



Manuál k projektu
LDAP server

Janečka Tomáš - xjanec35

12. listopadu 2023

Obsah

1	Shrnutí teorie	3
2	Implementace	4
3	Testování	7
4	Použité odkazy	18

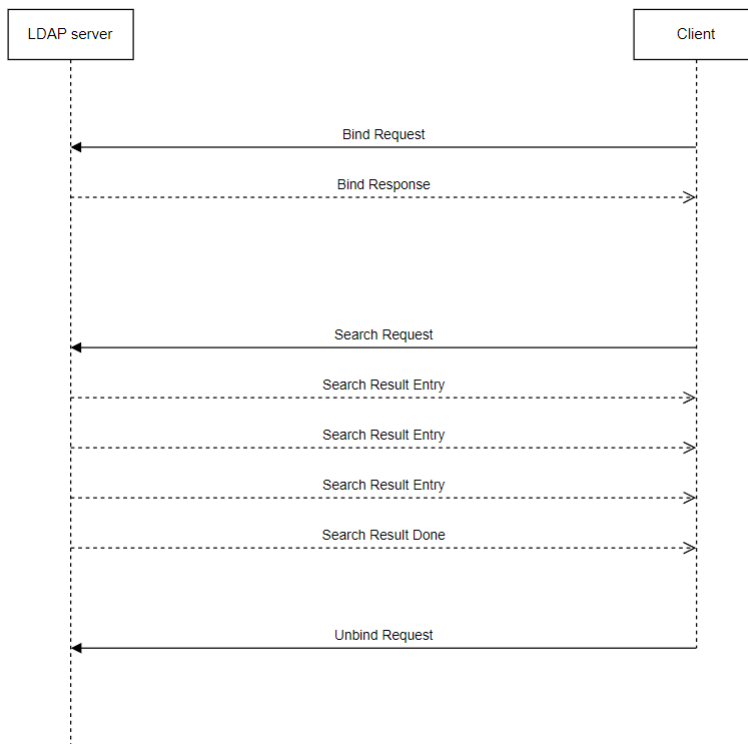
1 Shrnutí teorie

LDAP (Lightweight Directory Access Protocol) je definovaný protokol pro ukládání a přístup k datům na adresářovém serveru. Podle tohoto protokolu jsou jednotlivé položky na serveru ukládány formou záznamů a uspořádány do stromové struktury (jako ve skutečné adresářové architektuře). Je vhodný pro udržování adresářů a práci s informacemi o uživateli (např. pro vyhledávání adres konkrétních uživatelů v příslušných adresářích, resp. databázích). V našem případě je LDAP protokol využit pro implementaci serveru pouze pro vyhledávání v jednom souboru.

Zpráva LDAP protokolu se skládá z oktetu nebo taky osmibitových bloků dat, každá hodnota oktetu označuje nějaký typ, operaci nebo hodnotu. Zpráva zpravidla začíná oktetem 0x30, který symbolizuje typ sekvence, takovýto oktet označující typ, je vždy následován délkou, zde by to byla délka celé sekvence. Po uvedení celé sekvence následuje id zprávy, to může vypadat například takto: "0x02(typ integer) 0x01(délka) 0x02(hodnota)". Stejným způsobem je poskládán zbytek zprávy. Bližší popis fungování serveru a dotazů na něj bude popsán v následujících kapitolách.

2 Implementace

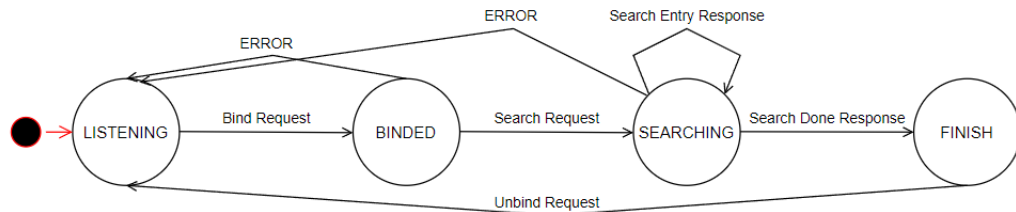
1. Průběh interakce mezi serverem a klientem



Obrázek 1: Komunikace mezi serverem a klientem

Client začíná komunikaci zasláním zprávy bind request, na kterou server odpovídá zprávou bind response. Následně client po přijetí zprávy o úspěšném spojení od serveru posílá search request. Server zpracuje tento request a začne posílat výsledky hledání(bližší popis bude v následujících kapitolách). Průběžné výsledky server posílá jako search result entry, těchto zpráv může být nula a více. Server ukončuje hledání zasláním search request done, toto může být zapříčiněno překročením size limitu(maximálního počtu výsledků), prohledáním celého souboru, nebo nějakou chybou například nepodporovaný atribut. Client po přijetí zprávy search response done od serveru zasílá unbind request a tím ukončuje komunikaci.

2. Funkcionalita serveru



Obrázek 2: Stavy serveru

(a) Spuštění programu

Zkompilovat pomocí přiloženého Makefile příkazem "make".

Spuštění:

```
./isa-ldapserver {-p <port>} -f <soubor>
```

Například:

```
sudo ./isa-ldapserver -p 389 -f ldap-lidi-ascii.txt
```

```
./isa-ldapserver -p 1234 -f ldap-lidi-ascii.txt
```

```
sudo ./isa-ldapserver -f ldap-lidi-ascii.txt
```

(b) Listening

Po spuštění programu začne server naslouchat na zadaném portu (implicitně 389). Server je nabíndovaný jak na IPv4 tak na IPv6.

(c) Binded

Po vytvoření spojení a obdržení bind requestu od klienta se na serveru spouští nový proces, který obsluhuje klienta, mateřský proces pokračuje v naslouchání. Server odešle bind response o úspěšném nabíndování. Pokud search request od klienta obsahuje nepodporované atributy server odešle search done response s chybovou hláškou, uzavře spojení a proces se ukončí.

