VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

LDAP SERVER

SÍŤOVÉ APLIKACE A SPRÁVÁ SÍTÍ
NETWORK APPLICATIONS AND NETWORK ADMINISTRATION

AUTOR PRÁCE **DO LONG THANH**
AUTHOR

BRNO 2017

Obsah

1 Úvod do problematiky **2**
1.1 Popis LDAP 2

2 Základní informace o programu **5**
2.1 Vyhledávací filter (search request) 6
2.2 Limit počtu navrácených záznamů (size limit) 6
2.3 Formát výstupu 6

3 Návrh a implementace aplikace **7**
3.1 Implementace 7
3.2 Rozšíření a omezení 7
3.3 Testování 7

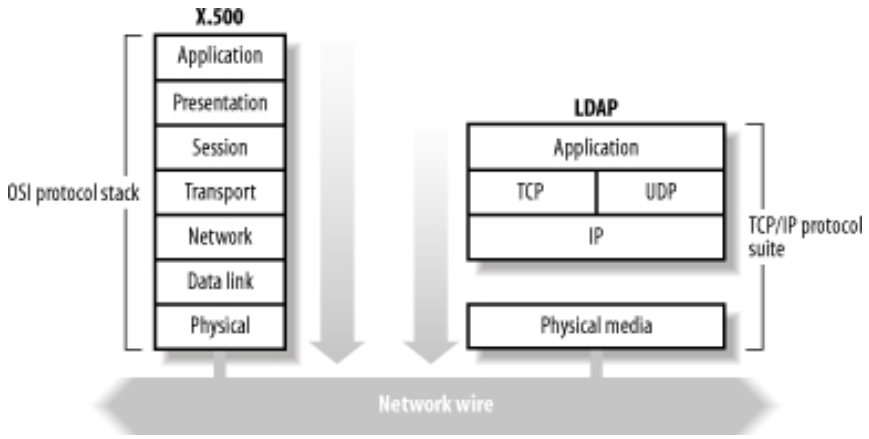
Literatura **8**

Kapitola 1

Úvod do problematiky

1.1 Popis LDAP

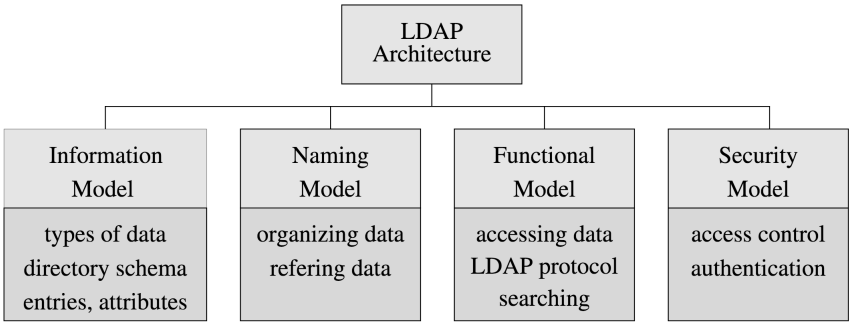
Lightweight Directory Access Protocol, ve zkratce LDAP [RFC 2251][1], je definovaný aplikační protokol pro dotazování a modifikaci adresářových služeb nad TCP/IP [2]. Protokol LDAP je zjednodušený protokol X.500, které bylo vyvinuto ve světě ISO/OSI. LDAPv3 má devět základních operací a poskytuje jednodušší model. Poskytování menšího a jednoduššího souboru operací umožňuje vývojářům soustředit se na sémantiku svých programů bez nutnosti pochopit zřídka používané vlastnosti protokolu.



Obrázek 1.1: X.500 u OSI oproti LDAP u TCP/IP[5]

LDAP je popsán pomocí čtyř modelů: informační, jmenný, funkční a bezpečnostní model.

[1] tools.ietf.org/html/rfc4510



Obrázek 1.2: Modely u LDAP

1. **Informační model**

   Jmenný prostor tvoří hierarchický uspořádání záznamů do stromové struktury, které se jinak nazývá Directory Information Tree (DIT). Její organizace se zabývá jmenný model.

2. **Jmenný model**

   Pro identifikaci objektů se používá Distinguished Name (DN), což je jednoznačný identifikátor objektu a obsahuje úplnou cestu k záznamu (pozici ve stromě).

