

Instalace OpenLDAP serveru na Ubuntu/Lubuntu

Protokol LDAP (Lightweight Directory Access Protocol) umožňuje dotazování a úpravy adresářové služby založené na X.500. Jinými slovy, LDAP se používá přes místní síť (LAN) ke správě a přístupu k distribuované adresářové službě. Primárním účelem LDAP je poskytovat sadu záznamů v hierarchické struktuře. Co s těmi záznamy můžete dělat? Nejlepším případem použití je ověření uživatele/autentizace na počítačích. Pokud jsou server i klient správně nastaveny, můžete mít všechny své linuxové desktopy ověřené proti vašemu serveru LDAP. Díky tomu je skvělý jediný vstupní bod, takže můžete lépe spravovat (a ovládat) uživatelské účty.

Nejoblíbenější iterací LDAP pro Linux je OpenLDAP. OpenLDAP je bezplatná implementace protokolu Lightweight Directory Access Protocol s otevřeným zdrojovým kódem, která neuvěřitelně usnadňuje uvedení serveru LDAP do provozu.

V textu budou popsány následující kroky:

1. Instalace serveru OpenLDAP.
2. Instalace webového správce účtů LDAP.
3. Konfigurace linuxových desktopů tak, aby mohly komunikovat s LDAP serverem.

Jako první bude provedena instalace a konfigurace OpenLDAP na Serverové/Desktopové variantě Ubuntu.

Update/Upgradovat

První věc, kterou je třeba udělat, je aktualizovat a upgradovat váš server/desktop. Pamatujte, že pokud se jádro aktualizuje, bude nutné server restartovat (pokud nemáte spuštěnou Live Patch nebo podobnou službu). Z tohoto důvodu spusťte aktualizaci/upgrade v době, kdy lze server restartovat.

Aktualizaci a upgrade Ubuntu/Lubuntu spustíme příkazy:

```
sudo apt update  
  
sudo apt upgrade
```

Po dokončení upgradu restartujte server (je-li to nutné) a připravte se na instalaci a konfiguraci OpenLDAP.

1. Instalace OpenLDAP

Protože budeme používat OpenLDAP jako náš serverový software LDAP, lze jej nainstalovat ze standardního úložiště. Chcete-li nainstalovat potřebné součásti, přihlaste se k Ubuntu/Lubuntu a zadejte příkaz:

```
sudo apt install slapd ldap-utils
```

Během instalace budete nejprve požádáni o vytvoření a ověření hesla správce pro adresář LDAP.

Konfigurace LDAP

Po dokončení instalace součástí je třeba nakonfigurovat LDAP. Použijeme k tomu konfigurační nástroj. Z okna terminálu zadejte příkaz:

```
sudo dpkg-reconfigure slapd
```

V prvním okně vyberte No (prvotní konfiguraci a databázi necháme vytvořit) a pokračujte dál. Ve druhém okně konfiguračního nástroje musíte zadat název domény DNS pro váš server. To bude sloužit jako základní DN (bod, odkud bude server vyhledávat uživatele) pro váš adresář LDAP.



V dalším okně zadejte název organizace (tj. název vaší společnosti nebo oddělení). Poté budete vyzváni (ještě jednou) k vytvoření hesla správce (můžete použít stejné heslo, jaké jste použili při instalaci). Poté budou položeny následující otázky:

- Chcete, aby byla databáze odstraněna zároveň s odstraněním slapd? – Vyberte Ne.
- Přesunout starou databázi? – Vyberte možnost Ano.

OpenLDAP je nyní připraven pro data.

Přidání počátečních dat

Po instalaci a spuštění OpenLDAP je třeba naplnit adresář daty. Později nainstalujeme webové grafické uživatelské rozhraní, které zadávání dat značně usnadní, ale vždy je dobré vědět, jak přidávat data ručně.