(d) **Searching**

Server dekóduje search request od klienta. Pokud search request od klienta obsahuje nepodporované atributy server odešle search done response s chybovou hláškou, uzavře spojení a proces se ukončí. Při úspěšném dekódování začne server vyhledávat v souboru zadaného na vstupu. Vyhledávání kontroluje každý řádek souboru a při případné shodě odešle klientovi zprávu search result entry s atributy "cn" a "mail". Při překročení size limitu(maximálního počtu výsledků), nebo dosažení konce souboru se odešle search request done s odpovídajícím obsahem například atribut indikující překročení size limitu.

(e) **Finish**

Po obdržení unbind requestu od klienta, server ukončí spojení a proces obsluhující daného klienta.

(f) **Ukončení programu**

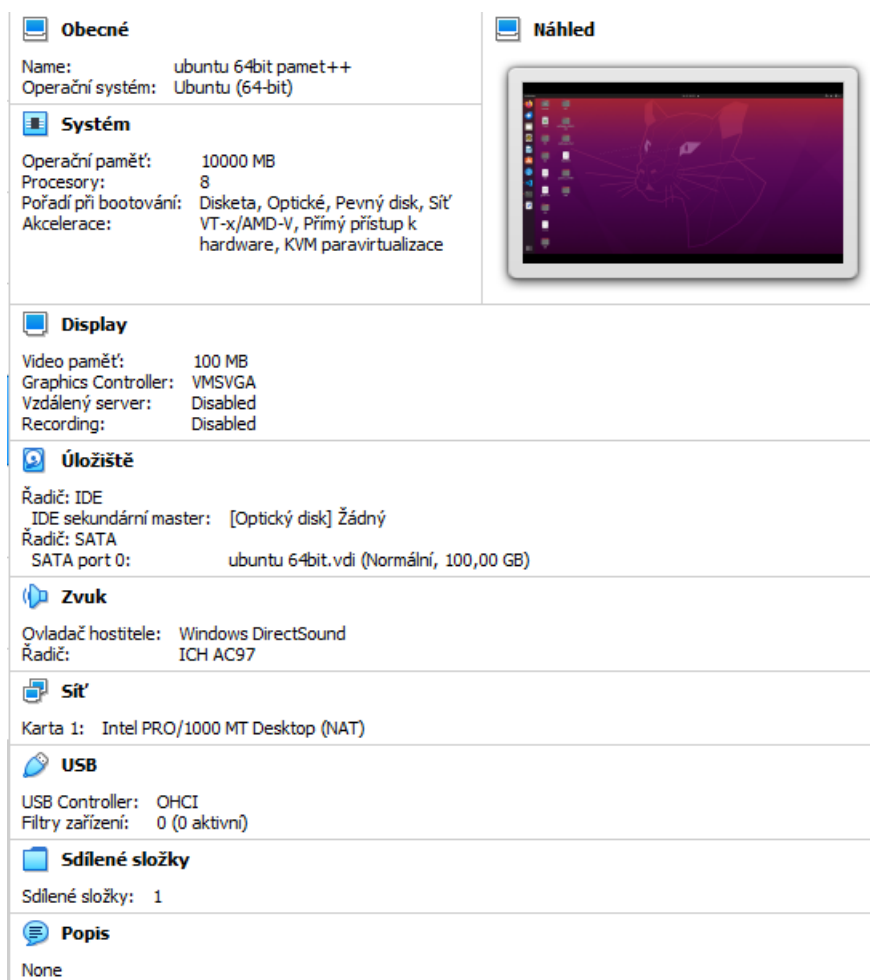
Program se ukončuje stisknutím ctrl+c.

3 Testování

Při testování se počítá s daným formátem souboru a to například: "Janecka Tomas;xjanec35;xjanec35@stud.fit.vutbr".

1. Vývojové a testovací prostředí

Vývoj a testování probíhalo na virtuálním disku na operačním systému linux Ubuntu 20.04.6 LTS.

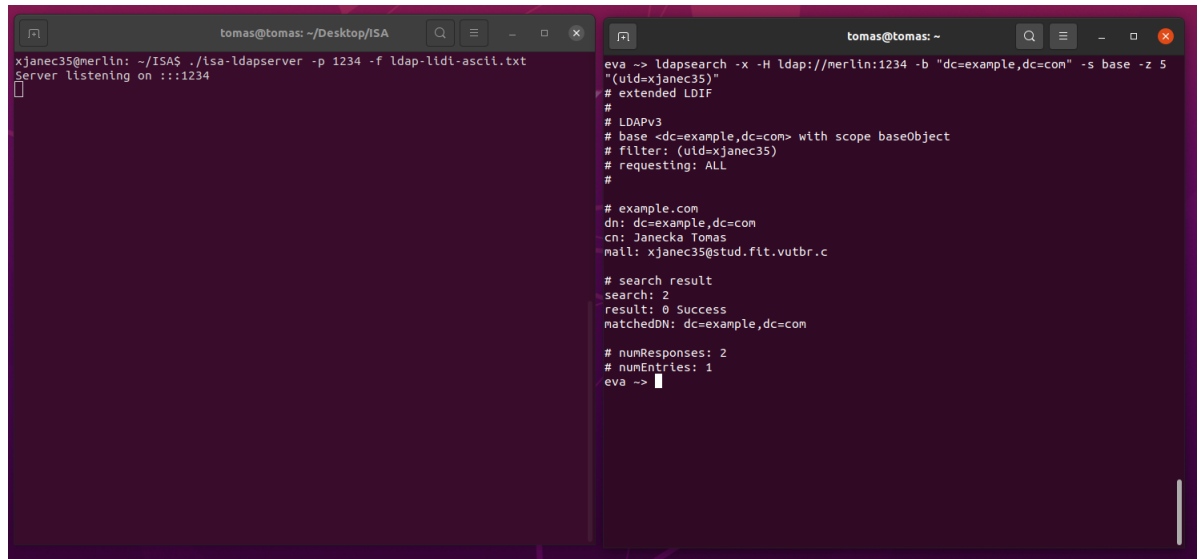


Obrázek 3: Nastavení VM ve VirtualBoxu

2. Testovací vstupy a výstupy

(a) Nabindování na IPv4 i na IPv6

Zaslání search requestu ze serveru eva na server merlin na IPv4.
Během testování se nenašly chyby.



