



Klient IMAP s podporou TLS

Dokumentace k projektu

Autor:

Slabik Yaroslav

Login:

xslabi01

Obsah

1. Úvod
 2. Popis zadání
 3. Návrh aplikace
 - 3.1 Architektura programu
 - 3.2 Struktura kódu
 4. Popis implementace
 - 4.1 Zpracování argumentů příkazové řádky
 - 4.2 Navázání spojení se serverem
 - 4.3 Autentizace uživatele
 - 4.4 Výběr schránky
 - 4.5 Stahování a ukládání zpráv
 - 4.6 Práce se SSL/TLS certifikáty
 5. Návod na použití
 - 5.1 Formát souboru s autentizačními údaji
 - 5.2 Příklady spuštění programu
 6. Popis testování aplikace
 - 6.1 Popis provedených testů
 - 6.2 Výsledky testování
 7. Použitá literatura
-

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 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.
- **Sítový 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, save_message:** Implementace hlavních funkcí IMAP protokolu.
- **read_credentials, directory_exists:** Pomocné funkce pro práci se soubory a adresáři.
- **base64_encode, base64_decode, decode_encoded_word, decode_quoted_printable:** 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 TLS.
- **-c certfile:** Soubor s certifikáty pro ověření 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.

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 Použití

./imapcl server [-p port] [-T [-c certfile] [-C certaddr]] [-n] [-h] -a auth_file [-b MAILBOX] -o out_dir

5.2 Formát souboru s autentizačními údaji

Soubor musí obsahovat:

username = uživatelské_jméno

password = heslo

5.3 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 a výsledky testování

1. Test připojení s a bez TLS:

1.1. *Vstup: ./imapcl eva.fit.vutbr.cz -o maildir -a credentials.txt*
Výstup: Staženo 9 zpráv ze schránky INBOX.

1.2. *Vstup: ./imapcl eva.fit.vutbr.cz -o maildir -a credentials.txt -T*
Výstup: TSL connection established

Staženo 9 zpráv ze schránky INBOX.

2. Test připojení na správnou a nesprávnou adresu:

2.1. *Vstup: ./imapcl eva.fit.vutbr.cz -o maildir -a credentials.txt*
Výstup: Staženo 9 zpráv ze schránky INBOX.

2.2. *Vstup: ./imapcl fit.vutbr.cz -o maildir -a credentials.txt*
Výstup: Invalid address/Domain name not supported

3. Test parametrů portu:

3.1. *Vstup: ./imapcl eva.fit.vutbr.cz -p 143 -o maildir -a credentials.txt*
Výstup: Staženo 9 zpráv ze schránky INBOX.

3.2. *Vstup: ./imapcl eva.fit.vutbr.cz -p 14 -o maildir -a credentials.txt*
Výstup: Connection Failed

3.3. *Vstup: ./imapcl eva.fit.vutbr.cz -p asdf -o maildir -a credentials.txt*
Výstup: Error: port must contain only numbers.

4. Test autentizace s platnými a neplatnými údaji:

4.1. *Vstup: ./imapcl eva.fit.vutbr.cz -o maildir -a credentials.txt*
Výstup: Staženo 9 zpráv ze schránky INBOX.

4.2. *Vstup: ./imapcl eva.fit.vutbr.cz -o maildir -a wrong_credentials.txt*
Výstup: Login failed
Authentication failed

5. Stažení různých typů zpráv:

5.1. *Vstup: ./imapcl eva.fit.vutbr.cz -o maildir -a credentials.txt -n*
Výstup: Žádné nové zprávy ve schránce INBOX. - pokud není k dispozici

Staženo 1 nových zpráv ze schránky INBOX. - pokud je k dispozici

5.2. *Vstup: ./imapcl eva.fit.vutbr.cz -o maildir -a credentials.txt -h*
Výstup: Staženy hlavičky 6 zpráv ze schránky INBOX.

