamžitě po výskytu změny do 10:00 hodin dopoledne. Aktualizace provedené mezi 10:00 dopoledne a 14:00 odpoledne čekají na svou replikaci do 14:00 dopoledne. Všechny aktualizace provedené mezi 14:00 odpoledne a 16:00 odpoledne čekají na replikační událost naplánovanou na 16:00 odpoledne, potom se aktualizace replikace stále provádějí do další naplánované replikační události ve 20:00 večer. Jakékoli aktualizace provedené po 20:00 večer čekají do doby další naplánované replikační události.

Poznámka: Jsou-li replikační události naplánovány příliš blízko sebe, replikační událost může být promeškána, pokud stále probíhají aktualizace z předchozí události v čase příští naplánované události.

Jak provádět správu front

Tato úloha umožňuje monitorovat stav replikace pro každé ujednání o replikaci (každou frontu) používanou tímto serverem.

V navigační oblasti rozbalte kategorii **Replication management** a klepněte na **Manage queues**.

Vyberte repliku, pro kterou chcete spravovat frontu.

- V závislosti na stavu repliky můžete klepnutím na **Suspend/resume** zastavit nebo spustit replikaci.
- Klepnutím na **Force replication** provedete replikaci všech nevyřízených změn bez ohledu na dobu, na kterou je naplánována další replikace.
- Další podrobnější informace o frontách replik zobrazíte klepnutím na **Queue details**. Pomocí této volby můžete rovněž provádět správu fronty.
- Klepnutím na **Refresh** provedete aktualizaci front a vymažete zprávy serveru.

Podrobnosti o frontě

Po klepnutí na **Queue details** se zobrazí tři karty:

- Status.
- Last attempted details.
- Pending changes.

Karta **Status** zobrazuje jméno repliky, její podstrom, stav a záznam časů replikací. Z tohoto dialogového okna můžete pozastavit nebo obnovit replikace klepnutím na **Resume**. Klepnutím na **Refresh** provedete aktualizaci fronty.

Karta **Last attempted details** uvádí informace o posledním pokusu o aktualizaci. Pokud systém není schopen zavést některý záznam, stiskem **Skip blocking entry** můžete pokračovat v replikaci dalšího nevyřízeného záznamu. Klepnutím na **Refresh** provedete aktualizaci fronty.

Karta **Pending changes** zobrazuje všechny nevyřízené změny repliky. V případě, že je replikace zablokována, můžete vymazat všechny nevyřízené změny klepnutím na **Skip all**. Klepnutím na **Refresh** aktualizujete seznam nevyřízených změn tak, že zobrazuje všechny nové aktualizace, které byly zpracovány.

Poznámka: Chcete-li přeskočit blokující změny, musíte zabezpečit, aby byl odběratelský server nakonec aktualizován. Další informace najdete v tématu "ldapdiff" na stránce 213.

| Jak nastavit replikaci přes zabezpečené spojení

| Replikaci přes SSL je potřeba nastavovat postupně, abyste mohli v průběhu procesu vše ověřovat.

- | Dříve než se budete pokoušet konfigurovat replikaci přes zabezpečené spojení, měli byste provést tyto úlohy (v libovolném pořadí):
- | • Nakonfigurovat replikace přes nezabezpečené spojení.
- | • Nakonfigurovat odběratelský server, aby přijímal zabezpečená připojení přes bezpečnostní port. Ověřte, že klient může používat zabezpečené připojení k odběratelskému serveru; například pomocí obslužného programu ldapsearch. Pokud chcete, aby dodavatelský server používal k autentizaci certifikát, jako např. při externím připojení SASL přes SSL, měli byste nejprve nastavit autentizaci serveru a potom autentizaci klienta a serveru, kde "server" je odběratelský server a klient je dodavatelský server.

| **Poznámka:** Když je server nakonfigurován, aby používal autentizaci klienta a serveru, všichni klienti používající SSL musí mít klientský certifikát.

- | • Nakonfigurovat dodavatelský server, aby důvěřoval vydavateli certifikátu, který vydal certifikát odběratele.
- | 1. Ve webovém administračním nástroji klepněte na **Manage topology** v rámci kategorie **Replication management**.
- | 2. Vyberte jedno z existujících ujednání, které chcete zabezpečit.
- | 3. Vyberte **Edit agreement...** a vyberte použití SSL, abyste zajistili, že se bude používat správné číslo portu. Standardní číslo zabezpečeného portu je 636.
- | 4. Ověřte, že replikace v rámci tohoto ujednání funguje správně.

| Pokud se pokoušíte nastavit replikaci přes zabezpečené spojení pro autentizaci pouze za použití DN a hesla, pak jste to v rámci předcházejících kroků provedli. Autentizace používající klientský certifikát vyžaduje, aby dodavatelský server ve svém ujednání použil jiný objekt pověření, a dále nakonfigurování odběratelského serveru tak, aby akceptoval tento certifikát jako dodavatelský server.

| Jak spravovat vlastnosti zabezpečení

| Server adresářů obsahuje řadu mechanismů pro zajištění bezpečnosti vašich dat. Patří k nim správa hesel, šifrování pomocí SSL a TLS, autentizace Kerberos a autentizace DIGEST-MD5. Podrobnější informace o koncepcích zabezpečení najdete v tématu "Server adresářů - Zabezpečení ochrany dat" na stránce 46.

| Další informace najdete v těchto částech:

- | • "Jak spravovat hesla"
- | • "Jak aktivovat SSL a TLS (Transport Layer Security) na serveru adresářů" na stránce 151
- | • "Jak aktivovat autentizaci Kerberos na serveru adresářů" na stránce 153
- | • "Jak aktivovat autentizaci DIGEST-MD5 na serveru adresářů" na stránce 154

| Jak spravovat hesla

| Chcete-li provádět správu hesel, rozbalte v navigační oblasti webového administračního nástroje kategorii **Manage security properties** a vyberte kartu **Password policy**.

| Další informace najdete v těchto částech:

- | • "Jak nastavit vlastnosti hesel"
- | • "Rady k zásadám pro správu hesel" na stránce 149

| Jak nastavit vlastnosti hesel

| Server adresářů poskytuje mnoho voleb týkajících se hesel, pomocí kterých lze zajistit, aby přístup do adresáře měli pouze oprávnění uživatelé. Tyto volby jsou seskupeny na kartách pro zásadu pro správu hesel, zamčení hesel a ověřování platnosti hesel.

| Zásada pro správu hesel

| Chcete-li nastavit zásadu správy hesel, postupujte takto:

1. V navigační oblasti webového administračního nástroje rozbalte kategorii **Manage security properties** a vyberte kartu **Password policy**. Tento panel zobrazuje needitovatelné pole **Password attribute** obsahující jméno atributu, které používá tato zásada pro správu hesel.
2. Vyberte z rozbalovacího seznamu typ šifrování hesla:
 - None** Žádné šifrování. Hesla se ukládají ve formátu čistého textu.
 - crypt** Hesla jsou před uložením v adresáři zakódována pomocí šifrovacího algoritmu UNIX crypt.
 - SHA-1** Hesla jsou před uložením v adresáři zakódována pomocí šifrovacího algoritmu SHA-1.
3. Označte zaškrťovací okénko **Password policy enabled**, abyste aktivovali zásadu pro správu hesel.

Poznámka: Jestliže zásada pro správu hesel není aktivována, žádná další funkce na tomto nebo jiném panelu týkajícím se hesel nebude k dispozici, dokud se zaškrťovací okénko nezaktivuje. Zásada pro správu hesel je předvoleně deaktivována.
4. Označte zaškrťovací okénko **User can change password**, abyste zadali, zda uživatel může heslo měnit.
5. Označte zaškrťovací okénko **User must change password after reset**, abyste zadali, zda uživatel musí měnit heslo poté, co se přihlásil pomocí resetovaného hesla.
6. Označte zaškrťovací okénko **User must send password when changing**, abyste zadali, že uživatel po počátečním přihlášení musí zadat heslo znovu předtím, než může heslo změnit.
7. Nastavte limit pro ukončení platnosti hesla. Klepněte na tlačítko **Password Never Expires**, pokud chcete, aby heslo nemuselo být měněno v nějakém konkrétním časovém intervalu, nebo klepněte na tlačítko **Days** a zadejte časový interval ve dnech, kdy je nutno heslo resetovat.
8. Zadejte, zda má systém před ukončením platnosti hesla vydávat varování o ukončení platnosti hesla.

Pokud klepnete na tlačítko **Never warn**, uživatel nebude před ukončením platnosti předchozího hesla varován. Uživatel nebude moci přistupovat k serveru adresářů, dokud mu administrátor nevytvoří nové heslo.

Pokud klepnete na tlačítko **Days before expiration** a zadáte počet dnů (n), uživatel obdrží varovnou výzvu ke změně hesla pokaždé, když se bude přihlašovat, a to počínaje n dnů před ukončením platnosti hesla. Uživatel může stále přistupovat k adresáři, dokud platnost hesla neskončí.
9. Zadejte, kolikrát (pokud vůbec) se může uživatel přihlásit poté, co platnost jeho hesla skončila. Tato volba umožňuje uživateli přístup do adresáře s heslem, jehož platnost skončila.
10. Klepněte na **OK**.

Poznámka: Pro nastavení zásady správy hesla je možné použít rovněž obslužný program `ldapmodify` (viz “`ldapmodify` a `ldapadd`” na stránce 187).

Další informace o zásadě pro správu hesla najdete v tématu “Zásada pro správu hesel” na stránce 67.

Uzamčení hesla

1. V navigační oblasti webového administračního nástroje rozbalte kategorii **Manage security properties** a vyberte kartu **Password lockout**.

Poznámka: Pokud na serveru není aktivována zásada pro správu hesel, funkce na tomto panelu nebudou mít účinek.
2. Zadejte počet vteřin, minut, hodin nebo dnů, které musí uplynout předtím, než lze heslo změnit.
3. Zadejte, zda nesprávné přihlášení uzamče heslo.
 - Vyberte tlačítko **Passwords are never locked out**, pokud chcete povolit neomezený počet přihlašovacích pokusů. Tento výběr deaktivuje funkci uzamčení hesla.
 - Vyberte tlačítko **Attempts** a zadejte počet přihlašovacích pokusů povolených předtím, než se heslo uzamče. Tento výběr aktivuje funkci uzamčení hesla.
4. Zadejte dobu trvání uzamčení. Vyberte tlačítko **Lockouts never expire**, chcete-li zadat, že heslo musí resetovat systémový administrátor, nebo vyberte tlačítko **Seconds** a zadejte počet vteřin, než uzamčení vyprší a lze pokračovat v pokusech o přihlášení.

5. Zadejte dobu ukončení platnosti pro nesprávné přihlášení. Klepněte na tlačítko **Incorrect logins only cleared with correct password**, chcete-li zadat, že nesprávná přihlášení se vymažou z paměti pouze po úspěšném přihlášení, nebo klepněte na tlačítko **Seconds** a zadejte počet vteřin, než je neúspěšný pokus o přihlášení vymazán z paměti.

Poznámka: Tato volba funguje pouze tehdy, pokud heslo není uzamčeno.

6. Když skončíte, klepněte buď na tlačítko **Apply**, abyste změny uložili a pokračovali, nebo klepněte na tlačítko **OK**, abyste změny uložili a odešli z tohoto panelu, nebo klepněte na tlačítko **Cancel**, abyste z tohoto panelu odešli bez provedení jakýchkoliv změn.

Ověření platnosti hesla

1. V navigační oblasti webového administračního nástroje rozbalte kategorii **Manage security properties** a vyberte kartu **Password validation**.

Poznámka: Pokud na serveru není aktivována zásada pro správu hesel, funkce na tomto panelu nebudou mít účinek.

2. Nastavte, kolik dalších hesel je nutno použít, než je možno původní heslo opět použít. Zadejte počet od 0 do 30. Pokud zadáte nulu, lze heslo opětovně použít bez omezení.
3. Z rozbalovacího menu vyberte, zda se heslo kontroluje z hlediska syntaxe definované v níže uvedených vstupních polích. Můžete vybrat:

Do not check syntax

Neprovádí se žádná kontrola syntaxe.

Check syntax (except encrypted)

Kontrola syntaxe se provádí u všech nezašifrovaných hesel.

Check syntax

Kontrola syntaxe se provádí u všech hesel.

4. Zadejte číselnou hodnotu, která udává minimální délku hesla. Pokud je tato hodnota nastavena na nulu, neprovádí se žádná kontrola syntaxe.
- Zadejte číselnou hodnotu, která udává minimální počet abecedních znaků požadovaný pro heslo.
 - Zadejte číselnou hodnotu, která udává minimální počet numerických a speciálních znaků požadovaný pro heslo.

Poznámka: Součet minimálních počtů abecedních, numerických a speciálních znaků musí být roven nebo menší než počet znaků zadaný jako minimální délka hesla.

5. Zadejte maximální počet znaků, které se v hesle mohou opakovat. Tato volba omezuje, kolikrát se určitý speciální znak může v hesle objevit. Pokud je tato hodnota nastavena na nulu, počet opakovaných znaků se nekontroluje.
6. Zadejte minimální počet znaků, které se musí lišit od předchozího hesla, a počet předchozích hesel specifikovaný v poli **Minimum number of passwords before reuse**. Pokud je tato hodnota nastavena na nulu, počet odlišných znaků se nekontroluje.
7. Když skončíte, klepněte buď na tlačítko **Apply**, abyste změny uložili a pokračovali, nebo klepněte na tlačítko **OK**, abyste změny uložili a odešli z tohoto panelu, nebo klepněte na tlačítko **Cancel**, abyste z tohoto panelu odešli bez provedení jakýchkoliv změn.

Rady k zásadám pro správu hesel

Dotazy na zásadu správy hesel

Operační atributy zásady správy hesel lze použít k zobrazení stavu určitého záznamu adresáře nebo k dotazu na záznamy vyhovující zadaným kritériím. Operační atributy se při vyhledávacím požadavku vracejí pouze tehdy, pokud to klient konkrétně požaduje. Chcete-li tyto atributy používat ve vyhledávacích operacích, musíte mít oprávnění ke kritickým atributům nebo oprávnění ke konkrétně použitým atributům.

Chcete-li zobrazit všechny atributy zásady správy hesel pro daný záznam, zadejte:

```
| > ldapsearch -b "uid=user1,cn=users,o=ibm" -s base "(objectclass=*)"
|   pwdChangedTime pwdAccountLockedTime pwdExpirationWarned
|   pwdFailureTime pwdGraceUseTime pwdReset
```

| Chcete-li se dotázat na záznamy, u kterých má právě skončit platnost hesla, použijte atribut pwdChangedTime.
| Například kdybyste chtěli najít hesla, jejichž platnost končí 26. srpna 2004 a která mají zásadu ukončení platnosti hesla
| 186 dnů, dotážete se na záznamy, jejichž heslo bylo změněno nejméně před 186 dny (22. února 2004).

```
| > ldapsearch -b "cn=users,o=ibm" -s sub
| "(! (pwdChangedTime>20040222000000Z))" 1.1
```

| kde filtr se rovná pwdChangedTime půlnoc, 22. února 2004.

| Chcete-li se dotázat na uzamčené účty, použijte atribut pwdAccountLockedTime:

```
| > ldapsearch -b "cn=users,o=ibm" -s sub "(pwdAccountLockedTime=*)" 1.1
```

| kde "1.1" indikuje, že se vrátí pouze DN záznamů.

| Chcete-li se dotázat na účty, u kterých je nutno změnit heslo, protože bylo heslo resetováno, použijte atribut pwdReset:

```
| > ldapsearch -b "cn=users,o=ibm" -s sub "(pwdReset=TRUE)" 1.1
```

| **Jak potlačit zásadu správy hesel**

| Administrátor adresáře může potlačit normální chování zásady správy hesel u konkrétního záznamu tak, že změní
| operační atributy zásady správy hesel a použije administrační řízení serveru (volba -k obslužných programů
| příkazového řádku LDAP).

| Zabránit tomu, aby určitému účtu vypršela platnost hesla, můžete tak, že při nastavování atributu userPassword
| nastavíte atribut pwdChangedTime na datum v daleké budoucnosti. V následujícím příkladě je tato doba nastavena na
| půlnoc 1. ledna 2200.

```
| > ldapmodify -D cn=root -w ? -k
| dn: uid=wasadmin,cn=users,o=ibm
| changetype: modify
| replace: pwdChangedTime
| pwdChangedTime: 22000101000000Z
```

| Odemknout účet, který byl uzamknut kvůli nadměrnému počtu neúspěšných pokusů o přihlášení, můžete tak, že
| odstraníte atributy pwdAccountLockedTime a pwdFailureTime:

```
| > ldapmodify -D cn=root -w ? -k
| dn: uid=user1,cn=users,o=ibm
| changetype: modify
| delete: pwdAccountLockedTime
| -
| delete: pwdFailureTime
```

| Odemknout účet, který vypršel, můžete tak, že změníte atribut pwdChangedTime a odstraníte atributy
| pwdExpirationWarned a pwdGraceUseTime:

```
| > ldapmodify -D cn=root -w ? -k
| dn: uid=user1,cn=users,o=ibm
| changetype: modify
| replace: pwdChangedTime
| pwdChangedTime: 20040826000000Z
| -
| delete: pwdExpirationWarned
| -
| delete: pwdGraceUseTime
```

| Odstranit nebo nastavit stav "password must be changed" můžete tak, že nastavíte atribut pwdReset:

```

| > ldapmodify -D cn=root -w ? -k
| dn: uid=user1,cn=users,o=ibm
| changetype: modify
| delete: pwdReset
|
| > ldapmodify -D cn=root -w ? -k
| dn: uid=user2,cn=users,o=ibm
| changetype: modify
| replace: pwdReset
| pwdReset: TRUE

```

Účet lze administračně zamknout tak, že nastavíte operační atribut `ibm-pwdAccountLocked` na `TRUE`. Účet lze odemknout tak, že tento atribut nastavíte na `FALSE`. Odemknutí účtu tímto způsobem neovlivní stav účtu z hlediska jeho uzamknutí kvůli nadměrnému počtu neúspěšných přihlášení nebo ukončení platnosti hesla.

Uživatel, který nastavuje tento atribut, musí mít oprávnění k zápisu do atributu `ibm-pwdAccountLocked`, což je definováno jako přístupová třída `CRITICAL`.

```

| > ldapmodify -D uid=useradmin,cn=users,o=ibm -w ?
| dn: uid=user1,cn=users,o=ibm
| changetype: modify
| replace: ibm-pwdAccountLocked
| ibm-pwdAccountLocked: TRUE

```

Chcete-li účet odemknout:

```

| > ldapmodify -D uid=useradmin,cn=users,o=ibm -w ?
| dn: uid=user1,cn=users,o=ibm
| changetype: modify
| replace: ibm-pwdAccountLocked
| ibm-pwdAccountLocked: FALSE

```

Další tipy k zásadám pro správu hesel

Existují dvě oblasti, kde se implementace zásady správy hesel nemusí chovat podle očekávání:

1. Pokud byl pro určitý záznam nastaven atribut `pwdReset`, klient se může připojovat po neurčitou dobu za použití DN záznamu a resetovaného hesla. Pokud existuje ovladač požadavků zásady správy hesel, bude výsledkem úspěšné připojení s varováním v řízení odezvy. Pokud ale klient nezadá ovladač požadavku, zaznamená tento klient, který není informován o zásadě správy hesel, úspěšné připojení bez jakékoliv indikace, že je nutno heslo změnit. Následné operace pod tímto DN však selžou s chybou "unwilling to perform"; počáteční úspěšné připojení se může jevit zavádějící. Mohl by to být problém, pokud by připojení bylo provedeno pouze kvůli autentizaci, což je případ webových aplikací používajících adresář pro autentizaci.
2. Zásady `pwdSafeModify` a `pwdMustChange` se nemusí chovat podle očekávání v případě aplikace, která mění heslo pod identitou jinou, než je DN záznamu, pro který se heslo mění. V tomto scénáři bude nastavení atributu `pwdReset` výsledkem např. bezpečné změny hesla provedené pod identitou administrátora. Aplikace měnící heslo může použít účet administrátora a odstranit atribut `pwdReset` jak bylo popsáno výše.

Jak aktivovat SSL a TSL (Transport Layer Security) na serveru adresářů

SSL

Máte-li v systému nainstalován produkt Digital Certificate Manager, můžete k zabezpečení přístupů k serveru adresářů použít SSL (Secure Sockets Layer). Než budete aktivovat na serveru adresářů SSL, je vhodné si prostudovat téma "SSL (Secure Sockets Layer) a TLS (Transport Layer Security) u serveru adresářů" na stránce 47.

K aktivaci SSL na serveru LDAP použijte tento postup:

1. **Přiřaďte serveru adresářů certifikát.**

- a. Chcete-li provádět správu serveru adresářů prostřednictvím připojení SSL z produktu iSeries Navigator, prostudujte si uživatelskou příručku iSeries Access for Windows (instaluje se volitelně na PC při instalaci produktu iSeries Navigator. Chcete-li umožňovat připojení k serveru adresářů s použitím SSL i bez něj, můžete tento bod vynechat.
- b. Spusťte produkt IBM Digital Certificate Manager. Další informace najdete v tématu Start Digital Certificate Manager v tématu Digital Certificate Manager.
- c. Pokud potřebujete získat či vytvořit certifikáty nebo jinak nastavit či změnit svůj certifikační systém, učíte tak nyní. Informace o nastavování certifikačního systému najdete v tématu o produktu Správce digitálního certifikátu. Existují dvě serverové aplikace a jedna aplikace typu klient přidružené k serveru adresářů. Tyto aplikace jsou:

Aplikace serveru adresářů

Tato aplikace serveru adresářů je server samotný.

Publikační aplikace serveru adresářů

Publikační aplikace serveru adresářů určuje certifikát používaný funkcí publikování.

Aplikace typu klient serveru adresářů

Aplikace typu klient serveru adresářů určuje předvolený certifikát používaný aplikacemi využívajícími rozhraní ILE API klienta LDAP.

- d. Klepněte na tlačítko **Select a Certificate Store**.
- e. Vyberte ***SYSTEM**. Klepněte na **Continue**.
- f. Zadejte odpovídající heslo pro paměť certifikátů ***SYSTEM**. Klepněte na **Continue**.
- g. Po novém zavedení levého navigačního menu rozbalte **Manage Applications**.
- h. Klepněte na **Update Certificate Assignment**.
- i. Na další obrazovce vyberte aplikaci **Server**. Klepněte na **Continue**.
- j. Vyberte **Directory Server server**.
- k. Klepnutím na **Update Certificate Assignment** přiřadíte k serveru adresářů certifikát, který se bude používat k prokazování jeho identity pro klienty iSeries Access for Windows.

Poznámka: Jestliže si zvolíte takový certifikát od vydavatele certifikátu (CA), který není obsažen v databázi klíčů vašeho klienta iSeries Access for Windows, budete jej muset přidat, aby mohl používat SSL. To budete muset učinit ještě před zahájením výběru certifikátu.

- l. Ze seznamu vyberte certifikát, který chcete přiřadit k serveru.
- m. Klepněte na **Assign New Certificate**.
- n. DCM se znovu zavede se zobrazenou stránkou **Update Certificate Assignment** a s výzvou k potvrzení. Po dokončení nastavování certifikátů pro server adresářů klepněte na **Done**.

2. Přiřaďte certifikát pro publikování serveru adresářů (volitelný krok). Pokud chcete rovněž aktivovat publikování ze systému do serveru adresářů prostřednictvím připojení SSL, bude možná nutné také přiřadit certifikát k publikování serveru adresářů. Ten určuje předvolený certifikát a důvěryhodné vydavatele certifikátů (CA) pro takové aplikace využívající rozhraní ILE API LDAP, které neuvádějí svůj vlastní aplikační ID ani alternativní databázi klíčů.

- a. Spusťte produkt IBM Digital Certificate Manager.
- b. Klepněte na tlačítko **Select a Certificate Store**.
- c. Vyberte ***SYSTEM**. Klepněte na **Continue**.
- d. Zadejte odpovídající heslo pro paměť certifikátů ***SYSTEM**. Klepněte na **Continue**.
- e. Po novém zavedení levého navigačního menu rozbalte **Manage Applications**.
- f. Klepněte na **Update Certificate Assignment**.
- g. Na další obrazovce vyberte aplikaci **Client**. Klepněte na **Continue**.
- h. Vyberte **Directory Server publishing**.
- i. Klepnutím na **Update Certificate Assignment** přiřadíte k publikování serveru adresářů certifikát, který bude prokazovat jeho identitu.

- l j. Ze seznamu vyberte certifikát, který chcete přiřadit k serveru.
- l k. Klepněte na **Assign new certificate**.
- l l. DCM se znovu zavede se zobrazenou stránkou **Update Certificate Assignment** a s výzvou k potvrzení.

Poznámka: U těchto kroků se předpokládá, že již publikujete informace do serveru adresářů s připojením nevyužívajícím SSL. Úplné informace o nastavování publikování najdete v tématu “Publikování informací na server adresářů” na stránce 92.

- l 3. **Přiřaďte certifikát pro klienta serveru adresářů** (volitelný krok). Pokud máte jiné aplikace, které používají připojení SSL k serveru adresářů, musíte rovněž přiřadit certifikát ke klientu serveru adresářů.
 - l a. Spusťte produkt IBM Digital Certificate Manager.
 - l b. Klepněte na tlačítko **Select a Certificate Store**.
 - l c. Vyberte ***SYSTEM**. Klepněte na **Continue**.
 - l d. Zadejte odpovídající heslo pro paměť certifikátů ***SYSTEM**. Klepněte na **Continue**.
 - l e. Po novém zavedení levého navigačního menu rozbalte **Manage Applications**.
 - l f. Klepněte na **Update Certificate Assignment**.
 - l g. Na další obrazovce vyberte aplikaci **Client**. Klepněte na **Continue**.
 - l h. Vyberte **Directory Server client**.
 - l i. Klepnutím na **Update Certificate Assignment** přiřadíte ke klientu serveru adresářů certifikát, který bude prokazovat jeho identitu.
 - l j. Ze seznamu vyberte certifikát, který chcete přiřadit k serveru.
 - l k. Klepněte na **Assign New Certificate**.
 - l l. DCM se znovu zavede se zobrazenou stránkou **Update Certificate Assignment** a s výzvou k potvrzení.

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

l TLS

l Chcete-li používat SSL nebo TSL, musíte je povolit v prostředí produktu iSeries Navigator.

- l 1. V prostředí produktu iSeries Navigator rozbalte položku **Sítě**.
- l 2. Rozbalte položku **Servery**.
- l 3. Pravým tlačítkem myši klepněte na **Adresář** a vyberte volbu **Vlastnosti**.
- l 4. Na kartě **Sítě** zaškrtněte zaškrtačkové okénko vedle volby **Zabezpečit**.

l Můžete také zadat číslo portu, který chcete zabezpečit. Klepnutím na zaškrtačkové okénko **Zabezpečit** indikujete, že aplikace může spustit připojení SSL nebo TSL přes zabezpečený port. Je to také indikace toho, že aplikace může vydat operaci StartTLS a tak povolit spojení TSL přes nezabezpečený port. Anebo může být TSL vyvoláno použitím volby -Y z obslužného programu příkazového řádku klienta. Používá-li se příkazový řádek, musí se atribut `ibm-slapdSecurity` rovnat buď TLS nebo SSLTLS.

l Další informace o SSL a TLS najdete v tématu “SSL (Secure Sockets Layer) a TLS (Transport Layer Security) u serveru adresářů” na stránce 47.

l Jak aktivovat autentizaci Kerberos na serveru adresářů

l Máte-li v systému nakonfigurovány služby síťové autentizace, můžete nastavit server adresářů pro používání autentizace Kerberos. Autentizace Kerberos se vztahuje na uživatele i na administrátora. Než budete aktivovat na serveru adresářů Kerberos, je vhodné si prostudovat základní informace o použití autentizace Kerberos s produktem Server adresářů.

l K aktivaci autentizace Kerberos použijte tento postup:

- l 1. V prostředí produktu iSeries Navigator rozbalte položku **Sítě**.
- l 2. Rozbalte položku **Servery**.

- | 3. Klepněte na **TCP/IP**.
- | 4. Pravým tlačítkem myši klepněte na **Server adresářů IBM** a vyberte volbu **Vlastnosti**.
- | 5. Klepněte na kartu **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.

| **Jak aktivovat autentizaci DIGEST-MD5 na serveru adresářů**

| DIGEST-MD5 je autentizační mechanismus na bázi protokolu SASL. Když klient použije volbu DIGEST-MD5, heslo se nepřenáší jako čistý text a protokol zabrání útokům na bázi přehrávání. Ke konfiguraci autentizace DIGEST-MD5 se používá webový administrační nástroj.

- | 1. Pod položkou **Server administration** rozbalte v prostředí webového administračního nástroje kategorii **Manage security properties** a vyberte kartu **DIGEST-MD5**.

| **Poznámka:** Chcete-li měnit konfigurační nastavení serveru pomocí úloh v kategorii Server administration, musíte se na server autentizovat jako uživatelský profil i5/OS, který má speciální oprávnění *ALLOBJ a IOSYSCFG. Toho lze docílit tak, že se budete autentizovat jako projektovaný uživatel s heslem pro tento profil. Chcete-li se přihlásit z webového administračního nástroje jako projektovaný uživatel, zadejte uživatelské jméno ve formě `os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM`, kde řetězce MYUSERNAME a MYSYSTEM.COM nahradíte vašim jménem uživatelského profilu a konfigurovanou systémovou projektovanou příponou.

- | 2. Pod položkou **Server realm** použijte předvolené nastavení **Default**, což je plně kvalifikované hostitelské jméno serveru, nebo můžete klepnout na **Realm** a napsat jméno sféry, jakožto kterou chcete server konfigurovat. Toto jméno sféry používá klient, aby určil, které uživatelské jméno a heslo použít. Když se používá replikace, budete chtít mít všechny servery nakonfigurované se stejnou sférou.
- | 3. U atributu **Username** použijte předvybrané nastavení **Default**, což je uid, nebo může klepnout na **Attribute** a zapsat jméno atributu, který má server používat při jedinečné identifikaci záznamu uživatele během připojení DIGEST-MD5 SASL.
- | 4. Pokud jste přihlášení jako administrátor adresáře, u položky **Administrator username** zapište uživatelské jméno administrátora. Toto pole nemohou členové administrační skupiny editovat. Pokud jméno uživatele zadané v připojení DIGEST-MD5 SASL odpovídá tomuto řetězci, uživatel je administrátorem.

| **Poznámka:** Uživatelské jméno administrátora je citlivé na velikost písmen.

- | 5. Po dokončení klepněte na **OK**.

Jak provádět správu schématu

Další informace o schématu najdete v tématu “Schéma” na stránce 15.

Správu schématu je možné provádět pomocí webového administračního nástroje nebo aplikace LDAP, jako např. ldapmodify, v kombinaci se soubory LDIF. Při prvním definování nových tříd objektů nebo atributů bude vhodnější použít webový administrační nástroj. Pokud potřebujete kopírovat nové schéma na jiné servery (například jako součást produktu nebo nástroje, který nasazujete), může být vhodnější obslužný program ldapmodify, více informací najdete v tématu “Jak kopírovat schéma na jiné servery” na stránce 164.

Další informace najdete v těchto částech:

- “Jak prohlížet třídy objektů” na stránce 155
- “Jak přidat třídu objektu” na stránce 155
- “Jak editovat třídu objektu” na stránce 156
- “Jak kopírovat třídu objektu” na stránce 157
- “Jak vymazat třídu objektu” na stránce 158
- “Jak prohlížet atributy” na stránce 159

- “Jak přidat atribut” na stránce 160
- “Jak editovat atribut” na stránce 161
- “Jak kopírovat atribut” na stránce 162
- “Jak vymazat atribut” na stránce 163

Jak prohlížet třídy objektů

Třídy objektů obsažené ve schématu můžete prohlížet buď pomocí webového administračního nástroje, což je preferovaná metoda, nebo pomocí příkazového řádku.

Webová administrace

V navigační oblasti rozbalte **Schema management** a klepněte na **Manage object classes**. Zobrazí se panel pouze pro čtení, který umožňuje prohlížet třídy objektů obsažené ve schématu a jejich charakteristiky. Třídy objektů se zobrazují v abecedním pořadí. Je možné se přesouvat o jednu stránku zpět nebo dopředu klepnutím na Previous nebo Next. Pole vedle těchto tlačítek označuje stránku, na které se právě nalzáte. K přechodu na určitou stránku můžete použít rovněž rozbalovací menu tohoto pole. První třída objektu uvedená na stránce se zobrazuje spolu s číslem této stránky, což usnadňuje nalezení třídy objektu, kterou chcete prohlížet. Například, jestliže hledáte třídu objektu **person**, rozbalíte rozbalovací menu, které přesouváte dolů, dokud nenajdete **Page 14 of 16 nsLiServer** a **Page 15 of 16 printerLPR**. Protože person je abecedně mezi nsLiServer a printerLPR, vyberete stranu 14 a klepnete na **Go**.

Zobrazit můžete i třídy objektů setříděné podle typu. Vyberte **Type** a klepněte na **Sort**. Třídy objektů se setřídí abecedně v rámci svého typu, abstraktní, pomocné a strukturální (Abstract, Auxiliary, Structural). Podobným způsobem můžete převrátit pořadí seznamu výběrem **Descending** a klepnutím na **Sort**.

Jakmile jste našli požadovanou třídu objektu, můžete prohlížet její typ, dědičnost, povinné atributy a volitelné atributy. Úplný přehled všech charakteristik můžete zobrazit rozbalením rozbalovacích menu pro dědičnost, povinné i volitelné atributy.

V panelu nástrojů na pravé straně můžete volit operace, které chcete pro třídu objektu použít, jako například:

- Add (přidat).
- Edit (editovat).
- Copy (kopírovat).
- Delete (mázat).

Po dokončení klepněte na **Close** a vrátíte se do dialogového okna **Vítejte** serveru adresářů IBM.

Příkazový řádek

Chcete-li prohlížet třídy objektů obsažené ve schématu, zadejte tento příkaz:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Jak přidat třídu objektu

Webová administrace

Pokud jste tak již neučinili, v navigační oblasti rozbalte **Schema management** a klepněte na **Manage object classes**. Novou třídu objektu vytvoříte takto:

1. Klepněte na tlačítko **Add**.

Poznámka: Toto dialogové okno zobrazíte rovněž rozbalením **Schema management** v navigační oblasti a potom klepnutím na **Add an object class**.

2. Na kartě **General properties**:

- Zadejte **Object class name** (jméno třídy objektu). To je povinné pole a obsahuje popisnou zkratku funkce třídy objektu. Například **tempEmployee** je třída objektu používaná pro sledování dočasných zaměstnanců.
- Zadejte **Description** (popis) třídy objektu, například **Třída objektu používaná pro dočasné zaměstnance**.
- Zadejte **OID** pro třídu objektu. To je povinné pole. Další informace najdete v tématu “Identifikátor objektu (OID)” na stránce 26. Pokud nemáte OID, můžete použít **Object class name** s doplňkem **-oid**. Například, jestliže je jméno třídy objektu **tempEmployee**, OID je **tempEmployee-oid**. Hodnotu tohoto pole je možné měnit.
- Z rozbalovacího seznamu vyberte **Superior object class**. Tato nadřazená třída určuje třídu objektu, z níž jsou odvozeny jiné atributy. Obvykle platí, že **Superior object class** je **top**, může to však být i jiná třída objektu. Například nadřazenou třídou objektu pro **tempEmployee** by mohla být **ePerson**.
- Vyberte **Object class type** (typ třídy objektu). Více informací o typech tříd objektů najdete v tématu “Třídy objektů” na stránce 18.
- Po klepnutí na kartu **Attributes** můžete určit povinné i volitelné atributy pro třídu objektu a prohlížet zděděné atributy nebo po klepnutí na **OK** přidat novou třídu objektu, případně můžete klepnout na **Cancel** a vrátit se zpět na **Manage object classes** bez provedení jakýchkoli změn.

3. Na kartě **Attributes**:

- Z abecedního seznamu **Available attributes** vyberte příslušný atribut a klepnutím na **Add to required** převedete tento atribut na povinný nebo klepnutím na **Add to optional** převedete tento atribut na volitelný pro danou třídu objektu. Atribut se zobrazuje v příslušném seznamu vybraných atributů.
- Opakujte tento postup pro všechny atributy, které chcete vybrat.
- Atribut je možné po jeho výběru klepnutím na příslušné tlačítko **Move to** nebo **Delete** přesouvat z jednoho seznamu do druhého, případně z vybraných seznamů vymazat.
- Produkt umožňuje prohlížet seznamy povinných a volitelných zděděných atributů. Zděděné atributy jsou založeny na **Superior object class** (nadřazené třídě objektu) vybrané na kartě **General**. Zděděné atributy není možné měnit. Pokud však změníte **Superior object class** na kartě **General**, zobrazí se rozdílná sada zděděných atributů.

4. Klepnutím na **OK** je možné přidat novou třídu objektu, případně se můžete klepnutím na **Cancel** vrátit zpět na **Manage object classes** bez provedení jakýchkoli změn.

Poznámka: Pokud klepnete na **OK** na kartě **General** bez přidání jakýchkoli atributů, můžete přidávat atributy editováním nové třídy objektu.

Příkazový řádek

Chcete-li přidat třídu objektu pomocí příkazového řádku, zadejte tento příkaz:

```
ldapmodify -D <adminDN> -w <adminPW> -i
<jméno_souboru>
```

kde <jméno_souboru> obsahuje:

```
dn: cn=Schema
changetype: modify
add: objectclasses
objectclasses: ( <myobjectClass-oid> NAME '<myObjectClass>' DESC '<Třída objektu,
                kterou jsem definoval pro svou aplikaci LDAP>' SUP '<objectclassinheritance>'
                <objectclasstype> MAY (<attribute1> $ <attribute2>))
```

Jak editovat třídu objektu

Přípustné jsou pouze některé změny schématu. Informace o omezeních změn najdete v tématu “Zakázané změny schématu” na stránce 28.

Webová administrace

Pokud jste tak již neučinili, v navigační oblasti rozbalte **Schema management** a klepněte na **Manage object classes**. Třídu objektu můžete editovat takto:

2. Klepněte na **Copy**.
3. Vyberte kartu:
 - Kartu **General** můžete využít k těmto činnostem:
 - Změna **object class name**. Předvolené jméno je jméno kopírované třídy objektu s připojeným slovem COPY. Například třída objektu **tempPerson** se kopíruje jako **tempPersonCOPY**.
 - Změna **Description**.
 - Změna **OID**. Předvolený OID je OID kopírované třídy objektu s připojeným slovem COPY. Například **tempPerson-oid** se zkopíruje jako **tempPerson-oidCOPY**.
 - Změna **Superior object class** (nadřazené třídy objektu). Z rozbalovacího seznamu vyberte superior object class. Tato nadřazená třída určuje třídu objektu, z níž jsou odvozeny jiné atributy. Obvykle platí, že **Superior object class** je **top**, může to však být i jiná třída objektu. Například nadřazenou třídou objektu pro **tempEmployeeCOPY** by mohla být **ePerson**.
 - Změna **Object class type** (typu třídy objektu). Vyberte typ třídy objektu. Více informací o typech tříd objektů najdete v tématu “Třídy objektů” na stránce 18.
 - Po klepnutí na kartu **Attributes** můžete změnit povinné i volitelné atributy pro třídu objektu a prohlížet zděděné atributy nebo klepnutím na **OK** uplatnit provedené změny, případně můžete klepnout na **Cancel** a vrátit se zpět na **Manage object classes** bez provedení jakýchkoli změn.
 - Kartu **Attributes** můžete využít k těmto činnostem:

Z abecedního seznamu **Available attributes** vyberte příslušný atribut a klepnutím na **Add to required** převedete tento atribut na povinný nebo klepnutím na **Add to optional** převedete tento atribut na volitelný pro danou třídu objektu. Atribut se zobrazuje v příslušném seznamu vybraných atributů.

Opakujte tento postup pro všechny atributy, které chcete vybrat.

Atribut je možné po jeho výběru klepnutím na tlačítko **Move to** nebo **Delete** buď přesouvat z jednoho seznamu do druhého, nebo z vybraných seznamů vymazat.

Produkt umožňuje prohlížet seznamy povinných a volitelných zděděných atributů. Zděděné atributy jsou založeny na **Superior object class** (nadřazené třídě objektu) vybrané na kartě **General**. Zděděné atributy není možné měnit. Pokud však změníte **Superior object class** na kartě **General**, zobrazí se rozdílná sada zděděných atributů.
4. Klepnutím na **OK** uplatníte provedené změny, klepnutím na **Cancel** se vrátíte zpět na **Manage object classes** bez provedení jakýchkoli změn.

Příkazový řádek

Chcete-li prohlížet třídy objektů obsažené ve schématu, zadejte tento příkaz:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Vyberte třídu objektu, kterou chcete kopírovat. Příslušné informace změňte pomocí editoru a změny uložte do souboru `<jméno_souboru>`. Zadejte tento příkaz:

```
ldapmodify -D <adminDN> -w <adminPW> -i <filename>
```

kde `<jméno_souboru>` obsahuje:

```
dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: ( <mynewobjectClass-oid> NAME 'mynewObjectClass'
DESC '<Nová třída objektu,
kterou jsem kopíroval pro svou aplikaci LDAP>'
SUP '<superiorclassobject>'<objectclasstype> MAY (attribute1
$ <attribute2> $ <attribute3> ) )
```

Jak vymazat třídu objektu

Přípustné jsou pouze některé změny schématu. Informace o omezeních změn najdete v tématu “Zakázané změny schématu” na stránce 28.