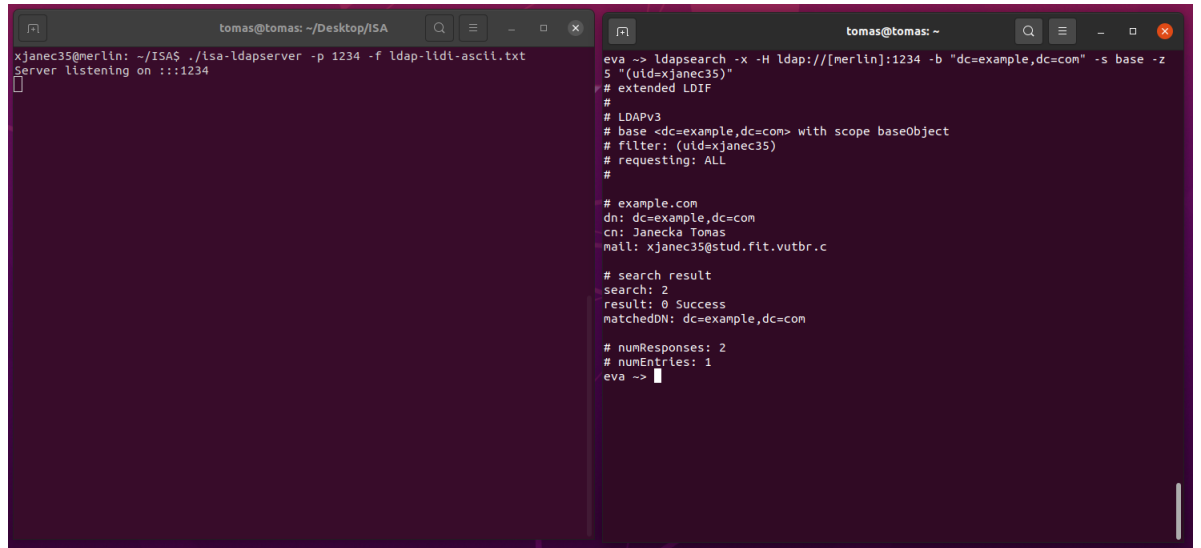
The image shows two terminal windows side-by-side. The left window, titled 'tomas@tomas: ~/Desktop/ISA', shows the output of the command 'xjanec35@merlin: ~/ISA\$./isa-ldapserver -p 1234 -f ldap-ldif-ascii.txt'. The output is 'Server listening on :::1234'. The right window, titled 'tomas@tomas: ~', shows the output of the command 'eva -> ldapsearch -x -H ldap://merlin:1234 -b "dc=example,dc=com" -s base -z 5 "(uid=xjanec35)"'. The output is a standard LDAP search result for the entry 'dc=example,dc=com' with fields 'cn: Janecka Tomas' and 'mail: xjanec35@stud.flt.vutbr.c'.

```
tomas@tomas: ~/Desktop/ISA
xjanec35@merlin: ~/ISA$ ./isa-ldapserver -p 1234 -f ldap-ldif-ascii.txt
Server listening on :::1234

tomas@tomas: ~
eva -> ldapsearch -x -H ldap://merlin:1234 -b "dc=example,dc=com" -s base -z 5
"(uid=xjanec35)"
# extended LDIF
#
# LDAPv3
# base <dc=example,dc=com> with scope baseObject
# filter: (uid=xjanec35)
# requesting: ALL
#
# example.com
dn: dc=example,dc=com
cn: Janecka Tomas
mail: xjanec35@stud.flt.vutbr.c
# search result
search: 2
result: 0 Success
matchedDN: dc=example,dc=com
# numResponses: 2
# numEntries: 1
eva ->
```

Obrázek 4: Odeslání requestu na IPv4

Zaslání search requestu ze serveru eva na server merlin na IPv6.
Během testování se nenašly chyby.



The image shows two terminal windows side-by-side. The left window, titled 'tomas@tomas: ~/Desktop/ISA', shows the command 'xjanec35@merlin: ~/ISA\$./isa-ldapsrv -p 1234 -f ldap-ldi-ascii.txt' and the output 'server listening on :::1234'. The right window, titled 'tomas@tomas: ~', shows the command 'eva -> ldapsearch -x -H ldap://[merlin]:1234 -b "dc=example,dc=com" -s base -z 5 "(uid=xjanec35)"' and its output, which includes LDAPv3 search details and user information for 'dc=example,dc=com'.