Jedním z nejlepších způsobů, jak přidat data do adresáře LDAP, je pomocí textového souboru, který lze poté importovat pomocí příkazu `ldapadd`. Nový soubor vytvoříme pomocí příkazu:

```
vi ldap_data.ldif
```

Do tohoto souboru vložte následující obsah:

```
dn: ou=People,dc=EXAMPLE,dc=COM
objectClass: organizationalUnit
ou: People

dn: ou=group,dc=EXAMPLE,dc=COM
objectClass: organizationalUnit
ou: group
```

```
dn: cn=DEPARTMENT,ou=group,dc=EXAMPLE,dc=COM
objectClass: posixGroup
cn: SUBGROUP
gidNumber: 5000
```

```
dn: uid=USER,ou=People,dc=EXAMPLE,dc=COM
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: USER
sn: LASTNAME
givenName: FIRSTNAME
cn: FULLNAME
displayName: DISPLAYNAME
uidNumber: 10000
gidNumber: 5000
userPassword: PASSWORD
gecos: FULLNAME
loginShell: /bin/bash
homeDirectory: USERDIRECTORY
```

Ve výše uvedeném souboru musí být každý záznam ve všech velkých písmenech upraven tak, aby vyhovoval vašim potřebám. Jakmile výše uvedený soubor upravíte, uložte jej a zavřete.

Pro přidání dat ze souboru do adresáře LDAP, zadejte příkaz:

```
ldapadd -x -D cn=admin,dc=EXAMPLE,dc=COM -W -f ldap_data.ldif
```

Nezapomeňte upravit položky dc (EXAMPLE a COM) ve výše uvedeném příkazu tak, aby odpovídaly názvu vaší domény. Po spuštění příkazu budete vyzváni k zadání hesla správce LDAP. Po úspěšném ověření na serveru LDAP budou data přidána. Pro ujištění, že tam data opravdu jsou, spusťte vyhledávání:

```
ldapsearch -x -LLL -b dc=EXAMPLE,dc=COM 'uid=USER' cn gidNumber
```

kde EXAMPLE a COM je název vaší domény a USER je uživatel, kterého chcete vyhledat. Příkaz by měl hlásit položku, kterou jste hledali.

```
jack@hive4:~$ ldapadd -x -D cn=admin,dc=example,dc=com -W -f ldap_data.ldif
Enter LDAP Password:
adding new entry "ou=People,dc=example,dc=com"
adding new entry "ou=Groups,dc=example,dc=com"
adding new entry "cn=Editorial,ou=Groups,dc=example,dc=com"
adding new entry "uid=jack,ou=People,dc=example,dc=com"
jack@hive4:~$ ldapsearch -x -LLL -b dc=example,dc=com 'uid=jack' cn gidNumber
dn: uid=jack,ou=People,dc=example,dc=com
cn: Jack Wallen
gidNumber: 5000
jack@hive4:~$
```

Nyní, když je v adresáři LDAP uložen první záznam, můžete výše uvedený soubor dle potřeby upravit a vytvořit tak ještě více záznamů. Nebo lze počkat na instalaci LDAP Account Manageru a proces vkládání záznamů řešit pomocí webového GUI.

2. Instalace Správce účtů LDAP na server/desktop Ubuntu/Lubuntu

Proces ručního přidávání dat je těžkopádný a není pro každého. Existuje ale velmi solidní webový nástroj, díky kterému je zadávání nových uživatelů hračkou. Tím nástrojem je [správce účtů LDAP \(LAM\)](#).

Vlastnosti LAM:

- Podpora dvoufaktorové autentizace
- Schéma a prohlížeč LDAP
- Podpora více serverů LDAP
- Podpora profilů vytváření účtů
- Kvóty souborového systému
- Nahrání souboru CSV
- Automatické vytváření/mazání domovských adresářů
- PDF výstup pro všechny účty
- A mnohem víc

LAM budeme instalovat na stejný server/desktop, na který jsme nainstalovali OpenLDAP.

Instalace

LAM nachází ve standardním úložišti Ubuntu, takže instalace je jednoduchá zadáním příkazu:

```
sudo apt install ldap-account-manager
```

Po dokončení instalace lze omezit připojení k LAM pouze na místní IP adresy (v případě potřeby), otevřením konkrétního souboru .conf pomocí příkazu:

```
sudo vi /etc/apache2/conf-enabled/ldap-account-manager.conf
```

V tomto souboru vyhledejte řádek:

```
Require all granted
```

Zakomentujte tento řádek (na začátek řádku přidejte znak #) a přidejte pod něj následující položku:

```
Require ip 192.168.1.0/24
```