3. **Funkční model**

   Standardní operace protokolu LDAP lze rozdělit do tří kategorií: aktualizace, dotazování a aktualizace. Celkově LDAP definuje 9 operací.

oblast	operace	popis
autentizace (Authentication)	bind	navázání spojení mezi LDAP serverem a klientem.
	unbind	zrušení spojení mezi LDAP serverem a klientem.
	abandon	klient žádá o ukončení posílání výsledků na poslední dotaz
dotazování (Interrogation)	search	výběr dat z určitého regionu pomocí filtru
	compare	porovná hodnotu atributu se zadanou hodnotou
aktualizace (Update)	add	přidání záznamu do adresářového stromu
	modify	upraví atributy záznamu (vytvořit, smazat, upravit)
	modifyRDN	slouží k přesunutí objektu v rámci stromu adresáře
	delete	smazání záznamu z adresáře

Tabulka 1.1: Operace u LDAP

4. **Bezpečnostní model**

   Bezpečnostní model zajišťuje prokázání identity uživatele (autentizace) pro přístup k záznamům uložený v adresářovém serveru.[4] Autentizaci je možné rozdělit do tří

kategorií.

Anonymní autentizace
Nejjednodušší přístup, určený obvykle pouze pro čtení veřejných položek, je anonymní. Při posílání `bind` se serveru nezasílají žádné identifikační údaje. V tomto případě není potřeba provádět žádnou autentizaci.

Základní autentizace
Jednoduchá metoda prokázání identity uživatele. Klient specifikuje DN uživatele a jeho heslo.

SASL (Simple Authentication and Security Layer)
SASL [RFC 2222][2] je standardizovaná cesta zabezpečení. Jedná se o jasně definované rozhraní. Podpora SASL je novou vlastností standardu LDAP verze 3.

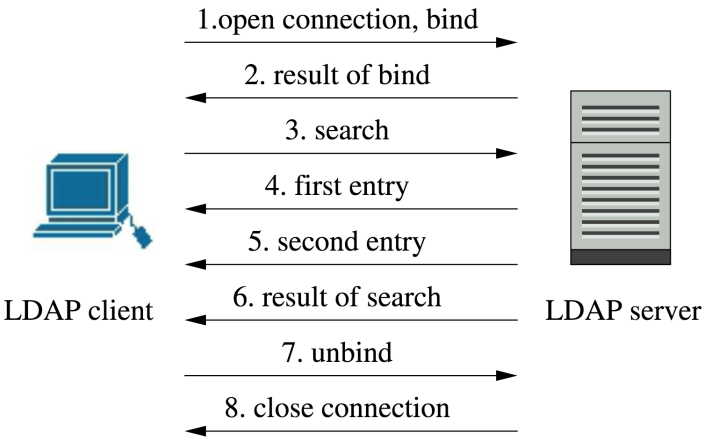
[2] buildbot.tools.ietf.org/html/rfc2222

Kapitola 2

Základní informace o programu

Příklad typické komunikace klienta se serverem při hledání záznamu pomocí protokolu LDAP je na obr. 2.1.

1. Klient zahajuje TCP spojení se serverem a zasílá příkaz `BindRequest`. Ten slouží jako autentizace klienta.
2. Server ověří klientovo identitu, pokud je nastavena autentizace a odpovídá zprávou `BindResponse`. V opačném případě ukončí s klientem spojení.
3. Klient žádá o vyhledání záznamu pomocí `SearchRequest`.
4. Server odpovídá na dotazy typu `SearchRequest` pro každý záznam zprávou `SearchResEntry`. Server informuje klienta o ukončení vyhledávání `SearchResDone`.
5. Klient uzavírá komunikaci se serverem díky `UnbindRequest`.
6. Server uzavře spojení



Obrázek 2.1: Typická komunikace protokolu LDAP

Implementovaná komunikace mezi klientem a serverem je konkurentní a neblokující. Server tudíž je schopen při paralelní komunikaci zpracovávat více procesů nezávisle na

sobě. Při neblokujícím serveru říkáme jádru operačního systému, aby proces, který čeká na data, jež nejsou k dispozici, nepřeváděl do stavu `sleep`, ale zaslal mu chybovou zprávu `EWOULDBLOCK` a vrátí řízení aplikaci. [3]

2.1 Vyhledávací filter (search request)

Slouží pro vyjádření hledání výrazů v adresářovém stromu. Filtry jsou specifikovány v [RFC 2254][1]. Jednotlivé filtry lze mezi sebou kombinovat. V mojí aplikaci je podporováno `and`, `or`, `not`, `equalityMatch` a `substrings`.