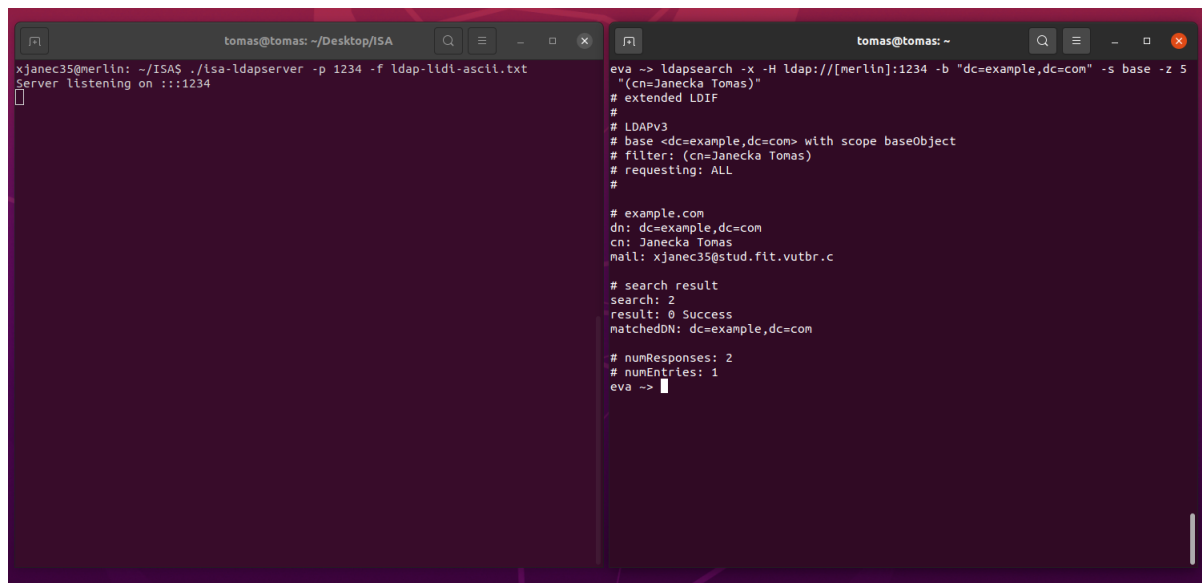
```
tomas@tomas: ~/Desktop/ISA
xjanec35@merlin: ~/ISA$ ./isa-ldapsrv -p 1234 -f ldap-ldi-ascii.txt
server listening on :::1234

tomas@tomas: ~
eva -> ldapsearch -x -H ldap://[merlin]:1234 -b "dc=example,dc=com" -s base -z
5 "(uid=xjanec35)"
# extended LDIF
#
# LDAPv3
# base <dc=example,dc=com> with scope baseObject
# filter: (uid=xjanec35)
# requesting: ALL
#
# example.com
dn: dc=example,dc=com
cn: Janecka Tomas
mail: xjanec35@stud.fit.vutbr.c
# search result
search: 2
result: 0 Success
matchedDN: dc=example,dc=com
# numResponses: 2
# numEntries: 1
eva ->
```

Obrázek 5: Odeslání requestu na IPv6

(b) **LDAP Search Requests**

Jednoduché vyhledání podle jména(cn), výstup byl očekávaný, během testování se nanašly chyby.

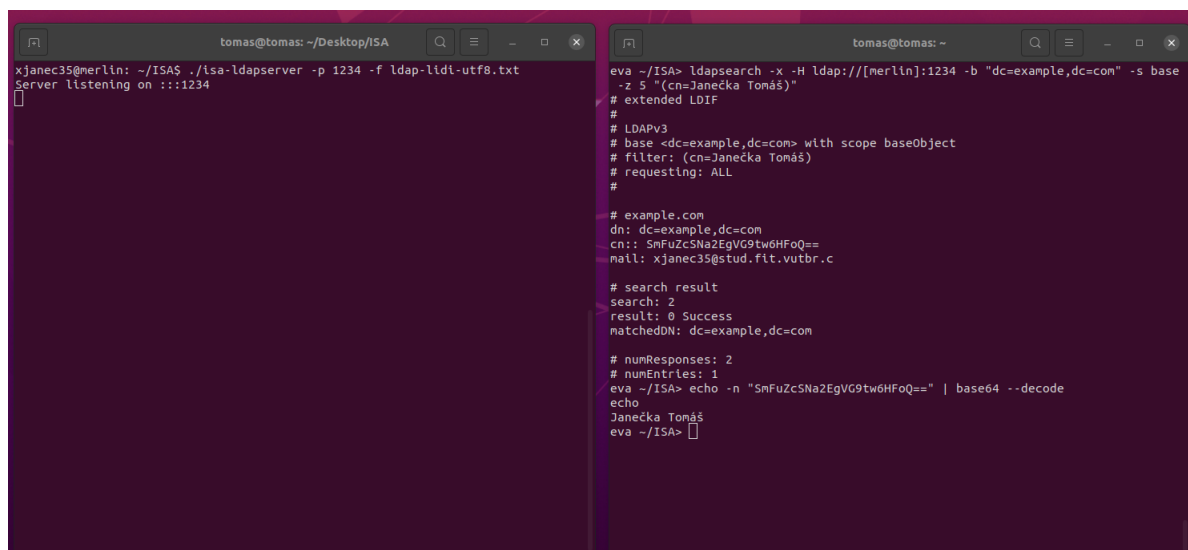


```
xjanec35@merlin: ~/ISA$ ./isa-ldapsrv -p 1234 -f ldap-lidi-ascii.txt
Server listening on :::1234

eva -> ldapsearch -x -H ldap://[merlin]:1234 -b "dc=example,dc=com" -s base -z 5
"(cn=Janecka Tomas)"
# extended LDIr
#
# LDAPv3
# base <dc=example,dc=com> with scope baseObject
# filter: (cn=Janecka Tomas)
# requesting: ALL
#
# example.com
dn: dc=example,dc=com
cn: Janecka Tomas
mail: xjanec35@stud.fit.vutbr.c
# search result
search: 2
result: 0 Success
matchedDN: dc=example,dc=com
# numResponses: 2
# numEntries: 1
eva ->
```

Obrázek 6: Match test

Jednoduché vyhledání podle jména(cn) v utf8, zde byla použita část souboru, kde byly vměněny oddělovače „,“ za „;“, který server podpo-ruje, jiné oddělovače způsobí chybový stav. Client nevypsál zprávu od serveru ve správném dekódování, ale po příkazu „base64 –decode“ se ukázalo, že zpráva serveru je správná.