Webová administrace

Pokud jste tak již neučinili, v navigační oblasti rozbalte **Schema management** a klepněte na **Manage object classes**. Třidu objektu vymažete takto:

1. Klepněte na přepínač vedle třídy objektu, kterou chcete vymazat.
2. Klepněte na **Delete**.
3. Zobrazí se výzva k potvrzení výmazu třídy objektu. Klepnutím na **OK** třídu objektu vymažete, klepnutím na **Cancel** se vrátíte zpět na **Manage object classes** bez provedení jakýchkoli změn.

Příkazový řádek

Chcete-li prohlížet třídy objektů obsažené ve schématu, zadejte tento příkaz:

```
ldapsearch -b cn=schema -s base objectclass=* objectclasses
```

Vyberte třídu objektu, kterou chcete vymazat a zadejte tento příkaz:

```
ldapmodify -D <adminDN> -w <adminPW> -i  
<jméno_souboru>
```

kde <jméno_souboru> obsahuje:

```
dn: cn=schema  
changetype: modify  
delete: objectclasses  
objectclasses: (<myobjectClass-oid>)
```

Jak prohlížet atributy

Atributy ve schématu můžete prohlížet buď pomocí webového administračního nástroje, což je preferovaná metoda, nebo pomocí příkazového řádku.

Webová administrace

V navigační oblasti rozbalte **Schema management** a klepněte na **Manage attributes**. Zobrazí se panel pouze pro čtení, který umožňuje prohlížet atributy obsažené ve schématu a jejich charakteristiky. Atributy se zobrazují v abecedním pořadí. Je možné se přesouvat o jednu stránku zpět nebo dopředu klepnutím na Previous nebo Next. Pole vedle těchto tlačítek označuje stránku, na které se právě nalézáte. K přechodu na určitou stránku můžete použít rovněž rozbalovací menu tohoto pole. První třída objektu uvedená na stránce se zobrazuje spolu s číslem této stránky, což usnadňuje nalezení třídy objektu, kterou chcete prohlížet. Například, jestliže hledáte atribut **authenticationUserID**, rozbalíte rozbalovací menu, které přesouváte dolů, dokud nenajdete **Page 3 of 62 applSystemHint** a **Page 4 of 62 authorityRevocatonList**. Protože authenticationUserID je abecedně mezi applSystemHint a authorityRevocatonList, vyberete stranu 3 a klepnete na **Go**.

Zobrazit můžete i atributy setříděné podle syntaxe. Vyberte **Syntax** a klepněte na **Sort**. Atributy se setřídí abecedně v rámci své syntaxe. Přehled typů syntaxe najdete v tématu “Syntaxe atributu” na stránce 24. Podobným způsobem můžete převrátit pořadí seznamu výběrem **Descending** a klepnutím na **Sort**.

Jakmile jste našli požadovaný atribut, můžete prohlížet jeho syntaxi, zjistit počet jeho hodnot a zobrazit třídy objektů, které jej obsahují. Seznam tříd objektů pro daný atribut zobrazíte rozbalením rozbalovacího menu tříd objektů.

Po dokončení klepněte na **Close** a vrátíte se do dialogového okna **Vítejte** serveru adresářů IBM.

Příkazový řádek

Chcete-li prohlížet atributy obsažené ve schématu, zadejte tento příkaz:

```
ldapsearch -b cn=schema -s  
base objectclass=* attributeTypes IBMAttributeTypes
```

Jak přidat atribut

Pro tvorbu nového atributu je možné použít kteroukoli z níže uvedených metod. Preferovaný způsob je webový nástroj administrace.

Webová administrace

Pokud jste tak již neučinili, v navigační oblasti rozbalte **Schema management** a klepněte na **Manage attributes**.

Nový atribut vytvoříte takto:

1. Klepněte na tlačítko **Add**.

Poznámka: Toto dialogové okno zobrazíte rovněž rozbalením **Schema management** v navigační oblasti a potom klepnutím na **Add an attribute**.

2. Zadejte jméno **Attribute name**, například **tempId**. Jméno atributu je povinné pole, jehož hodnota musí začínat abecedním znakem.
3. Zadejte **Description** (popis) atributu, například **Číslo ID přiřazené dočasnému zaměstnanci**.
4. Zadejte **OID** pro atribut. To je povinné pole. Další informace najdete v tématu “Identifikátor objektu (OID)” na stránce 26. Pokud nemáte OID, můžete použít jméno atributu s připojeným -oid. Například, jestliže je jméno atributu **tempID**, předvolený OID je **tempID-oid**. Hodnotu tohoto pole je možné měnit.
5. Z rozbalovacího seznamu vyberte **Superior attribute**. Toto pole (nadřazený atribut) určuje atribut, z něhož jsou odvozeny vlastnosti.
6. Z rozbalovacího seznamu vyberte **Syntax**. Více informací o syntaxi najdete v tématu “Syntaxe atributu” na stránce 24.
7. Zadejte hodnotu **Attribute length**, která určuje maximální délku tohoto atributu. Délka je vyjádřena jako počet bajtů.
8. Výběrem zaškrtačovacího políčka **Allow multiple values** aktivujete pro tento atribut možnost použití více hodnot.
9. Z každého z rozbalovacích menu vyberte příslušné porovnávací pravidlo pro rovnost, řazení a podřetězec. Úplný přehled porovnávacích pravidel najdete v tématu “Porovnávací pravidla” na stránce 22.
10. Po klepnutí na kartu **IBM extensions** můžete určit další rozšíření pro daný atribut, po klepnutí na **OK** je možné přidat nový atribut, případně můžete klepnout na **Cancel** a vrátit se zpět na **Manage attributes** bez provedení jakýchkoliv změn.
11. Na kartě **IBM extensions**:
 - Změňte **DB2 table name**. Pokud se toto pole nechá prázdné, jméno tabulky DB2 generuje server. Jestliže zadáte jméno tabulky DB2, musíte zadat také jméno sloupce DB2.
 - Změňte **DB2 column name**. Pokud se toto pole nechá prázdné, jméno sloupce DB2 generuje server. Jestliže zadáte jméno sloupce DB2, musíte zadat také jméno tabulky DB2.
 - Nastavte **Security class** (třídu zabezpečení) výběrem volby **normal**, **sensitive** nebo **critical** z rozbalovacího seznamu.
 - Výběrem jednoho nebo více pravidel indexování nastavte **Indexing rules**. Další informace o pravidlech indexování najdete v tématu “Pravidla indexování” na stránce 23.

Poznámka: Jako minimum se doporučuje určit indexování rovnosti (Equality) pro každý atribut, který se má používat ve filtrech pro hledání.

12. Klepnutím na **OK** je možné přidat nový atribut, klepnutím na **Cancel** se vrátíte zpět na **Manage attributes** bez provedení jakýchkoliv změn.

Poznámka: Pokud klepnete na OK na kartě General bez přidání jakýchkoliv rozšíření, můžete přidávat rozšíření editováním nového atributu.

Příkazový řádek

Následující příklad znázorňuje definici typu atributu pro atribut nazvaný "myAttribute", se syntaxí adresářového řetězce (viz část "Syntaxe atributu" na stránce 24) a porovnáváním rovnosti při ignorování velikosti písmen (viz část "Porovnávací pravidla" na stránce 22). Část definice specifická pro IBM uvádí, že data atributu jsou uložena ve sloupci nazvaném "myAttrColumn" v tabulce nazvané "myAttrTable". Pokud by tato jména nebyla určena, jméno sloupce i tabulky by mělo předvolenou hodnotu "myAttribute". Atributu je přiřazena "normální" přístupová třída a hodnoty mají maximální délku 200 bajtů.

```
ldapmodify -D <admin> -w <adminpw> -i myschema.ldif
```

kde soubor **myschema.ldif** obsahuje:

```
dn: cn=schema
changetype: modify
add: attributetypes
attributetypes: ( myAttribute-oid NAME ( 'myAttribute' )
                 DESC 'Atribut, který jsem definoval pro svou aplikaci LDAP'
                 EQUALITY 2.5.13.2 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
                 USAGE userApplications )
-
add: ibmattributetypes
ibmattributetypes: ( myAttribute-oid DBNAME ( 'myAttrTable' 'myAttrColumn' )
                   ACCESS-CLASS normal LENGTH 200 )
```

Více informací o tomto příkazu najdete v tématu "ldapmodify a ldapadd" na stránce 187.

Jak editovat atribut

Přípustné jsou pouze některé změny schématu. Informace o omezeních změn najdete v tématu "Zakázané změny schématu" na stránce 28.

Jakoukoli část definice je možné změnit předtím, než přidáte záznamy, které atribut používají. Pro editaci atributu můžete použít kteroukoli z níže uvedených metod. Preferovaný způsob je webový nástroj administrace.

Webová administrace

Pokud jste tak již neučinili, v navigační oblasti rozbalte **Schema management** a klepněte na **Manage attributes**. Atribut můžete editovat takto:

1. Klepněte na přepínač vedle atributu, který chcete editovat.
2. Klepněte na **Edit**.
3. Vyberte kartu:
 - Kartu **General** můžete využít k těmto činnostem:
 - Výběr karet, a to:
 - **General** k těmto operacím:
 - Změna **Description** (popisu).
 - Změna **Syntax** (syntaxe).
 - Nastavení **Attribute length** (délky atributu).
 - Změna nastavení **Multiple value** (více hodnot).
 - Výběr **Matching rule** (porovnávacího pravidla).
 - Změna **Superior attribute** (nadřazeného atributu).
 - Klepněte na kartu **IBM extensions**, chcete-li editovat rozšíření pro atribut, nebo klepněte na **OK**, chcete-li provedené změny uplatnit, nebo klepněte na **Cancel** a vrátíte se na **Manage attributes** bez provedení jakýchkoliv změn.
 - **IBM extensions**, pokud používáte server adresářů IBM k těmto činnostem:
 - Změna **Security class** (třída zabezpečení).
 - Změna **Indexing rules** (pravidel indexování).

- Klepnutím na **OK** uplatníte provedené změny, klepnutím na **Cancel** se vrátíte zpět na **Manage attributes** bez provedení jakýchkoli změn.
4. Klepnutím na **OK** uplatníte provedené změny, klepnutím na **Cancel** se vrátíte zpět na **Manage attributes** bez provedení jakýchkoli změn.

Příkazový řádek

Tento příklad znázorňuje přidávání indexování do příslušného atributu, aby jeho hledání probíhalo rychleji. Pomocí příkazu `ldapmodify` společně se souborem LDIF můžete změnit definici:

```
ldapmodify -D <adminDn> -w <adminpw> -i myschemachange.ldif
```

kde soubor **myschemachange.ldif** obsahuje:

```
dn: cn=schema
changetype: modify
replace: attributetypes
attributetypes: ( myAttribute-oid NAME ( 'myAttribute' ) DESC 'Atribut,
                  který jsem definoval pro svou aplikaci LDAP' EQUALITY 2.5.13.2
                  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications )
-
replace: ibmattributetypes
ibmattributetypes: ( myAttribute-oid DBNAME ( 'myAttrTable' 'myAttrColumn' )
                   ACCESS-CLASS normal LENGTH 200 EQUALITY SUBSTR )
```

Poznámka: V operaci nahrazení musí být začleněny obě části definice (**attributetypes** i **ibmattributetypes**), i kdyby se měnila pouze část **ibmattributetypes**. Jedinou změnou je přidání "EQUALITY SUBSTR" na konec definice, za účelem aktivace požadavku na indexování s porovnáváním rovnosti a podřetězce. Více informací o tomto příkazu najdete v tématu "ldapmodify a ldapadd" na stránce 187.

Jak kopírovat atribut

Pro kopírování atributu můžete použít kteroukoli z níže uvedených metod. Preferovaný způsob je webový nástroj administrace.

Webová administrace

Pokud jste tak již neučinili, v navigační oblasti rozbalte **Schema management** a klepněte na **Manage attributes**. Atribut můžete kopírovat takto:

1. Klepněte na přepínač vedle atributu, který chcete kopírovat.
2. Klepněte na **Copy**.
3. Změňte **Attribute name**. Předvolené jméno je jméno kopírovaného atributu s připojeným slovem COPY. Například **tempID** se zkopíruje jako **tempIDCOPY**.
4. Změňte **Description** (popis) atributu, například **Číslo ID přiřazené dočasnému zaměstnanci**.
5. Změňte **OID**. Předvolený OID je OID kopírovaného atributu s připojeným slovem COPYOID. Například **tempID-oid** se zkopíruje jako **tempID-oidCOPYOID**.
6. Z rozbalovacího seznamu vyberte **Superior attribute**. Toto pole (nadřazený atribut) určuje atribut, z něhož jsou odvozeny vlastnosti.
7. Z rozbalovacího seznamu vyberte **Syntax**. Více informací o syntaxi najdete v tématu "Syntaxe atributu" na stránce 24.
8. Zadejte hodnotu **Attribute length**, která určuje maximální délku tohoto atributu. Délka je vyjádřena jako počet bajtů.
9. Výběrem zaškrtnutí políčka **Allow multiple values** aktivujete pro tento atribut možnost použití více hodnot.
10. Z každého z rozbalovacích menu vyberte příslušné porovnávací pravidlo pro rovnost, řazení a podřetězec. Úplný přehled porovnávacích pravidel najdete v tématu "Porovnávací pravidla" na stránce 22.

11. Klepněte na kartu **IBM extensions**, chcete-li změnit další rozšíření pro daný atribut, nebo klepněte na **OK**, chcete-li provedené změny uplatnit, nebo klepněte na **Cancel** a vrátíte se na **Manage attributes** bez provedení jakýchkoliv změn.

12. Na kartě **IBM extensions**:

- Změňte **DB2 table name**. Pokud se toto pole nechá prázdné, jméno tabulky DB2 generuje server. Jestliže zadáte jméno tabulky DB2, musíte zadat také jméno sloupce DB2.
- Změňte **DB2 column name**. Pokud se toto pole nechá prázdné, jméno sloupce DB2 generuje server. Jestliže zadáte jméno sloupce DB2, musíte zadat také jméno tabulky DB2.
- Změňte **Security class** (třidu zabezpečení) výběrem volby **normal**, **sensitive** nebo **critical** z rozbalovacího seznamu.
- Změňte **Indexing rules** výběrem jednoho nebo více pravidel indexování. Další informace o pravidlech indexování najdete v tématu “Pravidla indexování” na stránce 23.

Poznámka: Jako minimum se doporučuje určit indexování rovnosti (Equal) pro každý atribut, který se má používat ve filtrech pro vyhledávání.

13. Klepnutím na **OK** uplatníte provedené změny, klepnutím na **Cancel** se vrátíte zpět na **Manage attributes** bez provedení jakýchkoli změn.

Poznámka: Pokud klepnete na **OK** na kartě **General** bez přidání jakýchkoli rozšíření, můžete přidávat nebo měnit rozšíření editováním nového atributu.

Příkazový řádek

Chcete-li prohlížet atributy obsažené ve schématu, zadejte tento příkaz:

```
ldapsearch -b cn=schema -s  
base objectclass=* attributeTypes IBMAttributeTypes
```

Vyberte atribut, který chcete kopírovat. Příslušné informace změňte pomocí editoru a změny uložte do souboru `<jméno_souboru>`. Potom zadejte tento příkaz:

```
ldapmodify -D <adminDN> -w <adminPW> -i  
<jméno_souboru>
```

kde `<jméno_souboru>` obsahuje:

```
dn: cn=schema  
changetype: modify  
add: attributetypes  
attributetypes: ( <mynewAttribute-oid> NAME  
'<mynewAttribute>' DESC '<Nový  
atribut, který jsem zkopíroval pro svou aplikaci LDAP>' EQUALITY 2.5.13.2  
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications )  
-  
add: ibmattributetypes  
ibmattributetypes: ( myAttribute-oid DBNAME ( 'myAttrTable' 'myAttrColumn' )  
ACCESS-CLASS normal LENGTH 200 )
```

Jak vymazat atribut

Přípustné jsou pouze některé změny schématu. Informace o omezeních změn najdete v tématu “Zakázané změny schématu” na stránce 28.

Pro vymazání atributu můžete použít kteroukoli z níže uvedených metod. Preferovaný způsob je webový nástroj administrace.

Webová administrace

Pokud jste tak již neučinili, v navigační oblasti rozbalte **Schema management** a klepněte na **Manage attributes**. Atribut můžete vymazat takto:

1. Klepněte na přepínač vedle atributu, který chcete vymazat.
2. Klepněte na **Delete**.
3. Zobrazí se výzva k potvrzení vymazání atributu. Klepnutím na **OK** vymažete příslušný atribut, klepnutím na **Cancel** se vrátíte zpět na **Manage attributes** bez provedení jakýchkoli změn.

Příkazový řádek

```
ldapmodify -D <admindn> -w <adminpw> -i
myschemadelete.ldif
```

kde soubor **myschemadelete.ldif** obsahuje:

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

Více informací o tomto příkazu najdete v tématu “ldapmodify a ldapadd” na stránce 187.

Jak kopírovat schéma na jiné servery

Schéma můžete zkopírovat na jiné servery pomocí tohoto postupu:

1. S použitím obslužného programu ldapsearch zkopírujete schéma do souboru:

```
ldapsearch -b cn=schema -L
"(objectclass=*)" > schema.ldif
```

2. Soubor schématu bude obsahovat všechny třídy objektů a atributy. Pokud chcete, aby soubor LDIF obsahoval pouze vybrané prvky schémat, musíte jej editovat nebo můžete filtrovat výstup příkazu ldapsearch pomocí některého nástroje, jako je např. grep. Zkontrolujte, že atributy vkládáte před třídy objektů, které na ně odkazují. Výsledkem by mohl být například tento soubor (povšimněte si, že každý řádek, který má pokračování, je ukončen jednou mezerou a pokračování na dalším řádku začíná také alespoň jednou mezerou).

```
attributetypes: ( myattr1-oid NAME 'myattr1' DESC 'Nějaká
informace.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
USAGE userApplications )
IBMAttributetypes: ( myattr1-oid DBNAME( 'myattr1' 'myattr1' )
ACCESS-CLASS normal LENGTH 500 )
attributetypes: ( myattr2-oid NAME 'myattr2' DESC 'Nějaká
informace.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
USAGE userApplications )
IBMAttributetypes: ( myattr2-oid DBNAME( 'myattr2' 'myattr2' )
ACCESS-CLASS normal LENGTH 500 )
objectclasses: ( myobject-oid NAME 'myobject' DESC 'Zastupuje
něco.' SUP 'top' STRUCTURAL MUST ( cn ) MAY ( myattr1 $ myattr2 ) )
```

3. Před každý řádek s třídou objektu (objectclasses) nebo typem atributu (attributetype) je vhodné vkládat řádky, pomocí kterých můžete vytvořit instrukce LDIF pro přidání těchto hodnot do záznamu cn=schema. Každá třída objektu a atribut se musí přidat jako individuální modifikace.

```
dn: cn=schema
changetype: modify
add: attributetypes ibmattributetypes
attributetypes: ( myattr1-oid NAME 'myattr1' DESC 'Nějaká
informace.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
USAGE userApplications )
IBMAttributetypes: ( myattr1-oid DBNAME( 'myattr1' 'myattr1' )
ACCESS-CLASS normal LENGTH 500 )
```

```
dn: cn=schema
changetype: modify
add: attributetypes ibmattributetypes
attributetypes: ( myattr2-oid NAME 'myattr2' DESC 'Nějaká
informace.' SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 EQUALITY 2.5.13.2
USAGE userApplications )
IBMAttributetypes: ( myattr2-oid DBNAME( 'myattr2' 'myattr2' )
ACCESS-CLASS normal LENGTH 500 )
```

```
dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: ( myobject-oid NAME 'myobject' DESC 'Zastupuje
něco.' SUP 'top' STRUCTURAL MUST ( cn ) MAY ( myattr1 $ myattr2 ) )
```

4. Pomocí obslužného programu ldapmodify zaveďte toto schéma na další servery:

```
ldapmodify -D
cn=administrator -w <password> -f schema.ldif
```

Jak provádět správu záznamů adresáře

Záznamy adresáře můžete spravovat po rozbalení kategorie **Directory management** v navigační oblasti webového administračního nástroje.

Další informace najdete v těchto částech:

- “Jak procházet strom”
- “Jak přidat záznam”
- “Jak přidat záznam obsahující atribut s jazykovým příznakem” na stránce 166
- “Kopírování uživatelů z ověřovacího seznamu HTTP serveru do serveru adresářů” na stránce 94
- “Jak vymazat záznam” na stránce 167
- “Jak editovat záznam” na stránce 167
- “Jak kopírovat záznam” na stránce 167
- “Jak editovat seznamy přístupových práv” na stránce 168
- “Jak přidat pomocnou třídu objektu” na stránce 168
- “Jak vymazat pomocnou třídu” na stránce 168
- “Jak změnit skupinové členství” na stránce 169
- “Jak prohledávat záznamy adresáře” na stránce 169
- “Jak změnit binární atributy” na stránce 171

Jak procházet strom

Pokud jste tak již neučinili, v navigační oblasti rozbalte kategorii **Directory management** a klepněte na **Manage entries**. Je možné rozbalit různé podstromy a vybrat záznam, na kterém chcete pracovat. V panelu nástrojů na pravé straně můžete volit operace, které chcete provést.

Jak přidat záznam

Pokud jste tak již neučinili, v navigační oblasti rozbalte kategorii **Directory management**.

1. Klepněte na **Add an entry**.
2. Z rozbalovacího seznamu vyberte jednu strukturní třídu objektu (**Structural object class**).
3. Klepněte na **Next**.
4. Z okénka Available vyberte kteroukoli z **Auxiliary object classes**, kterou chcete použít, a klepněte na **Add**. Tento postup opakujte pro každou pomocnou třídu objektu, která se má přidat. Pomocnou třídu objektu můžete také vymazat z okénka Selected jejím vybráním a klepnutím na **Remove**.
5. Klepněte na **Next**.
6. V poli **Relative DN** zadejte relativní rozlišovací jméno (RDN) záznamu, který přidáváte, například cn=John Doe.
7. V poli **Parent DN** zadejte rozlišovací jméno stromového záznamu, který jste vybrali, například ou=Austin, o=IBM. Můžete také klepnout na **Browse** a vybrat nadřazené DN (Parent DN) ze seznamu. Je možné i rozbalit výběr a prohlížet další volby níže v daném podstromu. Vyberte svou volbu a klepnutím na **Select** určete požadované Parent DN. Záznam vybraný v daném stromu se stane předvolenou hodnotou pro **Parent DN**.

Poznámka: Pokud jste zahájili tuto úlohu v dialogovém okně **Manage entries**, je toto pole automaticky vyplněno.

8. Na kartě **Required attributes** zadejte hodnoty pro povinné atributy. Jestliže chcete pro příslušný atribut přidat více než jednu hodnotu, klepněte na **Multiple values** a potom hodnoty přidávejte postupně jednu po druhé.
9. Klepněte na **Optional attributes**.
10. Na kartě **Optional attributes** zadejte příslušné hodnoty pro volitelné atributy. Informace o přidávání binárních hodnot najdete v tématu “Jak změnit binární atributy” na stránce 171. Jestliže chcete pro příslušný atribut přidat více než jednu hodnotu, klepněte na **Multiple values** a potom hodnoty přidávejte postupně jednu po druhé.
11. Klepnutím na OK vytvoříte záznam.
12. Klepnutím na tlačítko **ACL** můžete modifikovat přístupový seznam pro tento záznam. Informace o seznamech ACL najdete v tématu “Seznamy přístupových práv” na stránce 55.
13. Po vyplnění alespoň povinných polí můžete klepnutím na **Add** nový záznam přidat, klepnutím na **Cancel** se vrátíte zpět na **Browse tree** bez provedení změn v adresáři.

Jak přidat záznam obsahující atribut s jazykovým příznakem

K hodnotám v adresáři můžete přiřadit kódy jazyka, a umožnit tak klientům vyhledávat v adresáři hodnoty, které splňují určité jazykové požadavky. Jazykový příznak je komponentou popisu atributu. Další informace o jazykových příznacích najdete v tématu “Jazykové příznaky” na stránce 44.

Chcete-li aktivovat jazykové příznaky, postupujte takto (předvolené jsou deaktivovány):

1. V navigační oblasti klepněte na **Manage server properties** v rámci kategorie **Server administration**.

Poznámka: Chcete-li měnit konfigurační nastavení serveru pomocí úloh v kategorii Server administration, musíte se na server autentizovat jako uživatelský profil i5/OS, který má speciální oprávnění *ALLOBJ a IOSYSCFG. Toho lze docílit tak, že se budete autentizovat jako projektovaný uživatel s heslem pro tento profil. Chcete-li se přihlásit z webového administračního nástroje jako projektovaný uživatel, zadejte uživatelské jméno ve formě `os400-profile=MYUSERNAME,cn=accounts,os400-sys=MYSYSTEM.COM`, kde řetězce MYUSERNAME a MYSYSTEM.COM nahradíte vašim jménem uživatelského profilu a konfigurovanou systémovou projektovanou příponou.

2. Předvolena je karta General. Klepněte na zaškrtačkové okénko **Enable language tag support**, abyste aktivovali podporu jazykových příznaků.

Poznámka: Když po aktivaci funkce jazykových příznaků přidružíte jazykové příznaky k atributům nějakého záznamu, server bude vracet záznam s jazykovými příznaky. To nastane i tehdy, když později funkci jazykových příznaků deaktivujete. Protože chování serveru nemusí být takové, jak aplikace očekává, a abyste se vyhnuli potenciálním problémům, doporučuje se neprovádět deaktivaci funkce jazykových příznaků poté, co byla aktivována.

Vytvoření záznamu obsahujícího atributy s jazykovými příznaky:

1. V navigační oblasti rozbalte kategorii **Directory management** a klepněte na **Manage entries**.
2. Klepněte na tlačítko **Edit attributes**.
3. Vyberte atribut, pro který chcete vytvořit jazykový příznak.
4. Klepnutím na tlačítko **Language tag value** se dostanete na panel **Language tag values**.
5. Do pole **Language tag** zadejte jméno příznaku, který tvoříte. Příznak musí začínat příponou lang-.
6. Do pole **Value** zadejte hodnotu příznaku.
7. Klepněte na tlačítko **Add**. Jazykový příznak a jeho hodnota se zobrazí v seznamu menu.
8. Vytvořte další jazykové příznaky nebo změňte existující jazykové příznaky opakováním kroků 3, 4 a 5. Po vytvoření všech požadovaných jazykových příznaků klepněte na **OK**.
9. Rozbalte menu **Display with language tag** a vyberte jazykový příznak. Klepněte na **Change view** a zobrazí se hodnoty atributu, které jste zadali pro tento jazykový příznak. Veškeré hodnoty, které přidáte nebo upravíte v tomto pohledu se týkají pouze vybraného jazykového příznaku.

10. Po dokončení klepněte na **OK**.

Jak vymazat záznam

Pokud jste tak již neučinili, v navigační oblasti rozbalte kategorii **Directory management** a klepněte na **Manage entries**. Je možné rozbalit různé podstromy a vybrat podstrom, příponu nebo záznam, na kterém chcete pracovat. Na pravém panelu nástrojů klepněte na **Delete**.

- Zobrazí se výzva k potvrzení vymazání. Klepněte na **OK**.
- Záznam se z adresáře vymaže a vy se vrátíte na seznam záznamů.

Jak editovat záznam

Pokud jste tak již neučinili, v navigační oblasti rozbalte kategorii **Directory management** a klepněte na **Manage entries**. Je možné rozbalit různé podstromy a vybrat záznam, na kterém chcete pracovat. Na pravém panelu nástrojů klepněte na **Edit attributes**.

1. Na kartě **Required attributes** zadejte hodnoty pro povinné atributy. Informace o přidávání binárních hodnot najdete v tématu “Jak změnit binární atributy” na stránce 171. Jestliže chcete pro příslušný atribut přidat více než jednu hodnotu, klepněte na **Multiple values** a potom hodnoty přidávejte postupně jednu po druhé.
2. Klepněte na **Optional attributes**.
3. Na kartě **Optional attributes** zadejte příslušné hodnoty pro volitelné atributy. Jestliže chcete pro příslušný atribut přidat více než jednu hodnotu, klepněte na **Multiple values** a potom hodnoty přidávejte postupně jednu po druhé.
4. Klepněte na **Memberships**.
5. Pokud jste vytvořili jakékoli skupiny, na kartě **Memberships** můžete:
 - Ze seznamu **Available groups** vybrat nějakou skupinu a klepnutím na **Add** zařadit příslušný záznam mezi členy vybraného **Static group membership** (členství ve statické skupině).
 - Ze **Static group memberships** vybrat skupinu a klepnutím na **Remove** záznam z vybrané skupiny odstranit.
6. Pokud v případě daného záznamu jde o skupinový záznam, je dostupná karta **Members**. Karta **Members** zobrazuje členy vybrané skupiny. Do skupiny je možné přidávat členy, případně je z ní odstraňovat.
 - Chcete-li přidat člena do skupiny:
 - a. Buď klepněte na **Multiple values** vedle karty **Members**, nebo na kartě **Members** klepněte na **Members**.
 - b. V poli **Member** zadejte DN záznamu, který chcete přidat.
 - c. Klepněte na tlačítko **Add**.
 - d. Klepněte na **OK**.
 - Chcete-li odstranit člena ze skupiny:
 - a. Buď klepněte na **Multiple values** vedle karty **Members**, nebo na kartě **Members** klepněte na **Members**.
 - b. Vyberte záznam, který chcete odstranit.
 - c. Klepněte na tlačítko **Remove**.
 - d. Klepněte na **OK**.
 - Obnovení zobrazení seznamu členů provedete klepnutím na **Update**.
7. Klepnutím na **OK** záznam změníte.

Jak kopírovat záznam

Tato funkce je užitečná při tvorbě podobných záznamů. Kopie dědí všechny atributy původního záznamu. K tomu, aby bylo možné nový záznam pojmenovat, musíte v něm provést modifikace.

Pokud jste tak již neučinili, v navigační oblasti rozbalte kategorii **Directory management** a klepněte na **Manage entries**. Je možné rozbalit různé podstromy a vybrat záznam, na kterém chcete pracovat, jako například John Doe. Na pravém panelu nástrojů klepněte na **Copy**.

- V poli DN změňte záznam RDN. Například změňte cn=John Doe na cn=Jim Smith.
- Na kartě povinných atributů změňte záznam cn na nové RDN. V tomto příkladě je to Jim Smith.

- Podle potřeby změňte ostatní povinné atributy. V tomto příkladě změňte atribut sn z Doe na Smith.
- Po dokončení nezbytných změn vytvoříte nový záznam klepnutím na **OK**.
- Na konec seznamu záznamů je přidán nový záznam Jim Smith.

Poznámka: Tento postup kopíruje pouze atributy záznamu. Do nového záznamu se nekopíruje skupinové členství původního záznamu. Pro přidávání členství se používá funkce editace atributů (Edit attributes).

Jak editovat seznamy přístupových práv

Informace o prohlížení vlastností seznamu ACL pomocí webového administračního nástroje a o práci se seznamy ACL najdete v tématu “Jak provádět správu seznamů přístupových práv (ACL)” na stránce 181.

Další informace najdete v tématu “Seznamy přístupových práv” na stránce 55.

Jak přidat pomocnou třídu objektu

Tlačítko **Add auxiliary class** na panelu nástrojů se používá pro přidávání pomocné třídy objektů do existujícího záznamu v adresářovém stromu. Pomocná třída objektu doplňuje dodatečné atributy do záznamu, do kterého je přidána.

Pokud jste tak již neučinili, v navigační oblasti rozbalte kategorii **Directory management** a klepněte na **Manage entries**. Je možné rozbalit různé podstromy a vybrat záznam, na kterém chcete pracovat, jako například John Doe. Na pravém panelu nástrojů klepněte na **Add auxiliary class**.

1. Z okénka **Available** vyberte kteroukoli z **Auxiliary object classes**, kterou chcete použít, a klepněte na **Add**. Tento postup opakujte pro každou pomocnou třídu objektu, která se má přidat. Pomocnou třídu objektu můžete také vymazat z okénka **Selected** jejím vybráním a klepnutím na **Remove**.
2. Na kartě **Required attributes** zadejte hodnoty pro povinné atributy. Jestliže chcete pro příslušný atribut přidat více než jednu hodnotu, klepněte na **Multiple values** a potom hodnoty přidávejte postupně jednu po druhé.
3. Klepněte na **Optional attributes**.
4. Na kartě **Optional attributes** zadejte příslušné hodnoty pro volitelné atributy. Jestliže chcete pro příslušný atribut přidat více než jednu hodnotu, klepněte na **Multiple values** a potom hodnoty přidávejte postupně jednu po druhé.
5. Klepněte na **Memberships**.
6. Pokud jste vytvořili jakékoli skupiny, na kartě **Memberships** můžete:
 - Ze seznamu **Available groups** vybrat nějakou skupinu a klepnutím na **Add** zařadit příslušný záznam mezi členy vybraného **Static group membership** (členství ve statické skupině).
 - Ze **Static group memberships** vybrat skupinu a klepnutím na **Remove** záznam z vybrané skupiny odstranit.
7. Klepnutím na **OK** záznam změníte.

Jak vymazat pomocnou třídu

Ačkoli je možné vymazat pomocnou třídu během postupu pro přidávání pomocné třídy, je pro vymazání jedné pomocné třídy ze záznamu snadnější použít funkci vymazání pomocné třídy. Postup pro přidávání pomocné třídy by však mohl být vhodnější, pokud chcete vymazat ze záznamu několik pomocných tříd.

1. Pokud jste tak již neučinili, v navigační oblasti rozbalte kategorii **Directory management** a klepněte na **Manage entries**. Je možné rozbalit různé podstromy a vybrat záznam, na kterém chcete pracovat, jako například John Doe. Na pravém panelu nástrojů klepněte na **Delete auxiliary class**.
2. Ze seznamu pomocných tříd vyberte tu třídu, kterou chcete vymazat, a stiskněte **OK**.
3. Když se zobrazí výzva k potvrzení vymazání, klepněte na **OK**.
4. Pomocná třída se ze záznamu vymaže a vy se vrátíte na seznam záznamů.

Opakujte tyto kroky pro každou pomocnou třídu, kterou chcete vymazat.

Jak změnit skupinové členství

Pokud jste tak již neučinili, v navigační oblasti rozbalte kategorii **Directory management**.

1. Klepněte na **Manage entries**.
2. Z adresářového stromu vyberte uživatele a klepněte na ikonu **Edit attributes** na panelu nástrojů
3. Klepněte na kartu **Memberships**.
4. Chcete-li změnit členství pro uživatele, postupujte následovně. Dialogové okno **Change memberships** zobrazí **Available groups**, do nichž lze přidat daného uživatele i **Static Group Memberships** (členství ve statické skupině) záznamu.
 - Ze seznamu **Available groups** vyberte skupinu a potom klepnutím na **Add** zařadíte příslušný záznam mezi členy vybrané skupiny.
 - Ze seznamu **Static Group Memberships** vyberte skupinu a potom klepnutím na **Remove** příslušný záznam z vybrané skupiny odstraňte.
5. Klepnutím na **OK** uložíte provedené změny, klepnutím na **Cancel** se vrátíte zpět do dialogového okna bez provedení jakýchkoli změn.

Jak prohledávat záznamy adresáře

Pro prohledávání adresářového stromu existují tři volby:

- Jednoduché hledání pomocí předdefinované sady výběrových kritérií.
- Rozšířené hledání pomocí uživatelsky definované sady výběrových kritérií.
- Ruční hledání.

Volby hledání jsou přístupné po rozbalení kategorie **Directory management** v navigační oblasti a klepnutí na **Find entries**. Vyberte buď kartu **Search filters**, nebo **Options**.

Poznámka: Není však možné hledat binární záznamy, například hesla.

Filtry hledání

Vyberte jeden z těchto typů prohledávání:

Simple search

Jednoduché hledání používá předvolenou sadu výběrových kritérií:

- Základní DN je **Všechny přípony**.
- Rozsah prohledávání je **Podstrom**.
- Objem prohledávání je **Neomezený**.
- Časový limit je **Neomezený**.
- Dereference aliasů je **Nikdy**.
- Zaškrtnutí sledování odkazů je zrušeno (vyp).

Chcete-li provést jednoduché hledání:

1. Na kartě **Search filter** klepněte na **Simple search**.
2. Z rozbalovacího seznamu vyberte třídu objektu.
3. Pro vybraný typ záznamu vyberte specifický atribut. Jestliže chcete vyhledávat specifický atribut, vyberte tento atribut z rozbalovacího seznamu a do okénka **Is equal to** zadejte jeho hodnotu. Pokud atribut neurčíte, hledání vrátí všechny záznamy adresáře, které odpovídají vybranému typu záznamu.

Advanced search

Rozšířené hledání umožňuje určit omezující podmínky hledání a aktivují filtry vyhledávání. Chcete-li uplatnit předvolená výběrová kritéria, použijte jednoduché hledání.

- Chcete-li provést rozšířené hledání:
 1. Na kartě **Search filter** klepněte na **Advanced search**.
 2. Z rozbalovacího seznamu vyberte **Attribute**.
 3. Vyberte operátor **Comparison**.
 - =atribut je roven této hodnotě.
 - ! atribut není roven této hodnotě.
 - < atribut je menší nebo roven této hodnotě.
 - > atribut je větší nebo roven této hodnotě.
 - ~ atribut je přibližně roven této hodnotě.
 4. Zadejte **Value** (hodnotu) pro porovnávání.
 5. Pomocí tlačítek operátorů hledání je možno provést komplexní dotazy.
 - Jestliže jste již přidali alespoň jeden filtr hledání, určete další kritéria a klepněte na **AND**. Příkaz **AND** vrátí záznamy, které odpovídají oběma sadám výběrových kritérií.
 - Jestliže jste již přidali alespoň jeden filtr hledání, určete další kritéria a klepněte na **OR**. Příkaz **OR** vrátí záznamy, které odpovídají jedné nebo druhé sadě výběrových kritérií.
 6.
 - Klepnutím na **Add** přidáte kritéria filtru hledání do rozšířeného hledání.
 - Klepnutím na **Delete** odstraníte kritéria filtru hledání z rozšířeného hledání.
 - Klepnutím na **Reset** vymažete všechny filtry hledání.

Manual search

Ruční hledání se používá pro vytvoření filtru hledání. Například, jestliže hledáte příjmení, zadejte v tomto poli `sn=*`. Pokud hledáte více atributů, musíte použít syntaxi filtru hledání. Hledáte-li například příjmení osob z konkrétního oddělení, zadáte:

```
(&(sn=*)(dept=<departmentname>))
```

Volby

Na kartě **Options**:

- **Search base DN** - Po výběru přípony z rozbalovacího seznamu můžete hledat pouze v rámci této přípony.

Poznámka: Pokud jste zahájili tuto úlohu z panelu **Manage entries**, je toto pole automaticky vyplněno. Přidávání záznamu zahájíte klepnutím na **Add**, nejprve je však nutné vybrat **Parent DN**.

Možné je i vybrat **All suffixes**, což nastaví prohledávání celého stromu.

| **Poznámka:** Prohledávání podstromu s výběrem **All suffixes** nevrátí informace schématu, informace protokolu
| změn ani žádné informace z procedury Backend projektované systémem.

- **Search scope** (Rozsah vyhledávání).
 - Po výběru **Object** se vyhledává pouze v rozmezí vybraného objektu.
 - Po výběru **Single level** se vyhledává pouze v rozmezí bezprostředních podřízených záznamů vybraného objektu.
 - Po výběru **Subtree** se prohledávají všechny podřízené záznamy vybraného záznamu.
- **Search size limit** - zde zadejte maximální počet záznamů, které se mají vyhledat, nebo vyberte **Unlimited**.
- **Search time limit** - zde zadejte maximální počet sekund, po které má hledání trvat, nebo vyberte **Unlimited**.
- Z rozbalovacího seznamu vyberte typ **Alias dereferencing**.
 - **Never** - pokud je vybraný záznam alias, pro hledání není zrušena reference, to znamená, že hledání ignoruje odkaz na alias.
 - **Finding** - pokud je vybraný záznam alias, hledání zruší referenci aliasu a vyhledává z umístění aliasu.

- **Searching** - není zrušena reference vybraného záznamu, ale reference jakýchkoli záznamů nalezených při hledání jsou zrušeny.
- **Always** - reference všech aliasů nalezených při hledání jsou zrušeny.
- V případě, že jsou z hledání vráceny nějaké odkazy, výběrem zaškrtačacího políčka **Chase referrals** umožníte sledování takových odkazů na jiný server. Když odkaz přesměruje hledání na jiný server, připojení na server používá aktuálních pověření. Pokud jste přihlášení jako Anonymous, budete se pravděpodobně muset přihlásit k serveru s použitím autentizovaného DN.

Další informace o hledání najdete v tématu “Jak přizpůsobit nastavení vyhledávání” na stránce 124.