Příklad možných dotazů pro LDAP:

- `(uid=xdolon00)`
- `(!(cn=Tim Howes))`
- `(&(cn=Person)(|(cn=Jensen)(email=*vutbr.z)))`
- `(cn=univ*of*mich*)`

2.2 Limit počtu navrácených záznamů (size limit)

Udává maximální počet záznamů které je klient ochoten akceptován. V případě, že není implicitně nastavena velikost, se vypíšou všechny záznamy. Při překročení limitu je vrácen `Sizelimit Exceeded`[1]. Limit nastavený na hodnotu 0 informuje, že není žádný limit nastaven.

2.3 Formát výstupu

Aplikace se spouští přes příkazový řádek (command line) následujícím způsobem:
`./myldap -p <port> -f <soubor>`
Význam parametrů a jejich hodnot:

- `-p <port>`: Umožňuje specifikovat konkrétní port, na kterém začne server naslouchat požadavkům klientů. Výchozí hodnota čísla portu je 389. V případě použití portu bez uživatelských práv se doporučuje používat registrované porty v rozmezí 1024-49151[2]. Jedná se o volitelný parametr.
- `-f <soubor>`: Cesta k textovému souboru. Jedná se o povinný parametr.
- `-h` nebo `-help`: Vypíše nápovědu a ukončí aplikaci.

[1] tools.ietf.org/html/rfc2254
[2] iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

Kapitola 3

Návrh a implementace aplikace

3.1 Implementace

Aplikace je implementována v jazyce C++ se standardními knižnicemi pro práci s vstupem a výstupem. Dále knižnice pro práci se sokety a regexy. Zdrojový kód je členěný do sedmy souborů.

Aplikace je rozdělena na dvě hlavní části. V první části probíhá inicializace spojení, zpracování argumentu a příprava databáze. Při úspěšném navázání spojení s LDAP klientem očekává server požadavek pro hledání v databázi. Každá LDAP zpráva má hlavičku která má pevně danou strukturu ve které se nachází i typ zprávy. LDAP server reaguje na tři typy zpráv: `BindRequest`, `SearchRequest` a `UnbindRequest` (viz. tabulka č. 1.1).

Při dotazu `SearchRequest` se aplikace dostává do hlavní části. Je nejdříve zavolána funkce `parseSearchResponseHeader`, která zpracuje hlavičku zprávy a získá `SizeLimit`. Poté je zavolána funkce `processSearchRequest`, která se rekurzivně zanořuje dokud nenalezne operaci `equalityMatch`, nebo `substrings`. Po zpracování operace vrací množinu ukazatelů na položky, které splňuje podmínku. Při vynořování se aplikovávají zbylé logické operace. Ve výsledku získáme množinu záznamů, které splňují dotazu a záznamy jsou poslány zpět LDAP klientovi.

3.2 Rozšíření a omezení

LDAP server umožňuje načítat dotazy od LDAP klientů a vyhledávat odpovědi v lokální textové databázi. Kromě alfanumerických znaků podporuje LDAP server čtení a vyhledávání s UTF-8 znaky. Server rozeznává pouze anonymní autentizaci. V případě nepodporovaných operátorů při hledání, nebo neznámé operace je klientovi poslána chybová odpověď, případně je zpráva ignorována.

3.3 Testování

Aplikace byla testována na referenčním stroji `merlin.fit.vutbr.cz` s překladačem `g++` za pomocí souboru `Makefile`. Testování probíhalo pomocí `ldapsearch`, který je součástí OS serveru `eva.fit.vutbr.cz`. Bylo také realizováno manuální testování. Dotazy pro LDAP server je přiložen v projektu ve složce `tests`. Při testu nebyly zjišťeny nedostatky při implementaci.

Literatura

[1] Allen, R.; Hunter, L. E.: *Active directory cookbook*. "O'Reilly Media, Inc.", 2006.

[2] Carter, G.: *LDAP System Administration: Putting Directories to Work*. "O'Reilly Media, Inc.", 2003.

[3] Matoušek, P.: *Síťové aplikace a jejich architektura*. Brno: VUTIUM, 2014.

[4] Wahl, M.; Alvestrand, H. T.; Hodges, J.: Authentication methods for LDAP. 2000.

[5] Zeilenga, K.: Lightweight directory access protocol (ldap): Technical specification road map. 2006.