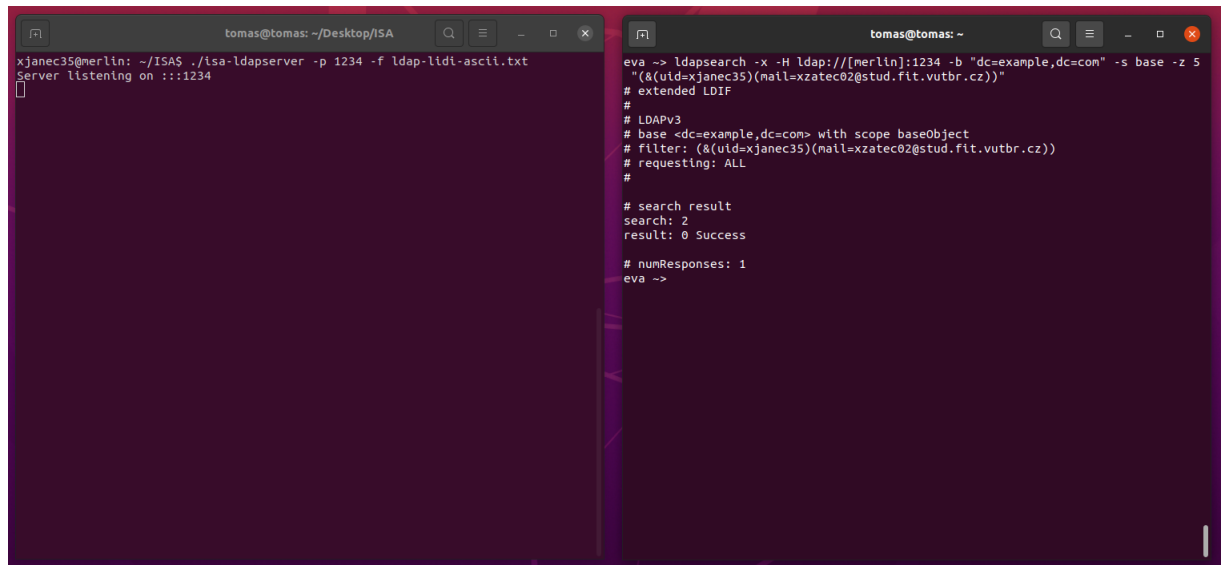


```
tomas@tomas: ~/Desktop/ISA
xjanec35@merlin: ~/ISA$ ./isa-ldapserver -p 1234 -f ldap-ldf-utf8.txt
server listening on :::1234

eva ~/ISA> ldapsearch -x -H ldap://[merlin]:1234 -b "dc=example,dc=com" -s base
-z 5 "(cn=Janečka Tomáš)"
# extended LDIF
#
# LDAPv3
# base <dc=example,dc=com> with scope baseObject
# filter: (cn=Janečka Tomáš)
# requesting: ALL
#
# example.com
dn: dc=example,dc=com
cn: SnFuZc5Na2EgVG9tw6HfOQ==
mail: xjanec35@stud.fit.vutbr.c
# search result
search: 2
result: 0 Success
matchedDN: dc=example,dc=com
# numResponses: 2
# numEntries: 1
eva ~/ISA> echo -n "SnFuZc5Na2EgVG9tw6HfOQ==" | base64 --decode
echo
Janečka Tomáš
eva ~/ISA>
```

Obrázek 7: UTF-8 match test

Test filtru and na loginu(uid) a emailu(mail) dvou různých řádků, výstup byl očekávaný, během testování se nanašly chyby.



The image shows two terminal windows side-by-side. The left window is titled 'tomas@tomas: ~/Desktop/ISA' and shows the command 'xjanec35@merlin: ~/ISA\$./isa-ldapserver -p 1234 -f ldap-lidi-ascii.txt' being executed, with the output 'Server listening on :::1234'. The right window is titled 'tomas@tomas: ~' and shows the command 'eva -> ldapsearch -x -H ldap://[merlin]:1234 -b "dc=example,dc=com" -s base -z 5 "(uid=xjanec35)(mail=xzatec02@stud.fit.vutbr.cz))"' being executed, with the output showing LDAP search details and a successful result.

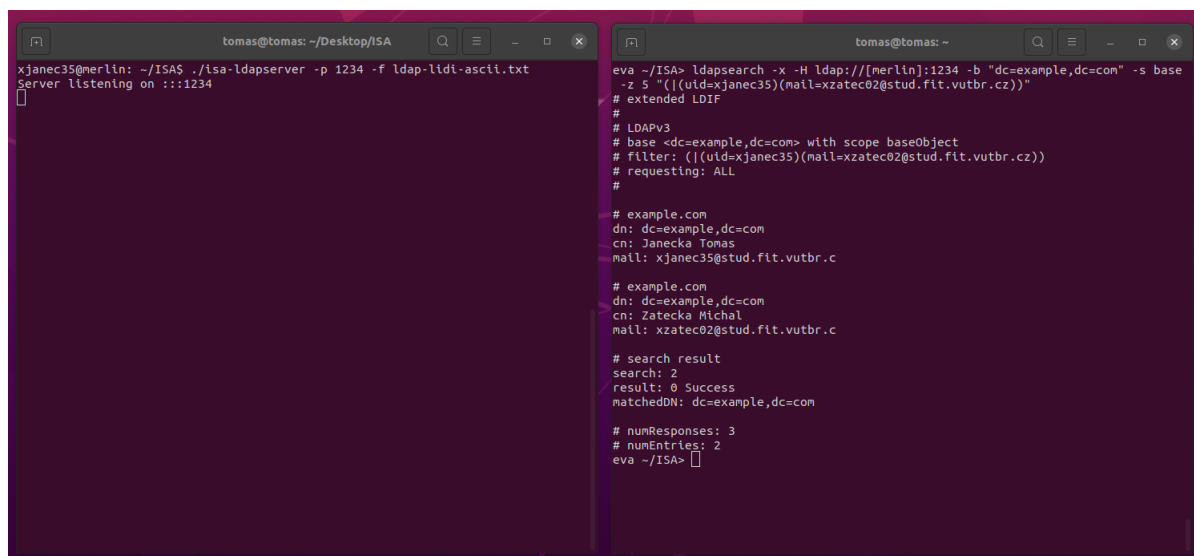
```
tomas@tomas: ~/Desktop/ISA
xjanec35@merlin: ~/ISA$ ./isa-ldapserver -p 1234 -f ldap-lidi-ascii.txt
Server listening on :::1234

tomas@tomas: ~
eva -> ldapsearch -x -H ldap://[merlin]:1234 -b "dc=example,dc=com" -s base -z 5
"(uid=xjanec35)(mail=xzatec02@stud.fit.vutbr.cz))"
# extended LDIF
#
# LDAPv3
# base <dc=example,dc=com> with scope baseObject
# filter: (&(uid=xjanec35)(mail=xzatec02@stud.fit.vutbr.cz))
# requesting: ALL
#
# search result
search: 2
result: 0 Success

# numResponses: 1
eva ->
```