Jak změnit binární atributy

Jestliže nějaký atribut vyžaduje binární data, zobrazí se vedle pole atributu tlačítko **Binary data**. Pokud tento atribut neobsahuje žádná data, je toto pole prázdné. Protože binární atributy nelze zobrazit, v případě atributu obsahujícího binární data toto pole zobrazuje **Binary Data - 1**. Pokud atribut obsahuje více hodnot, pole se zobrazuje jako rozbalovací seznam.

Po klepnutí na tlačítko **Binary data** můžete zahájit práci s binárními atributy.

Binární data můžete importovat, exportovat nebo mazat.

Chcete-li přidat binární data do atributu:

1. Klepněte na tlačítko **Binary data**.
2. Klepněte na **Import**.
3. Je možné buď zadat jméno cesty požadovaného souboru, nebo klepnout na **Browse** a binární soubor vyhledat a vybrat.
4. Klepněte na **Submit file**. Zobrazí se zpráva File uploaded.
5. Klepněte na **Close**. V poli **Binary data entries** se nyní zobrazuje **Binary Data - 1**.
6. Postup pro import opakujte pro všechny binární soubory, které chcete přidat. Následující záznamy jsou v seznamu uváděny jako **Binary Data - 2**, **Binary Data -3** a tak dále.
7. Po dokončení přidávání binárních dat klepněte na **OK**.

Chcete-li exportovat binární data:

1. Klepněte na tlačítko **Binary data**.
2. Klepněte na **Export**.
3. Klepněte na odkaz **Binary data to download**.
4. Postupujte podle pokynů průvodce, pomocí kterého můžete binární soubor buď zobrazit, nebo uložit na nové místo.
5. Klepněte na **Close**.
6. Postup pro export opakujte pro všechny binární soubory, které chcete exportovat.
7. Po dokončení exportu dat klepněte na **OK**.

Chcete-li vymazat binární data:

1. Klepněte na tlačítko **Binary data**.
2. Zaškrtněte soubor binárních dat, který chcete vymazat. Je možné vybrat několik souborů.
3. Klepněte na **Delete**.
4. Když se zobrazí výzva k potvrzení vymazání, klepněte na **OK**. Binární data označená k vymazání se odstraní ze seznamu.
5. Po dokončení mazání dat klepněte na **OK**.

Poznámka: Binární atributy lze vyhledávat pouze z hlediska existence.

Jak provádět správu uživatelů a skupin

Uživatelé a skupiny můžete spravovat po rozbalení kategorie **Users and groups** v navigační oblasti webového administračního nástroje.

Další informace najdete v těchto částech:

- “Jak provádět správu uživatelů”
- “Jak provádět správu skupin” na stránce 173

Jak provádět správu uživatelů

Po dokončení nastavení sfér a šablon můžete tyto položky přenést k uživatelům. Další informace najdete v těchto částech:

- “Jak přidávat uživatele”
- “Jak ve sféře najít uživatele”
- “Jak editovat informace uživatele”
- “Jak kopírovat uživatele” na stránce 173
- “Jak odstranit uživatele ze seznamu” na stránce 173

Jak přidávat uživatele

V navigační oblasti webového administračního nástroje rozbalte kategorii **Users and groups**.

1. Klepněte na **Add user** nebo klepněte na **Managing users** a potom na **Add**.
2. Z rozbalovacího menu vyberte sféru, do které chcete přidat uživatele.
3. Klepněte na **Next**. Zobrazí se šablona, která je přiřazena k dané sféře. Na kartách vyplňte povinná pole označená hvězdičkou (*) a jakákoli další pole. Pokud jste již v rámci sféry vytvořili nějaké skupiny, je také možné přidat uživatele do jedné nebo více skupin.
4. Po dokončení klepněte na **Finish**.

Jak ve sféře najít uživatele

V navigační oblasti webového administračního nástroje rozbalte kategorii **Users and groups**.

1. Klepněte na **Find user** nebo klepněte na **Manage users** a potom na **Find**.
2. Z pole **Select realm** vyberte sféru, kterou chcete prohledávat.
3. V poli **Naming attribute** zadejte hledaný řetězec. Tato funkce podporuje zástupné znaky; jestliže zadáte například ***smith**, výsledkem jsou všechny záznamy, jejichž atribut pojmenování končí řetězcem “smith”.
4. U vybraného uživatele můžete provádět tyto operace:
 - **Editace** - viz část “Jak editovat informace uživatele”.
 - **Kopírování** - viz část “Jak kopírovat uživatele” na stránce 173.
 - **Vymazání** - viz část “Jak odstranit uživatele ze seznamu” na stránce 173.
5. Po dokončení klepněte na **OK**.

Jak editovat informace uživatele

V navigační oblasti webového administračního nástroje rozbalte kategorii **Users and groups**.

1. Klepněte na **Manage users**.
2. Z rozbalovacího menu vyberte příslušnou sféru. Pokud v okénku **Users** nejsou zobrazeni uživatelé, klepněte na **View users**.
3. Vyberte uživatele, jehož informace chcete editovat, a klepněte na **Edit**.
4. Změňte příslušné informace na kartách, změňte skupinové členství.
5. Po dokončení klepněte na **OK**.

Jak kopírovat uživatele

Jestliže potřebujete vytvořit několik uživatelů, kteří mají většinou totožné informace, můžete vytvořit další uživatele kopírováním původního uživatele a potom modifikovat jejich informace.

V navigační oblasti webového administračního nástroje rozbalte kategorii **Users and groups**.

1. Klepněte na **Manage users**.
2. Z rozbalovacího menu vyberte příslušnou sféru. Pokud v okénku **Users** nejsou zobrazeni uživatelé, klepněte na **View users**.
3. Vyberte uživatele, jehož informace chcete kopírovat, a klepněte na **Copy**.
4. Pro nového uživatele změňte příslušné informace, například povinné informace, které určují totožnost určitého uživatele, jako např. sn nebo cn. Informace, které jsou společné pro oba uživatele, není nutné měnit.
5. Po dokončení klepněte na **OK**.

Jak odstranit uživatele ze seznamu

V navigační oblasti webového administračního nástroje rozbalte kategorii **Users and groups**.

1. Klepněte na **Manage users**.
2. Z rozbalovacího menu vyberte příslušnou sféru. Pokud v okénku **Users** nejsou zobrazeni uživatelé, klepněte na **View users**.
3. Vyberte uživatele, jehož chcete odstranit ze seznamu, a klepněte na **Delete**.
4. Když se zobrazí výzva k potvrzení vymazání, klepněte na **OK**.
5. Daný uživatel je odstraněn ze seznamu uživatelů.

Jak provádět správu skupin

Po dokončení nastavení sféry a šablon můžete vytvořit skupiny. Další informace najdete v těchto částech:

- “Jak přidávat skupiny”
- “Jak ve sféře najít skupinu”
- “Jak editovat informace skupiny” na stránce 174
- “Jak kopírovat skupinu” na stránce 174
- “Jak odebrat skupinu” na stránce 174

Jak přidávat skupiny

V navigační oblasti webového administračního nástroje rozbalte kategorii **Users and groups**.

1. Klepněte na **Add group** nebo klepněte na **Manage groups** a potom na **Add**.
2. Zadejte jméno skupiny, kterou chcete vytvořit.
3. Z rozbalovacího menu vyberte sféru, do které chcete přidat uživatele.
4. Klepnutím na **Finish** skupinu vytvoříte. Pokud již máte ve sféře uživatele, můžete klepnout na **Next** a vybrat uživatele, kteří se mají do skupiny přidat. Potom klepněte na **Finish**.

Další informace najdete v tématu “Skupiny a role” na stránce 48.

Jak ve sféře najít skupinu

V navigační oblasti webového administračního nástroje rozbalte kategorii **Users and groups**.

1. Klepněte na **Find group** nebo klepněte na **Manage groups** a potom na **Find**.
2. Z pole **Select realm** vyberte sféru, kterou chcete prohledávat.
3. V poli **Naming attribute** zadejte hledaný řetězec. Tato funkce podporuje zástupné znaky; jestliže zadáte například ***klub**, výsledkem jsou všechny skupiny, jejichž atribut pojmenování obsahuje slovo klub, například knižní klub, šachový klub, zahrádkářský klub a tak dále.
4. U vybrané skupiny můžete provádět tyto operace:
 - **Editace** - viz část “Jak editovat informace skupiny” na stránce 174.
 - **Kopírování** - viz část “Jak kopírovat skupinu” na stránce 174.

- **Vymazání** - viz část "Jak odebrat skupinu".

5. Po dokončení klepněte na **Close**.

Jak editovat informace skupiny

V navigační oblasti webového administračního nástroje rozbalte kategorii **Users and groups**.

1. Klepněte na **Manage groups**.
2. Z rozbalovacího menu vyberte příslušnou sféru. Pokud v okénku **Groups** nejsou zobrazeny skupiny, klepněte na **View groups**.
3. Vyberte skupinu, kterou chcete editovat, a klepněte na **Edit**.
4. Klepnutím na **Filter** můžete omezit počet **Available users** (dostupných uživatelů). Například zadáním *ář v poli Last name omezíte dostupné uživatele na takové, jejichž jméno končí řetězcem "ář" jako například Pavel Kolář, Jan Kolář, Jan Šindelář, Josef Kovář a podobně.
5. Do skupiny je možné přidávat uživatele, případně je z ní odstraňovat.
6. Po dokončení klepněte na **OK**.

Jak kopírovat skupinu

Jestliže potřebujete vytvořit několik skupin, které mají většinou stejné členy, můžete vytvořit další skupiny kopírováním původní skupiny a potom modifikovat jejich informace.

V navigační oblasti webového administračního nástroje rozbalte kategorii **Users and groups**.

1. Klepněte na **Manage groups**.
2. Z rozbalovacího menu vyberte příslušnou sféru. Pokud v okénku **Groups** nejsou zobrazeny skupiny, klepněte na **View groups**.
3. Vyberte skupinu, kterou chcete kopírovat, a klepněte na **Copy**.
4. V poli **Group name** změňte jméno skupiny. Nová skupina má stejné členy jako původní skupina.
5. Členy skupiny můžete změnit.
6. Po dokončení klepněte na **OK**. Nová skupina je vytvořena a obsahuje stejné členy jako původní skupina, ale odráží všechna doplnění nebo odebrání, která jste provedli během kopírování.

Jak odebrat skupinu

V navigační oblasti webového administračního nástroje rozbalte kategorii **Users and groups**.

1. Klepněte na **Manage groups**.
2. Z rozbalovacího menu vyberte příslušnou sféru. Pokud v okénku **Groups** nejsou zobrazeny skupiny, klepněte na **View groups**.
3. Vyberte skupinu, kterou chcete odstranit, a klepněte na **Delete**.
4. Když se zobrazí výzva k potvrzení vymazání, klepněte na **OK**.
5. Daná skupina je odstraněna ze seznamu skupin.

Jak provádět správu sfér a uživatelských šablon

Sféry a uživatelské šablony můžete spravovat po klepnutí na **Realms and templates** v navigační oblasti webového administračního nástroje. Použití sfér a uživatelských šablon usnadňuje ostatním zadávat data do adresáře. Více informací o koncepcích sfér a uživatelských šablon najdete v tématu "Sféry a uživatelské šablony" na stránce 41.

Další informace najdete v těchto částech:

- "Jak vytvořit sféru" na stránce 175
- "Jak vytvořit administrátora sféry" na stránce 175
- "Jak vytvořit šablonu" na stránce 176
- "Jak přidat šablonu do sféry" na stránce 177
- "Jak vytvářet skupiny" na stránce 178

- “Jak přidat uživatele do sféry” na stránce 178
- “Jak provádět správu sfěr” na stránce 178
- “Jak provádět správu šablon” na stránce 179

Jak vytvořit sféru

Více informací o koncepcích sfěr a uživatelských šablon najdete v tématu “Sféry a uživatelské šablony” na stránce 41.

Při tvorbě sféry postupujte takto:

1. V navigační oblasti webového administračního nástroje rozbalte kategorii **Realms and templates**.
2. Klepněte na **Add realm**.
 - Zadejte jméno sféry, například **realm1**.
 - Zadejte Parent DN, které určuje umístění sféry. Tento záznam se zadává ve formě přípony, např. **o=ibm,c=us**. Tento záznam může být přípona nebo záznam kdekoli v adresáři. Další možností je klepnout na **Browse** a vybrat požadované umístění podstromu.
3. Pokračovat můžete klepnutím na **Next**, případně na **Finish**.
4. Jestliže klepnete na **Next**, můžete ještě zkontrolovat zadané informace. V tomto okamžiku jste vlastně sféru ještě nevytvořili, proto je možno ignorovat **User template** a **User search filter**.
5. Sféru vytvoříte klepnutím na **Finish**.

Jak vytvořit administrátora sféry

K tomu, aby bylo možno vytvořit administrátora sféry, musíte pro tuto sféru nejprve vytvořit skupinu administrace, a to takto:

1. Vytvoření skupiny administrace.
 - a. V navigační oblasti webového administračního nástroje rozbalte kategorii **Directory management**.
 - b. Klepněte na **Manage entries**.
 - c. Rozbalte strom a vyberte sféru, kterou jste právě vytvořili (**cn=realm1,o=ibm,c=us**).
 - d. Klepněte na **Edit ACL**.
 - e. Klepněte na kartu **Owners**.
 - f. Zkontrolujte, zda je zaškrtnuto políčko **Propagate owner**.
 - g. Zadejte DN pro danou sféru, **cn=realm1,o=ibm,c=us**.
 - h. Změňte **Type** skupinu (group).
 - i. Klepněte na tlačítko **Add**.
2. Vytvoření záznamu administrátora. Pokud dosud nemáte uživatelský záznam pro administrátora, musíte jeden vytvořit.
 - a. V navigační oblasti webového administračního nástroje rozbalte kategorii **Directory management**.
 - b. Klepněte na **Manage entries**.
 - c. Rozbalte strom do místa, kde má být záznam administrátora umístěn.

Poznámka: Umístěním záznamu administrátora mimo sféru zabráníte situaci, kdy by měl možnost sám sebe neúmyslně vymazat. V tomto případě by umístění mohlo být **o=ibm,c=us**.

- d. Klepněte na tlačítko **Add**.
- e. Vyberte **Structural object class** (strukturní třídu objektu), například **inetOrgPerson**.
- f. Klepněte na **Next**.
- g. Vyberte jakoukoli pomocnou třídu objektu, kterou chcete přidat.
- h. Klepněte na **Next**.
- i. Pro daný záznam zadejte povinné atributy. Například:
 - **RDN** **cn=JohnDoe**

- **DN** o=ibm,c=us
 - **cn** John Doe
 - **sn** Doe
- j. Na kartě **Other attributes** zkontrolujte, že jste přiřadili heslo.
- k. Po dokončení klepněte na **Finish**.
3. Přidání administrátora do skupiny administrace.
- a. V navigační oblasti webového administračního nástroje rozbalte kategorii **Directory management**.
 - b. Klepněte na **Manage entries**.
 - c. Rozbalte strom a vyberte sféru, kterou jste právě vytvořili (**cn=realm1,o=ibm,c=us**).
 - d. Klepněte na **Edit attributes**.
 - e. Klepněte na kartu **Members**.
 - f. Klepněte na **Members**.
 - g. V poli **Members** zadejte DN administrátora, v tomto případě **cn=John Doe,o=ibm,c=us**.
 - h. Klepněte na tlačítko **Add**. DN se zobrazí v seznamu **Members**.
 - i. Klepněte na **OK**.
 - j. Klepněte na **Update**. DN se zobrazí v seznamu **Current members**.
 - k. Klepněte na **OK**.
4. Tím jste vytvořili administrátora, který může provádět správu záznamů v rámci této sféry.

Jak vytvořit šablonu

Dalším krokem po vytvoření sféry je vytvoření uživatelské šablony. Šablona pomáhá uspořádat informace, které chcete zadávat. V navigační oblasti webového administračního nástroje rozbalte kategorii **Realms and templates**.

1. Klepněte na **Add user template**.
 - Zadejte pro šablonu jméno, například **template1**.
 - Zadejte místo, kde má být šablona umístěna. Pro účely replikací umístěte šablonu do podstromu sféry, která bude tuto šablonu využívat. Například do podstromu sféry vytvořené v předchozích operacích **cn=realm1,o=ibm,c=us**. Můžete také klepnout na **Browse** a vybrat pro umístění šablony jiný podstrom.
2. Klepněte na **Next**. Klepnutím na **Finish** můžete vytvořit prázdnou šablonu. Potřebné informace je možné do šablony přidat později, viz část “Jak editovat šablonu” na stránce 181.
3. Pokud jste klepnuli na **Next**, zvolte pro šablonu strukturní třídu objektu, například **inetOrgPerson**. Můžete také přidat jakékoli pomocné třídy objektů, které požadujete.
4. Klepněte na **Next**.
5. V šabloně byla vytvořena karta **Required**. Informace obsažené na této kartě je možné měnit.
 - a. V menu karty vyberte **Required** a klepněte na **Edit**. Zobrazí se dialogové okno **Edit tab**. Na něm uvidíte jméno karty **Required** a vybrané atributy, které jsou požadovány pro třídu objektu **inetOrgPerson**:
 - *sn - příjmení
 - *cn - obecné jméno

Poznámka: Hvězdička * označuje povinné informace.
 - b. Jestliže chcete na tuto kartu přidat další informace, vyberte potřebný atribut z menu **Attributes**. Například vyberte **departmentNumber** a klepněte na **Add**. Vyberte **employeeNumber** a klepněte na **Add**. Vyberte **title** a klepněte na **Add**. Menu **Selected attributes** nyní obsahuje:
 - title
 - employeeNumber
 - departmentNumber
 - *sn
 - *cn

- c. Způsob zobrazení těchto polí na šabloně můžete znovu uspořádat zvýrazněním vybraného atributu a klepnutím na **Move up** nebo **Move down**. Tím se změní poloha atributu o jednu pozici. Opakujte tento postup do té doby, než uspořádáte atributy do požadovaného pořadí. Například:
- *sn
 - *cn
 - title
 - employeeNumber
 - departmentNumber
- d. Rovněž je možné měnit každý vybraný atribut.
- 1) V okénku **Selected attributes** zvýrazněte příslušný atribut a klepněte na **Edit**.
 - 2) Jméno, pod kterým se na šabloně zobrazují pole, můžete rovněž změnit. Jestliže například chcete, aby se pole **departmentNumber** zobrazovalo jako **Číslo oddělení**, zadejte tento název do pole **Display name**.
 - 3) Kromě toho můžete zadat i předvolenou hodnotu, která se bude předem vyplňovat v poli atributu na šabloně. Jestliže je například většina uživatelů, kteří se mají zadávat, členy oddělení 789, můžete jako předvolenou hodnotu určit 789. Pole v šabloně je předem vyplněno hodnotou 789. Hodnotu je možné změnit během přidávání informací aktuálního uživatele.
 - 4) Klepněte na **OK**.
- e. Klepněte na **OK**.
6. Jestliže chcete vytvořit jinou kategorii karty pro další informace, klepněte na **Add**.
- Zadejte jméno pro novou kartu, například Údaje bydliště.
 - Pro tuto kartu vyberte z menu **Attributes** příslušné atributy. Vyberte například **homePostalAddress** a klepněte na **Add**. Vyberte **postOfficeBox** a klepněte na **Add**. Vyberte **telephoneNumber** a klepněte na **Add**. Vyberte **homePhone** a klepněte na **Add**. Vyberte **facsimileTelephoneNumber** a klepněte na **Add**. Menu **Selected attributes** nyní obsahuje:
 - homePostalAddress
 - postOfficeBox
 - telephoneNumber
 - homePhone
 - facsimileTelephoneNumber
 - Způsob zobrazení těchto polí na šabloně můžete znovu uspořádat zvýrazněním vybraného atributu a klepnutím na **Move up** nebo **Move down**. Tím se změní poloha atributu o jednu pozici. Opakujte tento postup do té doby, než uspořádáte atributy do požadovaného pořadí. Například:
 - homePostalAddress
 - postOfficeBox
 - telephoneNumber
 - facsimileTelephoneNumber
 - homePhone
 - Klepněte na **OK**.
7. Tento postup opakujte pro všechny karty, které chcete vytvořit. Po dokončení klepněte na **Finish**, čímž se šablona vytvoří.

Jak přidat šablonu do sféry

Po vytvoření sféry a šablony musíte přidat šablonu do sféry. V navigační oblasti webového administračního nástroje rozbalte kategorii **Realms and templates**.

1. Klepněte na **Manage realms**.
2. Vyberte sféru, do které chcete šablonu přidat, v tomto případě **cn=realm1,o=ibm,c=us**, a klepněte na **Edit**.
3. Přesuňte se dolů na **User template** a rozbalte rozbalovací menu.
4. Vyberte šablonu, v tomto případě **cn=template1,cn=realm1,o=ibm,c=us**.

5. Klepněte na **OK**.
6. Klepněte na **Close**.

Jak vytvářet skupiny

V navigační oblasti webového administračního nástroje rozbalte kategorii **Users and groups**.

1. Klepněte na **Add group**.
2. Zadejte jméno skupiny, kterou chcete vytvořit, například **group1**.
3. Z rozbalovacího menu vyberte sféru, do které chcete přidat uživatele. V tomto příkladě je to **realm1**.
4. Klepnutím na **Finish** skupinu vytvoříte. Pokud již máte ve sféře uživatele, můžete klepnout na **Next** a vybrat uživatele, kteří se mají do skupiny group1 přidat. Potom klepněte na **Finish**.

Další informace najdete v tématu “Skupiny a role” na stránce 48.

Jak přidat uživatele do sféry

V navigační oblasti webového administračního nástroje rozbalte kategorii **Users and groups**.

1. Klepněte na **Add user**.
2. Z rozbalovacího menu vyberte sféru, do které chcete přidat uživatele. V tomto příkladě je to **realm1**.
3. Klepněte na **Next**. Zobrazí se šablona, kterou jste právě vytvořili, template1. Na kartách vyplňte povinná pole označená hvězdičkou (*) a jakákoli další pole. Pokud jste již v rámci sféry vytvořili nějaké skupiny, je také možné přidat uživatele do jedné nebo více skupin.
4. Po dokončení klepněte na **Finish**.

Jak provádět správu sfér

Jakmile jste nastavili a zaplnili svou výchozí sféru, můžete přidávat další sféry nebo měnit stávající sféry.

V navigační oblasti rozbalte kategorii **Realms and templates** a klepněte na **Manage realms**. Zobrazí se seznam existujících sfér. Z tohoto panelu můžete přidat sféru, editovat sféru, odstranit sféru nebo editovat seznam přístupových práv (ACL) dané sféry. Další informace najdete v těchto částech:

- “Jak přidat sféru”
- “Jak editovat sféru” na stránce 179
- “Jak odstranit sféru” na stránce 179
- “Jak editovat seznamy ACL ve sféře” na stránce 179

Jak přidat sféru

V navigační oblasti webového administračního nástroje rozbalte kategorii **Realms and templates**.

1. Klepněte na **Add realm**.
 - Zadejte jméno sféry, například **realm2**.
 - Jestliže máte nějaké existující sféry, v našem příkladě **realm1**, můžete vybrat sféru a nechat zkopírovat její nastavení do sféry, kterou právě vytváříte.
 - Zadejte Parent DN, které určuje umístění sféry. Tento záznam se zadává ve formě přípony, např. **o=ibm,c=us**. Další možností je klepnout na **Browse** a vybrat požadované umístění podstromu.
2. Pokračovat můžete klepnutím na **Next**, případně na **Finish**.
3. Jestliže klepnete na **Next**, můžete ještě zkontrolovat zadané informace.
4. Z rozbalovacího seznamu vyberte **User template**. Pokud jste kopírovali nastavení z již existující sféry, její šablona je v tomto poli předem vyplněná.
5. Zadejte **User search filter**.
6. Sféru vytvoříte klepnutím na **Finish**.

Jak editovat sféru

V navigační oblasti webového administračního nástroje rozbalte kategorii **Realms and templates**.

- Klepněte na **Manage realms**.
- Ze seznamu sfér vyberte sféru, kterou chcete editovat.
- Klepněte na **Edit**.
 - Tlačítko **Browse** je možné použít ke změně těchto položek:
 - Skupina administrátorů.
 - Zásobník skupiny.
 - Zásobník uživatele.
 - Z rozbalovacího menu můžete vybrat jinou šablonu.
 - Po klepnutí na **Edit** můžete měnit **User search filter** (uživatelský filtr vyhledávání).
- Po dokončení klepněte na **OK**.

Jak odstranit sféru

V navigační oblasti webového administračního nástroje rozbalte kategorii **Realms and templates**.

1. Klepněte na **Manage realms**.
2. Vyberte sféru, kterou chcete odstranit.
3. Klepněte na **Delete**.
4. Když se zobrazí výzva k potvrzení vymazání, klepněte na **OK**.
5. Daná sféra je odstraněna ze seznamu sfér.

Jak editovat seznamy ACL ve sféře

Informace o prohlížení vlastností seznamu ACL pomocí webového administračního nástroje a o práci se seznamy ACL najdete v tématu “Jak provádět správu seznamů přístupových práv (ACL)” na stránce 181.

Další informace najdete v tématu “Seznamy přístupových práv” na stránce 55.

Jak provádět správu šablon

Po vytvoření výchozí šablony můžete přidat další šablony nebo měnit existující šablony.

V navigační oblasti rozbalte kategorii **Realms and templates** a klepněte na **Manage user templates**. Zobrazí se seznam existujících šablon. Z tohoto panelu můžete přidat šablonu, editovat šablonu, odstranit šablonu nebo editovat seznam přístupových práv (ACL) dané šablony. Další informace najdete v těchto částech:

- “Jak přidat uživatelskou šablonu”
- “Jak editovat šablonu” na stránce 181
- “Jak odstranit šablonu” na stránce 181
- “Jak editovat seznamy ACL v šabloně” na stránce 181

Jak přidat uživatelskou šablonu

V navigační oblasti webového administračního nástroje rozbalte kategorii **Realms and templates**.

1. Klepněte na **Add user template** nebo klepněte na **Manage user templates** a potom na **Add**.
 - Zadejte jméno pro novou šablonu, například **template2**.
 - Jestliže máte nějaké předchozí existující šablony, například **template1**, můžete vybrat šablonu a nechat zkopírovat její nastavení do šablony, kterou právě vytváříte.
 - Zadejte Parent DN, které určuje umístění šablony. Tento záznam se zadává ve formě DN, například **cn=realm1,o=ibm,c=us**. Další možností je klepnout na **Browse** a vybrat požadované umístění podstromu.
2. Klepněte na **Next**. Klepnutím na **Finish** můžete vytvořit prázdnou šablonu. Potřebné informace je možné do šablony přidat později, viz část “Jak editovat šablonu” na stránce 181.

3. Pokud jste klepnuli na **Next**, zvolte pro šablonu strukturní třídu objektu, například **inetOrgPerson**. Můžete také přidat jakékoli pomocné třídy objektů, které požadujete.
4. Klepněte na **Next**.
5. V šabloně byla vytvořena karta **Required**. Informace obsažené na této kartě je možné měnit.
 - a. V menu karty vyberte **Required** a klepněte na **Edit**. Zobrazí se dialogové okno **Edit tab**. Na něm uvidíte jméno karty **Required** a vybrané atributy, které jsou požadovány pro třídu objektu **inetOrgPerson**:
 - *sn - příjmení
 - *cn - obecné jméno

Poznámka: Hvězdička * označuje povinné informace.
 - b. Jestliže chcete na tuto kartu přidat další informace, vyberte potřebný atribut z menu **Attributes**. Například vyberte **departmentNumber** a klepněte na **Add**. Vyberte **employeeNumber** a klepněte na **Add**. Vyberte **title** a klepněte na **Add**. Menu **Selected attributes** nyní obsahuje:
 - title
 - employeeNumber
 - departmentNumber
 - *sn
 - *cn
 - c. Způsob zobrazení těchto polí na šabloně můžete znovu uspořádat zvýrazněním vybraného atributu a klepnutím na **Move up** nebo **Move down**. Tím se změní poloha atributu o jednu pozici. Opakujte tento postup do té doby, než uspořádáte atributy do požadovaného pořadí. Například:
 - *sn
 - *cn
 - title
 - employeeNumber
 - departmentNumber
 - d. Rovněž je možné měnit každý vybraný atribut.
 - 1) V okénku **Selected attributes** zvýrazněte příslušný atribut a klepněte na **Edit**.
 - 2) Jméno, pod kterým se na šabloně zobrazují pole, můžete rovněž změnit. Jestliže například chcete, aby se pole **departmentNumber** zobrazovalo jako **Číslo oddělení**, zadejte tento název do pole **Display name**.
 - 3) Kromě toho můžete zadat i předvolenou hodnotu, která se bude předem vyplňovat v poli atributu na šabloně. Jestliže je například většina uživatelů, kteří se mají zadávat, členy oddělení 789, můžete jako předvolenou hodnotu určit 789. Pole v šabloně je předem vyplněno hodnotou 789. Hodnotu je možné změnit během přidávání informací aktuálního uživatele.
 - 4) Klepněte na **OK**.
 - e. Klepněte na **OK**.
6. Jestliže chcete vytvořit jinou kategorii karty pro další informace, klepněte na **Add**.
 - Zadejte jméno pro novou kartu, například Údaje bydliště.
 - Pro tuto kartu vyberte z menu **Attributes** příslušné atributy. Vyberte například **homePostalAddress** a klepněte na **Add**. Vyberte **postOfficeBox** a klepněte na **Add**. Vyberte **telephoneNumber** a klepněte na **Add**. Vyberte **homePhone** a klepněte na **Add**. Vyberte **facsimileTelephoneNumber** a klepněte na **Add**. Menu **Selected attributes** nyní obsahuje:
 - homePostalAddress
 - postOfficeBox
 - telephoneNumber
 - homePhone
 - facsimileTelephoneNumber

- Způsob zobrazení těchto polí na šabloně můžete znovu uspořádat zvýrazněním vybraného atributu a klepnutím na **Move up** nebo **Move down**. Tím se změní poloha atributu o jednu pozici. Opakujte tento postup do té doby, než uspořádáte atributy do požadovaného pořadí. Například:
 - homePostalAddress
 - postOfficeBox
 - telephoneNumber
 - facsimileTelephoneNumber
 - homePhone
 - Klepněte na **OK**.
7. Tento postup opakujte pro všechny karty, které chcete vytvořit. Po dokončení klepněte na **Finish**, čímž se šablona vytvoří.

Jak editovat šablonu

V navigační oblasti webového administračního nástroje rozbalte kategorii **Realms and templates**.

- Klepněte na **Manage user templates**.
- Ze seznamu sfér vyberte sféru, kterou chcete editovat.
- Klepněte na **Edit**.
- Jestliže máte nějaké předchozí existující šablony, například template1, můžete vybrat šablonu a nechat zkopírovat její nastavení do šablony, kterou právě vytváříte.
- Klepněte na **Next**.
 - Zde můžete využít rozbalovací menu ke změně strukturní třídy objektu šablony.
 - Zde můžete také přidávat nebo odstraňovat pomocné třídy objektů.
- Klepněte na **Next**.
- Karty a atributy obsažené v šabloně je možné měnit. Informace o tom jak měnit karty najdete v tématu 5 na stránce 180.
- Po dokončení klepněte na **Finish**.

Jak odstranit šablonu

V navigační oblasti webového administračního nástroje rozbalte kategorii **Realms and templates**.

1. Klepněte na **Manage user templates**.
2. Vyberte šablonu, kterou chcete odstranit.
3. Klepněte na **Delete**.
4. Když se zobrazí výzva k potvrzení vymazání, klepněte na **OK**.
5. Daná šablona je odstraněna ze seznamu šablon.

Jak editovat seznamy ACL v šabloně

V navigační oblasti webového administračního nástroje rozbalte kategorii **Realms and templates**.

1. Klepněte na **Manage user templates**.
2. Vyberte šablonu, pro kterou chcete editovat seznamy ACL.
3. Klepněte na **Edit ACL**.

Informace o prohlížení vlastností seznamu ACL pomocí webového administračního nástroje a o práci se seznamy ACL najdete v tématu “Jak provádět správu seznamů přístupových práv (ACL)”.

Další informace najdete v tématu “Seznamy přístupových práv” na stránce 55.

Jak provádět správu seznamů přístupových práv (ACL)

Další informace o přístupových seznamech najdete v tématu “Seznamy přístupových práv” na stránce 55.

Chcete-li prohlížet vlastnosti seznamu ACL pomocí webového administračního nástroje nebo pracovat se seznamy ACL, postupujte takto:

1. Vyberte záznam adresáře, například `cn=John Doe,ou=Advertising,o=ibm,c=US`.
2. Klepněte na **Edit ACL**. Zobrazí se dialogové okno Edit Acl s předvolenou kartou **Effective ACLs**.

Toto dialogové okno má pět oušek:

- “Efektivní seznamy ACL”
- “Efektivní vlastníci”
- “Nefiltrované seznamy ACL”
- “Filtrované seznamy ACL” na stránce 184
- “Vlastníci” na stránce 185

Karty **Effective ACLs** a **Effective owners** obsahují informace pouze pro čtení týkající se seznamů ACL.

Efektivní seznamy ACL

Efektivní seznamy ACL jsou explicitní a zděděné seznamy ACL vybraného záznamu. Přístupová práva pro určitý efektivní seznam ACL můžete prohlížet po jeho výběru a klepnutí na tlačítko **View**. Otevře se dialogové okno **View access rights**.

Prohlížení přístupových práv

- Sekce **Rights** zobrazuje práva subjektu k přidávání nebo mazání.
 - **Add child** uděluje nebo odpírá subjektu právo přidat záznam adresáře pod vybraný záznam.
 - **Delete entry** uděluje nebo odpírá subjektu právo vymazat vybraný záznam.
- Sekce **Security class** definuje povolení pro třídy zabezpečení. Atributy jsou seskupeny do těchto tříd zabezpečení:
 - **Normal** - normální třídy atributů vyžadují nejnižší zabezpečení, příkladem je atribut `commonName`.
 - **Sensitive** - citlivé třídy atributů vyžadují průměrnou úroveň zabezpečení, příkladem může být `homePhone`.
 - **Critical** - kritické třídy atributů vyžadují nejvyšší zabezpečení, jako příklad může sloužit atribut `userpassword`.
 - **System** - systémové atributy jsou atributy pouze ke čtení, které spravuje server.
 - **Restricted** - omezené atributy se používají k definování řízení přístupu.

Ke každé třídě zabezpečení jsou přiřazena určitá povolení.

- **Read** - subjekt může číst atributy.
- **Write** - subjekt může zapisovat atributy
- **Search** - subjekt může vyhledávat atributy.
- **Compare** - subjekt může porovnávat atributy.

Klepnutím na **OK** se vrátíte zpět na kartu Effective ACLs.

Klepnutím na **Cancel** se vrátíte zpět do dialogového okna Edit ACL.

Efektivní vlastníci

Efektivní vlastníci jsou explicitní a zdědění vlastníci vybraného záznamu.

Nefiltrované seznamy ACL

Do záznamu můžete přidávat nové nefiltrované seznamy ACL nebo můžete editovat existující nefiltrované seznamy ACL.

Nefiltrované seznamy ACL lze propagovat. To znamená, že informace o řízení přístupu definované pro jeden záznam mohou být použity pro všechny z jeho podřízených záznamů. Zdroj ACL je zdroj aktuálního seznamu ACL pro vybraný záznam. Jestliže záznam nemá žádný seznam ACL, dědí seznam ACL od nadřazených objektů na základě nastavení seznamu ACL nadřazených objektů.

Na kartě **Non-filtered** seznamů ACL zadejte tyto informace:

- Propagate ACLs - Výběrem zaškrtnutí políčka **Propagate** umožníte podřízeným záznamům bez explicitně definovaných seznamů ACL dědit z tohoto záznamu. Jestliže je toto zaškrtnuté políčko vybráno, podřízené záznamy dědí seznamy ACL z tohoto záznamu a pokud je seznam ACL pro podřízený záznam explicitně definován, seznam ACL, který byl zděděn od nadřazeného záznamu, je nahrazen novým seznamem ACL, který byl přidán. Pokud toto zaškrtnuté políčko není vybráno, podřízené záznamy bez explicitně definovaných seznamů ACL převezmou seznamy ACL od takového záznamu nadřazeného tomuto záznamu, který má tuto volbu aktivovanou.
- DN (Distinguished Name) - Zadejte **DN (rozlišovací jméno)** subjektu požadujícího přístup k provedení operaci na vybraném záznamu, například cn=Marketing Group.
- Type - Zadejte **Typ** jména DN. Například pokud DN je uživatel, vyberte access-id.

Přidávání a editace přístupových práv

Klepněte buď na tlačítko **Add**, chcete-li přidat DN v poli DN (Distinguished Name) do seznamu ACL, nebo na tlačítko **Edit**, chcete-li měnit seznamy ACL existujícího jména DN.

Dialogová okna **Add access rights** a **Edit access rights** umožňují nastavovat přístupová práva pro nové nebo stávající seznamy ACL (Access Control List). Předvolenou hodnotou pole **Type** je typ, který jste vybrali v dialogovém okně **Edit ACL**. Pokud přidáte nějaký seznam ACL, předvolená hodnota všech ostatních polí bude prázdná. Jestliže editujete seznam ACL, pole obsahují hodnoty nastavené při poslední změně tohoto seznamu ACL.

Dialogové okno umožňuje:

- Změnit typ seznamu ACL.
- Nastavit práva pro přidávání a mazání.
- Nastavit povolení pro třídy zabezpečení.

Nastavení přístupových práv:

1. Vyberte **Type** (typ) záznamu pro seznam ACL. Například pokud DN je uživatel, vyberte access-id.
2. Sekce **Rights** zobrazuje práva subjektu k přidávání nebo mazání.
 - **Add child** uděluje nebo odpírá subjektu právo přidat záznam adresáře pod vybraný záznam.
 - **Delete entry** uděluje nebo odpírá subjektu právo vymazat vybraný záznam.
3. Sekce **Security class** definuje povolení pro třídy atributů. Atributy jsou seskupeny do těchto tříd zabezpečení:
 - **Normal** - normální třídy atributů vyžadují nejnížší zabezpečení, příkladem je atribut commonName.
 - **Sensitive** - citlivé třídy atributů vyžadují průměrnou úroveň zabezpečení, příkladem může být homePhone.
 - **Critical** - kritické třídy atributů vyžadují nejvyšší zabezpečení, jako příklad může sloužit atribut userpassword.
 - **System** - systémové atributy jsou atributy pouze ke čtení, které spravuje server.
 - **Restricted** - omezené atributy se používají k definování řízení přístupu.

Ke každé třídě zabezpečení jsou přiřazena určitá povolení.

- Read - subjekt může číst atributy.
- Write - subjekt může měnit atributy.
- Search - subjekt může vyhledávat atributy.
- Compare - subjekt může porovnávat atributy.

Kromě toho můžete zadat povolení na základě atributu namísto třídy zabezpečení, ke které daný atribut přísluší. Sekce atributů je uvedena v seznamu pod **Critical security class**.

- Z rozbalovacího seznamu **Define an attribute** vyberte příslušný atribut.
- Klepněte na **Define**. Atribut se zobrazí s tabulkou povolení.
- Pro každé ze čtyř povolení tříd zabezpečení přiřazených k danému atributu určete, zda se má udělit nebo odeprít.
- Tento postup můžete opakovat pro všechny požadované atributy.
- Chcete-li nějaký atribut odstranit, jednoduše atribut tento vyberte a klepněte na **Delete**.

- Po dokončení klepněte na **OK**.

Odstraňování seznamů ACL

Seznamy ACL lze odstraňovat kterýmukoli z těchto dvou způsobů:

- Vyberte přepínač vedle seznamu ACL, který chcete vymazat. Klepněte na tlačítko **Remove**.
- Klepnutím na **Remove all** vymažete všechna jména DN ze seznamu.

Filtrované seznamy ACL

Do záznamu můžete přidávat nové filtrované seznamy ACL nebo v něm můžete editovat existující filtrované seznamy ACL.

Seznamy ACL na základě filtru uplatňují porovnávání založené na filtru, přičemž využívají zadaný filtr objektu k nalezení odpovídajících cílových objektů s efektivním přístupem, který pro ně platí.

Standardním chováním seznamů ACL založených na filtru je akumulovat se od nejnižšího obsahujícího záznamu vzhůru podél řetězce nadřazených záznamů až po nejvyšší obsahující záznam v DIT. Efektivní přístup se počítá jako souhrn udělených nebo odepřených přístupových práv podle zúčastněných nadřazených záznamů. Z tohoto chování existuje výjimka. Z důvodu kompatibility s funkcí replikace podstromu a s cílem umožnit lepší řízení administrace se jako prostředku k zastavení akumulace v záznamu, v němž je obsažen, používá atribut dovoleného maxima.