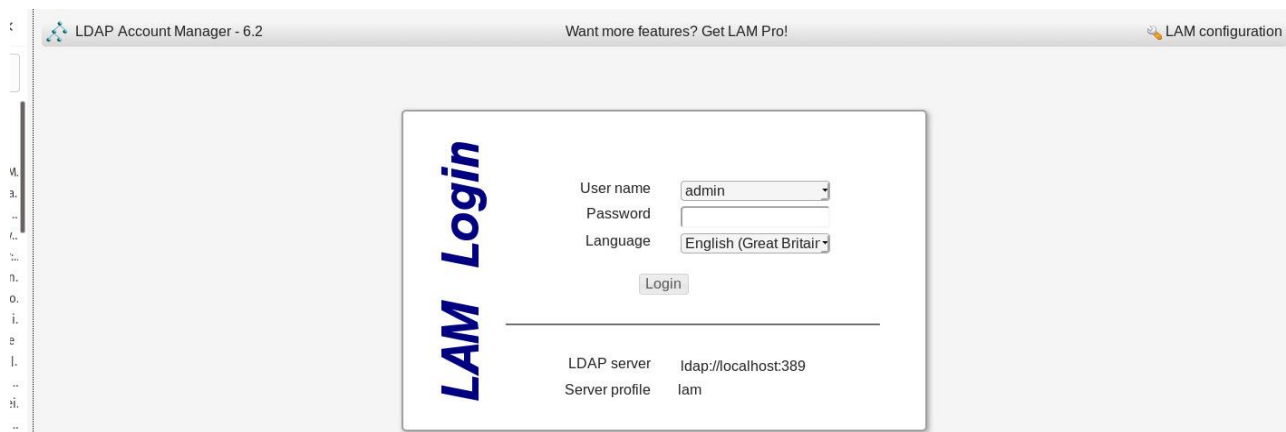
Ujistěte se, že jste nahradili schéma IP adresy vaší sítě místo výše uvedeného (pokud se vaše liší). Uložte a zavřete tento soubor a restartujte webový server Apache příkazem:

```
sudo systemctl restart apache2
```

Nyní je možné přistoupit k webovému rozhraní LAM.

Otevření LAM

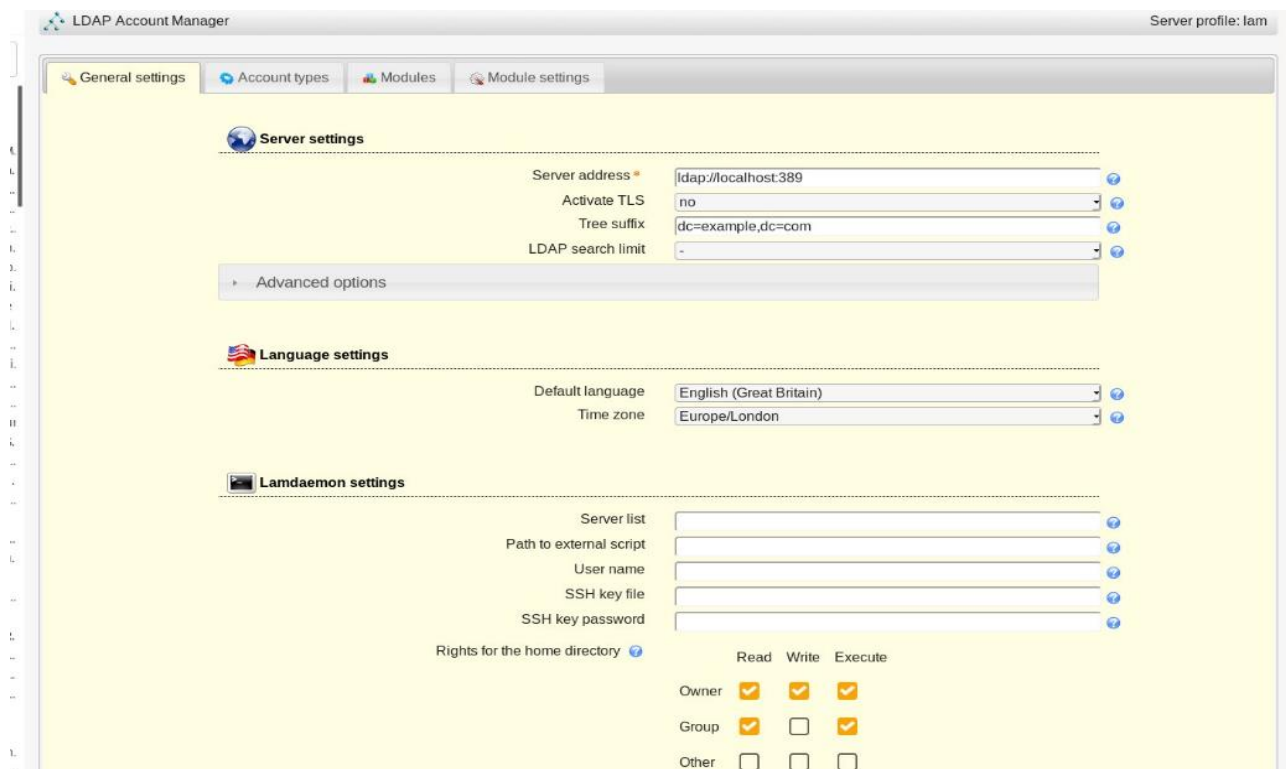
Nasměrujte svůj webový prohlížeč na http://SERVER_IP/lam (kde SERVER_IP je IP adresa serveru hostujícího LAM). Na výsledné obrazovce (obrázek 1) klikněte na Konfigurace LAM v pravém horním rohu okna.