Obrázek 8: And test

Test filtru or na loginu(uid) a emailu(mail) dvou různých řádků, při testování se zjistilo, že server nesprávně porovnává atribut mail, tato chyba byla odstraněna a zde je správný výstup



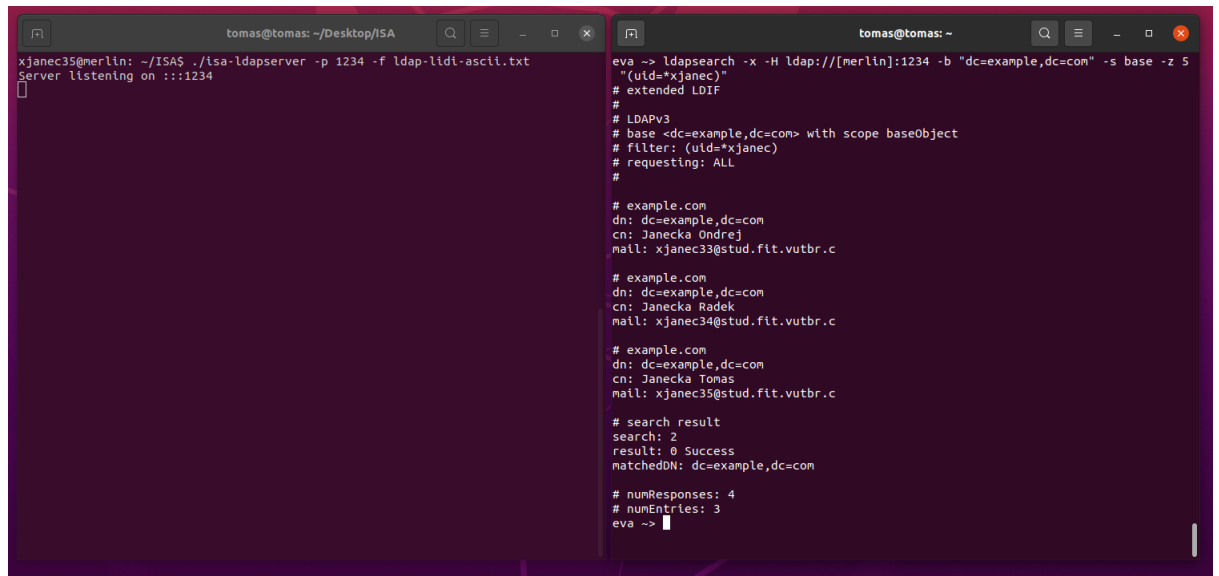
The image shows two terminal windows side-by-side. The left window is titled 'tomas@tomas: ~/Desktop/ISA' and shows the command 'xjanec35@merlin: ~/ISA\$./isa-ldapsrv -p 1234 -f ldap-ldi-ascii.txt' and the output 'Server listening on :::1234'. The right window is titled 'tomas@tomas: ~' and shows the command 'eva ~/ISA> ldapsearch -x -H ldap://[merlin]:1234 -b "dc=example,dc=com" -s base -z 5 "([uid=xjanec35)(mail=xzatec02@stud.fit.vutbr.cz))"' and its output, which includes LDAPv3 search details and two entries for 'dc=example,dc=com' with different email addresses.

```
tomas@tomas: ~/Desktop/ISA
xjanec35@merlin: ~/ISA$ ./isa-ldapsrv -p 1234 -f ldap-ldi-ascii.txt
Server listening on :::1234

tomas@tomas: ~
eva ~/ISA> ldapsearch -x -H ldap://[merlin]:1234 -b "dc=example,dc=com" -s base
-z 5 "([uid=xjanec35)(mail=xzatec02@stud.fit.vutbr.cz))"
# extended LDIF
#
# LDAPv3
# base <dc=example,dc=com> with scope baseObject
# filter: ([uid=xjanec35)(mail=xzatec02@stud.fit.vutbr.cz))
# requesting: ALL
#
# example.com
dn: dc=example,dc=com
cn: JANECKA Tomas
mail: xjanec35@stud.fit.vutbr.c
# example.com
dn: dc=example,dc=com
cn: ZATECKA Michal
mail: xzatec02@stud.fit.vutbr.c
# search result
search: 2
result: 0 Success
matchedDN: dc=example,dc=com
# numResponses: 3
# numEntries: 2
eva ~/ISA>
```