Na kartě Filtered ACLs zadejte tyto informace:

- Accumulate filtered ACLs (akumulovat filtrované seznamy ACL).
 - Výběrem přepínače **Not specified** odstraníte atribut `ibm-filterACLInherit` z vybraného záznamu.
 - Výběrem přepínače **True** umožníte seznamům ACL pro vybraný záznam akumulovat se z tohoto záznamu vzhůru podél řetězce nadřazených záznamů až po nejvyšší filtrovaný seznam ACL obsahující záznam v DIT.
 - Výběrem přepínače **False** zastavíte akumulaci filtrovaných seznamů ACL ve vybraném záznamu.
- DN (Distinguished Name) - Zadejte **DN (rozlišovací jméno)** subjektu požadujícího přístup k provedení operací na vybraném záznamu, například `cn=Marketing Group`.
- Type - Zadejte **Typ** jména DN. Například pokud DN je uživatel, vyberte `access-id`.

Přidávání a editace přístupových práv

Klepněte buď na tlačítko **Add**, chcete-li přidat DN v poli DN (Distinguished Name) do seznamu ACL, nebo na tlačítko **Edit**, chcete-li měnit seznamy ACL existujícího jména DN.

Dialogová okna **Add access rights** a **Edit access rights** umožňují nastavovat přístupová práva pro nové nebo stávající seznamy ACL (Access Control List). Předvolenou hodnotou pole Type je typ, který jste vybrali v dialogovém okně **Edit ACL**. Pokud přidáte nějaký seznam ACL, předvolená hodnota všech ostatních polí bude prázdná. Jestliže editujete seznam ACL, pole obsahují hodnoty nastavené při poslední změně tohoto seznamu ACL.

Dialogové okno umožňuje:

- Změnit typ seznamu ACL.
- Nastavit práva pro přidávání a mazání.
- Nastavit filtr objektu pro filtrované seznamy ACL.
- Nastavit povolení pro třídy zabezpečení.

Nastavení přístupových práv:

1. Vyberte **Type** (typ) záznamu pro seznam ACL. Například pokud DN je uživatel, vyberte `access-id`.
2. Sekce **Rights** zobrazuje práva subjektu k přidávání nebo mazání.
 - **Add child** uděluje nebo odírá subjektu právo přidat záznam adresáře pod vybraný záznam.

- **Delete entry** uděluje nebo odpírá subjektu právo vymazat vybraný záznam.
3. Nastavte filtr objektu pro porovnávání na základě filtru. V poli **Object filter** zadejte požadovaný filtr objektu pro vybraný seznam ACL. Klepnutím na tlačítko **Edit filter** vyvoláte pomoc při sestavování řetězce filtru hledání. Aktuální filtrovaný seznam ACL se propaguje na jakýkoli podřízený objekt v přiřazeném podstromu, který odpovídá filtru v tomto poli.
 4. Sekce **Security class** definuje povolení pro třídy atributů. Atributy jsou seskupeny do těchto tříd zabezpečení:
 - **Normal** - normální třídy atributů vyžadují nejnižší zabezpečení, příkladem je atribut commonName.
 - **Sensitive** - citlivé třídy atributů vyžadují průměrnou úroveň zabezpečení, příkladem může být homePhone.
 - **Critical** - kritické třídy atributů vyžadují nejvyšší zabezpečení, jako příklad může sloužit atribut userpassword.
 - **System** - systémové atributy jsou atributy pouze ke čtení, které spravuje server.
 - **Restricted** - omezené atributy se používají k definování řízení přístupu.

Ke každé třídě zabezpečení jsou přiřazena určitá povolení.

- Read - subjekt může číst atributy.
- Write - subjekt může měnit atributy.
- Search - subjekt může vyhledávat atributy.
- Compare - subjekt může porovnávat atributy.

Kromě toho můžete zadat povolení na základě atributu namísto třídy zabezpečení, ke které daný atribut přísluší. Sekce atributů je uvedena v seznamu pod **Critical security class**.

- Z rozbalovacího seznamu **Define an attribute** vyberte příslušný atribut.
- Klepněte na **Define**. Atribut se zobrazí s tabulkou povolení.
- Pro každé ze čtyř povolení tříd zabezpečení přiřazených k danému atributu určete, zda se má udělit nebo odepřít.
- Tento postup můžete opakovat pro všechny požadované atributy.
- Chcete-li nějaký atribut odstranit, jednoduše atribut tento vyberte a klepněte na **Delete**.
- Po dokončení klepněte na **OK**.

Odstraňování seznamů ACL

Seznamy ACL lze odstraňovat kterýmkoli z těchto dvou způsobů:

- Vyberte přepínač vedle seznamu ACL, který chcete vymazat. Klepněte na tlačítko **Remove**.
- Klepnutím na **Remove all** vymažete všechna jména DN ze seznamu.

Vlastníci

Vlastníci záznamů mají úplná povolení k provádění jakékoli operace na daném objektu. Vlastníci záznamů mohou být explicitní nebo propagovaní (zdeděnění).

Na kartě **Owners** zadejte tyto informace:

- Výběrem zaškrtnutí políčka **Propagate owners** umožníte podřízeným záznamům bez explicitně definovaného vlastníka dědit z tohoto záznamu. Pokud toto zaškrtnuté políčko není vybráno, podřízené záznamy bez explicitně definovaného vlastníka převezmou vlastníka od takového záznamu nadřazeného tomuto záznamu, který má tuto volbu aktivovanou.
- DN (Distinguished Name) - Zadejte **DN (rozlišovací jméno)** subjektu požadujícího přístup k provedení operaci na vybraném záznamu, například cn=Marketing Group.
Použití cn=this u objektů, které propagují svoje vlastnictví na jiné objekty, usnadňuje vytvoření takového podstromu adresáře, v němž je každý objekt svým vlastním vlastníkem.
- Type - Zadejte **Typ** jména DN. Například pokud DN je uživatel, vyberte access-id.

Přidávání vlastníka

Klepnutím na **Add** přidáte jméno DN v poli **DN (Distinguished Name)** do příslušného seznamu.

Odstraňování vlastníka

Vlastníka lze odstraňovat kterýmkoli z těchto dvou způsobů:

- Vyberte přepínač vedle DN vlastníka, kterého chcete odstranit ze seznamu. Klepněte na tlačítko **Remove**.
- Klepnutím na **Remove all** vymažete ze seznamu jména DN všech vlastníků.

Kapitola 8. Odkazy

Další referenční informace najdete v těchto částech:

- “Obslužné programy pro příkazový řádek”
- “LDAP data interchange format (LDIF)” na stránce 216
- “Schéma konfigurace serveru adresářů” na stránce 219
- “Identifikátory objektů (OID)” na stránce 259

Obslužné programy pro příkazový řádek

Tato část popisuje obslužné programy, které lze spustit z prostředí příkazů Qshell operačního systému i5/OS. Další informace o jednotlivých příkazech najdete v těchto tématech:

- “ldapmodify a ldapadd”
- “ldapdelete” na stránce 191
- “ldapexpop” na stránce 194
- “ldapmodrdrn” na stránce 199
- “ldapsearch” na stránce 202
- “ldapchangepwd” na stránce 211
- “ldapdiff” na stránce 213
- “Jak používat SSL s obslužnými programy příkazového řádku LDAP” na stránce 216

Povšimněte si, že pokud mají být některé řetězce správně zpracovány v prostředí příkazů Qshell, musí být uzavřeny v uvozovkách. To se všeobecně týká řetězců, které představují jména DN, filtry hledání a seznam atributů, které se mají vrátit z příkazu ldapsearch. Některé příklady najdete v tomto seznamu:

- Řetězce, které obsahují mezery: "cn=John Smith,cn=users".
- Řetězce, které obsahují zástupné znaky: "*".
- Řetězce, které obsahují závorky: "(objectclass=person)".

Další informace o prostředí příkazů Qshell najdete v tématu “Qshell”.

ldapmodify a ldapadd

Nástroje pro modifikaci a přidávání záznamů LDAP

Přehled

```
ldapmodify [-a] [-b] [-c] [-C charset] [-d debuglevel] [-D binddn] [-g]
[-f file] [-F] [-g] [-G realm] [-h ldaphost] [-i file] [-k] [-K keyfile]
[-m mechanism] [-M] [-n] [-N certificatename] [-O maxhops] [-p ldapport]
[-P keyfilepw] [-r] [-R] [-U username] [-v] [-V] [-w passwd | ?] [-y proxydn]
[-Y] [-Z]
```

```
ldapadd [-a] [-b] [-c] [-C charset] [-d debuglevel] [-D binddn] [-g]
[-f file] [-F] [-g] [-G realm] [-h ldaphost] [-i file] [-k] [-K keyfile]
[-m mechanism] [-M] [-n] [-N certificatename] [-O maxhops] [-p ldapport]
[-P keyfilepw] [-r] [-R] [-U username] [-v] [-V] [-w passwd | ?] [-y proxydn]
[-Y] [-Z]
```

Popis

ldapmodify je rozhraní příkazového řádku pro rozhraní API (application programming interfaces) příkazů `ldap_modify`, `ldap_add`, `ldap_delete` a `ldap_modrdn`. Příkaz **ldapadd** je začleněn jako přejmenovaná verze příkazu `ldapmodify`. Když je vyvolán jako `ldapadd`, automaticky se zapne příznak **-a** (přidání nového záznamu).

ldapmodify otevírá propojení k serveru LDAP a připojuje se k serveru. Příkaz **ldapmodify** se používá ke změně nebo přidávání záznamů. Informace o záznamu se čtou ze standardního vstupu nebo ze souboru s využitím volby **-i**.

Chcete-li zobrazit nápovědu k syntaxi příkazů **ldapmodify** nebo **ldapadd**, napište

```
ldapmodify -?
```

nebo

```
ldapadd -?
```

Volby

-a Přidává nové záznamy. Předvolená akce pro příkaz **ldapmodify** je změna existujících záznamů. Pokud je vyvolán jako **ldapadd**, je tento příznak vždy nastaven.

-b Předpokládá, že všechny hodnoty začínající ``/`` jsou binární hodnoty a že skutečná hodnota je v souboru, jehož cesta je uvedena namísto hodnoty.

-c Nepřerušovaný operační režim. Chyby jsou oznamovány, ale program **ldapmodify** pokračuje v modifikacích. V ostatních případech je jako standardní činnost nastaveno ukončení programu po zaznamenání chyby.

-C charset

Specifikuje, že řetězce, které jsou dodávány jako vstup do programů **ldapmodify** a **ldapadd**, jsou znázorněny v lokální znakové sadě tak, jak je určeno volbou `charset` a musí se konvertovat na kódování UTF-8. Volba **-C charset** se používá tehdy, když je kódová stránka vstupního řetězce odlišná od hodnoty kódové stránky úlohy. Podporované hodnoty volby `charset` najdete v API `ldap_set_iconv_local_charset()`.

-d debuglevel

Nastavuje úroveň ladění LDAP na `debuglevel`.

-D binddn

Hodnota **binddn** se používá k připojení k adresáři LDAP. Hodnotou parametru **binddn** je řetězec vyjadřující jméno DN. Při použití s parametrem `-m DIGEST-MD5` se používá pro zadání ID autorizace. Může to být buď DN nebo řetězec `authId` začínající `"u:"` nebo `"dn:"`.

-f file Čte informace o změně záznamu ze souboru LDIF namísto ze standardního vstupu. Není-li soubor LDIF zadán, musíte pomocí standardního vstupu zadat aktualizované záznamy ve formátu LDIF.

-F Vynutí aplikaci všech změn bez ohledu na obsah řádků vstupu, které začínají replikou (předvoleně, replika: řádky se porovnávají proti používanému hostiteli a portu LDAP serveru, aby se rozhodlo, zda by se měl skutečně aplikovat záznam protokolu replikace).

-g Neodstraňuje koncové mezery v hodnotách atributů.

-G Zadejte sféru. Tento parametr je volitelný. Při použití s parametrem `-m DIGEST-MD5` se tato hodnota postupuje na server během připojování.

-h ldaphost

Určuje alternativního hostitele, na kterém je spuštěn server `ldap`.

-i file Čte informace o změně záznamu ze souboru LDIF namísto ze standardního vstupu. Není-li soubor LDIF zadán, musíte pomocí standardního vstupu zadat aktualizované záznamy ve formátu LDIF.

-k Určuje, že se má používat administrační řízení serveru.

-K keyfile

Specifikuje jméno souboru databáze klíčů SSL s předvolenou příponou **kdb**. Není-li soubor databáze klíčů umístěn v aktuálním adresáři, zadejte plně kvalifikované jméno souboru databáze klíčů. V případě, že soubor

databáze klíčů není určen, tento program nejprve hledá přítomnost proměnné prostředí SSL_KEYRING s přiřazeným jménem souboru. Jestliže proměnná prostředí SSL_KEYRING není definována, použije se systémový soubor klíčového řetězce, pokud existuje.

Tento parametr účinně aktivuje přepínač **-Z**. Pokud u serveru adresářů v operačním systému i5/OS použijete volbu **-Z** a nepoužijete volbu **-K** nebo **-N**, použije se certifikát přiřazený k ID aplikace klienta adresářových služeb.

-m *mechanism*

Hodnota **mechanism** specifikuje mechanismus SSL, kterým se klient připojuje k serveru. Použije se API `ldap_sasl_bind_s()`. Parametr **-m** se ignoruje v případě, že je nastaven parametr **-V 2**. Pokud parametr **-m** není určen, použije se jednoduchá autentizace. Platné mechanismy jsou tyto:

- CRAM-MD5 - provádí ochranu hesla odesílaného na server.
- EXTERNAL - používá certifikát SSL. Vyžaduje volbu **-Z**.
- GSSAPI - používá pověření Kerberos uživatele.
- DIGEST-MD5 - vyžaduje, aby klient odeslal na serveru hodnotu `username`. Vyžaduje volbu **-U**. Pro specifikaci ID autorizace se používá parametr **-D** (obvykle připojovací DN). Může to být buď DN nebo řetězec `authzId` začínající `u:` nebo `dn:`.
- OS400_PRFTKN - autentizuje se na lokální LDAP server jako aktuální uživatel i5/OS používající DN uživatele v proceduře backend projektované systémem. Parametry **-D** (připojovací DN) and **-w** (heslo) by neměly být zadány.

-M Referenční objekty jsou spravovány jako řádné záznamy.

-n Zobrazuje, co by se provedlo, ale záznamy se ve skutečnosti nemění. Ve spojení s parametrem **-v** lze využít při ladění.

-N *certificatename*

Specifikuje návěští asociované s certifikátem klienta v souboru databáze klíčů. Jestliže je server LDAP konfigurován pouze pro provádění autentizace serveru, certifikát klienta není povinný. Je-li server LDAP konfigurován pro provádění autentizace klienta i serveru, certifikát klienta povinný být může. Parametr **certificatename** není povinný, pokud byl pro soubor databáze klíčů jako předvolený označen určitý pár certifikát/soukromý klíč. Podobně není parametr **certificatename** povinný, jestliže v označeném souboru databáze klíčů existuje jediný pár certifikát/soukromý klíč. Tento parametr se ignoruje v případě, že není zadán ani jeden z parametrů **-Z** a **-K**. Pokud u serveru adresářů v operačním systému i5/OS použijete volbu **-Z** a nepoužijete volbu **-K** nebo **-N**, použije se certifikát přiřazený k ID aplikace klienta adresářových služeb.

-O *maxhops*

Hodnota **maxhops** se používá pro nastavení maximálního počtu přechodů, které knihovna klienta vykoná při vyhledávání odkazů. Předvolená hodnota pro počet přechodů je 10.

-p *ldapport*

Specifikuje alternativní port TCP (Transmission Control Protocol), na kterém server LDAP naslouchá. Předvolený port LDAP je 389. Není-li port **-p** specifikován a přitom je zadán parametr **-Z**, použije se předvolený port LDAP SSL 636.

-P *keyfilepw*

Specifikuje heslo pro databázi klíčů. Toto heslo je povinné pro přístup ke kódovaným informacím v souboru databáze klíčů, který může obsahovat jeden nebo více soukromých klíčů. Je-li se souborem databáze klíčů asociován soubor pro uložení hesla, získá se heslo ze souboru pro uložení hesla a parametr **-P** není povinný. Tento parametr se ignoruje v případě, že není zadán ani jeden z parametrů **-Z** a **-K**.

-r Standardně přepisuje existující hodnoty.

-R Specifikuje, že se odkazy nemají automaticky sledovat.

-U Zadejte `username`. Vyžaduje se při použití parametru **-m** DIGEST-MD5, u jiných mechanismů se ignoruje.

-v Používá komentovaný režim s mnoha diagnostickými zprávami zapsanými do standardního výstupu.

-V version

Určuje verzi LDAP, kterou má program **ldapmodify** používat při připojování k serveru LDAP. Standardně se nastavuje připojení LDAP V3. Chcete-li explicitně vybrat LDAP V3, zadejte **-V 3**. Chcete-li spustit aplikaci LDAP V2, zadejte **-V 2**.

-w passwd | ?

Hodnota **passwd** je heslo pro autentizaci. Parametr **?** se používá, chcete-li vytvořit výzvu k zadání hesla.

| -y proxydn

| Nastavuje proxy ID pro volbu proxy autorizace.

| -Y Použije zabezpečené spojení LDAP (TLS).

-Z Ke komunikaci se serverem LDAP se použije připojení přes SSL. Pokud u serveru adresářů v operačním systému i5/OS použijete volbu **-Z** a nepoužijete volbu **-K** nebo **-N**, použije se certifikát přiřazený k ID aplikace klienta adresářových služeb.

Vstupní formát

Obsah souboru (nebo standardního vstupu, pokud na příkazovém řádku není zadán příznak **-i**) by měl odpovídat formátu LDIF. Více informací o formátu LDIF najdete v tématu "LDAP data interchange format (LDIF)" na stránce 216.

Příklady

Předpokládáme, že existuje soubor /tmp/entrymods, který má tento obsah:

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

potom příkaz:

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

nahradí obsah atributu pošty záznamu Modify Me hodnotou modme@student.of.life.edu, přidá titul Grand Poobah a obsah souboru /tmp/modme.jpeg jako jpegPhoto a zcela odstraní atribut popisu. Tytéž modifikace je možné provést s použitím staršího vstupního 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
```

apříkladu:

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

Předpokládáme, že existuje soubor /tmp/newentry, který má tento obsah:

```
dn: cn=John Doe, o=University of Higher Learning, c=US
objectClass: person
cn: John Doe
cn: Johnny
```



```
sn: Doe
titul: Nejslavnější bájná postava na světě
mail: johndoe@student.of.life.edu
uid: jdoe
```

potom příkaz:

```
ldapadd -i /tmp/entrymods
```

přidá nový záznam pro osobu jménem John Doe s použitím hodnot ze souboru /tmp/newentry.

Poznámky

Pokud nejsou ze souboru dodány informace prostřednictvím volby **-i**, příkaz **ldapmodify** bude očekávat načtení záznamů ze standardního vstupu.

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.

ldapdelete

Nástroj LDAP pro vymazání záznamu

Přehled

```
ldapdelete [-c] [-C charset] [-d debuglevel] [-D binddn] [-f file]
[-G realm] [-h ldaphost] [-i file] [-k] [-K keyfile] [-m mechanism]
[-M] [-n] [-N certificatename] [-O maxops] [-p ldapport]
[-P keyfilepw] [-R] [-s] [-U username] [-v] [-V version]
[-w passwd | ?] [-y proxydn] [-Y] [-Z] [dn].....
```

Popis

ldapdelete je rozhraní příkazového řádku pro rozhraní API (application programming interfaces) příkazu `ldap_delete`.

ldapdelete otevře propojení k serveru LDAP, připojí se a vymaže jeden nebo více záznamů. Jestliže se zadá jeden nebo více argumentů s DN (rozlišovací jmény), vymažou se záznamy s těmito DN. Každé DN je řetězcové vyjádření jména DN. Jestliže není zadán žádný argument pro DN, čte se seznam jmen DN ze standardního vstupu nebo v případě použití příznaku **-i** ze souboru.

Chcete-li zobrazit nápovědu k syntaxi příkazu **ldapdelete**, napište:

```
ldapdelete -?
```

Volby

-c Nepřerušovaný operační režim. Chyby jsou oznamovány, ale program **ldapdelete** pokračuje v odstraňování záznamů. V ostatních případech je jako standardní činnost nastaveno ukončení programu po zaznamenání chyby.

-C charset

Specifikuje, že rozlišovací jména (DN), která jsou poskytnuta jako vstup do programu **ldapdelete**, jsou vyjádřena v lokální znakové sadě tak, jak je určeno volbou `charset`. Volba **-C charset** se používá tehdy, když je kódová stránka vstupního řetězce odlišná od hodnoty kódové stránky úlohy. Podporované hodnoty volby `charset` najdete v API `ldap_set_iconv_local_charset()`.

-d debuglevel

Nastavuje úroveň ladění LDAP na `debuglevel`.

-D binddn

Hodnota **binddn** se používá k připojení k adresáři LDAP. Hodnotou parametru **binddn** je řetězec vyjadřující jméno DN. Při použití s parametrem **-m DIGEST-MD5** se používá pro zadání ID autorizace. Může to být buď DN nebo řetězec authzId začínající "u:" nebo "dn:".

-f file Čte sérii řádek ze souboru a pro každou řádku souboru provede jeden výmaz LDAP. Každá řádka v tomto souboru by měla obsahovat jedno rozlišovací jméno (DN).

-G realm

Zadejte sféru. Tento parametr je volitelný. Při použití s parametrem **-m DIGEST-MD5** se tato hodnota postupuje na server během připojování.

-h ldaphost

Specifikuje alternativního hostitele, na kterém je spuštěn server LDAP.

-i file Čte sérii řádek ze souboru a pro každou řádku souboru provede jeden výmaz LDAP. Každá řádka v tomto souboru by měla obsahovat jedno rozlišovací jméno (DN).

-k Určuje, že se má používat administrační řízení serveru.

-K keyfile

Specifikuje jméno souboru databáze klíčů SSL. Není-li soubor databáze klíčů umístěn 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 se rovněž označují jako důvěryhodné zdroje.

Tento parametr účinně aktivuje přepínač **-Z**. Pokud u serveru adresářů v operačním systému i5/OS použijete volbu **-Z** a nepoužijete volbu **-K** nebo **-N**, použije se certifikát přiřazený k ID aplikace klienta adresářových služeb.

-m mechanism

Hodnota **mechanism** specifikuje mechanismus SSL, kterým se klient připojuje k serveru. Použije se API ldap_sasl_bind_s(). Parametr **-m** se ignoruje v případě, že je nastaven parametr **-V 2**. Pokud parametr **-m** není určen, použije se jednoduchá autentizace. Platné mechanismy jsou tyto:

- CRAM-MD5 - provádí ochranu hesla odesílaného na server.
- EXTERNAL - používá certifikát SSL. Vyžaduje volbu **-Z**.
- GSSAPI - používá pověření Kerberos uživatele.
- DIGEST-MD5 - vyžaduje, aby klient odeslal na serveru hodnotu username. Vyžaduje volbu **-U**. Pro specifikaci ID autorizace se používá parametr **-D** (obvykle připojovací DN). Může to být buď DN nebo řetězec authzId začínající u: nebo dn:.
- OS400_PRFTKN - autentizuje se na lokální LDAP server jako aktuální uživatel i5/OS používající DN uživatele v proceduře backend projektované systémem. Parametry **-D** (připojovací DN) and **-w** (heslo) by neměly být zadány.

-M Referenční objekty jsou spravovány jako řádné záznamy.

-n Zobrazuje, co by se provedlo, ale záznamy se ve skutečnosti nemění. Tento parametr ve spojení s parametrem **-v** lze využít k ladění.

-N certificatename

Specifikuje návěští asociované s certifikátem klienta v souboru databáze klíčů. Jestliže je server LDAP konfigurován pouze pro provádění autentizace serveru, certifikát klienta není povinný. Je-li server LDAP konfigurován pro provádění autentizace klienta i serveru, certifikát klienta povinný být může. Parametr **certificatename** není povinný, pokud byl pro soubor databáze klíčů jako předvolený označen určitý pár certifikát/soukromý klíč. Podobně není parametr **certificatename** povinný, jestliže v označeném souboru databáze klíčů existuje jediný pár certifikát/soukromý klíč. Tento parametr se ignoruje v případě, že není zadán ani jeden z parametrů **-Z** a **-K**. Pokud u serveru adresářů v operačním systému i5/OS použijete volbu **-Z** a nepoužijete volbu **-K** nebo **-N**, použije se certifikát přiřazený k ID aplikace klienta adresářových služeb.

- O maxhops**
Hodnota *maxhops* se používá pro nastavení maximálního počtu přechodů, které knihovna klienta vykoná při vyhledávání odkazů. Předvolená hodnota pro počet přechodů je 10.
- p ldapport**
Specifikuje alternativní port TCP (Transmission Control Protocol), na kterém server LDAP naslouchá. Předvolený port LDAP je 389. Není-li port **-p** specifikován a přitom je zadán parametr **-Z**, použije se předvolený port LDAP SSL 636.
- P keyfilepw**
Specifikuje heslo pro databázi klíčů. Toto heslo je povinné pro přístup ke kódovaným informacím v souboru databáze klíčů, který může obsahovat jeden nebo více soukromých klíčů. Je-li se souborem databáze klíčů asociován soubor pro uložení hesla, získá se heslo ze souboru pro uložení hesla a parametr **-P** není povinný. Tento parametr se ignoruje v případě, že není zadán ani jeden z parametrů **-Z** a **-K**.
- R**
Specifikuje, že se odkazy nemají automaticky sledovat.
- s**
Tato volba se používá pro vymazání podstromu s kořenem v určeném záznamu.
- U username**
Zadejte username. Vyžaduje se při použití parametru **-m DIGEST-MD5**, u jiných mechanismů se ignoruje.
- v**
Používá komentovaný režim s mnoha diagnostickými zprávami zapsanými do standardního výstupu.
- V version**
Určuje verzi LDAP, kterou má program **ldapdelete** používat při připojování k serveru LDAP. Standardně se ustavuje připojení LDAP V3. Chcete-li explicitně vybrat LDAP V3, zadejte **-V 3**. Chcete-li spustit aplikaci LDAP V2, zadejte **-V 2**.
- w passwd | ?**
Hodnota *passwd* je heslo pro autentizaci. Parametr **?** se používá, chcete-li vytvořit výzvu k zadání hesla.
- y proxydn**
Nastavuje proxy ID pro operaci proxy autorizace.
- Y**
Použije zabezpečené spojení LDAP (TLS).
- Z**
Ke komunikaci se serverem LDAP se použije připojení přes SSL. Pokud u serveru adresářů v operačním systému i5/OS použijete volbu **-Z** a nepoužijete volbu **-K** nebo **-N**, použije se certifikát přiřazený k ID aplikace klienta adresářových služeb.
- dn**
Specifikuje jeden nebo více argumentů DN. Každé DN by mělo být řetězcové vyjádření jména DN.

Příklady

Příkaz

```
ldapdelete -D cn=administrator -w secret "cn=Delete Me, o=University of Life, c=US"
```

se pokusí vymazat záznam, který má commonName "Delete Me" a nachází se přímo pod organizačním záznamem University of Life.

Poznámky

Jestliže není zadán žádný argument pro DN, čte se seznam jmen DN ze standardního vstupu nebo v případě použití příznaku **-i** ze souboru.

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.

Ldapexop

Nástroj přídatných operací LDAP

Přehled

```
ldapexop [-C charset] [-d debuglevel] [-D binddn] [-e] [-G realm]
[-h ldaphost] [-help] [-K keyfile] [-m mechanism] [-N certificatename]
[-p ldapport] [-P keyfilepw] [-?] [-U] [-v] [-w passwd | ?] [-Y] [-Z]
-op {cascrepl | controlqueue | controlrepl | getAttributes |
getusertype | quiesce | readconfig | uniqueattr}
```

Popis

Utilita **ldapexop** je rozhraní příkazového řádku, které poskytuje možnost připojit se k serveru adresářů a zveřejnit jedinou přídatnou operaci spolu s jakýmkoli daty, která tvoří hodnotu přídatné operace.

Program **ldapexop** podporuje volby standardního hostitele, portu, SSL a autentizace, používané všemi klientskými obslužnými programy LDAP. Kromě toho se definuje sada voleb pro určení operací, které se mají provést, a argumenty pro každou přídatnou operaci

Chcete-li zobrazit nápovědu k syntaxi příkazu **ldapexop**, napište:

```
ldapexop -?
```

nebo

```
ldapexop -help
```

Volby

Volby pro příkaz **ldapexop** jsou rozděleny do dvou kategorií:

1. Obecné volby, které určují způsob připojení k serveru adresářů. Tyto volby se musí zadávat před volbami specifickými pro danou operaci.
2. Volba přídatné operace, která označuje přídatnou operaci, která se má provést.

Obecné volby

Tyto volby určují způsob připojení k serveru adresářů a je nutné je zadávat před volbou **-op**.

-C *charset*

Specifikuje, že rozlišovací jména (DN), která jsou poskytnuta jako vstup do programu **ldapexop** jsou vyjádřena v lokální znakové sadě tak, jak je určeno volbou *charset*. Volba **-C** *charset* se používá tehdy, když je kódová stránka vstupního řetězce odlišná od hodnoty kódové stránky úlohy. Podporované hodnoty volby *charset* najdete v API `ldap_set_iconv_local_charset()`.

-d *debuglevel*

Nastavuje úroveň ladění LDAP na *debuglevel*.

-D *binddn*

Hodnota *binddn* se používá k připojení k adresáři LDAP. Hodnotou parametru *binddn* je řetězec vyjadřující jméno DN. Při použití s parametrem **-m** DIGEST-MD5 se používá pro zadání ID autorizace. Může to být buď DN nebo řetězec `authzId` začínající "u:" nebo "dn:".

-e Zobrazí informace o verzi knihovny LDAP a potom ukončí činnost.

-G Zadejte sféru. Tento parametr je volitelný. Při použití s parametrem **-m** DIGEST-MD5 se tato hodnota postupuje na server během připojování.

-h *ldaphost*

Specifikuje alternativního hostitele, na kterém je spuštěn server LDAP.

-help Zobrazí syntaxi příkazu a informace o použití.

-K *keyfile*

Specifikuje jméno souboru databáze klíčů SSL. Není-li soubor databáze klíčů umístěn 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 se rovněž označují jako důvěryhodné zdroje.

Tento parametr účinně aktivuje přepínač **-Z**. Pokud u serveru adresářů v operačním systému i5/OS použijete volbu **-Z** a nepoužijete volbu **-K** nebo **-N**, použije se certifikát přiřazený k ID aplikace klienta adresářových služeb.

-m *mechanism*

Hodnota *mechanism* specifikuje mechanismus SSL, kterým se klient připojuje k serveru. Použije se API `ldap_sasl_bind_s()`. Parametr **-m** se ignoruje v případě, že je nastaven parametr **-V 2**. Pokud parametr **-m** není určen, použije se jednoduchá autentizace. Platné mechanismy jsou tyto:

- CRAM-MD5 - provádí ochranu hesla odesílaného na server.
- EXTERNAL - používá certifikát SSL. Vyžaduje volbu **-Z**.
- GSSAPI - používá pověření Kerberos uživatele.
- DIGEST-MD5 - vyžaduje, aby klient odeslal na serveru hodnotu `username`. Vyžaduje volbu **-U**. Pro specifikaci ID autorizace se používá parametr **-D** (obvykle přípojovací DN). Může to být buď DN nebo řetězec `authzId` začínající u: nebo `dn:`.
- OS400_PRFTKN - autentizuje se na lokální LDAP server jako aktuální uživatel i5/OS používající DN uživatele v proceduře backend projektované systémem. Parametry **-D** (přípojovací DN) and **-w** (heslo) by neměly být zadány.

-N *certificatename*

Specifikuje návěští asociované s certifikátem klienta v souboru databáze klíčů. Jestliže je server LDAP konfigurován pouze pro provádění autentizace serveru, certifikát klienta není povinný. Je-li server LDAP konfigurován pro provádění autentizace klienta i serveru, certifikát klienta povinný být může. Parametr *certificatename* není povinný, pokud byl pro soubor databáze klíčů jako předvolený označen určitý pár certifikát/soukromý klíč. Podobně není parametr *certificatename* povinný, jestliže v označeném souboru databáze klíčů existuje jediný pár certifikát/soukromý klíč. Tento parametr se ignoruje v případě, že není zadán ani jeden z parametrů **-Z** a **-K**. Pokud u serveru adresářů v operačním systému i5/OS použijete volbu **-Z** a nepoužijete volbu **-K** nebo **-N**, použije se certifikát přiřazený k ID aplikace klienta adresářových služeb.

-p *ldapport*

Specifikuje alternativní port TCP (Transmission Control Protocol), na kterém server LDAP naslouchá. Předvolený port LDAP je 389. Není-li port **-p** specifikován a přitom je zadán parametr **-Z**, použije se předvolený port LDAP SSL 636.

-P *keyfilepw*

Specifikuje heslo pro databázi klíčů. Toto heslo je povinné pro přístup ke kódovaným informacím v souboru databáze klíčů, který může obsahovat jeden nebo více soukromých klíčů. Je-li se souborem databáze klíčů asociován soubor pro uložení hesla, získá se heslo ze souboru pro uložení hesla a parametr **-P** není povinný. Tento parametr se ignoruje v případě, že není zadán ani jeden z parametrů **-Z** a **-K**.

-? Zobrazí syntaxi příkazu a informace o použití.

-U Zadejte `username`. Vyžaduje se při použití parametru **-m** DIGEST-MD5, u jiných mechanismů se ignoruje.

-v Používá komentovaný režim s mnoha diagnostickými zprávami zapsanými do standardního výstupu.

-w *passwd* | ?

Hodnota *passwd* je heslo pro autentizaci. Parametr `?` se používá, chcete-li vytvořit výzvu k zadání hesla.

-Y Použije zabezpečené spojení LDAP (TLS).

- Z Ke komunikaci se serverem LDAP se použije připojení přes SSL. Pokud u serveru adresářů v operačním systému i5/OS použijete volbu -Z a nepoužijete volbu -K nebo -N, použije se certifikát přiřazený k ID aplikace klienta adresářových služeb.

Volba přídavných operací

Volba přídavné operace **-op** označuje přídavnou operaci, která se má provést. Přídavná operace může být jedna z těchto hodnot:

- **cascrepl**: přídavná operace replikace kaskádového řízení. Požadovaná činnost se aplikuje na určený server a také se předává na všechny repliky daného podstromu. Pokud jsou některé z těchto replik předávací repliky, předávají přídavnou operaci dále na své repliky. Operace se řadí do kaskády přes celou replikační topologii.

-action quiesce | unquiesce | replnow | wait

Toto je povinný atribut, který určuje akci, která se má provést.

quiesce

Nejsou povoleny žádné další aktualizace, s výjimkou aktualizací provedených replikací.

unquiesce

Obnoví normální operaci, klientské aktualizace se přijímají.

replnow

Replikuje všechny změny čekající ve frontě co nejdříve, bez ohledu na časový plán.

wait

Čeká, až se všechny aktualizace replikují na všechny repliky.

-rc contextDn

Toto je povinný atribut, který určuje kořen podstromu.

-timeout secs

Toto je volitelný atribut, který, pokud existuje, určuje dobu časového limitu v sekundách. Pokud neexistuje nebo je-li jeho hodnota 0, operace čeká trvale.

Příklad:

```
ldapexop -op cascrepl -action -quiesce -rc "o=acme,c=us" -timeout 60
```

- **controlqueue**: přídavná operace řízení fronty replikace. Tato operace umožňuje vymazat nebo odstranit ze seznamu replikačních změn nevyřízené změny, které byly zařazeny do fronty a nebyly spuštěny z důvodu selhání replikace. Tato operace je užitečná pro případ manuálních oprav replikačních dat. Po takových opravách byste měli tuto operaci použít k odstranění některých nezdařených operací zařazených do fronty.

-skip all | change-id

Toto je povinný atribut.

- **-skip all** označuje přeskočení všech nevyřízených změn pro toto ujednání.
- **change-id** označuje jedinou změnu, která má být přeskočena. Pokud server v dané době tuto změnu nereplikuje, požadavek selže.

-ra agreementDn

Toto je povinný atribut, který určuje jméno DN ujednání o replikaci.

Příklady:

```
ldapexop -op controlqueue -skip all -ra "cn=server3,  
ibm-replicaSubentry=master1-id,ibm-replicaGroup=default,  
o=acme,c=us"
```

```
ldapexop -op controlqueue -skip 2185 -ra "cn=server3,  
ibm-replicaSubentry=master1-id,ibm-replicaGroup=default,  
o=acme,c=us"
```

- **controlrepl**: přídavná operace řízení replikace

-action suspend | resume | replnow

Toto je povinný atribut, který určuje akci, která se má provést.

-rc contextDn | -ra agreementDn

Parametr **-rc contextDn** je jméno DN kontextu replikace. Akce se provede pro všechna ujednání pro tento kontext. Parametr **-ra agreementDn** je jméno DN ujednání o replikaci. Akce se provede pro specifikované ujednání o replikaci.

Příklad:

```
ldapexop -op controlrepl -action suspend -ra "cn=server3,
        ibm-replicaSubentry=master1-id,ibm-replicaGroup=default,
        o=acme,c=us"
```

- **getattributes -attrType<type> -matches bool<value>**

-attrType {operational | language_tag | attribute_cache | unique | configuration}

Toto je povinný atribut, který určuje typ požadovaného atributu.

-matches bool {true | false}

Udává, zda seznam vrácených atributů má odpovídat typu atributu zadaného ve volbě **-attrType<**

Příklad

```
ldapexop -op getattributes -attrType unique -matches bool true
```

Vrátí seznam všech atributů, které byly označeny jako jedinečné atributy.