5.3. *Vstup: ./imapcl eva.fit.vutbr.cz -o maildir -a credentials.txt -h -n*
Výstup: Žádné nové zprávy ve schránce INBOX. - pokud není k dispozici

Staženy hlavičky 1 nových zpráv ze schránky INBOX. - pokud je k dispozici

6. Test práce s certifikáty:

6.1. *Vstup: ./imapcl eva.fit.vutbr.cz -T -C Sertificate/ -o maildir -a credentials.txt*
Výstup: TSL connection established
Staženo 9 zpráv ze schránky INBOX

6.2. *Vstup: ./imapcl eva.fit.vutbr.cz -T -C Wrong_Sertificate/ -o maildir -a credentials.txt*
Výstup: Certificate directory is empty or contains no valid certificates

6.3. *Vstup: ./imapcl eva.fit.vutbr.cz -T -c cacert.pem -o maildir -a credentials.txt*

Výstup: TSL connection established
Staženo 9 zpráv ze schránky INBOX.

6.4. *Vstup: ./imapcl eva.fit.vutbr.cz -T -c wrong.pem -o maildir -a credentials.txt*
Výstup: Error loading certificate

7. Test ukládání zpráv:

7.1. *Vstup: ./imapcl eva.fit.vutbr.cz -o maildir -a credentials.txt*
Výstup: Staženo 9 zpráv ze schránky INBOX.

7.2. *Vstup: ./imapcl eva.fit.vutbr.cz -o wrong_maildir -a credentials.txt*
Výstup: Error: output directory does not exist: wrong_maildir

8. Test parametrů schránky:

8.1. *Vstup: ./imapcl eva.fit.vutbr.cz -o maildir -a credentials.txt -b Sent*
Výstup: Staženo 67 zpráv ze schránky Sent.

8.2. *Vstup: ./imapcl eva.fit.vutbr.cz -o maildir -a credentials.txt -b Trash*
Výstup: Staženo 1568 zpráv ze schránky Trash.

8.3. *Vstup: ./imapcl eva.fit.vutbr.cz -o maildir -a credentials.txt -b Error*
Výstup: Failed to select mailbox

9. Testování neplatného formátu příkazového řádku:

9.1. *Vstup: ./imapcl -o maildir -a credentials.txt*
Výstup: Error: server IP or domain name is required
Usage: ./imapcl server [-p port] [-T [-c certfile] [-C certaddr]] [-n]
[-h] -a auth_file [-b MAILBOX] -o out_dir

9.2. *Vstup: ./imapcl eva.fit.vutbr.cz -o maildir*
Výstup: Error: credentials file is required (-a auth_file)
Usage: ./imapcl server [-p port] [-T [-c certfile] [-C certaddr]] [-n]
[-h] -a auth_file [-b MAILBOX] -o out_dir

9.3. *Vstup: ./imapcl eva.fit.vutbr.cz -a credentials.txt*

Výstup: Error: output directory is required (-o out_dir)
Usage: ./imapcl server [-p port] [-T [-c certfile] [-C certaddr]] [-n] [-h] -a auth_file [-b MAILBOX] -o out_dir

9.4. *Vstup: ./imapcl eva.fit.vutbr.cz -o maildir -a credentials.txt -z*

Výstup: ./imapcl: invalid option -- 'z'
Usage: ./imapcl server [-p port] [-T [-c certfile] [-C certaddr]] [-n] [-h] -a auth_file [-b MAILBOX] -o out_dir

9.5. *Vstup: ./imapcl eva.fit.vutbr.cz -o maildir -a credentials.txt -b*

Výstup: ./imapcl: option requires an argument -- 'b'
Usage: ./imapcl server [-p port] [-T [-c certfile] [-C certaddr]] [-n] [-h] -a auth_file [-b MAILBOX] -o out_dir

9.6. *Vstup: ./imapcl eva.fit.vutbr.cz extra_argument -o maildir -a credentials.txt*

Výstup: Error: unexpected argument(s): extra_argument
Usage: ./imapcl server [-p port] [-T [-c certfile] [-C certaddr]] [-n] [-h] -a auth_file [-b MAILBOX] -o out_dir

9.7. *Vstup: ./imapcl eva.fit.vutbr.cz -o maildir -a credentials.txt -C Sertificate/*

Výstup: Error: -C and -c options require -T to be specified.
Usage: ./imapcl server [-p port] [-T [-c certfile] [-C certaddr]] [-n] [-h] -a auth_file [-b MAILBOX] -o out_dir

7. Použitá literatura

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