Klient IMAP s podporou TLS

Dokumentace k projektu

Autor: Slabik Yaroslav

Login: xslabi01

Obsah

---

1. Úvod

Tato dokumentace popisuje IMAP klienta s názvem **imapcl**, vytvořeného v rámci projektu předmětu ISA na Fakultě informačních technologií VUT v Brně. Cílem projektu bylo implementovat klienta pro protokol IMAP4rev1 (RFC 3501), který umožňuje stahování elektronické pošty ze zadaného serveru a ukládání zpráv do specifikovaného adresáře.

2. Popis zadání

Program **imapcl** má následující funkce:

- Připojení k zadanému IMAP serveru pomocí protokolu IMAP4rev1.
- Autentizace uživatele pomocí poskytnutých přihlašovacích údajů.
- Stažení zpráv ze zadané schránky (výchozí je "INBOX") a jejich uložení do zadaného adresáře.
- Výpis informace o počtu stažených zpráv na standardní výstup.
- Možnost nastavení dodatečných parametrů pro změnu funkcionality (např. použití SSL/TLS, výběr portu, stahování pouze nových zpráv, stahování pouze hlaviček apod.).

3. Návrh aplikace

3.1 Architektura programu

Program byl navržen modulárně s důrazem na přehlednost a snadnou údržbu. Hlavní komponenty programu:

- **Parsers argumentů příkazové řádky**: Zpracovává vstupní parametry a nastavuje chování programu.
- **Síťový modul**: Zajišťuje navázání spojení se serverem a komunikaci pomocí IMAP protokolu.
- **Autentizační modul**: Provádí přihlášení uživatele k serveru.
- **Modul zpracování zpráv**: Stará se o stahování, zpracování a ukládání zpráv.
- **SSL/TLS modul**: Zajišťuje bezpečné spojení se serverem.

3.2 Struktura kódu

Kód je rozdělen do funkcí, z nichž každá plní specifickou úlohu:

- **initialize_ssl**, **create_context**, **cleanup_ssl**: Funkce pro práci s OpenSSL.
- **connect_to_server**: Navazuje spojení se serverem.
- **send_command**, **receive_response**: Komunikace se serverem pomocí IMAP příkazů.
- **login**, **select_mailbox**, **fetch_messages**: Implementace hlavních funkcí IMAP protokolu.
- **read_credentials**, **directory_exists**: Pomocné funkce pro práci se soubory a adresáři.
- **base64_encode**, **base64_decode**, **decode_encoded_word**: Funkce pro kódování a dekódování zpráv.

4. Popis implementace

4.1 Zpracování argumentů příkazové řádky

Program využívá knihovnu **getopt** pro zpracování parametrů:

- **server**: Adresa serveru (povinný parametr).
- **-p port**: Číslo portu (výchozí 143 nebo 993 při použití TLS).
- **-T**: Použití SSL/TLS.
- **-c certfile**: Soubor s certifikáty pro ověření SSL/TLS certifikátu.
- **-C certaddr**: Adresář s certifikáty (výchozí "/etc/ssl/certs").
- **-n**: Stahování pouze nových zpráv.
- **-h**: Stahování pouze hlaviček zpráv.
- **-a auth_file**: Soubor s autentizačními údaji (povinný parametr).
- **-b MAILBOX**: Název schránky (výchozí "INBOX").
- **-o out_dir**: Výstupní adresář (povinný parametr).

4.2 Navázání spojení se serverem

Funkce **connect_to_server**:

- Získá informace o serveru pomocí **getaddrinfo**.
- Vytvoří socket a naváže TCP spojení.
- Pokud je použit TLS, inicializuje SSL kontext a naváže zabezpečené spojení.
- Ověří certifikát serveru pomocí OpenSSL.

4.3 Autentizace uživatele

Funkce **login**:

- Přijme uvítací zprávu od serveru.
- Zjistí podporované autentizační metody.
- Provede přihlášení pomocí metody LOGIN nebo PLAIN.

4.4 Výběr schránky

Funkce **select_mailbox**:

- Odešle příkaz **SELECT** pro výběr schránky.
- Zpracuje odpověď a získá počet zpráv ve schránce.

4.5 Stahování a ukládání zpráv

Funkce **fetch_messages**:

- Zjistí, které zprávy je potřeba stáhnout.
- Odešle příkazy **FETCH** pro stažení zpráv nebo jejich hlaviček.
- Zpracuje odpovědi včetně literálů.
- Uloží zprávy do zadaného adresáře s potřebným zpracováním.

4.6 Práce se SSL/TLS certifikáty

- Načte certifikáty ze souboru nebo adresáře.
- Nastaví režim ověřování certifikátu serveru.
- Ověří výsledek ověření po navázání SSL spojení.

5. Návod na použití

5.1 Formát souboru s autentizačními údaji

Soubor musí obsahovat:

username = uživatelské_jméno
password = heslo

5.2 Příklady spuštění programu

1. Stažení všech zpráv bez TLS:

   ./imapcl server -a auth.txt -o zpravy

2. Stažení nových zpráv s TLS a certifikátem:

   ./imapcl server -T -c cert.pem -n -a auth.txt -o zpravy

3. Stažení hlaviček zpráv:

   ./imapcl server -h -a auth.txt -o hlavicky

6. Popis testování aplikace

6.1 Popis provedených testů

- **Test připojení** s a bez TLS.
- **Test autentizace** s platnými a neplatnými údaji.
- **Stažení různých typů zpráv**.
- **Test práce s certifikáty**.
- **Test ukládání zpráv** do různých adresářů.

6.2 Výsledky testování

- **Připojení** bylo úspěšné při správném nastavení.
- **Autentizace** proběhla úspěšně s platnými údaji.
- **Stažení zpráv** fungovalo ve všech režimech.
- **Certifikáty** byly správně zpracovány.
- **Ukládání** proběhlo úspěšně do přístupných adresářů.

7. Použitá literatura

1. RFC 3501 - IMAP4rev1
2. RFC 5322 - Internet Message Format
3. Dokumentace OpenSSL
4. Standardní knihovny C/C++