```
ldapexop -op getattributes -attrType unique -matches bool false
```

Vrátí seznam všech atributů, které nebyly označeny jako jedinečné atributy.

- **getusertype:** požaduje přídatnou operaci typu uživatele

Tato přídatná operace vrátí typ uživatele na základě připojeného DN.

Příklad:

```
ldapexop - D <AdminDN> -w <Adminpw> -op getusertype
```

vrátí:

```
User : root_administrator
```

```
Role(s) : server_config_administrator directory_administrator
```

- **quiesce:** přídatná operace uvedení do klidu nebo vybudení replikace podstromu.

-rc contextDn

Toto je povinný atribut, který určuje jméno DN kontextu replikace (podstromu), který se má uvést do klidu nebo vybudit.

-end Toto je volitelný atribut, který, pokud existuje, určuje, že se má příslušný podstrom vybudit. Pokud není uveden, předvolenou hodnotou je podstrom uvést do klidu.

Příklady:

```
ldapexop -op quiesce -rc "o=acme,c=us"
```

```
ldapexop -op quiesce -end -rc "o=ibm,c=us"
```

- **readconfig:** přídatná operace nového načtení konfiguračního souboru

-scope entire | single<entry DN><attribute>

Toto je povinný atribut.

— **entire** určuje, že se má znovu načíst celý konfigurační soubor.

— **single** znamená, že se má přečíst jediný záznam a určený atribut.

Příklady:

```
ldapexop -op readconfig -scope entire
```

```
ldapexop -op readconfig -scope single "cn=configuration" ibm-slappAdminPW
```


Poznámka: Níže uvedené záznamy označené:

- ¹ provedou se okamžitě po readconfig
- ² provedou se u nových operací
- ³ provedou se, jakmile se změní heslo (nevyžaduje se žádný readconfig)
- ⁴ jsou podporovány obslužným programem příkazového řádku operačního systému i5/OS, ale nejsou podporovány serverem adresářů v operačním systému

```
cn=Configuration
ibm-slapedadmin2
ibm-slapedadminpw2, 3
ibm-slapederrorlog1, 4
ibm-slapedpwencryption1
ibm-slapedsize1
ibm-slapedsysloglevel1, 4
ibm-slapedtime1
```

```
cn=Front End, cn=Configuration
ibm-slapedaclcache1
ibm-slapedaclcachesize1
ibm-slapedentrycachesize1
ibm-slapedfiltercachebypasslimit1
ibm-slapedfiltercachesize1
ibm-slapedidle1
```

```
cn=Event Notification, cn=Configuration
ibm-slapedmaxeventsperconnection2
ibm-slapedmaxeventstotal2
```

```
cn=Transaction, cn=Configuration
ibm-slapedmaxnumoftransactions2
ibm-slapedmaxoppertransaction2
ibm-slapedmaxtime2
```

```
cn=ConfigDB, cn=Config Backends, cn=IBM SecureWay, cn=Schemas, cn=Configuration
ibm-slapedreadonly2
```

```
cn=Directory, cn=RDBM Backends, cn=IBM SecureWay, cn=Schemas, cn=Configuration
ibm-slapedbulkloaderrors1, 4
ibm-slapedclierrors1, 4
ibm-slapedpagedresallownonadmin2
ibm-slapedpagedres2
ibm-slapedpagesize2
ibm-slapedreadonly2
ibm-slapedsortkey2
ibm-slapedsortsrchallownonadmin2
ibm-slapedsuffix2
```

- **unbind** {-dn<specificDN>| -ip<sourceIP> | -dn<specificDN> -ip<sourceIP> | all}:

odpojí připojení na základě DN, IP, DN/IP nebo odpojí všechna připojení. Všechna připojení bez nějaké operace a všechna připojení s operacemi v pracovní frontě jsou okamžitě ukončena. Pokud pracovník momentálně na připojení pracuje, je spojení ukončeno, jakmile pracovník danou operaci dokončí.

-dn<specificDN>

Vydá požadavek ukončit připojení pouze podle DN. Výsledkem požadavku je odstranění všech spojení připojených na zadané DN.

-ip<sourceIP>

Vydá požadavek ukončit připojení pouze podle IP. Výsledkem požadavku je odstranění všech spojení ze zadaného IP zdroje.

-dn<specificDN> **-ip**<sourceIP>

Vydá požadavek ukončit připojení podle DN/IP. Výsledkem požadavku je odstranění všech spojení připojených na zadané DN a ze zadaného IP zdroje.

-all Vydá požadavek ukončit všechna připojení. Výsledkem požadavku je odstranění všech spojení kromě spojení, ze kterého byl požadavek odeslán. Tento atribut nelze použít s atributy **-D** nebo **-IP**

Příklady:

```
ldapexop -op unbind -dn cn=john
ldapexop -op unbind -ip 9.182.173.43
ldapexop -op unbind -dn cn=john -ip 9.182.173.43
ldapexop -op unbind -all
```

- **uniqueattr -a <attributeType>**: identifikuje všechny nejedinečné hodnoty pro konkrétní atribut.

-a <attribute>

Udává atribut, pro který se zobrazí seznam všech konfliktních hodnot.

Poznámka: Duplicitní hodnoty pro binární atributy, operační atributy, konfigurační atributy a atribut `objectclass` se nezobrazí. Tyto atributy nejsou podporovány přídatnými operacemi pro jedineční atributy.

Příklad:

```
ldapexop -op uniqueattr -a "uid"
```

Pro tuto rozšířenou operaci se přidá následující řádek do konfiguračního souboru pod záznam "cn=Directory,cn=RDBM Backends,cn=IBM Directory,cn=schema,cn=Configuration":

```
ibm-slapdPlugin:extendedop /bin/libback-rdbm.dll initUniqueAttr
```

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.

ldapmodrdn

Nástroj LDAP pro modifikaci záznamu RDN

Přehled

```
ldapmodrdn [-c] [-C charset] [-d debuglevel] [-D binddn]
[-f file] [-G realm] [-h ldaphost] [-i file] [-k] [-K keyfile]
[-m mechanism] [-M] [-n] [-N certificatename] [-O hopcount]
[-p ldapport] [-P keyfilepw] [-r] [-R] [-U username] [-v] [-V version]
[-w passwd | ?] [-y proxydn] [-Y] [-Z] [dn newrdn | [-i file]]
```

Popis

ldapmodrdn je rozhraní příkazového řádku pro rozhraní API (application programming interfaces) příkazu `ldap_modrdn`.

ldapmodrdn otevře propojení k serveru LDAP, připojí se a modifikuje jména RDN záznamů. Informace o záznamu se čtou ze standardního vstupu, ze souboru s využitím volby **-f** nebo z páru `dn a rdn` příkazového řádku.

Informace o relativních rozlišovacích jménech RDN (Relative Distinguished Names) a rozlišovacích jménech DN (Distinguished Names) najdete v tématu "Rozlišovací jména (DN)" na stránce 11.

Chcete-li zobrazit nápovědu k syntaxi příkazu **ldapmodrdn**, napište:

```
ldapmodrdn -?
```

Volby

-c Nepřerušovaný operační režim. Chyby jsou oznamovány, ale program **ldapmodrdn** pokračuje v modifikacích. V ostatních případech je jako standardní činnost nastaveno ukončení programu po zaznamenání chyby.

-C charset

Specifikuje, že řetězce, které jsou dodávány jako vstup do obslužného programu **ldapmodrdn** jsou vyjádřeny

v lokální znakové sadě tak, jak je určeno volbou charset. Volba **-C charset** se používá tehdy, když je kódová stránka vstupního řetězce odlišná od hodnoty kódové stránky úlohy. Podporované hodnoty volby charset najdete v API `ldap_set_iconv_local_charset()`. Pověšněte si, že podporované hodnoty pro charset jsou stejné hodnoty, jaké jsou podporovány pro příznak charset, jak je volitelně definován v souborech LDIF Verze 1.

-d debuglevel

Nastavuje úroveň ladění LDAP na debuglevel.

-D binddn

Hodnota **binddn** se používá k připojení k adresáři LDAP. Hodnotou parametru **binddn** by měl být řetězec vyjadřující jméno DN. Při použití s parametrem **-m DIGEST-MD5** se používá pro zadání ID autorizace. Může to být buď DN nebo řetězec authzId začínající "u:" nebo "dn:".

-f file

Čte informace o změně záznamu ze souboru namísto ze standardního vstupu nebo z příkazového řádku (zadáním `rdn` a `newrdn`). Standardní vstup může být také dodán ze souboru (`< file`).

-G realm

Zadejte sféru. Tento parametr je volitelný. Při použití s parametrem **-m DIGEST-MD5** se tato hodnota postupuje na server během připojování.

-h ldaphost

Určuje alternativního hostitele, na kterém je spuštěn server ldap.

-i file

Čte informace o změně záznamu ze souboru namísto ze standardního vstupu nebo z příkazového řádku (zadáním `rdn` a `newrdn`). Standardní vstup může být poskytován také ze souboru ("`< file`").

-k

Určuje, že se má používat administrační řízení serveru.

-K keyfile

Specifikuje jméno souboru databáze klíčů SSL. Není-li soubor databáze klíčů umístěn 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 se rovněž označují jako důvěryhodné zdroje.

Tento parametr účinně aktivuje přepínač **-Z**. Pokud u serveru adresářů v operačním systému i5/OS použijete volbu **-Z** a nepoužijete volbu **-K** nebo **-N**, použije se certifikát přiřazený k ID aplikace klienta adresářových služeb.

-m mechanism

Hodnota **mechanism** specifikuje mechanismus SSL, kterým se klient připojuje k serveru. Použije se API `ldap_sasl_bind_s()`. Parametr **-m** se ignoruje v případě, že je nastaven parametr **-V 2**. Pokud parametr **-m** není určen, použije se jednoduchá autentizace. Platné mechanismy jsou tyto:

- CRAM-MD5 - provádí ochranu hesla odesílaného na server.
- EXTERNAL - používá certifikát SSL. Vyžaduje volbu **-Z**.
- GSSAPI - používá pověření Kerberos uživatele.
- DIGEST-MD5 - vyžaduje, aby klient odeslal na serveru hodnotu username. Vyžaduje volbu **-U**. Pro specifikaci ID autorizace se používá parametr **-D** (obvykle připojovací DN). Může to být buď DN nebo řetězec authzId začínající u: nebo dn:.
- OS400_PRFTKN - autentizuje se na lokální LDAP server jako aktuální uživatel i5/OS používající DN uživatele v proceduře backend projektované systémem. Parametry **-D** (připojovací DN) and **-w** (heslo) by neměly být zadány.

-M

Referenční objekty jsou spravovány jako řádné záznamy.

-n

Zobrazuje, co by se provedlo, ale záznamy se ve skutečnosti nemění. Tento parametr ve spojení s parametrem **-v** lze využít k ladění.

-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 není povinný. Je-li server LDAP konfigurován pro provádění autentizace klienta i serveru, certifikát klienta povinný být může. Parametr *certificatename* není povinný, pokud byl pro soubor databáze klíčů jako předvolený označen určitý pár certifikát/soukromý klíč. Podobně není parametr *certificatename* povinný, jestliže v označeném souboru databáze klíčů existuje jediný pár certifikát/soukromý klíč. Tento parametr se ignoruje v případě, že není zadán ani jeden z parametrů **-Z** a **-K**. Pokud u serveru adresářů v operačním systému i5/OS použijete volbu **-Z** a nepoužijete volbu **-K** nebo **-N**, použije se certifikát přiřazený k ID aplikace klienta adresářových služeb.

-O *hopcount*

Hodnota *hopcount* se používá pro nastavení maximálního počtu přechodů, které knihovna klienta vykoná při vyhledávání odkazů. Předvolená hodnota pro počet přechodů je 10.

-p *ldapport*

Specifikuje alternativní port TCP (Transmission Control Protocol), 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.

-P *keyfilepw*

Specifikuje heslo pro databázi klíčů. Toto heslo je povinné pro přístup ke kódovaným informacím v souboru databáze klíčů (který může obsahovat jeden nebo více soukromých klíčů). Je-li se souborem databáze klíčů asociován soubor pro uložení hesla, získá se heslo ze souboru pro uložení hesla a parametr **-P** není povinný. Tento parametr se ignoruje v případě, že není zadán ani jeden z parametrů **-Z** a **-K**.

-r Odstraňuje staré hodnoty RDN ze záznamu. Předvolená činnost je staré hodnoty uchovávat.

-R Specifikuje, že se odkazy nemají automaticky sledovat.

-U *username*

Zadejte username. Vyžaduje se při použití parametru **-m** DIGEST-MD5, u jiných mechanismů se ignoruje.

-v Používá komentovaný režim s mnoha diagnostickými zprávami zapsanými do standardního výstupu.

-V *version*

Určuje verzi LDAP, kterou má program **ldapmodrdn** používat při připojování k serveru LDAP. Standardně se ustavuje připojení LDAP V3. Chcete-li explicitně vybrat LDAP V3, zadejte **-V 3**. Chcete-li spustit aplikaci LDAP V2, zadejte **-V 2**. Aplikace jako např. **ldapmodrdn** vybírají přednostně protokol LDAP V3 použitím `ldap_init` namísto `ldap_open`.

-w *passwd* | ?

Hodnota *passwd* je heslo pro autentizaci. Parametr ? se používá, chcete-li vytvořit výzvu k zadání hesla.

-y *proxydn*

Nastavuje proxy ID pro operaci proxy autorizace.

-Y Použije zabezpečené spojení LDAP (TLS).

-Z Ke komunikaci se serverem LDAP se použije připojení přes SSL. Pokud u serveru adresářů v operačním systému i5/OS použijete volbu **-Z** a nepoužijete volbu **-K** nebo **-N**, použije se certifikát přiřazený k ID aplikace klienta adresářových služeb.

dn newrdn

Více informací najdete v následující části “Vstupní formát pro dn newrdn”.

Vstupní formát pro dn newrdn

Zadáte-li argumenty příkazového řádku *dn* a *newrdn*, nahradí zadané *newrdn* původní RDN záznamu, který je určen podle DN zadaného argumentem *dn*. Jinak se obsah souboru (nebo standardní vstup, když nezadáte žádný příznak **-i**) skládá z jednoho nebo více záznamů:

Rozlišovací jméno (DN)

Relativní rozlišovací jméno (RDN)

Koddělení každého páru DN a RDN je možno použít jeden nebo více prázdných řádků.

Příklady

Předpokládejme, že existuje soubor /tmp/entrymods, který má tento obsah:

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

potom příkaz:

```
ldapmodrdn -r -i /tmp/entrymods
```

změní RDN záznamu Modify Me z Modify Me na The New Me a staré cn, Modify Me, se odstraní.

Poznámky

Jestliže neposkytnete informace záznamu ze souboru prostřednictvím volby **-i** (nebo zadáním dvojice *dn a rdn* z příkazového řádku), bude příkaz **ldapmodrdn** očekávat načtení záznamů ze standardního vstupu.

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.

Idapsearch

Nástroj LDAP pro hledání a vzorový program

Přehled

```
ldapsearch [-a deref] [-A] [-b searchbase] [-B] [-C charset] [-d debuglevel]  
[-D binddn] [-e] [-f file] [-F sep] [-G realm] [-h ldaphost] [-i file] [-K keyfile]  
[-l timelimit] [-L] [-m mechanism] [-M] [-n] [-N certificatename]  
[-o attr_type] [-O maxhops] [-p ldapport] [-P keyfilepw] [-q pagesize]  
[-R] [-s scope] [-t] [-T seconds] [-U username] [-v] [-V version]  
[-w passwd | ?] [-z sizelimit] [-y proxydn] [-Y] [-Z]  
filter [-9 p] [-9 s] [attrs...]
```

Popis

Idapsearch je rozhraní příkazového řádku pro rozhraní API (application programming interfaces) příkazu `ldap_search`.

Idapsearch otevře propojení k serveru LDAP, připojí se a provede hledání s použitím filtru. Filtr by měl vyhovovat řetězcovému vyjádření stanovenému pro filtry LDAP (více informací o filtrech najdete v odstavci o `ldap_search` v tématu Rozhraní API serveru adresářů).

Jestliže **Idapsearch** nalezne jeden nebo více záznamů, vyhledají se atributy specifikované parametrem `attrs` a příslušné záznamy a hodnoty jsou zapsány na standardní výstup. Jestliže nejsou uvedeny žádné `attrs`, vrátí se všechny atributy.

Chcete-li zobrazit nápovědu k syntaxi příkazu **Idapsearch**, napište `ldapsearch -?`.

Volby

-a deref

Určuje, jak se provádí dereference aliasů. Hodnota `deref` by měla být `never`, `always`, `search` nebo `find`. Tyto hodnoty znamenají, že dereference aliasů se buď neprovádí nikdy, nebo se provádí vždy, nebo pouze při prohledávání, nebo pouze při hledání základního objektu pro prohledávání. Předvolená hodnota je nikdy neprovádět dereferenci aliasů (`never`).

-A Načte pouze atributy (bez hodnot). To je vhodné pro situaci, kdy chcete pouze zjistit, zda se v záznamu nachází určitý atribut, a nezajímá vás konkrétní hodnota.

-b searchbase

Hodnota searchbase slouží jako výchozí bod pro vyhledávání namísto předvolené hodnoty. Není-li zadána volba **-b**, obslužný program hledá definici v proměnné prostředí LDAP_BASEDN. Pokud není určena ani ta, předvolené východisko vyhledávání je nastaveno na "".

-B Nebude potlačeno zobrazování hodnot nespádajících do tabulky ASCII. To je výhodné, když pracujete s hodnotami, které přísluší do alternativních znakových sad, například ISO-8859.1. Tato volba se vztahuje na použití volby **-L**.

-C charset

Specifikuje, že řetězce, které jsou dodávány jako vstup do obslužného programu ldapsearch, jsou vyjádřeny v lokální znakové sadě tak, jak je určeno volbou charset. Vstupní řetězec obsahuje filtr, přípojovací DN a základní DN. Podobně při zobrazování dat zkonvertuje program **ldapsearch** data, která obdrží ze serveru LDAP, na zadanou znakovou sadu. Volba **-C charset** se používá tehdy, když je kódová stránka vstupního řetězce odlišná od hodnoty kódové stránky úlohy. Podporované hodnoty volby charset najdete v API ldap_set_iconv_local_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. Důvodem je to, že standardní soubory LDIF obsahují reprezentace dat řetězců pouze v UTF-8 (nebo v kódování base-64 UTF-8). Povšimněte si, že podporované hodnoty pro charset jsou stejné hodnoty, jaké jsou podporovány pro příznak charset, jak je volitelně definován v souborech LDIF Verze 1.

-d debuglevel

Nastavuje úroveň ladění LDAP na debuglevel.

-D binddn

Hodnota binddn se používá k připojení k adresáři LDAP. Hodnotou parametru **binddn** by měl být řetězec vyjadřující jméno DN (viz část rozlišovací jména LDAP). Při použití s parametrem **-m DIGEST-MD5** se používá pro zadání ID autorizace. Může to být buď DN nebo řetězec authzId začínající "u:" nebo "dn:".

-e Zobrazí informace o verzi knihovny LDAP a potom ukončí činnost.

-F sep Hodnota sep se používá jako oddělovač polí jmen atributů a hodnot. Předvolený oddělovač je '=', pokud nebyl zadán příznak **-L**; v tom případě je tato volba ignorována.

-G realm

Zadejte sféru. Tento parametr je volitelný. Při použití s parametrem **-m DIGEST-MD5** se tato hodnota postupuje na server během připojování.

-h ldaphost

Určuje alternativního hostitele, na kterém je spuštěn server ldap.

-i file Čte sérii řádek ze souboru a pro jeho každou řádku provede jedno vyhledávání LDAP. V tomto případě se filtr uvedený na příkazovém řádku považuje za vzor, kde první výskyt %s je nahrazen řádkem souboru. Jestliže je soubor jediný znak "-", řádky se čtou ze standardního vstupu.

-K keyfile

Specifikuje jméno souboru databáze klíčů SSL. Není-li soubor databáze klíčů umístěn 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 se rovněž označují jako důvěryhodné zdroje.

Tento parametr účinně aktivuje přepínač **-Z**. Pokud u serveru adresářů v operačním systému i5/OS použijete volbu **-Z** a nepoužijete volbu **-K** nebo **-N**, použije se certifikát přiřazený k ID aplikace klienta adresářových služeb.

-l timelimit

Čeká na dokončení vyhledání maximálně tolik sekund, kolik je uvedeno v hodnotě timelimit.

-L Zobrazí výsledky vyhledávání ve formátu LDIF. Tato volba rovněž zapíná volbu **-B** a způsobí, že se ignoruje volba **-F**.

-m mechanism

Hodnota **mechanism** specifikuje mechanismus SSL, kterým se klient připojuje k serveru. Použije se API ldap_sasl_bind_s(). Parametr **-m** se ignoruje v případě, že je nastaven parametr **-V 2**. Pokud parametr **-m** není určen, použije se jednoduchá autentizace. Platné mechanismy jsou tyto:

- CRAM-MD5 - provádí ochranu hesla odesílaného na server.
- EXTERNAL - používá certifikát SSL. Vyžaduje volbu **-Z**.
- GSSAPI - používá pověření Kerberos uživatele.
- DIGEST-MD5 - vyžaduje, aby klient odeslal na serveru hodnotu username. Vyžaduje volbu **-U**. Pro specifikaci ID autorizace se používá parametr **-D** (obvykle připojovací DN). Může to být buď DN nebo řetězec authzId začínající u: nebo dn:.
- OS400_PRFTKN - autentizuje se na lokální LDAP server jako aktuální uživatel i5/OS používající DN uživatele v proceduře backend projektované systémem. Parametry **-D** (připojovací DN) and **-w** (heslo) by neměly být zadány.

-M Referenční objekty jsou spravovány jako řádné záznamy.

-n Zobrazuje, co by se provedlo, ale záznamy se ve skutečnosti nemění. Tento parametr ve spojení s parametrem **-v** lze využít k ladění.

-N certificatename

Specifikuje návěští asociované s certifikátem klienta v souboru databáze klíčů.

Poznámka: Jestliže je server LDAP konfigurován pouze pro provádění autentizace serveru, certifikát klienta není povinný. Je-li server LDAP konfigurován pro provádění autentizace klienta i serveru, certifikát klienta povinný být může. Parametr *certificatename* není povinný, pokud byl pro soubor databáze klíčů jako předvolený označen určitý pár certifikát/soukromý klíč. Podobně není parametr *certificatename* povinný, jestliže v označeném souboru databáze klíčů existuje jediný pár certifikát/soukromý klíč. Tento parametr se ignoruje v případě, že není zadán ani jeden z parametrů **-Z** a **-K**.

Pokud u serveru adresářů v operačním systému i5/OS použijete volbu **-Z** a nepoužijete volbu **-K** nebo **-N**, použije se certifikát přiřazený k ID aplikace klienta adresářových služeb.

-o attr_type

Chcete-li určit atribut, který by se používal pro kritéria třídění výsledků vyhledávání, můžete použít parametr **-o** (order). K dalšímu definování pořadí třídění můžete použít více parametrů **-o**. V následujícím příkladě jsou výsledky hledání seříděny nejprve podle příjmení (sn), potom podle křestního jména (givenname) tříděného v obráceném (sestupném) pořadí, které je určeno znaménkem mínus (-) vloženým před tento parametr:

```
-o sn -o -givenname
```

Syntaxe parametrů třídění je tedy tato:

```
[-]<jméno_atributu>[:<OID_pravidla_porovnávání>]
```

kde:

- jméno_atributu je jméno atributu, podle kterého chcete třídít.
- OID_pravidla_porovnávání je volitelný OID pravidla porovnávání, které chcete použít pro třídění. Atribut OID pravidla porovnávání není podporován serverem adresářů, jiné servery LDAP však tento atribut podporovat mohou.
- Znaménko mínus (-) označuje, že se výsledky musejí třídít v obráceném pořadí.
- Kritičnost je vždy kritická.

Předvolená hodnota operace ldapsearch je netřídít vrácené výsledky.

-O maxhops

Hodnota maxhops se používá pro nastavení maximálního počtu přechodů, které knihovna klienta vykoná při vyhledávání odkazů. Předvolená hodnota pro počet přechodů je 10.

-p ldapport

Specifikuje alternativní port TCP (Transmission Control Protocol), 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.

-P keyfilepw

Specifikuje heslo pro databázi klíčů. Toto heslo je povinné pro přístup ke kódovaným informacím v souboru databáze klíčů (který může obsahovat jeden nebo více soukromých klíčů). Je-li se souborem databáze klíčů asociován soubor pro uložení hesla, získá se heslo ze souboru pro uložení hesla a parametr **-P** není povinný. Tento parametr se ignoruje v případě, že není zadán ani jeden z parametrů **-Z** a **-K**.

-q pagesize

Chcete-li určit stránkování výsledků prohledávání, je možné použít dva parametry: **-q** (dotaz na velikost stránky) a **-T** (čas mezi vyhledáváním v sekundách). V níže uvedeném příkladě se každých 15 sekund vracejí výsledky vyhledávání postupně po jedné stránce (25 záznamů), dokud nejsou vráceny všechny výsledky pro toto vyhledávání. Klient ldapsearch spravuje všechna pokračování připojení pro každý požadavek na stránkované výsledky po dobu trvání operace vyhledávání.

Tyto parametry mohou být užitečné v případě, že má klient omezené zdroje nebo když je připojen prostřednictvím spojení s nízkou šířkou frekvenčního pásma. Obecně umožňuje tento parametr řídit rychlost, kterou se vracejí data z požadavku na hledání. Namísto přijímání všech výsledků najednou je můžete získávat postupně po několika záznamech (jedné stránce). Navíc můžete určovat trvání prodlevy mezi každým požadavkem na stránku, což poskytuje klientovi čas na zpracování výsledků.

```
-q  
25 -T 15
```

Jestliže je zadán parametr **-v** (komentovaný), program ldapsearch po každé stránce záznamů vrácených ze serveru zobrazí přehled, kolik záznamů bylo zatím vráceno, například **30 total entries have been returned**.

Program umožňuje zadat více parametrů **-q**, takže je možné určit během doby trvání jediné operace hledání různé velikosti stránek. V následujícím příkladě má první stránka 15 záznamů, druhá stránka má 20 záznamů a třetí parametr ukončuje operaci hledání se stránkovanými výsledky:

```
-q 15 -q 20 -q 0
```

Vnásledujícím příkladě má první stránka 15 záznamů a celý zbytek stránek má 20 záznamů, což je poslední určená hodnota **-q**, která trvá do doby, než je operace hledání dokončena:

```
-q  
15 -q 20
```

Předvolenou operací ldapsearch je vrácení všech záznamů v jediném požadavku. U výchozí operace ldapsearch se neprovádí žádné stránkování.

-R Specifikuje, že se odkazy nemají automaticky sledovat.

-s scope

Specifikuje rozsah vyhledávání. Hodnota scope by měla být "base", "one" nebo "sub", přičemž tyto hodnoty znamenají vyhledávání v základním objektu, v jedné úrovni nebo v podstromu. Předvolená hodnota je "sub".

-t Zapiše vyhledané hodnoty do sady dočasných souborů. To je výhodné při práci s hodnotami nespadaajícími do tabulky ASCII, jako jsou jpegPhoto nebo audio.

-T seconds

Čas mezi vyhledáváním (v sekundách). Volba **-T** je podporována pouze tehdy, když je zadána volba **-q**.

-U username

Zadejte username. Vyžaduje se při použití parametru **-m DIGEST-MD5**, u jiných mechanismů se ignoruje.

- v Používá komentovaný režim s mnoha diagnostickými zprávami zapsanými do standardního výstupu.
- V Určuje verzi LDAP, kterou má program ldapmodify používat při připojování k serveru LDAP. Standardně se ustavuje připojení LDAP V3. Chcete-li explicitně vybrat LDAP V3, zadejte "-V 3". Chcete-li spustit aplikaci LDAP V2, zadejte "-V 2". Aplikace jako ldapmodify vybírají přednostně protokol LDAP V3 použitím ldap_init namísto ldap_open.

-w passwd | ?

Hodnota *passwd* je heslo pro autentizaci. Parametr ? se používá, chcete-li vytvořit výzvu k zadání hesla. .

-y proxydn

Nastavuje proxy ID pro operaci proxy autorizace.

-Y Použije zabezpečené spojení LDAP (TLS).

-z sizelimit


Omezí výsledky vyhledávání na maximálně takový počet záznamů, jaký je uveden v hodnotě sizelimit. Tato volba umožňuje stanovit pro operaci vyhledávání horní hranici počtu vrácených záznamů.

-Z Ke komunikaci se serverem LDAP se použije připojení přes SSL. Pokud u serveru adresářů v operačním systému i5/OS použijete volbu -Z a nepoužijete volbu -K nebo -N, použije se certifikát přiřazený k ID aplikace klienta adresářových služeb.

filter Určuje řetězcové vyjádření filtru, který se má použít ve vyhledávání. Je možné zadat jednoduché filtry jako `attributetype=attributevalue`. Složitější filtry se zadávají s využitím předponové notace podle pravidla BNF (Backus Naur Form):

```
<filter> ::= '(' <filtercomp> ')'
<filtercomp> ::= <and> | <or> | <not> | <simple>
<and> ::= '&' <filterlist>
<or> ::= '|' <filterlist>
<not> ::= '!' <filter>
<filterlist> ::= <filter> | <filter> <filterlist>
<simple> ::= <attributetype> <filtertype>
<attributevalue>
<filtertype> ::= '=' | '~=' | '<=' | '>='
```

Sled znaků '~=' se používá pro určení přibližného porovnávání. Znázornění pro `<attributetype>`

a `<attributevalue>` se řídí podle popisu v "RFC 2252, LDAP V3 Attribute Syntax Definitions"  . Kromě toho, jestliže filtertype je '=', hodnotou `<attributevalue>` může být jednoduchá hvězdička (*), pomocí které je možné provést test existence atributu, nebo může obsahovat text s roztroušenými hvězdičkami *, což umožňuje dosáhnout porovnávání podřetězce.

Například filtr "mail=*" hledá jakékoli záznamy, které mají atribut mail. Filtr "mail=@student.of.life.edu" hledá jakékoli záznamy, které mají atribut mail zakončený zadaným řetězcem. Chcete-li vložit do filtru závorky, uvolněte je znakem zpětného lomítka (\).

Poznámka: Filtr jako "cn=Daniel *", kde je mezera mezi slovem Daniel a hvězdičkou (*), v adresáři IBM odpovídá řetězci "Daniel Sedláček", ale ne "Daniela Sedláčková". Mezera mezi "Daniel" a zástupným znakem (*) ovlivňuje výsledek hledání s využitím filtrů.

Podrobnější popis přípustných filtrů najdete v "RFC 2254, A String Representation of LDAP Search Filters"



Výstupní formát

Pokud je nalezen jeden nebo více záznamů, je každý záznam zapsán do standardního výstupu ve tvaru:

Rozlišovací jméno (DN)

jménoatributu=hodnota

jménoatributu=hodnota

jménoatributu=hodnota

...

Jednotlivé záznamy se oddělují jednou prázdnou řádkou. Pokud se pro určení oddělovacího znaku používá volba **-F**, použije se místo znaku `=`. Použijete-li volbu **-t**, bude skutečná hodnota nahrazena jménem dočasného souboru. Jestliže je zadána volba **-A**, je zapsána pouze část "attributename".

Příklady

Příkaz:

```
ldapsearch "cn=john doe" cn telephoneNumber
```

vyhledá v podstromu (s použitím předvoleného výchozího bodu vyhledávání) záznamy, ve kterých commonName je "john doe". Hodnoty commonName a telephoneNumber se načtou a zapíše do standardního výstupu. Jestliže jsou nalezeny dva záznamy, výstup by mohl vypadat nějak 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
```

Příkaz:

```
ldapsearch -t "uid=jed" jpegPhoto audio
```

vyhledá v podstromu s použitím předvolené základny vyhledávání záznamy, ve kterých id uživatele je "jed". Hodnoty jpegPhoto a audio se načtou a zapíše 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
```

Příkaz:

```
ldapsearch -L -s one -b "c=US" "o=university*" o description
```

provede hledání s rozsahem jedné úrovně na úrovni c=US, ve kterém se budou hledat všechny organizace, jejichž organizationName začíná na university. Výsledky hledání se zobrazí ve formátu LDIF (viz část LDAP Data Interchange Format). Hodnoty atributů organizationName a description budou načteny a vypsány do standardního výstupu, který bude vypadat asi 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: UF1
description: Shaper of young minds

...
```

Příkaz:

```
ldapsearch -b "c=US" -o ibm-slapdDN "objectclass=person" ibm-slapdDN
```

provede hledání všech osob s rozsahem podstromu na úrovni c=US. Tento speciální atribut (ibm-slapdDN) při použití pro tříděná hledání setřídí výsledky hledání podle řetězcového vyjádření rozlišovacího jména (DN). Výstup by mohl vypadat nějak takto:

```
cn=A1 Edwards,ou=Widget Division,ou=Austin,o=IBM,c=US
cn=A1 Garcia,ou=Home Entertainment,ou=Austin,o=IBM,c=US
```

```
cn=Amy Nguyen,ou=In Flight Systems,ou=Austin,o=IBM,c=US
cn=Arthur Edwards,ou=Widget Division,ou=Austin,o=IBM,c=US
cn=Becky Garcia,ou=In Flight Systems,ou=Austin,o=IBM,c=US
cn=Ben Catu,ou=In Flight Systems,ou=Austin,o=IBM,c=US
cn=Ben Garcia Jr,ou=Home Entertainment,ou=Austin,o=IBM,c=US
cn=Bill Keller Jr.,ou=In Flight Systems,ou=Austin,o=IBM,c=US
cn=Bob Campbell,ou=In Flight Systems,ou=Austin,o=IBM,c=US
```

Příkaz:

```
ldapsearch -h hostname -o sn -b "o=ibm,c=us"
"title=engineer"
```

vrátí všechny záznamy v adresáři zaměstnanců IBM, jejichž titul je "engineer", přičemž výsledky jsou setříděny podle příjmení.

Příkaz:

```
ldapsearch -h hostname -o -sn -o cn -b "o=ibm,c=us"
"title=engineer"
```

vrátí všechny záznamy v adresáři zaměstnanců IBM, jejichž titul je "engineer", přičemž výsledky jsou setříděny podle příjmení (v sestupném pořadí) a potom podle obecného jména (ve vzestupném pořadí).

Příkaz:

```
ldapsearch -h hostname -q 5 -T 3 -b o=ibm,c=us "title=engineer"
```

vrátí pět záznamů na stránce s prodlevou tří sekund mezi stránkami pro všechny záznamy v adresáři zaměstnanců IBM, jejichž titul je "engineer".

Následující příklad je ukázkou vyhledávání, kde je zahrnut referenční objekt. Jak bylo uvedeno v tématu "Odkazy v adresáři LDAP" na stránce 45, adresáře LDAP produktu Server adresářů mohou obsahovat referenční objekty, za předpokladu, že obsahují pouze tyto atributy:

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

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 zadá požadavek na 'System_A', 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 zadání požadavku na systém System_B. Jestliže záznam v systému System_A obsahuje i jiné atributy než dn, objectclass a ref, server tyto atributy ignoruje (pokud nezádáte příznak **-R**, který určuje, že se nemají sledovat odkazy).

Když klient obdrží referenční odpověď ze serveru, znovu vyšle požadavek, tentokrát na server, na který se odkazuje vrácená URL. Tento nový požadavek má stejný rozsah jako původní požadavek. Výsledek tohoto vyhledávání se liší v závislosti na hodnotě, kterou zadáte jako rozsah vyhledávání (**-b**).

Zadáte-li **-s base**, jak je uvedeno zde:

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

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

Zadáte-li **-s sub**, jak je uvedeno zde:

```
ldapsearch -s sub "cn=John"
```

server by prohledal všechny přípony a vrátil všechny záznamy s "cn=John". Toto je známo jako prohledávání podstromu na nulové bázi. Celý adresář se prohledává pomocí jedné vyhledávací operace namísto toho, že by se muselo provést více prohledávání vždy pro každou odlišnou příponu jako výchozí bod hledání. Tento typ vyhledávací operace trvá déle a spotřebuje více systémových zdrojů, protože prohledává celý adresář (všechny přípony).

Poznámka: Prohledávání podstromu na nulové bázi nevrátí informace schématu, informace protokolu změn ani žádné informace z procedury Backend projektované systémem.

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

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
```

Klient na oplátku předá požadavek:

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

Ani to nevrátí žádné výsledky, protože záznam

```
dn:  
cn=Barb_Jensen, ou=Rochester, o=Big Company, c=US
```

je umístěn

ou=Rochester, o=Big Company, c=US

Hledání s parametrem `-s ONE` se pokusí najít záznamy bezprostředně pod

ou=Rochester, o=Big Company, c=US

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.

ldapchangepwd

Nástroj LDAP pro modifikaci hesla.

Přehled

```
ldapchangepwd -D binddn -w passwd | ? -n newpassword | ?  
[-C charset] [-d debuglevel] [-G realm] [-h ldaphost]  
[-K keyfile] [-m mechanism] [-M] [-N certificatename]  
[-O maxhops] [-p ldapport] [-P keyfilepw] [-R]  
[-U username] [-v] [-V version] [-y proxydn] [-Y] [-Z] [-?]
```

Popis

Odesílá požadavek na modifikaci hesla na server LDAP. Umožňuje změnu hesla pro záznam adresáře.

Volby

-C *charset*

Specifikuje, že rozlišovací jména (DN), která jsou poskytnuta jako vstup do programu **ldapdelete**, jsou vyjádřena v lokální znakové sadě tak, jak je určeno volbou *charset*. Volba **-C *charset*** se používá tehdy, když je kódová stránka vstupního řetězce odlišná od hodnoty kódové stránky úlohy. Podporované hodnoty volby *charset* najdete v API `ldap_set_iconv_local_charset()`.

-d *debuglevel*

Nastavuje úroveň ladění LDAP na *debuglevel*.

-D *binddn*

Hodnota ***binddn*** se používá k připojení k adresáři LDAP. Hodnotou parametru ***binddn*** je řetězec vyjadřující jméno DN. Při použití s parametrem **-m DIGEST-MD5** se používá pro zadání ID autorizace. Může to být buď DN nebo řetězec `authzId` začínající "u:" nebo "dn:".

-G *realm*

Zadejte sféru. Tento parametr je volitelný. Při použití s parametrem **-m DIGEST-MD5** se tato hodnota postupuje na server během připojování.

-h *ldaphost*

Určuje alternativního hostitele, na kterém je spuštěn server ldap.

-K *keyfile*

Specifikuje jméno souboru databáze klíčů SSL. Není-li soubor databáze klíčů umístěn 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 se rovněž označují jako důvěryhodné zdroje.

Tento parametr účinně aktivuje přepínač **-Z**. Pokud u serveru adresářů v operačním systému i5/OS použijete volbu **-Z** a nepoužijete volbu **-K** nebo **-N**, použije se certifikát přiřazený k ID aplikace klienta adresářových služeb.

-m mechanism

Hodnota **mechanism** specifikuje mechanismus SSL, kterým se klient připojuje k serveru. Použije se API `ldap_sasl_bind_s()`. Parametr **-m** se ignoruje v případě, že je nastaven parametr **-V 2**. Pokud parametr **-m** není určen, použije se jednoduchá autentizace. Platné mechanismy jsou tyto:

- CRAM-MD5 - provádí ochranu hesla odesílaného na server.
- EXTERNAL - používá certifikát SSL. Vyžaduje volbu **-Z**.
- GSSAPI - používá pověření Kerberos uživatele.
- DIGEST-MD5 - vyžaduje, aby klient odeslal na serveru hodnotu `username`. Vyžaduje volbu **-U**. Pro specifikaci ID autorizace se používá parametr **-D** (obvykle přípojovací DN). Může to být buď DN nebo řetězec `authzId` začínající `u:` nebo `dn:`.

-M Referenční objekty jsou spravovány jako řádné záznamy.

-n newpassword | ?

Určuje nové heslo. Parametr **?** se používá, chcete-li vytvořit výzvu k zadání hesla.

-N certificatename

Specifikuje návěští asociované s certifikátem klienta v souboru databáze klíčů. Jestliže je server LDAP konfigurován pouze pro provádění autentizace serveru, certifikát klienta není povinný. Je-li server LDAP konfigurován pro provádění autentizace klienta i serveru, certifikát klienta povinný být může. Parametr **certificatename** není povinný, pokud byl pro soubor databáze klíčů jako předvolený označen určitý pár certifikát/soukromý klíč. Podobně není parametr **certificatename** povinný, jestliže v označeném souboru databáze klíčů existuje jediný pár certifikát/soukromý klíč. Tento parametr se ignoruje v případě, že není zadán ani jeden z parametrů **-Z** a **-K**. Pokud u serveru adresářů v operačním systému i5/OS použijete volbu **-Z** a nepoužijete volbu **-K** nebo **-N**, použije se certifikát přiřazený k ID aplikace klienta adresářových služeb.

-O maxhops

Hodnota **maxhops** se používá pro nastavení maximálního počtu přechodů, které knihovna klienta vykoná při vyhledávání odkazů. Předvolená hodnota pro počet přechodů je 10.

-p ldapport

Specifikuje alternativní port TCP (Transmission Control Protocol), na kterém server LDAP naslouchá. Předvolený port LDAP je 389. Není-li port **-p** specifikován a přitom je zadán parametr **-Z**, použije se předvolený port LDAP SSL 636.

-P keyfilepw

Specifikuje heslo pro databázi klíčů. Toto heslo je povinné pro přístup ke kódovaným informacím v souboru databáze klíčů, který může obsahovat jeden nebo více soukromých klíčů. Je-li se souborem databáze klíčů asociován soubor pro uložení hesla, získá se heslo ze souboru pro uložení hesla a parametr **-P** není povinný. Tento parametr se ignoruje v případě, že není zadán ani jeden z parametrů **-Z** a **-K**.

-R Specifikuje, že se odkazy nemají automaticky sledovat.

-U username

Zadejte `username`. Vyžaduje se při použití parametru **-m DIGEST-MD5**, u jiných mechanismů se ignoruje.

-v Používá komentovaný režim s mnoha diagnostickými zprávami zapsanými do standardního výstupu.

-V version

Určuje verzi LDAP, kterou má program **ldapdchangepwd** používat při připojování k serveru LDAP. Standardně se ustavuje připojení LDAP V3. Chcete-li explicitně vybrat LDAP V3, zadejte **-V 3**. Chcete-li spustit aplikaci LDAP V2, zadejte **-V 2**. Aplikace jako **ldapdchangepwd** vybírají přednostně protokol LDAP V3 použitím `ldap_init` namísto `ldap_open`.

-w passwd | ?

Hodnota **passwd** je heslo pro autentizaci. Parametr **?** se používá, chcete-li vytvořit výzvu k zadání hesla.

-y proxydn

Nastavuje proxy ID pro operaci proxy autorizace.

-Y Použije zabezpečené spojení LDAP (TLS).

- Z Ke komunikaci se serverem LDAP se použije připojení přes SSL. Pokud u serveru adresářů v operačním systému i5/OS použijete volbu -Z a nepoužijete volbu -K nebo -N, použije se certifikát přiřazený k ID aplikace klienta adresářových služeb.
- ? Zobrazí nápovědu k syntaxi příkazu ldapchangepwd.

Příklady

Příkaz

```
ldapchangepwd -D cn=John Doe -w a1b2c3d4 -n wxyz9876
```

změní heslo pro záznam nazvaný obecným jménem commonName "John Doe" z hodnoty a1b2c3d4 na hodnotu wxyz9876

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.

ldapdiff

Nástroj pro synchronizaci replik LDAP.

Poznámka: Tento příkaz by mohl probíhat po dlouhou dobu v závislosti na počtu záznamů (a atributů pro takové záznamy), které se replikují.

Přehled

(Porovnává a synchronizuje datové záznamy mezi dvěma servery bez replikačního prostředí.)

```
ldapdiff -b baseDN -sh host -ch host [-a] [-C countnumber]
[-cD dn] [-cK keyStore] [-cw password] [-cN keyLabel]
[-cp port] [-cP keyStorePwd] [-cZ] [-F] [-L filename] [-sD dn] [-sK keyStore]
[-sw password] [-sN keyLabel] [-sp port] [-sP keyStorePwd]
[-sZ] [-v]
```

nebo

(Porovnává schéma mezi dvěma servery.)