Ve výsledném okně klikněte na Upravit profily serveru.



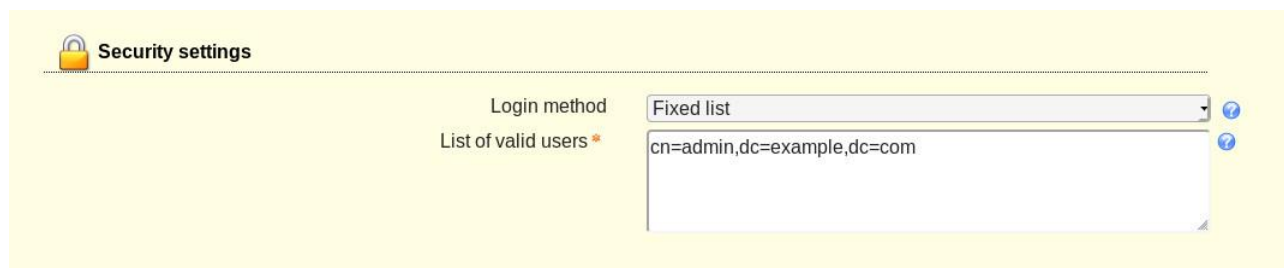
Budete vyzváni k zadání výchozího hesla profilu, zadejte tedy lam a klikněte na OK. Zobrazí se vám stránka nastavení serveru.



V části Nastavení serveru zadejte IP adresu vašeho LDAP serveru. Protože instalujeme LAM na stejný server jako OpenLDAP, ponecháme výchozí. Pokud vaše servery OpenLDAP a LAM nejsou na stejném počítači, ujistěte se, že zde zadáváte správnou IP adresu serveru OpenLDAP. Do položky Tree suffix (v části Tool Settings) přidejte komponenty domény vašeho OpenLDAP serveru ve tvaru dc=example,dc=com.

Dále bude potřeba provést následující konfigurace:

V části Security settings nakonfigurujte seznam platných uživatelů ve tvaru cn=admin,dc=example,dc=com (ujistěte se, že používáte komponenty uživatele a domény správce LDAP).