Obrázek 9: Or test

Test filtru substring na loginu(uid), zde se našla chyba při špatném dekódování, která měla dopad i na následné vyhledání, byla úspěšně odstraněna.



```
tomas@tomas: ~/Desktop/ISA
xjanec35@merlin: ~/ISA$ ./isa-ldapserver -p 1234 -f ldap-lidi-ascii.txt
server listening on :::1234

eva -> ldapsearch -x -H ldap://[merlin]:1234 -b "dc=example,dc=com" -s base -z 5
"(uid=*xjanec)"
# extended LDIF
#
# LDAPv3
# base <dc=example,dc=com> with scope baseObject
# filter: (uid=*xjanec)
# requesting: ALL
#
# example.com
dn: dc=example,dc=com
cn: Janecka Ondrej
mail: xjanec33@stud.fit.vutbr.c

# example.com
dn: dc=example,dc=com
cn: Janecka Radek
mail: xjanec34@stud.fit.vutbr.c

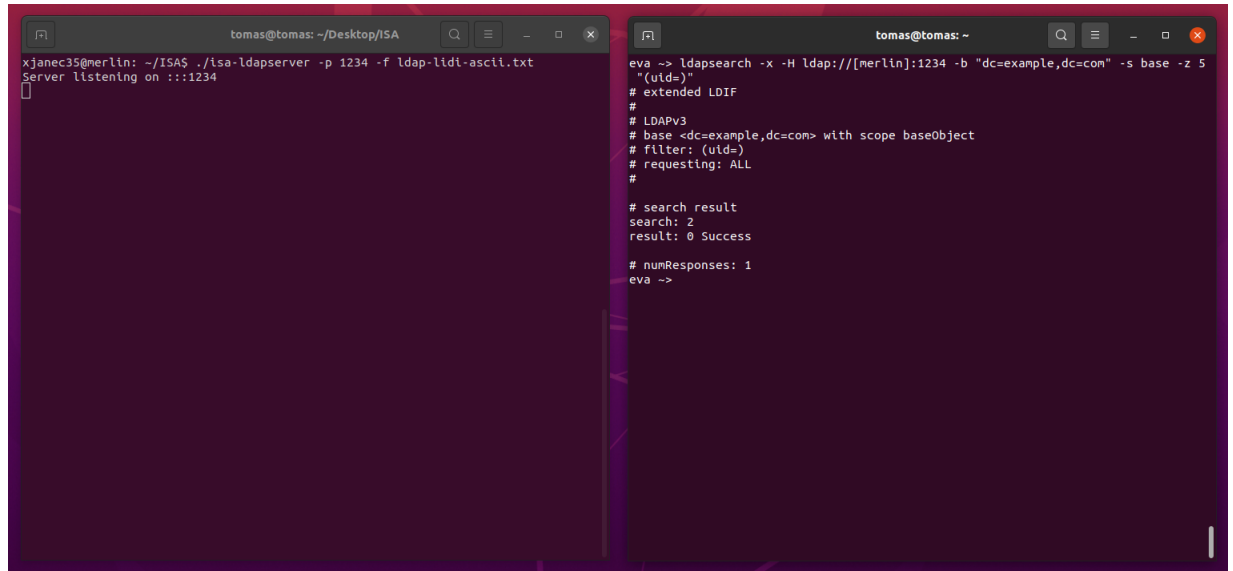
# example.com
dn: dc=example,dc=com
cn: Janecka Tomas
mail: xjanec35@stud.fit.vutbr.c

# search result
search: 2
result: 0 Success
matchedDN: dc=example,dc=com

# numResponses: 4
# numEntries: 3
eva ->
```

Obrázek 10: Substring test

Test prázdného atributu login(uid), výstup byl očekávaný, během testování se nanašly chyby.



The image shows two terminal windows side-by-side. The left window, titled 'tomas@tomas: ~/Desktop/ISA', shows the command 'xjanec35@merlin: ~/ISA\$./isa-ldapservice -p 1234 -f ldap-ldi-ascii.txt' and the output 'Server listening on :::1234'. The right window, titled 'tomas@tomas: ~', shows the command 'eva -> ldapsearch -x -H ldap://[merlin]:1234 -b "dc=example,dc=com" -s base -z 5 "(uid=)"' and its output, which includes LDAPv3 search details and a successful result for the filter '(uid=)'.

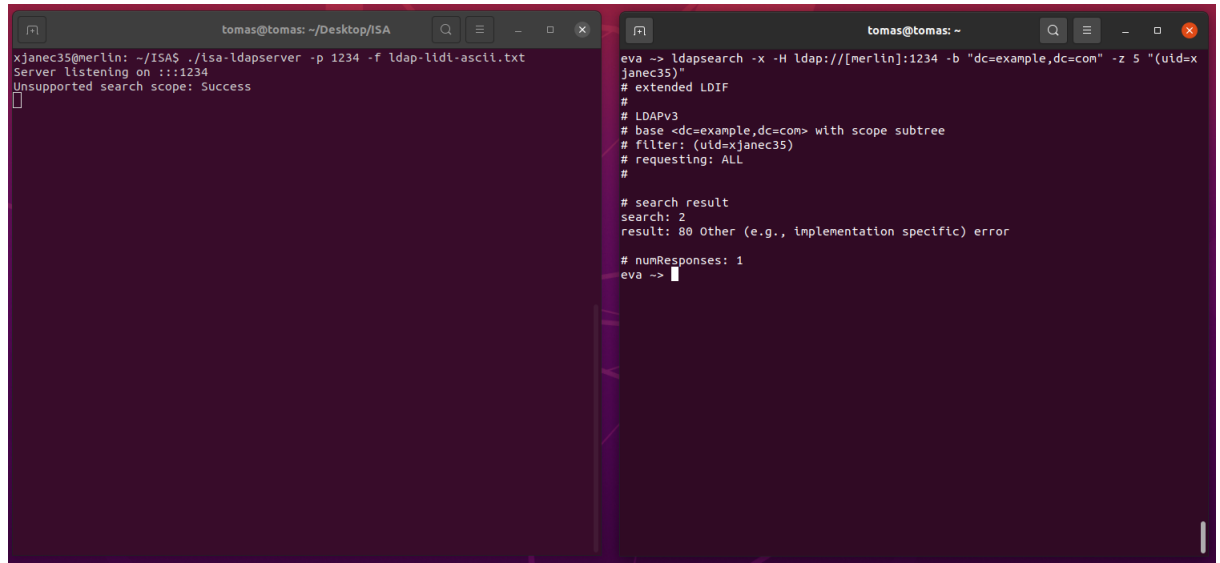
```
xjanec35@merlin: ~/ISA$ ./isa-ldapservice -p 1234 -f ldap-ldi-ascii.txt
Server listening on :::1234

eva -> ldapsearch -x -H ldap://[merlin]:1234 -b "dc=example,dc=com" -s base -z 5
"(uid=)"
# extended LDIF
#
# LDAPv3
# base <dc=example,dc=com> with scope baseObject
# filter: (uid=)
# requesting: ALL
#
# search result
search: 2
result: 0 Success

# numResponses: 1
eva ->
```

Obrázek 11: Null test

Test nepodporovaného atributu scope(whole subtree, podporuje se pouze base), výstup byl očekávaný, během testování se nanašly chyby.