```
ldapdiff -S -sh host -ch host [-a] [-C countnumber] [-cD dn]
[-cK keyStore] [-cw password] [-cN keyLabel] [-cp port]
[-cP keyStorePwd] [-cZ] [-L filename] [-sD dn]
[-sK keyStore] [-sw password] [-sN keyLabel] [-sp port]
[-sP keyStorePwd] [-sZ] [-v]
```

Popis

Tento nástroj synchronizuje replikovaný server s jeho hlavním serverem. Chcete-li zobrazit nápovědu k syntaxi příkazu **ldapdiff**, napište:

```
ldapdiff -?
```

Volby

Níže uvedené volby se vztahují na příkaz **ldapdiff**. Dělí se dvou podskupin, které se vztahují specificky buď na dodavatelský server, nebo na odběratelský server.

- a Určuje, že pro zápisy do repliky pouze pro čtení se má používat administrační řízení serveru.

-b *baseDN*

Hodnota searchbase slouží jako výchozí bod pro vyhledávání namísto předvolené hodnoty. Není-li volba **-b** zadána, obslužný program hledá definici v proměnné prostředí LDAP_BASEDN.

-C *countnumber*

Počítá počet záznamů, které se mají napravit. Pokud je nalezeno víc neshod, než je určený počet, nástroj ukončí činnost.

-F Toto je volba nápravy. Pokud je zadána, obsah odběratelské repliky je modifikován tak, aby odpovídal obsahu dodavatelského serveru. Tuto volbu nelze použít, je-li zadána volba **-S**.

-L Není-li zadána volba **-F**, použijte tuto volbu pro vytvoření souboru LDIF pro výstup. Soubor LDIF je možné použít pro aktualizaci odběratele a odstranění rozdílů.

-S Určuje, že se má porovnat schéma na obou serverech.

-v Používá komentovaný režim s mnoha diagnostickými zprávami zapsanými do standardního výstupu.

Volby pro dodavatele replikace

Níže uvedené volby se vztahují na odběratelský server a jsou označeny výchozím 's' ve jménu volby.

-sD dn Hodnota **dn** se používá k připojení k adresáři LDAP. Hodnotou parametru **dn** je řetězec vyjadřující jméno DN.

-sh *host*

Určuje jméno hostitele.

-sK *keyStore*

Specifikuje jméno souboru databáze klíčů SSL s předvolenou příponou **kdb**. Pokud tento parametr není specifikován nebo je hodnotou prázdný řetězec (**-sK""**), použije se systémový soubor pro ukládání klíčů. Není-li soubor databáze klíčů umístěn v aktuálním adresáři, zadejte plně kvalifikované jméno souboru databáze klíčů.

-sN *keyLabel*

Specifikuje návěští asociované s certifikátem klienta v souboru databáze klíčů. Je-li určeno návěští bez specifikace souboru pro ukládání klíčů, je návěštím identifikátor aplikace ve Správci digitálního certifikátu (DCM). Předvolené návěští (id aplikace) je QIBM_GLD_DIRSrv_CLIENT. Jestliže je server LDAP konfigurován pouze pro provádění autentizace serveru, certifikát klienta není povinný. Je-li server LDAP konfigurován pro provádění autentizace klienta i serveru, certifikát klienta povinný být může. Parametr **keyLabel** není povinný, pokud byl pro soubor databáze klíčů jako předvolený označen určitý pár certifikát/soukromý klíč. Podobně není parametr **keyLabel** povinný, jestliže v označeném souboru databáze klíčů existuje jediný pár certifikát/soukromý klíč. Tento parametr se ignoruje v případě, že není zadán ani jeden z parametrů **-sZ** a **-sK**.

-sp *ldapport*

Specifikuje alternativní port TCP (Transmission Control Protocol), na kterém server LDAP naslouchá. Předvolený port LDAP je 389. Není-li port **-sp h** specifikován a přitom je zadán parametr **-sZ**, použije se předvolený port LDAP SSL 636.

-sP *keyStorePwd*

Specifikuje heslo pro databázi klíčů. Toto heslo je povinné pro přístup ke kódovaným informacím v souboru databáze klíčů, který může obsahovat jeden nebo více soukromých klíčů. Je-li se souborem databáze klíčů asociován soubor pro uložení hesla, získá se heslo ze souboru pro uložení hesla a parametr **-sP** není povinný. Tento parametr se ignoruje v případě, že není zadán ani jeden z parametrů **-sZ** a **-sK**. Heslo se nepoužívá, pokud pro používaný soubor pro ukládání klíčů existuje soubor pro uložení hesla.

-st *trustStoreType*

Specifikuje návěští asociované s certifikátem klienta v souboru důvěryhodné databáze. Jestliže je server LDAP konfigurován pouze pro provádění autentizace serveru, certifikát klienta není povinný. Je-li server LDAP konfigurován pro provádění autentizace klienta i serveru, certifikát klienta povinný být může. Parametr **trustStoreType** není povinný, pokud byl pro soubor databáze klíčů jako předvolený označen určitý

pár certifikát/soukromý klíč. Podobně není parametr *trustStoreType* povinný, jestliže v označeném souboru databáze klíčů existuje jediný pár certifikát/soukromý klíč. Tento parametr se ignoruje v případě, že není zadán ani jeden z parametrů **-sZ** a **-sT**.

-sZ Ke komunikaci se serverem LDAP se použije připojení přes SSL.

Volby pro odběratele replikace

Níže uvedené volby se vztahují na odběratelský server a jsou označeny výchozím 'c' ve jménu volby. Pokud je volba **-cZ** zadána bez specifikace hodnot pro parametry **-cK**, **-cN** nebo **-cP**, používají tyto volby z praktických důvodů stejnou hodnotu určenou pro volby dodavatelského SSL. Chcete-li přepsat dodavatelské volby a použít předvolená nastavení, specifikujte **-cK "" -cN "" -cP ""**.

-cD dn Hodnota *dn* se používá k připojení k adresáři LDAP. Hodnotou parametru *dn* je řetězec vyjadřující jméno DN.

-ch host
Určuje jméno hostitele.

-cK keyStore
Specifikuje jméno souboru databáze klíčů SSL s předvolenou příponou *kdb*. Pokud je hodnotou prázdný řetězec (**-sK ""**), použije se systémový soubor pro ukládání klíčů. Není-li soubor databáze klíčů umístěn v aktuálním adresáři, zadejte plně kvalifikované jméno souboru databáze klíčů.

-cN keyLabel
Specifikuje návěští asociované s certifikátem klienta v souboru databáze klíčů. Jestliže je server LDAP konfigurován pouze pro provádění autentizace serveru, certifikát klienta není povinný. Je-li určeno návěští bez specifikace souboru pro ukládání klíčů, je návěštím identifikátor aplikace ve Správci digitálního certifikátu (DCM). Předvolené návěští (id aplikace) je *QIBM_GLD_DIRSrv_CLIENT*. Je-li server LDAP konfigurován pro provádění autentizace klienta i serveru, certifikát klienta povinný být může. Parametr *keyLabel* není povinný, pokud byl pro soubor databáze klíčů jako předvolený označen určitý pár certifikát/soukromý klíč. Podobně není parametr *keyLabel* povinný, jestliže v označeném souboru databáze klíčů existuje jediný pár certifikát/soukromý klíč. Tento parametr se ignoruje v případě, že není zadán ani jeden z parametrů **-cZ** a **-cK**.

-cp ldapport
Specifikuje alternativní port TCP (Transmission Control Protocol), na kterém server LDAP naslouchá. Předvolený port LDAP je 389. Není-li port **-cp** specifikován a přitom je zadán parametr **-cZ**, použije se předvolený port LDAP SSL 636.

-cP keyStorePwd
Specifikuje heslo pro databázi klíčů. Toto heslo je povinné pro přístup ke kódovaným informacím v souboru databáze klíčů, který může obsahovat jeden nebo více soukromých klíčů. Je-li se souborem databáze klíčů asociován soubor pro uložení hesla, získá se heslo ze souboru pro uložení hesla a parametr **-cP** není povinný. Tento parametr se ignoruje v případě, že není zadán ani jeden z parametrů **-cZ** a **-cK**.

-cw password | ?
Hodnota *password* je heslo pro autentizaci. Parametr *?* se používá, chcete-li vytvořit výzvu k zadání hesla.

-cZ Ke komunikaci se serverem LDAP se použije připojení přes SSL.

Příklady

```
ldapdiff -b <baseDN> -sh <supplierhostname> -ch <consumerhostname> [options]
```

nebo

```
ldapdiff -S -sh <supplierhostname> -ch <consumerhostname> [options]
```

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.

Jak používat SSL s obslužnými programy příkazového řádku LDAP

Část "SSL (Secure Sockets Layer) a TLS (Transport Layer Security) u serveru adresářů" na stránce 47 popisuje použití SSL na serveru Server adresářů 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 nutné pouze definovat jeden nebo více certifikátů z důvěryhodných zdrojů v paměti certifikátů. Při autentizaci serveru může být klient ujistěn, 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 rozhraní 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 ujistěn, 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 rozhraní 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.

LDAP data interchange format (LDIF)

Tato dokumentace popisuje LDIF (LDAP data interchange format), který se používá obslužnými programy ldapmodify, ldapsearch a ldapadd. Zde uvedený formát LDIF je rovněž podporován obslužnými programy serveru dodávanými s adresářem IBM.

LDIF se používá pro znázornění záznamů LDAP v textové formě. Základní tvar záznamu LDIF je tento:

```
dn:  
<rozlišovací jméno>  
<attrtype> : <attrvalue>  
<attrtype> : <attrvalue>  
...
```

Řádek může mít pokračování, které začíná na novém řádku jednou mezerou nebo znakem tabulátoru, například:

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

Několikanásobné hodnoty atributu se zadávají na samostatných řádcích, například:

```
cn: John E Doe  
cn: John Doe
```

Jestliže <attrvalue> obsahuje znak neobsažený v tabulce US-ASCII nebo začíná mezerou nebo dvojtečkou `', je za <attrtype> zapsána dvojitá dvojtečka a hodnota je uvedena v kódování base-64. Například hodnota " začíná jednou mezerou" by byla kódována takto:

```
cn:: IHph601u4SBqZWRub3UgbWV6ZXJvdQ==
```

Jednotlivé záznamy v témže souboru LDIF jsou odděleny prázdným řádkem. Několik prázdných řádků se považuje za logický konec souboru.

Další informace najdete v těchto částech:

- “Příklad: LDIF”
- “Podpora LDIF verze 1”
- “Příklad: LDIF verze 1” na stránce 218

Příklad: LDIF

Zde je příklad souboru LDIF obsahujícího tři záznamy.

```
dn: cn=John E Doe, o=University of High
  er Learning, c=US
cn: John E Doe
cn: John Doe
objectclass: person
sn: Doe

dn: cn=Bjorn L Doe, o=University of High
  er Learning, c=US
cn: Bjorn L Doe
cn: Bjorn Doe
objectclass: person
sn: Doe

dn: cn=Jennifer K. Doe, o=University of High
  er Learning, c=US
cn: Jennifer K. Doe
cn: Jennifer Doe
objectclass: person
sn: Doe
jpegPhoto:: /9j/4AAQSkZJRgABAAAAQABAAD/2wBDABALD
A4MChAODQ4SERATGCgaGBYWGDEjJR0o0jM9PDkzODdASFxOQ
ERXRTc4UG1RV19iZ2hnPk1xeXBkeFxlZ2P/2wBDARESEhgVG
...
```

Obrázek jpegPhoto v záznamu Jennifer Jensen je zapsán s použitím kódování base-64. Hodnoty textového atributu mohou být rovněž kódovány ve formátu base-64. Pokud tomu tak je, kódování base-64 však musí být v kódové stránce vláknového formátu pro daný protokol (to znamená pro LDAP V2 znaková sada IA5 a pro LDAP V3 kódování UTF-8).

Podpora LDIF verze 1

Klientské obslužné programy (ldapmodify a ldapadd) byly rozšířeny o funkci rozpoznávání nejnovější verze LDIF, podle přítomnosti příznaku "version: 1" v hlavičce souboru. Na rozdíl od původní verze LDIF podporuje novější verze LDIF hodnoty atributů vyjádřené v UTF-8 (namísto velmi omezeného formátu US-ASCII).

Manuální tvorba souboru LDIF obsahujícího hodnoty UTF-8 však může být obtížná. Za účelem zjednodušení tohoto procesu byla zavedena podpora rozšíření znakové sady pro formát LDIF. Toto rozšíření umožňuje zadání jména znakové sady IANA v hlavičce souboru LDIF (společně s číslem verze). Je podporována omezená množina znakových sad IANA.

Formát LDIF verze 1 rovněž podporuje adresu URL souboru. To poskytuje všestrannější způsob definování specifikace souboru. URL souborů mají tuto formu:

```
attribute:< file:///path (kde syntaxe
cesty závisí na platformě)
```

Platné webové adresy jsou například tyto:

```
jpegphoto:< file:///d:\temp\photos\myphoto.jpg
(cesty ve tvaru pro DOS/Windows)
jpegphoto:< file:///etc/temp/photos/myphoto.jpg (cesty tvaru pro Unix)
```

Poznámka: Obslužné programy adresáře IBM podporují jak novou specifikaci URL souboru, tak starší styl ("jpegphoto: /etc/temp/myphoto"), bez ohledu na specifikaci verze. Jinými slovy, nový formát URL souboru je možné používat bez doplňování příznaku verze do souborů LDIF.

Příklad: LDIF verze 1

V souboru LDIF lze používat volitelný příznak znakové sady umožňující obslužným programům provést automatickou konverzi z určené znakové sady na UTF-8, jako v tomto příkladě:

```
version: 1
charset: ISO-8859-1

dn: cn=Juan Griego, o=University of New Mexico, c=US
cn: Juan Griego
sn: Griego
description:: V2hhdCBhIGNhcmVmdWwgcmVhZGVyIH1vd
title: Associate Dean
title: [titulek ve španělštině]
jpegPhoto:> file:///usr/local/photos/jgriego.jpg
```

V tomto případě se všechny hodnoty následující za jménem atributu a jednoduchou dvojtečkou převádějí ze znakové sady ISO-8859-1 do UTF-8. Hodnoty zapsané za jménem atributu a dvojitou dvojtečkou (jako je description:: V2hhdCBhIGNhcm...) musí být kódovány ve formátu base-64 a očekává se, že to budou buď binární řetězce, nebo znakové řetězce ve formátu UTF-8. U hodnot čtených ze souboru, jako je například atribut jpegPhoto specifikovaný webovou adresou ve výše uvedeném příkladě, se rovněž očekává, že budou buď binární, nebo ve formátu UTF-8. U těchto hodnot se neprovádí žádný převod z určené znakové sady "charset" do UTF-8.

V tomto příkladě souboru LDIF bez příznaku charset se očekává, že jeho obsah bude ve formátu UTF-8 nebo se bude jednat o UTF-8 v kódování base-64 či o binární data kódovaná v base-64:

```
# Soubor LDIF IBM Directorysample
#
# Před pokusem o zavedení těchto dat by se měla definovat přípona
# "o=IBM, c=US".

version: 1

dn: o=IBM, c=US
objectclass: top
objectclass: organization
o: IBM

dn: ou=Austin, o=IBM, c=US
ou: Austin
objectclass: organizationalUnit
seealso: cn=Linda Carlesberg, ou=Austin, o=IBM, c=US
```

Stejný soubor jako tento by se mohl použít bez údaje version: 1 v hlavičce, jako v předchozích vydáních adresáře IBM:

```
# Soubor LDIF IBM Directorysample
#
# Před pokusem o zavedení těchto dat by se měla definovat přípona
# "o=IBM, c=US".

dn: o=IBM, c=US
objectclass: top
objectclass: organization
o: IBM
```



```
dn: ou=Austin, o=IBM, c=US
ou: Austin
objectclass: organizationalUnit
seealso: cn=Linda Carlesberg, ou=Austin, o=IBM, c=US
```

Poznámka: Hodnoty textového atributu mohou být kódovány ve formátu base-64.

Schéma konfigurace serveru adresářů

Tyto informace popisují strom DIT (Directory Information Tree) a atributy, které se používají při konfiguraci souboru `ibmslapd.conf`. V předchozích vydáních byla nastavení konfigurace adresáře uložena ve vlastním formátu v konfiguračním souboru. Nastavení adresáře se nyní ukládají s použitím formátu LDIF v konfiguračním souboru.

Tento konfigurační soubor je pojmenován `ibmslapd.conf`. Schéma používané konfiguračním souborem je nyní rovněž dostupné. Typy atributů se nacházejí v souboru `v3.config.at` a třídy objektů jsou uloženy v souboru `v3.config.oc`. Atributy je možné modifikovat pomocí příkazu `ldapmodify`. Další informace o příkazu `ldapmodify` najdete v tématu “`ldapmodify` a `ldapadd`” na stránce 187.

- “Informační strom adresáře (DIT - Directory information tree)”
- “Atributy” na stránce 228

Informační strom adresáře (DIT - Directory information tree)

`cn=Configuration`

- `cn=Admin`
- `cn=Event Notification`
- `cn=Front End`
- `cn=Kerberos`
- `cn=Master Server`
- `cn=Referral`
- `cn=Schema`
 - `cn=IBM Directory`
 - `cn=Config Backends`
 - `cn=ConfigDB`
 - `cn=RDBM Backends`
 - `cn=Directory`
 - `cn=ChangeLog`
 - `cn=LDCF Backends`
 - `cn=SchemaDB`
- `cn=SSL`
 - `cn=CRL`
- `cn=Transaction`

`cn=Configuration`

DN `cn=Configuration`

Popis Toto je záznam s nejvyšší úrovní v konfiguraci stromu DIT. Uchovává data globálního významu pro server, i když v praxi obsahuje rovněž různé další položky. Každý atribut v tomto záznamu pochází z první sekce (global stanza) souboru `ibmslapd.conf`.

Číslo 1 (povinné)

Třída objektu
`ibm-slapdTop`

Povinné atributy

- cn
- ibm-slapdAdminDN
- ibm-slapdAdminPW
- ibm-slapdErrorLog
- ibm-slapdPort
- ibm-slapdPwEncryption
- ibm-slapdSizeLimit
- ibm-slapdSysLogLevel
- ibm-slapdTimeLimit
- objectClass

Volitelné atributy

- ibm-slapdACLAccess
- ibm-slapdACIMechanism
- ibm-slapdConcurrentRW (upouští se)
- ibm-slapdMaxPendingChangesDisplayed
- ibm-slapdServerId
- ibm-slapdSupportedWebAdmVersion
- ibm-slapdVersion

cn=Admin

DN cn=Admin, cn=Configuration

Popis Globální nastavení konfigurace pro IBM Admin Daemon

Číslo 1 (povinné)

Třída objektu

ibm-slapdAdmin

Povinné atributy

- cn
- ibm-slapdErrorLog
- ibm-slapdPort

Volitelné atributy

- ibm-slapdSecurePort

cn=Event Notification

DN cn=Event Notification, cn=Configuration

Popis Nastavení globálního oznamování událostí pro server adresářů

Číslo 0 nebo 1 (volitelné; potřebné pouze tehdy, když chcete povolit oznamování událostí)

Třída objektu

ibm-slapdEventNotification

Povinné atributy

- cn
- ibm-slapdEnableEventNotification
- objectClass

Volitelné atributy

- ibm-slapdMaxEventsPerConnection
- ibm-slapdMaxEventsTotal

cn=Front End

DN cn=Front End, cn=Configuration

Popis Globální nastavení prostředí, která server použije při spuštění.

Číslo 0 nebo 1 (volitelné)

Třída objektu

ibm-slapdFrontEnd

Povinné atributy

- cn
- objectClass

Volitelné atributy

- ibm-slapdACLCache
- ibm-slapdACLCacheSize
- ibm-slapdDB2CP
- ibm-slapdEntryCacheSize
- ibm-slapdFilterCacheBypassLimit
- ibm-slapdFilterCacheSize
- ibm-slapdPlugin
- ibm-slapdSetenv
- ibm-slapdIdleTimeOut

cn=Kerberos

DN cn=Kerberos, cn=Configuration

Popis Globální nastavení autentizace Kerberos pro server adresářů.

Číslo 0 nebo 1 (volitelné)

Třída objektu

ibm-slapdKerberos

Povinné atributy

- cn
- ibm-slapdKrbEnable
- ibm-slapdKrbRealm
- ibm-slapdKrbKeyTab
- ibm-slapdKrbIdentityMap
- ibm-slapdKrbAdminDN
- objectClass

Volitelné atributy

- Žádné

cn=Master Server

DN cn=Master Server, cn=Configuration

Popis Při konfigurování repliky uchovává tento záznam pověření pro připojení a URL odkazu na hlavní server.

Číslo 0 nebo 1 (volitelné)

Třída objektu

ibm-slapdReplication

Povinné atributy

- cn
- ibm-slapdMasterPW (Povinné, pokud se nepoužívá autentizace Kerberos).

Volitelné atributy

- ibm-slapdMasterDN
- ibm-slapdMasterPW (Povinné, pokud se nepoužívá autentizace Kerberos).
- ibm-slapdMasterReferral
- objectClass

cn=Referral

DN cn=Referral, cn=Configuration

Popis Tento záznam obsahuje všechny záznamy odkazů z první sekce (global stanza) souboru ibmslapd.conf. Pokud neexistují žádné odkazy (standardně nejsou žádné), je tento záznam volitelný.

Číslo 0 nebo 1 (volitelné)

Třída objektu

ibm-slapdReferral

Povinné atributy

- cn
- ibm-slapdReferral
- objectClass

Volitelné atributy

- Žádné

cn=Schemas

DN cn=Schemas, cn=Configuration

Popis Tento záznam slouží jako zásobník pro schémata. Záznam není skutečně nezbytný, protože schémata je možné rozpoznávat podle třídy objektu ibm-slapdSchema. Záznam se začleňuje s cílem zlepšit čitelnost stromu DIT.

V současnosti je povolen pouze jeden záznam schématu: cn=IBM Directory.

Číslo 1 (povinné)

Třída objektu

Zásobník

Povinné atributy

- cn
- objectClass

Volitelné atributy

- Žádné

cn=IBM Directory

DN cn=IBM Directory, cn=Schemas, cn=Configuration

Popis Tento záznam obsahuje všechna konfigurační data schématu z první sekce (global stanza) souboru ibmslapd.conf. Slouží rovněž jako zásobník pro všechny procedury backend, které schéma využívají. Vícenásobná schémata nejsou v současnosti podporována, ale kdyby podporována byla, ke každému schématu by byl přiřazen jeden záznam ibm-slapdSchema. Pověšměte si, že vícenásobná schémata jsou považována za nekompatibilní. Procedura backend proto může být přiřazena pouze k jedinému schématu.

Číslo 1 (povinné)

Třída objektu

ibm-slapdSchema

Povinné atributy

- cn
- ibm-slapdSchemaCheck
- ibm-slapdIncludeSchema
- objectClass

Volitelné atributy

- ibm-slapdSchemaAdditions

cn=Config Backends

DN cn=Config Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Popis Tento záznam slouží jako zásobník pro procedury Config Backends.

Číslo 1 (povinné)

Třída objektu

Zásobník

Povinné atributy

- cn
- objectClass

Volitelné atributy

Žádné

cn=ConfigDB

DN cn=ConfigDB, cn=Config Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Popis Konfigurační procedura backend pro konfiguraci serveru adresářů IBM

Číslo 0 - n (volitelné)

Třída objektu

ibm-slapdConfigBackend

Povinné atributy

- ibm-slapdSuffix
- ibm-slapdPlugin

Volitelné atributy

- ibm-slapdReadOnly

cn=RDBM Backends

DN cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Popis Tento záznam slouží jako zásobník pro procedury RDBM Backends. Účinně nahrazuje řádek databáze rdbm ze souboru ibmslapd.conf označením všech podzáznamů jako procedury backend DB2. Tento záznam není skutečně nezbytný, protože RDBM backends je možné rozpoznávat podle třídy objektu ibm-slapdRdbmBackend. Záznam se začleňuje s cílem zlepšit čitelnost stromu DIT.

Číslo 0 nebo 1 (volitelné)

Třída objektu

Zásobník

Povinné atributy

- cn
- objectClass

Volitelné atributy

- Žádné

cn=Directory

DN cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Popis Tento záznam obsahuje všechna nastavení konfigurace databáze pro předvolenou proceduru backend RDBM databáze.

Ačkoli je možné vytvořit několik procedur backend s libovolnými jmény, administrace serveru předpokládá, že hlavní procedurou backend adresáře je "cn=Directory" a že "cn=ChangeLog Log" je volitelnou procedurou backend pro changelog. Pomocí administrace serveru lze konfigurovat pouze přípony zobrazené v "cn=Directory" (s výjimkou přípony protokolu změn, která se nastavuje transparentně při aktivaci protokolu změn).

Číslo 0 - n (volitelné)

Třída objektu

ibm-slapdRdbmBackend

Povinné atributy

- cn
- ibm-slapdDbInstance
- ibm-slapdDbName
- ibm-slapdDbUserID
- objectClass

Volitelné atributy

- ibm-slapdBulkloadErrors
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdDBAlias
- ibm-slapdDB2CP
- ibm-slapdDbConnections
- ibm-slapdDbLocation
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPageSizeLmt
- ibm-slapdPlugin
- ibm-slapdReadOnly
- ibm-slapdReplDbConns

- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSuffix
- ibm-slapdUseProcessIdPw

Poznámka: Jestliže používáte **ibm-slapdUseProcessIdPw**, musíte změnit schéma tak, aby byl atribut **ibm-slapdDbUserPW** volitelný.

cn=Change Log

DN cn=Change Log, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Popis Tento záznam obsahuje všechna nastavení konfigurace databáze pro proceduru typu "backend" změny protokolu.

Číslo 0 - n (volitelné)

Třída objektu

ibm-slapdRdbmBackend

Povinné atributy

- cn
- ibm-slapdDbInstance
- ibm-slapdDbName
- ibm-slapdDbUserID
- objectClass

Volitelné atributy

- ibm-slapdBulkloadErrors
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdDBAlias
- ibm-slapdDB2CP
- ibm-slapdDbConnections
- ibm-slapdDbLocation
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPageSizeLmt
- ibm-slapdPlugin
- ibm-slapdReadOnly
- ibm-slapdReplDbConns
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSuffix
- ibm-slapdUseProcessIdPw

Poznámka: Jestliže používáte **ibm-slapdUseProcessIdPw**, musíte změnit schéma tak, aby byl atribut **ibm-slapdDbUserPW** volitelný.

cn=LDCF Backends

DN cn=LDCF Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Popis Tento záznam slouží jako zásobník pro procedury LDCF Backends. Účinně nahrazuje řádek databáze

ldcf ze souboru ibmslapd.conf označením všech podzáznamů jako procedury LDCF backends. Tento záznam není skutečně nezbytný, protože procedury LDCF backend je možné rozpoznávat podle třídy objektu ibm-slapdLdcfBackend. Záznam se začleňuje s cílem zlepšit čitelnost stromu DIT.

Číslo 1 (povinné)

Třída objektu

Zásobník

Povinné atributy

- cn
- objectClass

Volitelné atributy

- ibm-slapdPlugin

cn=SchemaDB

DN cn=SchemaDB, cn=LDCF Backends, cn=IBM Directory, cn=Schemas, cn=Configuration

Popis Tento záznam obsahuje všechna konfigurační data databáze ze sekce databáze ldcf souboru ibmslapd.conf.

Číslo 1 (povinné)

Třída objektu

ibm-slapdLdcfBackend

Povinné atributy

- cn
- objectClass

Volitelné atributy

- ibm-slapdPlugin
- ibm-slapdSuffix

cn=SSL

DN cn=SSL, cn=Configuration

Popis Globální nastavení připojení SSL pro server adresářů.

Číslo 0 nebo 1 (volitelné)

Třída objektu

ibm-slapdSSL

Povinné atributy

- cn
- ibm-slapdSecurity
- ibm-slapdSecurePort
- ibm-slapdSslAuth
- objectClass

Volitelné atributy

- ibm-slapdSslCertificate
- ibm-slapdSslCipherSpec

Poznámka: Od atributu **ibm-slapdSslCipherSpecs** se nyní upouští. Namísto něj používejte atribut **ibm-slapdSslCipherSpec**. Pokud použijete **ibm-slapdSslCipherSpecs**, server jej převede na podporovaný atribut.

- **ibm-slapdSslKeyDatabase**
- **ibm-slapdSslKeyDatabasePW**

cn=CRL

DN cn=CRL, cn=SSL, cn=Configuration

Popis Tento záznam obsahuje data seznamu odvolaných certifikátů (CRL) z první sekce (global stanza) souboru **ibmslapd.conf**. Je nutný pouze v případě, že za účelem ověření platnosti CRL byl v záznamu **cn=SSL** a v certifikátech klienta zadán atribut **"ibm-slapdSslAuth = serverclientauth"**.

Číslo 0 nebo 1 (volitelné)

Třída objektu

ibm-slapdCRL

Povinné atributy

- **cn**
- **ibm-slapdLdapCrIHost**
- **ibm-slapdLdapCrIPort**
- **objectClass**

Volitelné atributy

- **ibm-slapdLdapCrIUser**
- **ibm-slapdLdapCrIPassword**

cn=Transaction

DN cn = Transaction, cn = Configuration

Popis Uvádí globální nastavení podpory transakcí. Podpora transakcí je poskytována s využitím modulu typu **"plugin"**:

```
extendedop /QSYS.LIB/QGLDTRANEX.SRVPGM tranExtOpInit 1.3.18.0.2.12.5  
1.3.18.0.2.12.6
```

Server (**slapd**) zavádí tento modul typu **"plugin"** automaticky při spuštění, pokud platí **ibm-slapdTransactionEnable = TRUE**. Tento modul typu **"plugin"** není nutné do souboru **ibmslapd.conf** explicitně doplňovat.

Číslo 0 nebo 1 (volitelné; vyžadováno pouze tehdy, když chcete používat transakce).

Třída objektu

ibm-slapdTransaction

Povinné atributy

- **cn**
- **ibm-slapdMaxNumOfTransactions**
- **ibm-slapdMaxOpPerTransaction**
- **ibm-slapdMaxTimeLimitOfTransactions**
- **ibm-slapdTransactionEnable**
- **objectClass**

Volitelné atributy

- Žádné

Atributy

- cn
- ibm-slapdACIMechanism
- ibm-slapdACLAccess
- ibm-slapdACLCache
- ibm-slapdACLCacheSize
- ibm-slapdAdminDN
- | • ibm-slapdAdminGroupEnabled
- ibm-slapdAdminPW
- | • ibm-slapdAllowAnon
- | • ibm-slapdAllReapingThreshold
- | • ibm-slapdAnonReapingThreshold
- | • ibm-slapdBoundReapingThreshold
- ibm-slapdBulkloadErrors
- | • ibm-slapdCachedAttribute
- | • ibm-slapdCachedAttributeAutoAdjust
- | • ibm-slapdCachedAttributeAutoAdjustTime
- | • ibm-slapdCachedAttributeAutoAdjustTimeInterval
- | • ibm-slapdCachedAttributeSize
- ibm-slapdChangeLogMaxEntries
- ibm-slapdCLIErrors
- ibm-slapdConcurrentRW
- ibm-slapdDB2CP
- ibm-slapdDBAlias
- ibm-slapdDbConnections
- ibm-slapdDbInstance
- ibm-slapdDbLocation
- ibm-slapdDbName
- ibm-slapdDbUserID
- ibm-slapdDbUserPW
- | • ibm-slapdDerefAliases
- | • ibm-slapdDigestAdminUser
- | • ibm-slapdDigestAttr
- | • ibm-slapdDigestRealm
- ibm-slapdEnableEventNotification
- ibm-slapdEntryCacheSize
- ibm-slapdErrorLog
- | • ibm-slapdESizeThreshold
- | • ibm-slapdEThreadActivate
- | • ibm-slapdEThreadEnable
- | • ibm-slapdETimeThreshold
- ibm-slapdFilterCacheBypassLimit
- ibm-slapdFilterCacheSize
- ibm-slapdIdleTimeOut
- ibm-slapdIncludeSchema

- ibm-slapdKrbAdminDN
- ibm-slapdKrbEnable
- ibm-slapdKrbIdentityMap
- ibm-slapdKrbKeyTab
- ibm-slapdKrbRealm
- | • ibm-slapdLanguageTagsEnabled
- ibm-slapdLdapCrIHost
- ibm-slapdLdapCrIPassword
- ibm-slapdLdapCrIPort
- ibm-slapdLdapCrIUser
- ibm-slapdMasterDN
- ibm-slapdMasterPW
- ibm-slapdMasterReferral
- ibm-slapdMaxEventsPerConnection
- ibm-slapdMaxEventsTotal
- ibm-slapdMaxNumOfTransactions
- ibm-slapdMaxOpPerTransaction
- ibm-slapdMaxPendingChangesDisplayed
- ibm-slapdMaxTimeLimitOfTransactions
- ibm-slapdPagedResAllowNonAdmin
- ibm-slapdPagedResLmt
- ibm-slapdPageSizeLmt
- ibm-slapdPlugin
- ibm-slapdPort
- ibm-slapdPwEncryption
- ibm-slapdReadOnly
- ibm-slapdReferral
- ibm-slapdReplDbConns
- ibm-slapdReplicaSubtree
- ibm-slapdSchemaAdditions
- ibm-slapdSchemaCheck
- ibm-slapdSecurePort
- ibm-slapdSecurity
- ibm-slapdServerId
- ibm-slapdSetenv
- ibm-slapdSizeLimit
- ibm-slapdSortKeyLimit
- ibm-slapdSortSrchAllowNonAdmin
- ibm-slapdSslAuth
- ibm-slapdSslCertificate
- ibm-slapdSslCipherSpec
- ibm-slapdSslKeyDatabase
- ibm-slapdSslKeyDatabasePW
- ibm-slapdSslKeyRingFile
- ibm-slapdSuffix

- ibm-slapdSupportedWebAdmVersion
- ibm-slapdSysLogLevel
- ibm-slapdTimeLimit
- ibm-slapdTransactionEnable
- ibm-slapdUseProcessIdPw
- ibm-slapdVersion
- ibm-slapdWriteTimeout
- objectClass

cn

Popis Toto je atribut obecného jména X.500, který obsahuje jméno objektu.

Syntaxe

Adresářový řetězec

Maximální délka

256

Počet hodnot

Více hodnot

ibm-slapdACIMechanism

Popis Určuje, který model seznamu ACL server používá (podporováno pouze v operačním systému i5/OS a OS/400 od verze 3.2, na ostatních platformách ignorováno).

- 1.3.18.0.2.26.1 = model ACL IBM SecureWay v3.1
- 1.3.18.0.2.26.2 = model ACL IBM SecureWay v3.2

Předvolená hodnota

1.3.18.0.2.26.2 = model ACL IBM SecureWay v3.2

Syntaxe

Adresářový řetězec

Maximální délka

256

Počet hodnot

Více hodnot

ibm-slapdACLAccess

Popis Určuje, zda je povolen přístup k seznamům ACL. Jestliže je nastaven na hodnotu TRUE, přístup k seznamům ACL je povolen. Pokud je nastaven na hodnotu FALSE, přístup k seznamům ACL je zakázán.

Předvolená hodnota

TRUE

Syntaxe

Booleovská hodnota

Maximální délka

5

Počet hodnot

Jedna hodnota

ibm-slapdACLCache

Popis Určuje, zda server ukládá informace seznamu ACL do rychlé vyrovnávací paměti.

- Jestliže je nastaven na hodnotu TRUE, server ukládá informace seznamu ACL do rychlé vyrovnávací paměti.
- Pokud je nastaven na hodnotu FALSE, server informace seznamu ACL do rychlé vyrovnávací paměti neukládá.

Předvolená hodnota

TRUE

Syntaxe

Booleovská hodnota

Maximální délka

5

Počet hodnot

Jedna hodnota

ibm-slapdACLCacheSize

Popis Maximální počet záznamů, které se mají uchovávat v rychlé vyrovnávací paměti seznamu ACL.

Předvolená hodnota

25000

Syntaxe

Celočíselná hodnota

Maximální délka

11

Počet hodnot

Jedna hodnota

ibm-slapdAdminDN

Popis Připojovací DN administrátora pro server adresářů.

Předvolená hodnota

cn=root

Syntaxe

DN

Maximální délka

Neomezená

Počet hodnot

Jedna hodnota

ibm-slapdAdminGroupEnabled

Popis Uvádí, zda je momentálně aktivována administrační skupina. Pokud je nastaven na TRUE, server povolí členům administrační skupiny přihlašovat se.

Předvolená hodnota

FALSE

Syntaxe

Booleovská hodnota

Maximální délka

128

| **Počet hodnot**
| Jedna hodnota

ibm-slapdAdminPW

Popis Heslo připojení administrátora pro server adresářů.

Předvolená hodnota
secret

Syntaxe
Binární hodnota

Maximální délka
128

Počet hodnot
Jedna hodnota

| **ibm-slapdAllowAnon**

| **Popis** Uvádí, zda jsou povolena anonymní připojení.

| **Předvolená hodnota**
| True

| **Syntaxe**
| Booleovská hodnota

| **Maximální délka**
| 128

| **Počet hodnot**
| Jedna hodnota

| **ibm-slapdAllReapingThreshold**

Popis Uvádí počet spojení, které se na serveru udržují, než je aktivována správa připojení.

Předvolená hodnota
1200

Syntaxe
Adresářový řetězec s přesným rozlišením velikosti písmen.

Maximální délka
1024

Počet hodnot
Jedna hodnota

| **ibm-slapdAnonReapingThreshold**

Popis Uvádí počet spojení, které se na serveru udržují, než je aktivována správa připojení pro anonymní spojení.

Předvolená hodnota
0

Syntaxe
Adresářový řetězec s přesným rozlišením velikosti písmen.

Maximální délka
1024

Počet hodnot

Jedna hodnota

| ibm-slapdBoundReapingThreshold

| Popis Uvádí počet spojení, které se na serveru udržují, než je aktivována správa připojení pro anonymní a připojená spojení.

| Předvolená hodnota

| 1100

| Syntaxe

| Adresářový řetězec s přesným rozlišením velikosti písmen.

| Maximální délka

| 1024

| Počet hodnot

| Jedna hodnota

ibm-slapdBulkloadErrors

Popis Cesta k souboru nebo zařízení na hostitelském počítači ibmslapd, do kterých budou zapsány chybové zprávy bulkload.

Předvolená hodnota

/var/bulkload.log

Syntaxe

Adresářový řetězec s přesným rozlišením velikosti písmen

Maximální délka

1024

Počet hodnot

Jedna hodnota

| ibm-slapdCachedAttribute

| Popis Obsahuje jména atributů, které se budou ukládat do paměti cache atributů, jedno jméno atributu na jednu hodnotu.

| Předvolená hodnota

| Žádné

| Syntaxe

| Adresářový řetězec

| Maximální délka

| 256

| Počet hodnot

| Více hodnot

| ibm-slapdCachedAttributeAutoAdjust

| Popis Řídí, zda server bude automaticky upravovat paměti cache atributů v nakonfigurovaných časových intervalech definovaných v `ibm-slapdCachedAttributeAutoAdjustTime` a `ibm-slapdCachedAttributeAutoAdjustTimeInterval`.

| Předvolená hodnota

| FALSE

| Syntaxe

| Booleovská hodnota

| **Maximální délka**

| 5

| **Počet hodnot**

| Jedna hodnota

| **ibm-slapdCachedAttributeAutoAdjustTime**

| **Popis** Řídí čas, kdy server automaticky upravuje paměti cache atributů, pokud je parametr
| ibm-slapdCachedAttributeAutoAdjust nastaven na hodnotu TRUE.

| Minimum = T000000

| Maximum = T235959

| **Předvolená hodnota**

| T000000

| **Syntaxe**

| Vojenský způsob udávání času

| **Maximální délka**

| 7

| **Počet hodnot**

| Jedna hodnota

| **ibm-slapdCachedAttributeAutoAdjustTimeInterval**

| **Popis** Řídí časový interval (v hodinách) mezi automatickými úpravami paměti cache atributů, pokud je
| parametr ibm-slapdCachedAttributeAutoAdjust nastaven na hodnotu TRUE.

| Minimum = 1

| Maximum = 24

| **Předvolená hodnota**

| 2

| **Syntaxe**

| Celočíselná hodnota

| **Maximální délka**

| 2

| **Počet hodnot**

| Jedna hodnota

| **ibm-slapdCachedAttributeSize**

Popis Množství paměti v bajtech, které lze použít pro paměť cache atributů. Hodnota 0 naznačuje, že se paměť
cache atributů nepoužívá.

Předvolená hodnota

0

Syntaxe

Celočíselná hodnota

Maximální délka

11

Počet hodnot

Jedna hodnota

ibm-slapdChangeLogMaxEntries

Popis Tento atribut je používán modulem plug-in protokolu změn pro určení maximálního počtu záznamů v protokolu změn povoleného v databázi RDBM. Každý protokol změn má svůj vlastní atribut changeLogMaxEntries.

Minimální počet = 0 (neomezeno)

Maximální počet = 2,147,483,647 (32bitové, podepsaná celočíselná hodnota)

Předvolená hodnota

0

Syntaxe

Celočíselná hodnota

Maximální délka

11

Počet hodnot

Jedna hodnota

ibm-slapdCLIErrors

Popis Cesta k souboru nebo zařízení na hostitelském počítači ibmslapd, do kterých budou zapsány chybové zprávy CLI.

Předvolená hodnota

/var/db2cli.log

Syntaxe

Adresářový řetězec s přesným rozlišením velikosti písmen

Maximální délka

1024

Počet hodnot

Jedna hodnota

ibm-slapdConcurrentRW

Popis Nastavení tohoto atributu na TRUE umožní provádět vyhledávání souběžně s aktualizacemi. To připouští tzv. 'nečistá čtení', to znamená, že může vést k výsledkům, které nejsou shodné s hlášeným stavem databáze.

Upozornění: Od tohoto atributu se nyní upouští.

Předvolená hodnota

FALSE

Syntaxe

Booleovská hodnota

Maximální délka

5

Počet hodnot

Jedna hodnota

ibm-slapdDB2CP

Popis Určuje kódovou stránku adresářové databáze. Kódová stránka pro databáze UTF-8 je 1208.

Syntaxe

Adresářový řetězec s přesným rozlišením velikosti písmen

Maximální délka

11

Počet hodnot

Jedna hodnota

ibm-slapdDBAlias

Popis Alias pro databázi DB2.

Syntaxe

Adresářový řetězec s přesným rozlišením velikosti písmen

Maximální délka

8

Počet hodnot

Jedna hodnota

ibm-slapdDbConnections

Popis Určuje počet připojení DB2, které server věnuje proceduře DB2 backend. Hodnota musí být v rozsahu od 5 do 50 (včetně).

Poznámka: Hodnotu této instrukce potlačuje proměnná prostředí ODBCCONS.

Pokud je hodnota `ibm-slapdDbConnections` (nebo `ODBCCONS`) nižší než 5 nebo vyšší než 50, server použije hodnotu 5, případně 50. Pro replikaci bude vytvořeno jedno přídavné připojení (i když není definována žádná replikace). Pro protokol změn budou vytvořena dvě další připojení (pokud je protokol změn aktivován).

Předvolená hodnota

15

Syntaxe

Celočíselná hodnota

Maximální délka

50

Počet hodnot

Jedna hodnota

ibm-slapdDbInstance

Popis Určuje instance databáze DB2 pro tuto proceduru backend.

Předvolená hodnota

ldapdb2

Syntaxe

Adresářový řetězec s přesným rozlišením velikosti písmen

Maximální délka

8

Počet hodnot

Jedna hodnota

Poznámka: Všechny objekty `ibm-slapdRdbmBackend` musí používat stejnou `ibm-slapdDbInstance`, `ibm-slapdDbUserID`, `ibm-slapdDbUserPW` a znakovou sadu DB2.

ibm-slapdDbLocation

Popis Cesta systému souborů k umístění databáze procedury backend.

Syntaxe

Adresářový řetězec s přesným rozlišením velikosti písmen

Maximální délka

1024

Počet hodnot

Jedna hodnota

ibm-slapdDbName**Popis** Určuje jméno databáze DB2 pro tuto proceduru backend.**Předvolená hodnota**

ldapdb2

Syntaxe

Adresářový řetězec s přesným rozlišením velikosti písmen

Maximální délka

8

Počet hodnot

Jedna hodnota

ibm-slapdDbUserID**Popis** Určuje jméno uživatele, se kterým se má provádět připojení k databázi DB2 pro tuto proceduru backend.**Předvolená hodnota**

ldapdb2

Syntaxe

Adresářový řetězec s přesným rozlišením velikosti písmen

Maximální délka

8

Počet hodnot

Jedna hodnota

Poznámka: Všechny objekty `ibm-slapdRdbmBackend` musí používat stejnou `ibm-slapdDbInstance`, `ibm-slapdDbUserID`, `ibm-slapdDbUserPW` a znakovou sadu DB2.**| ibm-slapdDerefAliases****| Popis** Maximální úroveň dereference aliasů u vyhledávacích požadavků, bez ohledu na parametry `derefAliases`, které by byly zadány v požadavcích klientů. Povolené hodnoty jsou **never**, **find**, **search** a **always**.**| Předvolená hodnota****|** always**| Syntaxe****|** Adresářový řetězec**| Maximální délka****|** 6**| Počet hodnot****|** Jedna hodnota**ibm-slapdDbUserPW****Popis** Určuje heslo uživatele, se kterým se má provádět připojení k databázi DB2 pro tuto proceduru backend. Heslo může být prostý text nebo šifrované metodou `imask`.

Předvolená hodnota

ldapdb2

Syntaxe

Binární hodnota

Maximální délka

128

Počet hodnot

Jedna hodnota

Poznámka: Všechny objekty `ibm-slapdRdbmBackend` musí používat stejnou `ibm-slapdDbInstance`, `ibm-slapdDbUserID`, `ibm-slapdDbUserPW` a znakovou sadu DB2.

| ibm-slapdDigestAdminUser

| Popis Uvádí uživatelské jméno Digest MD5 administrátora LDAP nebo člena administrační skupiny. Používá se, když se k ověřování identity administrátorů používá autentizace MD5 Digest.

| Předvolená hodnota

| Žádné

| Syntaxe

| Adresářový řetězec

| Maximální délka

| 512

| Počet hodnot

| Jedna hodnota

| ibm-slapdDigestAttr

| Popis Přepisuje předvolený atribut DIGEST-MD5 username. Jméno atributu, které se má použít pro vyhledávání připojovacího uživatelského jména DIGEST-MD5 SASL. Není-li tato hodnota zadána, server použije uid.

| Předvolená hodnota

| Není-li zadáno, server použije uid.

| Syntaxe

| Adresářový řetězec.

| Maximální délka

| 64

| Počet hodnot

| Jedna hodnota

| ibm-slapdDigestRealm

| Popis Přepisuje předvolenou sféru DIGEST-MD5. Řetězec, který uživatelům dává vědět, které uživatelské jméno a heslo mají použít, v případě, že mohou mít různá hesla na různé servery. Konceptně to je jméno sady účtů, která by mohla obsahovat účet uživatele. Tento řetězec by měl obsahovat alespoň jméno hostitele provádějícího autentizaci a kromě toho by mohl označovat sadu uživatelů, kteří mohou mít přístup. Příkladem by mohlo být: `registered_users@gotham.news.example.com`. Není-li tento atribut zadán, server použije plně kvalifikované jméno hostitele serveru.

| Předvolená hodnota

| Plně kvalifikované jméno hostitele serveru

| Syntaxe

| Adresářový řetězec

	Maximální délka
	1024
	Počet hodnot
	Jedna hodnota

ibm-slapdEnableEventNotification

Popis Určuje, zda se má aktivovat oznamování událostí. Tento atribut musí být nastaven buď na hodnotu TRUE, nebo FALSE.

Jestliže je nastaven na hodnotu FALSE, server zamítá všechny požadavky klientů na registraci oznámení událostí s rozšířeným výsledkem LDAP_UNWILLING_TO_PERFORM.

Předvolená hodnota
TRUE

Syntaxe
Booleovská hodnota

Maximální délka
5

Počet hodnot
Jedna hodnota

ibm-slapdEntryCacheSize

Popis Maximální počet záznamů, které se mají uchovávat v rychlé vyrovnávací paměti záznamu.

Předvolená hodnota
25000

Syntaxe
Celočíselná hodnota

Maximální délka
11

Počet hodnot
Jedna hodnota

ibm-slapdErrorLog

Popis Určuje cestu k souboru nebo zařízení na systému serveru adresářů, do kterého se zapisují chybové zprávy.

Předvolená hodnota
/var/ibmslapd.log

Syntaxe
Adresářový řetězec s přesným rozlišením velikosti písmen

Maximální délka
1024

Počet hodnot
Jedna hodnota

| **ibm-slapdESizeThreshold**

| **Popis** Uvádí počet položek v pracovní frontě předtím, než se aktivuje nouzové vlákno.

| **Předvolená hodnota**
| 50

| **Syntaxe**
| Celočíselná hodnota

| **Maximální délka**
| 1024

| **Počet hodnot**
| Jedna hodnota

| **ibm-slapdEThreadActivate**

| **Popis** Uvádí, při jakých podmínkách se aktivuje nouzové vlákno. Atribut musí být nastaven na jednu z těchto hodnot:

| **S** Pouze velikost

| **T** Pouze čas

| **SOT** Velikost nebo čas

| **SAT** Velikost a čas

| **Předvolená hodnota**
| SAT

| **Syntaxe**
| Řetězec

| **Maximální délka**
| 1024

| **Počet hodnot**
| Jedna hodnota

| **ibm-slapdEThreadEnable**

| **Popis** Uvádí, zda je nouzové vlákno aktivní.

| **Předvolená hodnota**
| True

| **Syntaxe**
| Booleovská hodnota

| **Maximální délka**
| 1024

| **Počet hodnot**
| Jedna hodnota

| **ibm-slapdETimeThreshold**

| **Popis** Uvádí množství času v minutách mezi položkami odstraněnými z pracovní fronty předtím, než je aktivováno nouzové vlákno.

| **Předvolená hodnota**
| 5

| **Syntaxe**
| Celočíselná hodnota

| **Maximální délka**
| 1024

| **Počet hodnot**
| Jedna hodnota

ibm-slapdFilterCacheBypassLimit

Popis Filtry hledání, které odpovídají více než tomuto počtu záznamů, nebudou přidány do rychlé vyrovnávací paměti filtru hledání. Poněvadž seznam ID záznamů, které odpovídají filtru, je obsažen v této rychlé vyrovnávací paměti, toto nastavení pomáhá omezovat použití paměti. Hodnota 0 označuje neomezený počet.

Předvolená hodnota

100

Syntaxe

Celočíselná hodnota

Maximální délka

11

Počet hodnot

Jedna hodnota

ibm-slapdFilterCacheSize

Popis Určuje maximální počet záznamů, které se mají uchovávat v rychlé vyrovnávací paměti seznamu filtru hledání.

Předvolená hodnota

25000

Syntaxe

Celočíselná hodnota

Maximální délka

11

Počet hodnot

Jedna hodnota

ibm-slapdIdleTimeOut

Popis Maximální doba, po kterou se má udržovat připojení LDAP otevřené, když na tomto spoji neprobíhá žádná činnost. Doba nečinnosti pro připojení LDAP je doba (v sekundách) mezi poslední činností na spoji a aktuálním časem. Pokud vypršela platnost tohoto připojení z důvodu větší délky doby nečinnosti, než je hodnota tohoto atributu, server LDAP se vyčistí, ukončí připojení LDAP a zpřístupní je pro ostatní příchozí požadavky.

Předvolená hodnota

300

Syntaxe

Celočíselná hodnota

Délka 11

Počítání

Jednoduché

Použití Činnost adresáře

Uživatelské modifikace

Ano

Přístupová třída

Kritická

Povinné

Ne

ibm-slapdIncludeSchema

Popis Určuje cestu k souboru na serverovém stroji serveru adresářů obsahujícím definice schémat.

Předvolená hodnota

/etc/V3.system.at
/etc/V3.system.oc
/etc/V3.config.at
/etc/V3.config.oc
/etc/V3.ibm.at
/etc/V3.ibm.oc
/etc/V3.user.at
/etc/V3.user.oc
/etc/V3.ldapsyntaxes
/etc/V3.matchingrules

Syntaxe

Adresářový řetězec s přesným rozlišením velikosti písmen

Maximální délka

1024

Počet hodnot

Více hodnot

ibm-slapdKrbAdminDN

Popis Určuje ID pro autentizaci Kerberos administrátora LDAP (například `ibm-kn=admin1@realm1`). Používá se tehdy, když se pro ověření identity administrátora při připojení k rozhraní administrace serveru využívá autentizace Kerberos. Tento ID může být určen místo `adminDN` a `adminPW` nebo navíc k nim.

Předvolená hodnota

Není definována žádná předvolená hodnota.

Syntaxe

Adresářový řetězec s přesným rozlišením velikosti písmen

Maximální délka

128

Počet hodnot

Jedna hodnota

ibm-slapdKrbEnable

Popis Určuje, zda server podporuje autentizaci Kerberos. Atribut musí být nastaven buď na hodnotu `TRUE`, nebo `FALSE`.

Předvolená hodnota

`TRUE`

Syntaxe

Booleovská hodnota

Maximální délka

5

Počet hodnot

Jedna hodnota

ibm-slapdKrbIdentityMap

Popis Určuje, zda se má použít mapování identity Kerberos. Tento atribut musí být nastaven buď na hodnotu TRUE, nebo FALSE. Jestliže je nastaven na TRUE a klient provádí autentizaci s ID Kerberos, server vyhledává všechny místní uživatele s odpovídajícími pověřeními Kerberos a přidá tato uživatelská jména DN do pověření daného připojení. To umožňuje u autentizace Kerberos stále využívat seznamy ACL na základě jmen DN uživatelů LDAP.

Předvolená hodnota

FALSE

Syntaxe

Booleovská hodnota

Maximální délka

5

Počet hodnot

Jedna hodnota

ibm-slapdKrbKeyTab

Popis Určuje soubor klíčů Kerberos pro server LDAP. Tento soubor obsahuje soukromý klíč serveru LDAP, který je přiřazen k jeho účtu Kerberos. Tento soubor má být chráněn (jako soubor databáze klíčů SSL serveru).

Předvolená hodnota

Není definována žádná předvolená hodnota.

Syntaxe

Adresářový řetězec s přesným rozlišením velikosti písmen

Maximální délka

1024

Počet hodnot

Jedna hodnota

ibm-slapdKrbRealm

Popis Určuje sféru Kerberos serveru LDAP. Používá se pro publikování atributu ldapservicename v kořenovém DSE. Povšimněte si, že server LDAP může sloužit jako schránka informací o účtech pro více KDC (a sfér), ale server LDAP jakožto server využívající autentizaci Kerberos může být členem pouze jediné sféry.

Předvolená hodnota

Není definována žádná předvolená hodnota.

Syntaxe

Adresářový řetězec bez rozlišení velikosti písmen

Maximální délka

256

Počet hodnot

Jedna hodnota

| **ibm-slapdLanguageTagsEnabled**

| **Popis** Uvádí, zda má server povolit jazykové příznaky. Hodnota pro tento atribut načtená ze souboru
| ibmslapd.conf je FALSE, ale lze ji nastavit na TRUE.

| **Předvolená hodnota**

| FALSE

	Syntaxe
	Booleovská hodnota
	Maximální délka
	5
	Počet hodnot
	Jedna hodnota

ibm-slapdLdapCrlHost

Popis Určuje hostitelské jméno serveru LDAP, který obsahuje seznamy odvolaných certifikátů CRL (Certificate Revocation List) pro ověřování platnosti certifikátů x.509v3 klienta. Tento parametr je nutný, pokud byly pro ověření platnosti CRL vydány `ibm-slapdSslAuth=serverclientauth` a certifikáty klienta.

Předvolená hodnota
Není definována žádná předvolená hodnota.

Syntaxe
Adresářový řetězec bez rozlišení velikosti písmen

Maximální délka
256

Počet hodnot
Jedna hodnota

ibm-slapdLdapCrlPassword

Popis Určuje heslo, které používá SSL na straně serveru pro připojení k serveru LDAP, který obsahuje seznamy odvolaných certifikátů CRL (Certificate Revocation List) pro ověřování platnosti certifikátů x.509v3 klienta. Tento parametr může být nutný, pokud byly pro ověření platnosti CRL vydány `ibm-slapdSslAuth=serverclientauth` a certifikáty klienta.

Poznámka: Jestliže server LDAP uchovávající seznamy CRL povoluje neautentizovaný přístup k seznamům CRL (to znamená anonymní přístup), atribut `ibm-slapdLdapCrlPassword` není povinný.

Předvolená hodnota
Není definována žádná předvolená hodnota.

Syntaxe
Binární hodnota

Maximální délka
128

Počet hodnot
Jedna hodnota

ibm-slapdLdapCrlPort

Popis Určuje port používaný pro připojení k serveru LDAP, který obsahuje seznamy odvolaných certifikátů CRL (Certificate Revocation List) pro ověřování platnosti certifikátů x.509v3 klienta. Tento parametr je nutný, pokud byly pro ověření platnosti CRL vydány `ibm-slapdSslAuth=serverclientauth` a certifikáty klienta. (porty IP jsou nepodepsané 16bitové celočíselné hodnoty v rozmezí 1 - 65535).

Předvolená hodnota
Není definována žádná předvolená hodnota.

Syntaxe
Celočíselná hodnota

Maximální délka

11

Počet hodnot

Jedna hodnota

ibm-slapdLdapCrlUser

Popis Určuje jméno bindDN, které používá SSL na straně serveru pro připojení k serveru LDAP, který obsahuje seznamy odvolaných certifikátů CRL (Certificate Revocation List) pro ověřování platnosti certifikátů x.509v3 klienta. Tento parametr může být nutný, pokud byly pro ověření platnosti CRL vydány `ibm-slapdSslAuth=serverclientauth` a certifikáty klienta.

Poznámka: Jestliže server LDAP uchovávající seznamy CRL povoluje neautentizovaný přístup k seznamům CRL (to znamená anonymní přístup), atribut `ibm-slapdLdapCrlUser` není povinný.

Předvolená hodnota

Není definována žádná předvolená hodnota.

Syntaxe

DN

Maximální délka

1000

Počet hodnot

Jedna hodnota

ibm-slapdMasterDN

Popis Určuje přípojovací DN hlavního serveru. Hodnota musí odpovídat atributu `replicaBindDN` v třídě objektu `replicaObject` definované pro hlavní server. Když se pro autentizaci do repliky používá Kerberos, musí atribut `ibm-slapdMasterDN` určit vyjádření DN pro ID Kerberos (například `ibm-kn=freddy@realm1`). Když se používá autentizace Kerberos, atribut `MasterServerPW` se ignoruje.

Předvolená hodnota

Není definována žádná předvolená hodnota.

Syntaxe

DN

Maximální délka

1000

Počet hodnot

Jedna hodnota

ibm-slapdMasterPW

Popis Určuje přípojovací heslo hlavního replikovaného serveru. Hodnota musí odpovídat atributu `replicaBindDN` v třídě objektu `replicaObject` definované pro hlavní server. Když se pro autentizaci do repliky používá Kerberos, musí atribut `ibm-slapdMasterDN` určit vyjádření DN pro ID Kerberos (například `ibm-kn=freddy@realm1`). Když se používá autentizace Kerberos, atribut `MasterServerPW` se ignoruje.

Předvolená hodnota

Není definována žádná předvolená hodnota.

Syntaxe

Binární hodnota

Maximální délka

128

Počet hodnot

Jedna hodnota

ibm-slapdMasterReferral**Popis** Určuje URL hlavního replikovaného serveru. Například:

ldap://master.us.ibm.com

Pro zabezpečení nastavené pouze na SSL:

ldaps://master.us.ibm.com:636

Pro zabezpečení nastavené na "none" (žádné) a používající nestandardní port:

ldap://master.us.ibm.com:1389

Předvolená hodnota

none

Syntaxe

Adresářový řetězec bez rozlišení velikosti písmen

Maximální délka

256

Počet hodnot

Jedna hodnota

ibm-slapdMaxEventsPerConnection**Popis** Určuje maximální počet oznámení událostí, které je možné registrovat při jednom připojení.

Minimální počet = 0 (neomezeno)

Maximální počet = 2,147,483,647

Předvolená hodnota

100

Syntaxe

Celočíselná hodnota

Maximální délka

11

Počet hodnot

Jedna hodnota

ibm-slapdMaxEventsTotal**Popis** Určuje maximální celkový počet oznámení událostí, které je možné registrovat při všech připojeních.

Minimální počet = 0 (neomezeno)

Maximální počet = 2,147,483,647

Předvolená hodnota

0

Syntaxe

Celočíselná hodnota

Maximální délka

11

Počet hodnot

Jedna hodnota

ibm-slapdMaxNumOfTransactions

Popis Určuje maximální počet transakcí na server.

Minimální počet = 0 (neomezeno)

Maximální počet = 2,147,483,647

Předvolená hodnota

20

Syntaxe

Celočíselná hodnota

Maximální délka

11

Počet hodnot

Jedna hodnota

ibm-slapdMaxOpPerTransaction

Popis Určuje maximální počet operací an transakci.

Minimální počet = 0 (neomezeno)

Maximální počet = 2,147,483,647

Předvolená hodnota

5

Syntaxe

Celočíselná hodnota

Maximální délka

11

Počet hodnot

Jedna hodnota

ibm-slapdMaxPendingChangesDisplayed

Popis Maximální počet nevyřízených změn, které se mají zobrazit.

Předvolená hodnota

200

Syntaxe

Celočíselná hodnota

Maximální délka

11

Počet hodnot

Jedna hodnota

ibm-slapdMaxTimeLimitOfTransactions

Popis Určuje maximální hodnotu časového limitu nevyřízených transakcí v sekundách.

Minimální počet = 0 (neomezeno)

Maximální počet = 2,147,483,647

Předvolená hodnota

300

Syntaxe

Celočíselná hodnota

Maximální délka

11

Počet hodnot

Jedna hodnota

ibm-slapdPagedResAllowNonAdmin

Popis Určuje, zda má server při požadavku vyhledávání u připojení uživatele nespádajícího do kategorie administrátorů povolit požadavek na stránkování výsledků. Jestliže hodnota načtená ze souboru ibmslapd.conf je FALSE, server zpracuje pouze takové klientské požadavky, které zadal uživatel s oprávněním administrátora. Pokud nějaký klient zadá požadavek na stránkování výsledků z operace vyhledávání, nemá oprávnění administrátora a hodnota načtená ze souboru ibmslapd.conf pro tento atribut je FALSE, server vrátí klientovi návratový kód insufficientAccessRights; nebude provedeno žádné hledání ani stránkování.

Předvolená hodnota

FALSE

Syntaxe

Booleovská hodnota

Délka 5**Počítání**

Jednoduché

Použití directoryOperation

Uživatelské modifikace

Ano

Přístupová třída

kritická

Třída objektu

ibm-slapdRdbmBackend

Povinné

Ne

ibm-slapdPagedResLmt

Popis Maximální počet souběžně aktivních povolených neprovedených požadavků na vyhledávání se stránkováním výsledků. Rozsah = 0.... Pokud nějaký klient zadá požadavek na stránkování výsledků z operace vyhledávání a aktuálně je aktivní maximální počet neprovedených stránkovaných výsledků, server vrátí klientovi návratový kód "busy" (zanepřázdněný); nebude provedeno žádné hledání ani stránkování.

Předvolená hodnota

3

Syntaxe

Celočíselná hodnota

Délka 11**Počítání**

Jednoduché

Použití directoryOperation

Uživatelské modifikace

Ano

Přístupová třída

kritická

Povinné

Ne

Třída objektu

ibm-slapdRdbmBackend

ibm-slapdPageSizeLmt

Popis Maximální počet záznamů, který se má vrátit z hledání na jednotlivé stránce, když je určeno řízení stránkovaných výsledků, bez ohledu na jakoukoli hodnotu pagesize, která mohla být určena v požadavku klienta na hledání. Rozsah = 0.... Jestliže klient zadal velikost stránky, načte se hodnota ze souboru ibmslapd.conf, porovná se s klientovou hodnotou a bude použita ta hodnota, která je nižší.

Předvolená hodnota

50

Syntaxe

Celočíselná hodnota

Délka 11**Počítání**

Jednoduché

Použití directoryOperation**Uživatelské modifikace**

Ano

Přístupová třída

kritická

Povinné

Ne

Třída objektu

ibm-slapdRdbmBackend

ibm-slapdPlugin

Popis Modul typu "plugin" je dynamicky zaváděná knihovna, která rozšiřuje možnosti serveru. Atribut ibm-slapdPlugin určuje serveru, jakým způsobem má zavádět a inicializovat knihovnu typu "plug-in".
Syntaxe je:

```
keyword filename init_function [args...]
```

Syntaxe je pro každou platformu poněkud odlišná z důvodu konvencí pojmenování knihovny.

Většina modulů typu "plug-in" je volitelná, ale modul "plugin" procedury "backend" RDBM je povinný pro všechny procedury RDBM typu "backend".

Předvolená hodnota

databáze /bin/libback-rdbm.dll rdbm_backend_init

Syntaxe

Adresářový řetězec s přesným rozlišením velikosti písmen

Maximální délka

2000

Počet hodnot

Více hodnot

ibm-slapdPort

Popis Určuje port TCP/IP používaný pro připojení nevyužívající zabezpečení SSL. Tento atribut nemůže mít stejnou hodnotu jako `ibm-slapdSecurePort` (porty IP jsou nepodepsané 16bitové celočíselné hodnoty v rozmezí 1 - 65535).

Předvolená hodnota

389

Syntaxe

Celočíselná hodnota

Maximální délka

5

Počet hodnot

Jedna hodnota

ibm-slapdPWEncryption

Popis Určuje mechanismus kódování pro hesla uživatelů, než jsou uložena v adresáři. Jeho hodnota se musí specifikovat jako "none", "imask", "crypt" nebo "sha" (pokud se má použít kódování SHA-1, musíte zadat klíčové slovo **sha**). Pokud má být připojení SASL cram-md5 úspěšné, musí být tato hodnota nastavena na "none".

Předvolená hodnota

none

Syntaxe

Adresářový řetězec bez rozlišení velikosti písmen

Maximální délka

5

Počet hodnot

Jedna hodnota

ibm-slapdReadOnly

Popis Tento atribut se normálně týká pouze procedury typu "backend" pro adresář. Určuje, zda je možné zapisovat do procedury typu "backend". Atribut musí být nastaven buď na hodnotu TRUE, nebo FALSE. Pokud není určen, je jeho předvolená hodnota FALSE. Jestliže je nastaven na TRUE, server jako odezvu na jakýkoli požadavek klienta, který má měnit data v databázi pouze pro čtení, vrátí návratový kód LDAP_UNWILLING_TO_PERFORM (0x35).

Předvolená hodnota

FALSE

Syntaxe

Booleovská hodnota

Maximální délka

5

Počet hodnot

Jedna hodnota

ibm-slapdReferral

Popis Určuje adresu URL odkazu LDAP, která se má poslat zpět, když místní přípony neodpovídají požadavku. Používá se pro nadřazený odkaz (to znamená, když se přípona nenachází uvnitř kontextu pojmenování serveru).

Předvolená hodnota

Není definována žádná předvolená hodnota.

Syntaxe

Adresářový řetězec s přesným rozlišením velikosti písmen

Maximální délka

32700

Počet hodnot

Více hodnot

ibm-slapdReplDbConns

Popis Maximální počet připojení databáze pro použití replikace.

Předvolená hodnota

4

Syntaxe

Celočíselná hodnota

Maximální délka

11

Počet hodnot

Jedna hodnota

ibm-slapdReplicaSubtree

Popis Označuje DN replikovaného podstromu.

Syntaxe

DN

Maximální délka

1000

Počet hodnot

Jedna hodnota

ibm-slapdSchemaAdditions

Popis Atribut `ibm-slapdSchemaAdditions` se používá k explicitnímu označení souboru, který uchovává nové záznamy schématu. Ten je standardně nastaven jako `/etc/V3.modifiedschema`. Není-li tento atribut definován, server se vrací k používání posledního souboru `ibm-slapdIncludeSchema` jako v předchozích vydáních.

Před verzí 3.2 byl poslední záznam `includeSchema` v **slapd.conf** soubor, do kterého přidával server jakékoli nové záznamy schématu, pokud obdržel od klienta požadavek na přidání. Poslední `includeSchema` je normálně soubor `V3.modifiedschema`, což je prázdný soubor instalovaný pouze pro tento účel.

Poznámka: Jméno "modified" je zavádějící, protože uchovává pouze nové záznamy. Změny záznamů stávajícího schématu se provádějí v jejich původních souborech.

Předvolená hodnota

`/etc/V3.modifiedschema`

Syntaxe

Adresářový řetězec s přesným rozlišením velikosti písmen

Maximální délka

1024

Počet hodnot

Jedna hodnota

ibm-slapdSchemaCheck

Popis Určuje mechanismus kontroly schématu pro operaci přidání/modifikace/vymazání. Musí být určen jako V2, V3 nebo V3_lenient.

- V2 - zachovává kontrolu v2 a v2.1. Doporučuje se pro účely migrace.
- V3 - provádí kontrolu v3.
- V3_lenient - není zapotřebí všech nadřazených tříd objektů. Při přidávání záznamů je potřebná pouze bezprostřední třída objektu.

Předvolená hodnota

V3_lenient

Syntaxe

Adresářový řetězec bez rozlišení velikosti písmen

Maximální délka

10

Počet hodnot

Jedna hodnota

ibm-slapdSecurePort

Popis Určuje port TCP/IP používaný pro připojení využívající zabezpečení SSL. Nemůže mít stejnou hodnotu jako ibm-slapdPort (porty IP jsou nepodepsané 16bitové celočíselné hodnoty v rozmezí 1 - 65535).

Předvolená hodnota

636

Syntaxe

Celočíselná hodnota

Maximální délka

5

Počet hodnot

Jedna hodnota

ibm-slapdSecurity

Popis Aktivuje připojení využívající zabezpečení SSL a TLS. Musí mít hodnotu "none", "SSL", "SSLOnly", "TLS" nebo "SSLTLS".

- none - server naslouchá pouze na nezabezpečeném portu.
- SSL - server naslouchá jak na portu, který využívá zabezpečení SSL, tak na portu, který je nevyužívá. Zabezpečený port je jediným prostředkem použití zabezpečeného spojení.
- SSLOnly - server naslouchá pouze na portu využívajícím zabezpečení SSL.
- TLS - server naslouchá pouze na nezabezpečeném portu. Přídavná operace StartTLS je jediným prostředkem použití zabezpečeného spojení.

- SSLTLS - server naslouchá jak na předvoleném portu tak na zabezpečeném portu. K zajištění zabezpečeného připojení přes nezabezpečený port je možno použít přídatnou operaci StartTLS, nebo klient může použít přímo zabezpečený port. Odeslání operace StartTLS přes zabezpečený port vrátí zprávu LDAP_OPERATIONS_ERROR.

Předvolená hodnota

none

Syntaxe

Adresářový řetězec bez rozlišení velikosti písmen

Maximální délka

7

Počet hodnot

Jedna hodnota

ibm-slapdServerId

Popis Označuje server pro využití v replikaci.

Syntaxe

Řetězec IA5 s rozlišením velikosti písmen

Maximální délka

240

Počet hodnot

Jedna hodnota

ibm-slapdSetenv

Popis Server při svém spuštění spustí **putenv()** pro všechny hodnoty **ibm-slapdSetenv** a tak mění provozní prostředí serveru. Proměnné nastavy (jako **%PATH%** nebo **\$LANG**) se nerozvádějí.

Předvolená hodnota

Není definována žádná předvolená hodnota.

Syntaxe

Adresářový řetězec s přesným rozlišením velikosti písmen

Maximální délka

2000

Počet hodnot

Více hodnot

ibm-slapdSizeLimit

Popis Určuje maximální počet záznamů, který se má vrátit z hledání, bez ohledu na jakýkoli limit velikosti, který mohl být určen v požadavku klienta na hledání (**Rozsah = 0...**). Jestliže klient zadal mezní hodnotu, tato hodnota se porovná s hodnotou načtenou ze souboru **ibmslapd.conf** a použije se ta nižší. Pokud klient nezadal mezní hodnotu a připojil se jako admin DN, je počet záznamů považován za neomezený. Jestliže klient nezadal mezní hodnotu a nepřipojil se jako admin DN, jako mezní hodnota se použije ta, která byla načtena ze souboru **ibmslapd.conf**. 0 = neomezeno.

Předvolená hodnota

500

Syntaxe

Celočíselná hodnota

Maximální délka

12

Počet hodnot

Jedna hodnota

ibm-slapdSortKeyLimit

Popis Maximální počet třídících podmínek (klíčů), který může být určen u jednotlivého požadavku na hledání. Rozsah = 0.... Jestliže klient zadal požadavek na hledání s větším počtem třídících klíčů, než mezní hodnota připouští a kritičnost řízení tříděného hledání je FALSE, server použije hodnotu načtenou ze souboru ibmslapd.conf a po dosažení této meze bude ignorovat jakékoli zadané třídící klíče - vyhledávání a třídění bude provedeno. Pokud klient zadal požadavek na hledání s větším počtem klíčů než mezní hodnota připouští a kritičnost řízení tříděného hledání je TRUE, server vrátí klientovi návratový kód **adminLimitExceeded** - nebude provedeno žádné hledání ani třídění.

Předvolená hodnota

3

Syntaxe

cis

Délka 11**Počítání**

Jednoduché

Použití directoryOperation

Uživatelské modifikace

Ano

Přístupová třída

kritická

Třída objektu

ibm-slapdRdbmBackend

Povinné

Ne

ibm-slapdSortSrchAllowNonAdmin

Popis Určuje, zda má server při požadavku vyhledávání u připojení uživatele nespádajícího do kategorie administrátorů povolit třídění výsledků. Jestliže hodnota načtená ze souboru ibmslapd.conf je FALSE, server zpracuje pouze takové klientské požadavky, které zadal uživatel s oprávněním administrátora. Pokud nějaký klient zadá požadavek na třídění výsledků z operace vyhledávání, nemá oprávnění administrátora a hodnota načtená ze souboru ibmslapd.conf pro tento atribut je FALSE, server vrátí klientovi návratový kód insufficientAccessRights- nebude provedeno žádné hledání ani třídění.

Předvolená hodnota

FALSE

Syntaxe

Booleovská hodnota

Délka 5**Počítání**

Jednoduché

Použití directoryOperation

Uživatelské modifikace

Ano

Přístupová třída

kritická

Třída objektu

ibm-slapdRdbmBackend

Povinné

Ne

ibm-slapdSslAuth**Popis** Určuje typ autentizace pro připojení přes SSL, buď serverauth, nebo serverclientauth.

- serverauth - podporuje autentizaci serveru u klienta. To je předvolená hodnota.
- serverclientauth - podporuje autentizaci serveru i klienta.

Předvolená hodnota

serverauth

Syntaxe

Adresářový řetězec bez rozlišení velikosti písmen

Maximální délka

16

Počet hodnot

Jedna hodnota

ibm-slapdSslCertificate**Popis** Určuje návěští, které označuje osobní certifikát serveru v souboru databáze klíčů. Toto návěští je specifikováno při vytvoření soukromého klíče a certifikátu serveru pomocí aplikace **gsk4ikm**. Pokud atribut `ibm-slapdSslCertificate` není definován, server LDAP použije pro připojení přes SSL předvolený soukromý klíč, definovaný v souboru databáze klíčů.**Předvolená hodnota**

Není definována žádná předvolená hodnota.

Syntaxe

Adresářový řetězec s přesným rozlišením velikosti písmen

Maximální délka

128

Počet hodnot

Jedna hodnota

ibm-slapdSslCipherSpec

Určuje metodu šifrování SSL pro klienty získávající přístup na server. Tento atribut musí být nastaven na jednu z těchto hodnot:

Tabulka 7. Metody šifrování SSL

Atribut	Úroveň šifrování
TripleDES-168	Trojité šifrování DES se 168bitovým klíčem a SHA-1 MAC
DES-56	Šifrování DES s 56bitovým klíčem a SHA-1 MAC
RC4-128-SHA	Šifrování RC4 se 128bitovým klíčem a SHA-1 MAC
RC4-128-MD5	Šifrování RC4 se 128bitovým klíčem a MD5 MAC
RC2-40-MD5	Šifrování RC4 se 40bitovým klíčem a MD5 MAC
RC4-40-MD5	Šifrování RC4 se 40bitovým klíčem a MD5 MAC
AES	Šifrování AES

Syntaxe

Řetězec IA5

Maximální délka

30

ibm-slapdSslKeyDatabase

Popis Určuje cestu k souboru databáze klíčů SSL serveru LDAP. Tento soubor databáze klíčů se používá pro zpracování připojení přes SSL od klientů LDAP, ale také pro vytváření zabezpečených připojení přes SSL na replikované servery LDAP.

Předvolená hodnota

/etc/key.kdb

Syntaxe

Adresářový řetězec s přesným rozlišením velikosti písmen

Maximální délka

1024

Počet hodnot

Jedna hodnota

ibm-slapdSslKeyDatabasePW

Popis Určuje heslo přiřazené k souboru databáze klíčů SSL serveru LDAP, specifikovanému v parametru `ibm-slapdSslKeyDatabase`. Má-li soubor databáze klíčů serveru LDAP přiřazený soubor pro uložení hesla, je možné parametr `ibm-slapdSslKeyDatabasePW` vynechat nebo nastavit na "none" (žádný).

Poznámka: Soubor pro uložení hesla musí být umístěn ve stejném adresáři jako soubor databáze klíčů a musí mít stejné jméno souboru jako soubor databáze klíčů, ale s příponou `.sth` namísto `.kdb`.

Předvolená hodnota

none

Syntaxe

Binární hodnota

Maximální délka

128

Počet hodnot

Jedna hodnota

ibm-slapdSslKeyRingFile

Popis Cesta k souboru databáze klíčů SSL serveru LDAP. Tento soubor databáze klíčů se používá pro zpracování připojení přes SSL od klientů LDAP, ale také pro vytváření zabezpečených připojení přes SSL na replikované servery LDAP.

Předvolená hodnota

key.kdb

Syntaxe

Adresářový řetězec s rozlišením velikosti písmen

Maximální délka

1024

Počet hodnot

Jedna hodnota

ibm-slapdSuffix

Popis Určuje kontext pojmenování, který se má uložit v této proceduře typu "backend".

Poznámka: Tento atribut má stejné jméno jako třída objektu.

Předvolená hodnota

Není definována žádná předvolená hodnota.

Syntaxe

DN

Maximální délka

1000

Počet hodnot

Více hodnot

ibm-slapdSupportedWebAdmVersion

Popis Tento atribut definuje nejstarší verzi webového administračního nástroje, který podporuje tento server s cn=configuration.

Předvolená hodnota

Syntaxe

Adresářový řetězec

Maximální délka

Počet hodnot

Jedna hodnota

ibm-slapdSysLogLevel

Popis Určuje úroveň, při které se statistika ladění programu a operace zapisují do souboru protokolu slapd.errors. Jeho hodnota se musí specifikovat jako l, m nebo h.

- h - vysoká (poskytuje nejvíce informací)
- m - střední (předvolená hodnota)
- l - nízká (poskytuje nejméně informací)

Předvolená hodnota

m

Syntaxe

Adresářový řetězec bez rozlišení velikosti písmen

Maximální délka

1

Počet hodnot

Jedna hodnota

ibm-slapdTimeLimit

Popis Určuje maximální počet sekund, které má obslužný program vynaložit na požadavek na hledání, bez ohledu na jakýkoli časový limit, který mohl být určen v požadavku klienta. Jestliže klient zadal mezní hodnotu, tato hodnota se porovná s hodnotou načtenou ze souboru **ibmslapd.conf** a použije se ta nižší. Pokud klient nezadal mezní hodnotu a připojil se jako admin DN, je čas považován za neomezený. Jestliže klient nezadal mezní hodnotu a nepřipojil se jako admin DN, jako mezní hodnota se použije ta, která byla načtena ze souboru **ibmslapd.conf**. 0 = neomezeno.

Předvolená hodnota

900

Syntaxe

Celočíselná hodnota

Maximální délka**Počet hodnot**

Jedna hodnota

ibm-slapdTransactionEnable

Popis V případě, že je zaveden modul typu "plugin", ale atribut `ibm-slapdTransactionEnable` je nastaven na FALSE, server zamítne všechny požadavky na StartTransaction s odezvou LDAP_UNWILLING_TO_PERFORM.

Předvolená hodnota

TRUE

Syntaxe

Booleovská hodnota

Maximální délka

5

Počet hodnot

Jedna hodnota

ibm-slapdUseProcessIdPw

Popis Jestliže je nastaven na TRUE, server ignoruje atributy `ibm-slapdDbUserID` a `ibm-slapdDbUserPW` a použije pro autentizaci do DB2 svá vlastní pověření procesu.

Předvolená hodnota

FALSE

Syntaxe

Booleovská hodnota

Maximální délka

5

Počet hodnot

Jedna hodnota

ibm-slapdVersion

Popis Číslo verze IBM Sladp

Předvolená hodnota**Syntaxe**

Adresářový řetězec s rozlišením velikosti písmen

Maximální délka**Počet hodnot**

Jedna hodnota

| ibm-slapdWriteTimeout

| **Popis** Uvádí časový limit ve vteřinách pro blokové zápisy. Když je tento časový limit dosažen, spojení se
| přeruší.

| Předvolená hodnota

| 120

Syntaxe

Celočíselná hodnota

Maximální délka

1024

Počet hodnot

Jedna hodnota

Třída objektu**Popis** Hodnoty atributu objectClass popisují druh objektu, který záznam reprezentuje.**Syntaxe**

Adresářový řetězec

Maximální délka

128

Počet hodnot

Více hodnot

Identifikátory objektů (OID)

Identifikátory objektů (OID) uvedené v následujících tabulkách jsou použity v serveru adresářů. Tyto OID se nacházejí v kořenovém DSE. Záznam kořenového DSE obsahuje informace o vlastním serveru.

Ovladače

Tabulka 8. Podporované ovladače serveru adresářů

Jméno	OID	Nejstarší vydání operačního systému i5/OS nebo OS/400	Nejstarší verze serveru adresářů IBM	Popis
Správa DSA IT	2.16.840.1.1137.30.3.4.2	V4R5	V3.2	Spravuje referenční objekty jako normální záznamy.
“Transakce” na stránce 46	1.3.18.0.2.10.5	V4R5	V3.2	Označuje operaci jako část transakce.
os400-dltusrprf-ownobjopt	1.3.18.0.2.10.8	V5R2		Volba výmazu uživatelského profilu pro vlastníka objektu. Podrobnosti najdete v tématu “Procedura Backend projektovaná operačním systémem” na stránce 74.
os400-dltusrprf-pgpopt	1.3.18.0.2.10.9	V5R2		Volba výmazu uživatelského profilu pro primární skupinu. Podrobnosti najdete v tématu “Procedura Backend projektovaná operačním systémem” na stránce 74.

Tabulka 8. Podporované ovladače serveru adresářů (pokračování)

Jméno	OID	Nejstarší vydání operačního systému i5/OS nebo OS/400	Nejstarší verze serveru adresářů IBM	Popis
Tříděné hledání	1.2.840.113556.1.4.473 (požadavek) a 1.2.840.113556.1.4.474 (odezva)	V5R2 s PTF	V4.1	Před vrácením záznamů klientovi třídí výsledky hledání. Další informace najdete v tématu “Parametry prohledávání” na stránce 42.
Stránkované hledání	1.2.840.113556.1.4.319	V5R2 s PTF	V4.1	Vrací výsledky hledání klientovi po stránkách namísto všech výsledků najednou. Další informace najdete v tématu “Parametry prohledávání” na stránce 42.
Ovladač Výmaz stromu	1.2.840.113556.1.4.805	V5R3	V5.1	Tento ovladač je připojen k požadavku na Výmaz a vyznačuje, že se má vymazat určený záznam spolu se všemi podřízenými záznamy. Uživatel musí být administrátor adresáře. Záznam, který se má vymazat, nemůže být kontext replikace.
“Zásada pro správu hesel” na stránce 67	1.3.6.1.4.1.42.2.27.8.5.1	V5R3	V5.1	Vrací klientovi dodatečné informace o chybě zásady pro správu hesel.
Administrace serveru	1.3.18.0.2.10.15	V5R3	V5.1	Umožňuje administrátorovi provádět nápravné operace, které by byly normálně odmítnuty (například aktualizace repliky pouze pro čtení, aktualizace serveru uvedeného do klidu nebo odeslání určitých operačních atributů).
“Proxy autorizace” na stránce 55	2.16.840.1.113730.3.4.18	V5R4	V5.2	Aplikace typu klient se může připojit k adresáři na základě své vlastní identity, ale je jí povoleno provádět operace i jménem jiné identity.
Kontrola připojení dodavatele replikace	1.3.18.0.2.10.18	V5R3	V5.2	Tento ovladač přidává dodavatel, pokud je dodavatelem server brány.

Přídavné operace

Tabulka 9. OID pro přídavné operace

Jméno	OID	Nejstarší vydání operačního systému i5/OS nebo OS/400	Nejstarší verze serveru adresářů IBM	Popis
Registrace pro události	1.3.18.0.2.12.1	V4R5	V3.2	Požadavek na registraci událostí v SecureWay V3.2 Event Support.
Odregistrace pro události	1.3.18.0.2.12.3	V4R5	V3.2	Odregistrace událostí, které byly zaregistrovány pro použití Event Registration Request.
Začátek transakce	1.3.18.0.2.12.5	V4R5	V3.2	Zahájení kontextu transakce pro SecureWay V3.2
Konec transakce	1.3.18.0.2.12.6	V4R5	V3.2	Ukončení kontextu transakce (commit/rollback) pro SecureWay V3.2
Požadavek normalizace DN	1.3.18.0.2.12.30	V5R3	V5.1	Požadavek na normalizaci DN nebo sekvence DN.
StartTLS	1.3.6.1.4.1.1466.20037	V5R4	V5.2	Požadavek na zahájení Transport Layer Security.

Jsou definovány i další přídavné operace, které však nejsou určeny k tomu, aby je spouštěli klienti. Tyto operace jsou využívány prostřednictvím obslužného programu ldapexop nebo operacemi prováděnými webovým nástrojem administrace. Seznam těchto operací a oprávnění požadovaných k jejich spuštění uvádí následující tabulka:

Tabulka 10. Další přídavné operace

Jméno	OID	Nejstarší vydání operačního systému i5/OS	Nejstarší verze serveru adresářů IBM	Popis
Řízení replikace	1.3.18.0.2.12.16	V5R3	V5.1	Tato operace provádí požadovanou činnost na serveru, pro který je vydána, a řadí do kaskády volání všem odběratelům pod sebou v replikační topologii. Klient musí být administrátor adresáře nebo musí mít oprávnění pro zápis do objektu ibm-replicagroup=default pro přiřazený replikační kontext.
Fronta řízení replikace	1.3.18.0.2.12.17	V5R3	V5.1	Tato operace označuje položky jako již replikované pro uvedené ujednání. Tato operace je povolena pouze tehdy, když má klient oprávnění pro zápis do ujednání o replikaci.

Tabulka 10. Další přídavné operace (pokračování)

Jméno	OID	Nejstarší vydání operačního systému i5/OS	Nejstarší verze serveru adresářů IBM	Popis
Uvedení do klidu nebo vybuzení	1.3.18.0.2.12.19	V5R3	V5.1	Tato operace uvede podstrom do stavu, ve kterém nepřijímá klientovy aktualizace (nebo tento stav ukončuje), s výjimkou aktualizací ze strany klientů s oprávněním administrátorů adresáře v případě použití řízení správy serveru. Klient musí být autentizován jako administrátor adresáře nebo musí mít oprávnění pro zápis do objektu <code>ibm-replicagroup=default</code> pro přiřazený replikační kontext.
Replikace kaskádového řízení	1.3.18.0.2.12.15	V5R3	V5.1	Tato operace provádí požadovanou činnost na serveru, pro který je vydána, a řadí do kaskády volání všem odběratelům pod sebou v replikační topologii. Klient musí být administrátor adresáře nebo musí mít oprávnění pro zápis do objektu <code>ibm-replicagroup=default</code> pro přiřazený replikační kontext.
Aktualizace konfigurace	1.3.18.0.2.12.28	V5R3	V5.1	Tato operace se používá tehdy, když chcete, aby server znovu načítl určená nastavení z jeho konfigurace. Operace je povolena pouze tehdy, když je klientem administrátor adresáře.
Požadavek na ukončení spojení	1.3.18.0.2.12.35	V5R4	V5.2	Požadavek na ukončení spojení na serveru.
Požadavek na jedinečný atribut	1.3.18.0.2.12.44	V5R4	V5.2	Požaduje na serveru, aby vrátil seznam všech nejedinečných hodnot pro dané jméno atributu. Viz volba <code>-op uniqueattr</code> v části "ldapexp" na stránce 194.
Požadavek na typ atributu	1.3.18.0.2.12.46	V5R4	V5.2	Požaduje na serveru, aby vrátil seznam jmen atributů, které mají určitou charakteristiku. Viz volba <code>-op getattributes</code> v části "ldapexp" na stránce 194.
Kontrola trasování serveru	1.3.18.0.2.12.40	V5R3	V5.2	Aktivuje nebo deaktivuje trasování v serveru adresářů IBM.
Požadavek na typ uživatele	1.3.18.0.2.12.37	V5R3	V5.2	Požaduje informaci o typu uživatele pro připojeného uživatele.

Podporované a povolené schopnosti

Následující tabulka uvádí OID pro podporované a povolené schopnosti. Tyto OID můžete použít ke zjištění, zda konkrétní server podporuje tyto funkce.

Tabulka 11. OID pro podporované a povolené schopnosti

Jméno	OID	Popis
Rozšířený model replikace	1.3.18.0.2.32.1	Identifikuje model replikace uvedený v produktu IBM Directory Server v5.1 včetně replikace podstromu a kaskádové replikace.
Entry Checksum	1.3.18.0.2.32.2	Indikuje, že server podporuje funkce ibm-entrychecksum a ibm-entrychecksumop.
Entry UUID	1.3.18.0.2.32.3	Identifikuje, že server podporuje operační atribut ibm-entryuuid.
Filtrované ACL	1.3.18.0.2.32.4	Identifikuje, že server podporuje model filtrovaných ACL.
Zásada pro správu hesel	1.3.18.0.2.32.5	Identifikuje, že server podporuje zásady pro správu hesel.
Třídění podle DN	1.3.18.0.2.32.6	Indikuje, že server podporuje použití atributu ibm-slapdDn pro třídění podle DN.
Delegace na administrační skupinu	1.3.18.0.2.32.8	Server podporuje delegaci serverové administrace na skupinu administrátorů, kteří jsou specifikováni v proceduře backend konfigurace.
Prevence odmítnutí služeb	1.3.18.0.2.32.9	Server podporuje funkci pro prevenci odmítnutí služeb. Včetně časových limitů pro čtení/zápis a nouzového vlákna.
Dynamická aktualizace záznamů a podstromů	1.3.18.0.2.32.15	Server podporuje dynamické aktualizace konfigurace ohledně záznamů a podstromů.
Volba dereference aliasů	1.3.18.0.2.32.10	Server podporuje volbu neprovádět dereferenci aliasů jako předvolenou hodnotu.
Limity hledání specifické pro skupinu	1.3.18.0.2.32.17	Limity hledání specifické pro skupinu podporují rozšířené možnosti hledání pro konkrétní skupinu lidí.
Dynamické trasování	1.3.18.0.2.32.14	Server podporuje aktivní trasování pro server s přídavnou operací LDAP.
Schopnosti TLS	1.3.18.0.2.32.28	Uvádí, že server je schopen provádět TLS.
Monitorování Admin Daemon	1.3.18.0.2.32.11	Server podporuje monitorování admin daemon.
Schopnosti Kerberos	1.3.18.0.2.32.30	Uvádí, že server je schopen provádět autentizaci Kerberos.
Neblokující replikace	1.3.18.0.2.32.29	Dodavatel se nepokouší pořad znovu odeslat aktualizaci, pokud odběratel vrátí chybu.
Operační atributy ibm-allMembers a ibm-allGroups	1.3.18.0.2.32.31	Procedura backend podporuje prohledávání statických, dynamických a vnořených skupin prostřednictvím operačních atributů ibm-allMembers a ibm-allGroups. Na základě vyhledávání pomocí atributu ibm-allMembers lze získat členy statických, dynamických a/nebo vnořených skupin. Na základě vyhledávání pomocí atributu ibm-allGroups lze získat statické, dynamické a/nebo vnořené skupiny, do kterých určité DN člena patří.
Globálně jedinečné atributy	1.3.18.0.2.32.16	Funkce serveru pro prosazení globálně jedinečných hodnot atributu.
Údaje z monitoru operací	1.3.18.0.2.32.24	Server poskytuje údaje z monitoru operací ohledně zahájených a dokončených typů operací.
Údaje z monitoru protokolování	1.3.18.0.2.32.20	Server poskytuje údaje z monitoru protokolování ohledně počtů zpráv přidaných do souborů protokolu serveru, CLI a monitorování.
Údaje z monitoru typu připojení	1.3.18.0.2.32.22	Server poskytuje údaje z monitoru ohledně počtu připojení typu SSL a TLS.
Údaje z monitoru aktivních pracovníků	1.3.18.0.2.32.21	Server poskytuje údaje z monitoru ohledně aktivních pracovníků (cn=workers,cn=monitor).

Tabulka 11. OID pro podporované a povolené schopnosti (pokračování)

Jméno	OID	Popis
Údaje z monitoru připojení	1.3.18.0.2.32.23	Server poskytuje informace monitoru ohledně připojení podle IP adresy namísto podle ID připojení (cn=connections, cn=monitor).
Údaje z monitoru trasování	1.3.18.0.2.32.25	Server poskytuje informace ohledně sledování voleb, které se aktuálně používají.
Řešení vyhledávacích filtrů s ukládáním do paměti cache atributu	1.3.18.0.2.32.13	Server podporuje ukládání do paměti cache pro řešení vyhledávacích filtrů.
Proxy Autorizace	1.3.18.0.2.32.27	Server podporuje proxy autorizaci pro skupinu uživatelů.
Podpora pro jazykové příznaky	1.3.6.1.4.1.4203.1.5.4	Indikuje, že server podporuje jazykové příznaky podle definice v RFC 2596.
Maximální doba záznamů protokolu změn	1.3.18.0.2.32.19	Uvádí, že je server schopen zachovávat záznamy protokolu změn na základě jejich stáří.
Replikace podstromu IBMpolicies	1.3.18.0.2.32.18	Server podporuje replikaci podstromu cn=IBMpolicies.
Prohledávání na nulové bázi	1.3.18.0.2.32.26	Server umožňuje prohledávání podstromů na nulové bázi, které prohledává celý DIT definovaný na serveru.
Autonomní paměť cache atributu	1.3.18.0.2.32.50	Podporuje autonomní ukládání do paměti cache atributu.
ibm-entrychecksumop	1.3.18.0.2.32.56	Funkce 6.0 IDS ibm-entrychecksumop.

OID pro mechanismy ACL

Následující tabulka uvádí OID pro mechanismy ACL.

Tabulka 12. OID pro mechanismy ACL

Jméno	OID	Popis
Model ACL IBM SecureWay V3.2	1.3.18.0.2.26.2	Indikuje, že server LDAP podporuje ACL model IBM SecureWay V3.2.
Mechanismus ACL na bázi filtrů IBM	1.3.18.0.2.26.3	Indikuje, že server LDAP podporuje ACL na bázi filtrů produktu IBM Directory Server v5.1.
Podpora systémových omezených ACL	1.3.18.0.2.26.4	Indikuje, že server podporuje třídu systémového a omezeného přístupu v záznamech ACL.

Kapitola 9. Odstraňování problémů s produktem Server adresářů

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

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

“Sledování chyb a přístupů v produktu Server adresářů pomocí protokolu úloh” na stránce 266

Když se vyskytne chyba na serveru adresářů a vy se chcete dozvědět více podrobností, můžete si také prohlédnout protokol úloh QDIRSRV.

“Použití příkazu TRCTCPAPP k vyhledání problémů” na stránce 266

V případě opakujících se chyb můžete ke sledování chyb použít příkaz TRCTCPAPP APP(*DIRSRV) (Trasování aplikace TCP/IP).

“Použití volby LDAP_OPT_DEBUG při sledování chyb” na stránce 267

Problémy je vhodné sledovat u klientů, kteří používají rozhraní API pro LDAP C.

“Běžné chyby klienta LDAP” na stránce 270


Znalost příčin obecných chyb u klienta LDAP vám může pomoci i při řešení problémů se serverem.

“Chyby související se zásadou pro správu hesel” na stránce 272

Povolení zásady pro správu hesel někdy může způsobit neočekávané chyby.

“Odstraňování problémů s rozhraním API QGLDCPYVL” na stránce 272

Pomocí poskytované služby User Trace lze vysvětlit chybu nebo určit, zda je služba zapotřebí.

Další informace o obecných problémech produktu Server adresářů najdete na domovské stránce produktu Server adresářů  na adrese (www.iseries.ibm.com/ldap).

Produkt Server adresářů používá několik serverů SQL (Structured Query Language), které pracují jako úlohy QSQRVR iSeries. Vyskytne-li se chyba SQL, objeví se v protokolu úlohy QDIRSRV obvykle tato zpráva:
SQL error -1 occurred

V těchto případech vás bude protokol úloh QDIRSRV odkazovat na protokoly úloh serverů SQL. V některých případech však QDIRSRV nemusí obsahovat tuto zprávu a tento odkaz, i když je příčinou problému právě server SQL. V těchto případech je vhodné vědět, které úlohy serveru SQL server spustil a ve kterých protokolech úloh QSQRVR tedy máte hledat další chyby.

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

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

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

Zprávy se vztahují k úlohám QSQSRVR, které byly spuštěny pro server. Počet zpráv se může na vašem serveru lišit v závislosti na konfiguraci a počtu úloh QSQSRVR potřebných pro úspěšné spuštění serveru.

Celkový počet serverů SQL, který server Server adresářů po spuštění používá pro adresářové operace, se zadává na serveru LDAP v prostředí produktu iSeries Navigator na stránce vlastností v poli **Databáze/Přípony**. Další servery SQL se spouštějí pro účely replikace.

Sledování chyb a přístupů v produktu Server adresářů pomocí protokolu úloh

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

- Zprávy o provozu serveru a jakýchkoli problémech v rámci serveru, jako např. selhání úloh serveru SQL nebo replikace.
- Zprávy týkající se zabezpečení, odrážející operace klientů jako např. chybná hesla.
- Zprávy uvádějící podrobnosti o chybách klientů, jako jsou např. chybějící povinné atributy.

Chyby klientů není nutné protokolovat, pokud neprovádíte ladění problémů klientů. Protokolování chyb klientů můžete nastavovat na kartě vlastností serveru adresářů **Obecné** v prostředí produktu iSeries Navigator.

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. Právým tlačítkem myši klepněte na **Server adresářů IBM** a vyberte volbu **Úlohy serveru**.
5. Z menu **Soubor** vyberte volbu **Protokol úlohy**.

Je-li server zastaven, můžete si prohlédnout protokol úlohy 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 dvojitým klepnutím na položku **Qpjoblog** vlevo od QDIRSRV na téže řádce.

Poznámka: Produkt 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 Server adresářů 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 Server adresářů 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, které slouží 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 je možné použít pro vyhledávání problémů s klienty nebo aplikacemi příkaz TRCTCPAPP (Trasování aplikace TCP/IP) s volbou *DIRSRV.

Podrobnější informace o použití příkazu TRCTCPAPP na serveru LDAP a také o omezeních týkajících se požadovaných oprávnění najdete v tématu **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

Volbu LDAP_OPT_DEBUG rozhraní API `ldap_set_option()` můžete použít 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 číslo klientské úlohy.

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

```
DSPPFM QAP0ZDMP QP0Znnnnnn
```

kde QAP0ZDMP obsahuje nulu a 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(QAP0ZDMP) LIB(QTEMP) DEV(*SAVF) SAVF(xxx)
```

kde QAP0ZDMP obsahuje nulu a xxx je jméno, které jste zadali pro soubor SAVF.

Identifikátory zpráv GLEnnnn

Identifikátory zpráv mají formát GLEnnnn, kde nnnn je desetinné číslo chyby. Například popis pro návratový kód 50 (0x32) můžete zobrazit zadáním tohoto příkazu:

```
DSPMSGD MSGID(GLE0050) MSGF(QGLDMSG)
```

To by poskytlo popis pro LDAP_INSUFFICIENT_ACCESS (nedostatečný přístup).

Následující tabulka uvádí seznam identifikátorů zpráv GLE a jejich popisy.

Identifikátor zprávy	Popis
GLE0000	Požadavek byl úspěšný (LDAP_SUCCESS)
GLE0001	Chyba operací (LDAP_OPERATIONS_ERROR)
GLE0002	Chyba protokolu (LDAP_PROTOCOL_ERROR)

Identifikátor zprávy	Popis
GLE0003	Překročen časový limit (LDAP_TIMELIMIT_EXCEEDED)
GLE0004	Překročen limit velikosti (LDAP_SIZELIMIT_EXCEEDED)
GLE0005	Porovnávaný typ a hodnota v záznamu neexistují (LDAP_COMPARE_FALSE)
GLE0006	Porovnávaný typ a hodnota v záznamu existuje (LDAP_COMPARE_TRUE)
GLE0007	Metoda autentizace není podporována (LDAP_AUTH_METHOD_NOT_SUPPORTED)
GLE0008	Vyžaduje se silná autentizace (LDAP_STRONG_AUTH_REQUIRED)
GLE0009	Přijaty částečné výsledky a odkazy (LDAP_PARTIAL_RESULTS)
GLE0010	Vrácen odkaz (LDAP_REFERRAL)
GLE0011	Překročen administrační limit (LDAP_ADMIN_LIMIT_EXCEEDED)
GLE0012	Kritické přípony nejsou podporovány (LDAP_UNAVAILABLE_CRITICAL_EXTENSION)
GLE0013	Vyžaduje se utajení (LDAP_CONFIDENTIALITY_REQUIRED)
GLE0014	Probíhá připojení SASL (LDAP_SASL_BIND_IN_PROGRESS)
GLE0016	Žádný takový atribut (LDAP_NO_SUCH_ATTRIBUTE)
GLE0017	Nedefinovaný typ atributu (LDAP_UNDEFINED_TYPE)
GLE0018	Nevhodné porovnávání (LDAP_INAPPROPRIATE_MATCHING)
GLE0019	Narušení omezení (LDAP_CONSTRAINT_VIOLATION)
GLE0020	Typ nebo hodnota existuje (LDAP_TYPE_OR_VALUE_EXISTS)
GLE0021	Neplatná syntaxe (LDAP_INVALID_SYNTAX)
GLE0032	Žádný takový objekt (LDAP_NO_SUCH_OBJECT)
GLE0033	Problém aliasu (LDAP_ALIAS_PROBLEM)
GLE0034	Neplatná syntaxe DN (LDAP_INVALID_DN_SYNTAX)
GLE0035	Objekt je koncový (LDAP_IS_LEAF)
GLE0036	Problém s dereferencí aliasu (LDAP_ALIAS_DEREF_PROBLEM)
GLE0048	Nevhodná autentizace (LDAP_INAPPROPRIATE_AUTH)
GLE0049	Neplatná pověření (LDAP_INVALID_CREDENTIALS)
GLE0050	Nedostatečný přístup (LDAP_INSUFFICIENT_ACCESS)
GLE0051	Server adresářů je zaneprázdněný (LDAP_BUSY)
GLE0052	Agent adresářových služeb není k dispozici (LDAP_UNAVAILABLE)
GLE0053	Server adresářů není ochoten provést požadovanou operaci (LDAP_UNWILLING_TO_PERFORM)
GLE0054	Detekovaný loop (LDAP_LOOP_DETECT)
LE0064	Narušení pravidel pojmenování (LDAP_NAMING_VIOLATION)

Identifikátor zprávy	Popis
LE0065	Narušení třídy objektu (LDAP_OBJECT_CLASS_VIOLATION)
GLE0066	Operace není na nekoncevném objektu povolena (LDAP_NOT_ALLOWED_ON_NONLEAF)
GLE0067	Operace není na relativním rozlišovacím jméně povolena (LDAP_NOT_ALLOWED_ON_RDN)
GLE0068	Již existuje (LDAP_ALREADY_EXISTS)
GLE0069	Nelze modifikovat třídu objektu (LDAP_NO_OBJECT_CLASS_MODS)
GLE0070	Výsledky jsou příliš velké (LDAP_RESULTS_TOO_LARGE)
GLE0071	Ovlivňuje více serverů (LDAP_AFFECTS_MULTIPLE_DSAS)
GLE0080	Neznámá chyba (LDAP_OTHER)
GLE0081	Nelze kontaktovat server LDAP (LDAP_SERVER_DOWN)
GLE0082	Lokální chyba (LDAP_LOCAL_ERROR)
GLE0083	Chyba zakódování (LDAP_ENCODING_ERROR)
GLE0084	Chyba dekodování (LDAP_DECODING_ERROR)
GLE0085	Požaduje časový limit (LDAP_TIMEOUT)
GLE0086	Neznámá metoda autentizace (LDAP_AUTH_UNKNOWN)
GLE0087	Chybný vyhledávací filtr (LDAP_FILTER_ERROR)
GLE0088	Uživatel zrušil operaci (LDAP_USER_CANCELLED)
GLE0089	Chybný parametr rutiny LDAP (LDAP_PARAM_ERROR)
GLE0090	Nedostatek paměti (LDAP_NO_MEMORY)
GLE0091	Chyba připojení (LDAP_CONNECT_ERROR)
GLE0092	Funkce není podporována (LDAP_NOT_SUPPORTED)
GLE0093	Ovladač nenalezen (LDAP_CONTROL_NOT_FOUND)
GLE0094	Žádné vrácené výsledky (LDAP_NO_RESULTS_RETURNED)
GLE0095	Další výsledky k vrácení (LDAP_MORE_RESULTS_TO_RETURN)
GLE0096	Není LDAP URL (LDAP_URL_ERR_NOTLDAP)
GLE0097	URL nemá DN (LDAP_URL_ERR_NODN)
GLE0098	Rozsah hodnoty URL není platný (LDAP_URL_ERR_BADSCOPE)
GLE0099	Chyba alokace paměti (LDAP_URL_ERR_MEM)
GLE0100	Klientský loop (LDAP_CLIENT_LOOP)
GLE0101	Překročený limit odkazů (LDAP_REFERRAL_LIMIT_EXCEEDED)
GLE0112	Prostředí SSL již inicializováno (LDAP_SSL_ALREADY_INITIALIZED)
GLE0113	Požadavek na inicializaci selhal (LDAP_SSL_INITIALIZE_FAILED)
GLE0114	Prostředí SSL neinicializováno (LDAP_SSL_CLIENT_INIT_NOT_CALLED)
GLE0115	Zadán neplatný parametr SSL (LDAP_SSL_PARAM_ERROR)

Identifikátor zprávy	Popis
GLE0116	Nedošlo k vyjednání zabezpečeného připojení (LDAP_SSL_HANDSHAKE_FAILED)
GLE0118	Nelze nalézt knihovnu SSL (LDAP_SSL_NOT_AVAILABLE)
GLE0128	Nebyl zjištěn explicitní vlastník (LDAP_NO_EXPLICIT_OWNER)
GLE0129	Nebylo možno zamknout požadovaný zdroj (LDAP_NO_LOCK)
GLE0133	V DNS nenalezeny žádné servery LDAP (LDAP_DNS_NO_SERVERS)
GLE0134	Zkrácené výsledky DNS (LDAP_DNS_TRUNCATED)
GLE0135	Nebylo možno analyzovat data DNS (LDAP_DNS_INVALID_DATA)
GLE0136	Nelze vyřešit systémovou doménu nebo server jmen (LDAP_DNS_RESOLVE_ERROR)
GLE0137	Chyba souboru konfigurace DNS (LDAP_DNS_CONF_FILE_ERROR)
GLE0160	Přetečení výstupu vyrovnávací paměti (LDAP_XLATE_E2BIG)
GLE0161	Vstup vyrovnávací paměti zkrácený (LDAP_XLATE_EINVAL)
GLE0162	Nepoužitelný vstupní znak (LDAP_XLATE_EILSEQ)
GLE0163	Znak není mapovaný na bodu kódové sady (LDAP_XLATE_NO_ENTRY)

Běžné chyby klienta LDAP

Znalost příčin obecných chyb u klienta LDAP vám může pomoci i při řešení problémů se serverem. Úplný seznam chybových stavů u klienta LDAP najdete v tématu “Rozhraní API serveru adresářů” pod heslem Programování 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 i5/OS. 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 tyto:

- “ldap_search: Timelimit exceeded”
- “[Selhávající operace LDAP]: Operations error” na stránce 271
- “ldap_bind: No such object” na stránce 271
- “ldap_bind: Inappropriate authentication” na stránce 271
- “[Selhávající operace LDAP]: Insufficient access” na stránce 271
- “[Selhávající operace LDAP]: Cannot contact LDAP server” na stránce 271
- “[Selhávající operace LDAP]: Failed to connect to SSL server” na stránce 271

ldap_search: Timelimit exceeded

K této chybě dochází, když vyhledávání v LDAP probíhá příliš pomalu. K nápravě této chyby můžete učinit jedno nebo obě z těchto opatření:

- Zvýšit časový limit pro vyhledávání na serveru adresářů. Informace o tom, jak to provést, najdete v tématu “Jak přizpůsobit nastavení výkonu” na stránce 125.
- 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 příčině této chyby pro konkrétní případ, podívejte se do protokolů úloh QDIRSRV (podle pokynů v tématu “Sledování chyb a přístupů v produktu Server adresářů pomocí protokolu úloh” na stránce 266) a do protokolů úloh serverů SQL (podle pokynů v tématu Kapitola 9, “Odstraňování problémů s produktem Server adresářů”, na stránce 265).

ldap_bind: No such object

Obecnou příčinou této chyby je, že uživatel v průběhu operace udělá chybu při psaní. Další obecná příčina je ta, 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 bude cn=Administrator.

Podrobné informace o této chybě najdete v protokolu úlohy QDIRSRV, přitom postupujte podle pokynů uvedených v tématu “Sledování chyb a přístupů v produktu Server adresářů pomocí protokolu úloh” na stránce 266.

ldap_bind: Inappropriate authentication

Server vrátí neplatná pověření (credentials) v případě, že je heslo nebo připojovací DN nesprávné. Server vrátí nepatřičnou autentizaci v případě, že se klient pokusí připojit jako:

- Záznam, který nemá atribut “userpassword”.
- Záznam, který reprezentuje uživatele operačního systému i5/OS, jenž má atribut UID a nemá atribut “userpassword”. Tím dojde k porovnání zadaného hesla a uživatelského hesla operačního systému i5/OS, která se neshodují.
- Záznam, který reprezentuje jiného projektovaného uživatele a jinou metodu připojení, 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, přitom postupujte podle pokynů uvedených v tématu “Sledování chyb a přístupů v produktu Server adresářů pomocí protokolu úloh” na stránce 266.

[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, přitom postupujte podle pokynů uvedených v tématu “Sledování chyb a přístupů v produktu Server adresářů pomocí protokolu úloh” na stránce 266.

[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, přitom postupujte podle pokynů uvedených v tématu “Sledování chyb a přístupů v produktu Server adresářů pomocí protokolu úloh” na stránce 266. Pokud byl server adresářů 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 ke čtení pro paměť certifikátů *SYSTEM (předvoleně /QIBM/userdata/ICSS/Cert/Server/default.kdb).

Pro aplikace operačního systému i5/OS napsané v jazyce C jsou k dispozici další informace o chybách SSL. Podrobnosti najdete v tématu “Server adresářů - rozhraní API” pod heslem Programování.

Chyby související se zásadou pro správu hesel

- | Když jsou povoleny určité zásady pro správu hesel, mohou způsobit selhání, která nemusí být zřejmá. Prostudujte si následující rady, které vám pomohou při odstraňování problémů s chybami souvisejícími se zásadami pro správu hesel.
- | **Připojení pomocí správného hesla selže s chybou “invalid credentials”:** Heslu mohla vypršet platnost nebo účet může být zamčený. Podívejte se na atributy pwdchangedtime a pwdaccountlockedtime záznamu, jak je popsáno v tématu “Rady k zásadám pro správu hesel” na stránce 149.
- | **Požadavky selhaly s chybou “unwilling to perform” po úspěšném připojení:** Heslo možná bylo resetováno, takže připojení je sice úspěšné, ale jedinou operací, kterou server uživateli povolí, je změna hesla. Jiné požadavky selžou s chybou “unwilling to perform”, dokud heslo nebude změněno.
- | **Autentizace pomocí hesla, které bylo resetováno, se chová neočekávaně:** Když bylo heslo resetováno, připojovací požadavek bude úspěšný, jak je popsáno výše. To znamená, že uživatel může být schopen se autentizovat pomocí resetovaného hesla neurčitě dlouhou dobu.




Odstraňování problémů s rozhraním API QGLDCPYVL

- | Toto API používá k zaznamenávání své činnosti poskytovanou službu User Trace. Pokud se vyskytnou chyby, nebo existuje podezření, že vzniknou, trasování může vysvětlit zjevnou chybu nebo zda je služba potřebná. Trasování lze získat takto:
- | STRTRC SSNID(COPYVLDL) JOBTRCTYPE(*TRCTYPE) TRCTYPE((*DIRSRV *INFO))
- | CALL QGLDCPYVL PARM(...)
- | ENDTRC SSNID(COPYVLDL) DTALIB(QTEMP) PRTRTC(*YES)
- | 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(QAP0ZDMP) LIB(QTEMP) DEV(*SAVF) SAVF(xxx)
- | kde QAP0ZDMP obsahuje nulu a xxx je jméno, které jste zadali pro soubor SAVF.



Kapitola 10. Související informace

Následuje seznam červených knih IBM (ve formátu PDF), webových stránek a témat aplikace Information Center, které se vztahují k oblasti serveru adresářů. Kterýkoli ze souborů PDF si můžete prohlédnout nebo vytisknout.

Červené knihy (www.redbooks.ibm.com)

- Understanding LDAP, SG24-4986  .
- Using LDAP for Directory Integration: A Look at IBM SecureWay Directory, Active Directory, and Domino, SG24-6163  .
- Implementation and Practical Use of LDAP on the iSeries Server, SG24-6193  .

Webové stránky

- Webové stránky IBM Directory Server for iSeries 
(www.ibm.com/servers/eserver/series/ldap)
- Webové stránky The Java Naming and Directory Interface (JNDI) Tutorial 
(java.sun.com/products/jndi/tutorial/)

Ostatní informace

“Rozhraní API serveru adresářů” v kategorii Programování.

Dodatek. Poznámky

Tyto informace platí pro produkty a služby nabízené v USA.

IBM nemusí v ostatních zemích nabízet produkty, služby a funkce popsané v tomto dokumentu. Informace o produktech a službách, které jsou momentálně dostupné ve vašem regionu, můžete získat od místního zástupce IBM. Žádný odkaz na produkt, program nebo službu IBM neznamená a ani z něj nelze vyvozovat, že smí být použit pouze uvedený produkt, program či služba společnosti IBM. Použit lze jakýkoli funkčně ekvivalentní produkt, program či službu neporušující práva IBM k duševnímu vlastnictví. Za vyhodnocení a ověření činnosti libovolného produktu, programu či služby jiného výrobce než IBM však odpovídá uživatel.

IBM může mít patenty nebo podané žádosti o patent, které zahrnují předmět tohoto dokumentu. Získání tohoto dokumentu uživateli Vám neuděluje licenci na tyto patenty. Písemné dotazy ohledně licencí můžete zaslat na adresu:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Pokud máte zájem o licenci v zemi s dvoubajtovou znakovou sadou (DBCS), kontaktujte zastoupení IBM ve vaší zemi, nebo písemně zastoupení IBM na adrese:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

Následující odstavec neplatí pro Velkou Británii a další země, ve kterých tato opatření nejsou v souladu s místními právními předpisy: IBM POSKYTUJE TUTO PUBLIKACI TAKOVOU, "JAKÁ JE", BEZ JAKÝCHKOLI ZÁRUK, VYJÁDŘENÝCH NEBO ODVOZENÝCH, VČETNĚ, BEZ OMEZENÍ, ODVOZENÉ ZÁRUKY NEPORUŠOVÁNÍ PRÁV TŘETÍCH STRAN, ZÁRUKY PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL. Právní rády některých zemí nepřipouštějí vyloučení vyjádřených nebo odvozených záruk v určitých transakcích a proto se na vás výše uvedené omezení nemusí vztahovat.

Tato publikace může obsahovat technické nepřesnosti nebo typografické chyby. Informace zde uvedené jsou pravidelně aktualizovány a v nových vydáních této publikace již budou tyto změny zahrnuty. IBM má právo kdykoliv bez upozornění zdokonalovat nebo měnit produkty a programy popsané v této publikaci.

Jakékoli odkazy v této publikaci na webové stránky jiných společností než IBM jsou poskytovány pouze pro pohodlí uživatele a nemohou být žádným způsobem vykládány jako doporučení těchto webových stránek ze strany IBM. Materiály obsažené na takovýchto webových stránkách nejsou součástí materiálů k tomuto produktu IBM a tyto webové stránky mohou být používány pouze na vlastní nebezpečí.

IBM může použít nebo distribuovat jakékoli informace, které jí sdělíte, libovolným způsobem, který společnost považuje za odpovídající, bez vzniku jakýchkoliv závazků vůči vám.

Držitelé licence na tento program, kteří si přejí mít přístup i k informacím o programu za účelem (i) výměny informací mezi nezávisle vytvořenými programy a jinými programy (včetně tohoto) a (ii) vzájemného použití sdílených informací, mohou kontaktovat:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N

Rochester, MN 55901
U.S.A.

Informace tohoto typu mohou být dostupné za určitých podmínek. V některých případech připadá v úvahu zaplacení poplatku.

- | IBM poskytuje licencovaný program popsany v těchto informacích a veškeré dostupné licencované materiály na základě podmínek uvedených ve smlouvě IBM Customer Agreement, v Mezinárodní licenční smlouvě na programy,
- | v Mezinárodní licenční smlouvě IBM na strojový kód nebo v jiné ekvivalentní smlouvě.

Všechny informace o provozu byly určeny v řízeném prostředí. Výsledky získané v jiném provozním prostředí se tudíž mohou výrazně lišit. Některá měření byla provedena v systémech s vývojovým prostředím a neexistuje žádná záruka, že tato měření budou stejná v obecně dostupných systémech. Některá měření byla odhadnuta extrapolací. Skutečné výsledky se mohou lišit. Uživatelé tohoto dokumentu by měli ověřit vhodnost dat pro svá specifická prostředí.

Informace týkající se produktů jiných společností byly získány od dodavatelů těchto produktů, z jejich tištěných materiálů nebo z jiných veřejně dostupných zdrojů. IBM nezkoumala tyto produkty a nemůže tudíž potvrdit spolehlivost, kompatibilitu a další konstatování, vztahující se k těmto produktům. Dotazy na možnosti produktů pocházejících z jiného zdroje než od IBM adresujte dodavatelům těchto produktů.

Všechna tvrzení o budoucím zaměření nebo úmyslech IBM mohou být bez upozornění změněna nebo zrušena a představují pouze hrubý nástin cílů a podmínek společnosti.

Všechny uváděné ceny IBM jsou maloobchodní ceny navržené společností IBM, jsou nyní platné a mohou se bez upozornění změnit. Ceny u prodejců se mohou lišit.

Tyto informace jsou poskytovány pouze za účelem plánování. Informace zde poskytované se mohou změnit dříve, než budou popisované produkty k dispozici.

Tyto informace obsahují příklady dat a sestav používaných v každodenních obchodních operacích. Příklady obsahují jména osob a názvy společností, značek a produktů, aby bylo možno je vysvětlit v plném rozsahu. Všechna tato jména a názvy jsou zcela fiktivní a jakákoliv podobnost se jmény či adresami existujících společností je zcela náhodná.

LICENČNÍ INFORMACE:

Tyto informace obsahují ukázkové aplikační programy ve zdrojovém jazyce ilustrující programovací techniky na různých operačních platformách. Jste oprávněni bezplatně kopírovat, modifikovat a distribuovat tyto vzorové programy v jakékoliv formě, a to pro účely vývoje, užívání, marketingu nebo distribuce aplikačních programů vhodných pro rozhraní API pro operační platformu, pro kterou byly vzorové programy napsány. Tyto ukázky nebyly náležitě otestovány pro všechny podmínky. Proto IBM nemůže zaručit ani naznačit spolehlivost, provozuschopnost ani funkčnost těchto programů.

Pokud si tyto informace prohlížíte ve formě softcopy, nemusí se zobrazit fotografie a barevné ilustrace.

Ochranné známky

Následující výrazy jsou ochrannými známkami IBM v USA anebo jiných zemích:

Application System/400
AS/400
DB2
e(logo)server
eServer
i5/OS

IBM
iSeries
Lotus
Lotus Notes
Operating System/400
OS/400
Redbooks
SecureWay
WebSphere
400

Microsoft, Windows, Windows NT a logo Windows jsou registrované ochranné známky společnosti Microsoft Corporation ve Spojených státech a případně v dalších jiných zemích.

Java a všechny ochranné známky obsahující jméno Java jsou ochranné známky společnosti Sun Microsystems ve Spojených státech a případně v dalších jiných zemích.

UNIX je registrovaná ochranná známka společnosti Open Group ve Spojených státech a případně v dalších jiných zemích.

Ostatní jména společností, produktů a služeb mohou být ochrannými známkami nebo servisními značkami jiných firem.

Ustanovení a podmínky

- | Oprávnění k užívání těchto publikací je uděleno na základě následujících ustanovení a podmínek.
- | **Osobní použití:** Pokud zachováte všechny výhrady týkající se vlastnických práv, můžete tyto publikace kopírovat pro své osobní nekomerční použití. Tyto publikace ani jakékoli jejich části nesmíte bez výslovného souhlasu IBM distribuovat, prezentovat ani z nich vytvářet odvozená díla.
- | **Komerční použití:** Pokud zachováte všechny výhrady týkající se vlastnických práv, můžete tyto publikace kopírovat, distribuovat a prezentovat výhradně uvnitř svého podniku. Bez výslovného souhlasu IBM nesmíte z těchto publikací vytvářet odvozená díla ani je (nebo jejich části) nesmíte kopírovat, distribuovat či prezentovat mimo rámec svého podniku.
- | Kromě oprávnění, která jsou zde výslovně udělena, se na publikace nebo jakékoli informace, data, software a další duševní vlastnictví obsažené v těchto publikacích nevztahují žádná další vyjádřená ani odvozená oprávnění, povolení či práva.
- | IBM si vyhrazuje právo odvolat oprávnění zde udělená, kdykoli usoudí, že používání publikací poškozuje jeho zájmy nebo že výše uvedené pokyny nejsou řádně dodržovány.
- | Tyto informace můžete stahovat, exportovat či reexportovat pouze při dodržení všech příslušných zákonů a nařízení včetně veškerých vývozních zákonů a nařízení USA.
- | IBM NEPOSKYTUJE ŽÁDNOU ZÁRUKU, POKUD JDE O OBSAH TĚCHTO PUBLIKACÍ. TYTO PUBLIKACE JSOU POSKYTOVÁNY NA BÁZI "JAK JSOU" (AS-IS), BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH NEBO ODVOZENÝCH VČETNĚ, BEZ OMEZENÍ, ODVOZENÝCH ZÁRUK PRODEJNOSTI, NEPORUŠENÍ PRÁV TŘETÍCH STRAN NEBO ZÁRUKY VHODNOSTI PRO URČITÝ ÚČEL.



Vytištěno v Dánsku společností IBM Danmark A/S.