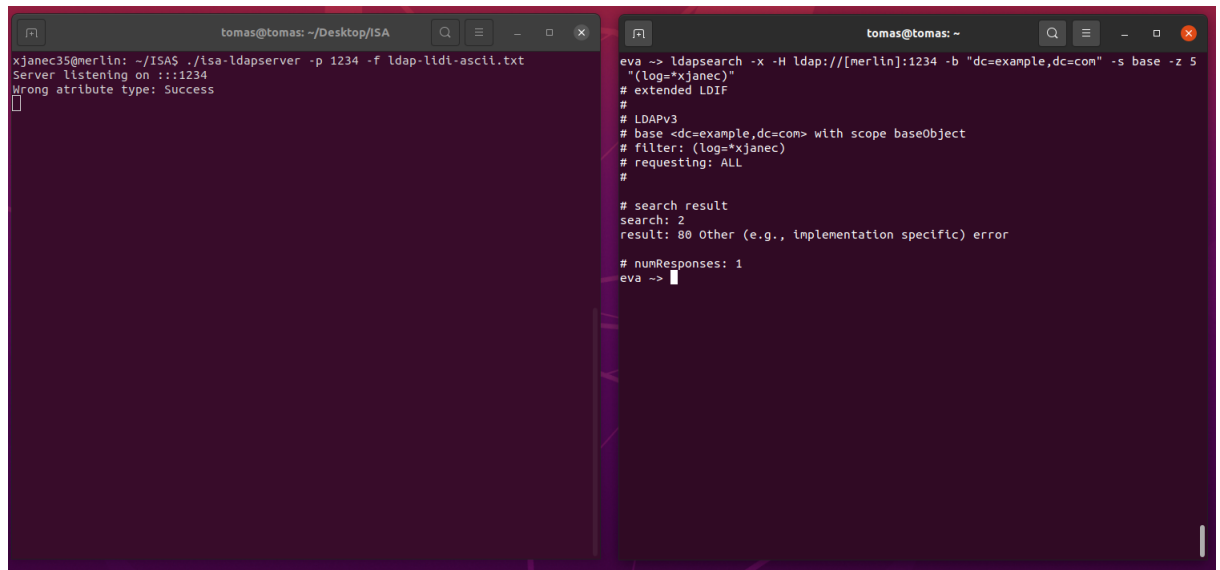
The image shows two terminal windows side-by-side. The left window is titled 'tomas@tomas: ~/Desktop/ISA' and shows the output of running 'isa-ldapservice' on a machine named 'merlin'. It displays 'Server listening on :::1234' and 'Unsupported search scope: Success'. The right window is titled 'tomas@tomas: ~' and shows the output of an 'ldapservice' command. It displays LDAP search details, including the base '<dc=example,dc=com>' with scope 'subtree', filter '(uid=xjanec35)', and requesting 'ALL'. The search result is '80 Other (e.g., implementation specific) error'.

```
tomas@tomas: ~/Desktop/ISA
xjanec35@merlin: ~/ISA$ ./isa-ldapservice -p 1234 -f ldap-ldi-ascii.txt
Server listening on :::1234
Unsupported search scope: Success
[]
```

```
tomas@tomas: ~
eva -> ldapservice -x -H ldap://[merlin]:1234 -b "dc=example,dc=com" -z 5 "(uid=xjanec35)"
# extended LDIF
#
# LDAPv3
# base <dc=example,dc=com> with scope subtree
# filter: (uid=xjanec35)
# requesting: ALL
#
# search result
search: 2
result: 80 Other (e.g., implementation specific) error
# numResponses: 1
eva ->
```

Obrázek 12: Wrong scope test

Test špatně zadaného atributu(log, podporují se pouze cn, uid, mail), zde byla nalezena chyba v dekodování, kdy stačilo, aby atribut měl stejnou délku jako jeden z podporovaných a byl vyhodnocen jako správný, chyba byla odstraněna a zde je správný výstup



The image shows two terminal windows side-by-side. The left window, titled 'tomas@tomas: ~/Desktop/ISA', shows the output of the 'isa-ldapserver' command. It indicates the server is listening on port 1234 and reports a 'Wrong attribute type: Success' message. The right window, titled 'tomas@tomas: ~', shows the output of an 'ldapsearch' command. It displays LDAP search details, including the base, filter, and a search result indicating an 'Other (e.g., implementation specific) error'.

```
tomas@tomas: ~/Desktop/ISA
xjanec35@merlin: ~/ISA$ ./isa-ldapserver -p 1234 -f ldap-ldi-ascii.txt
Server listening on :::1234
Wrong attribute type: Success
[]
```

```
tomas@tomas: ~
eva -> ldapsearch -x -H ldap://[merlin]:1234 -b "dc=example,dc=com" -s base -z 5
"(log=*xjanec)"
# extended LDIF
#
# LDAPv3
# base <dc=example,dc=com> with scope baseObject
# filter: (log=*xjanec)
# requesting: ALL
#
# search result
search: 2
result: 80 Other (e.g., implementation specific) error
# numResponses: 1
eva ->
```

Obrázek 13: Wrong type test

4 Použité odkazy

Popis LDAP: <https://cs.wikipedia.org/wiki/LDAP>

Dekódování: <https://www.oss.com/asn1/resources/asn1-made-simple/asn1-quick-reference/basic-encoding-rules.html>

Syntax LDAP zpráv: <https://ldap.com>