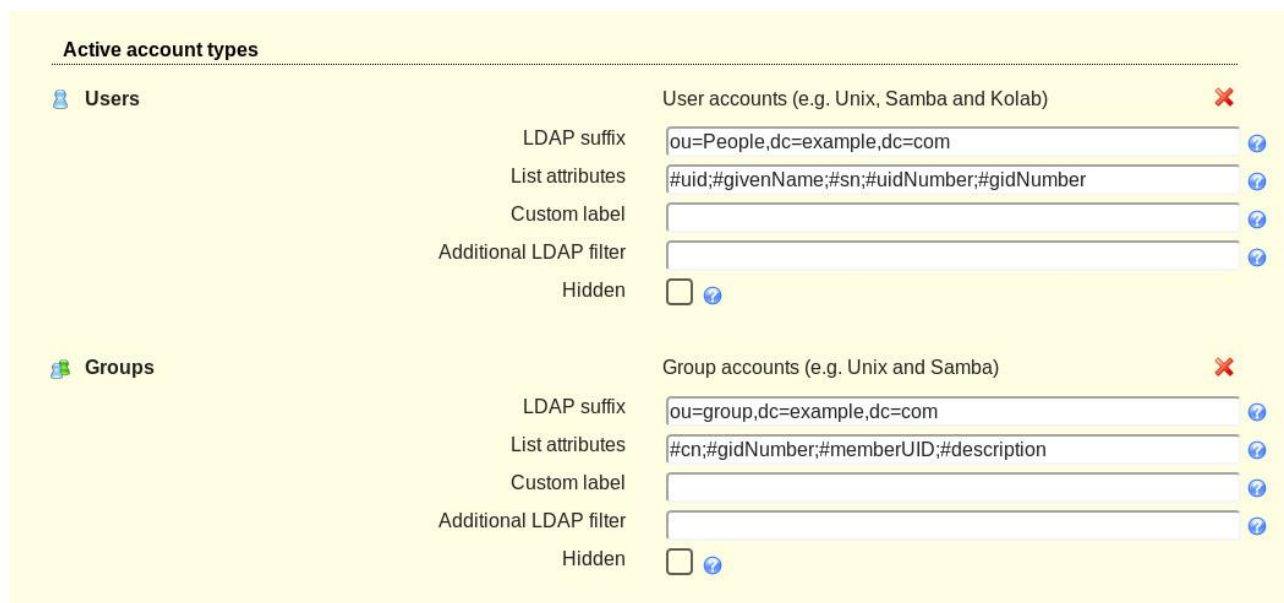


Security settings

Login method: Fixed list

List of valid users: cn=admin,dc=example,dc=com

Na kartě Account types nakonfigurujte možnosti LDAP typů aktivních účtů. Nejprve nakonfigurujte LDAP suffix, který bude ve tvaru ou=group,dc=example,dc=com. Toto je přípona LDAP stromu, odkud budete vyhledávat položky. V seznamu účtů se zobrazí pouze položky v tomto podstromu. Jinými slovy, použijte group attribute, pokud jste na svém OpenLDAP serveru vytvořili skupinu, jejíž členy budou všichni vaši uživatelé (kteří se budou ověřovat podle stromu adresářů LDAP).



Active account types

Users User accounts (e.g. Unix, Samba and Kolab)

LDAP suffix: ou=People,dc=example,dc=com

List attributes: #uid;#givenName;#sn;#uidNumber;#gidNumber

Custom label:

Additional LDAP filter:

Hidden: ☐

Groups Group accounts (e.g. Unix and Samba)

LDAP suffix: ou=group,dc=example,dc=com

List attributes: #cn;#gidNumber;#memberUID;#description

Custom label:

Additional LDAP filter:

Hidden: ☐

Dále nakonfigurujte atributy seznamu. Toto jsou atributy, které se zobrazí v seznamu účtů, a jsou to předdefinované hodnoty, jako je #uid, #givenName, #sn, #uidNumber atd. Vyplňte LDAP sufix a List attributes pro Users i Groups.

Po konfiguraci uživatelů i skupin klikněte na Uložit. Tím se také odhlásíte ze správce profilů serveru a vrátíte se zpět na přihlašovací obrazovku. Nyní se můžete přihlásit do LAM pomocí přihlašovacích údajů správce serveru LDAP. Vyberte uživatele z rozevíracího seznamu Uživatelské jméno, zadejte své heslo správce LDAP a klikněte na Přihlásit. Tím se dostanete na kartu Uživatelé LAM, kde můžete začít přidávat nové uživatele do stromu adresářů LDAP.

LDAP Account Manager - 6.2 (Logged in as: admin) Tree view Tools Help Logout

Users **Groups**

New user Delete selected users File upload

User count: 6

Select all	User name	First name	Last name	UID number	GID number
<input type="checkbox"/>	haversham	Haversham	Happenstance	10003	10000
<input type="checkbox"/>	jack	Jack	Wallen	10000	1011
<input type="checkbox"/>	mina	Mina	Murray	10004	10000
<input type="checkbox"/>	nathan	Nathan	Gage	10002	10000
<input type="checkbox"/>	olivia	Olivia	Nightingale	10001	1011
<input type="checkbox"/>	victor	Victor	Frankenstein	10005	10000

Select all

Klikněte na **New user** a otevře se okno nového uživatele, kde můžete vyplnit potřebná prázdná místa.

Users **Groups**

Save Set password default Load profile

New user Suffix People > example > com RDN identifier cn

Personal
Unix
Shadow

First name

Last name

Initials

Description

Address

Street

Post office box

Postal code

Location

State

Postal address

Registered address


Office name

Room number

Contact data

Telephone number

Home telephone number



Add photo

Nezapomeňte kliknout na **Nastavit heslo**, abyste mohli vytvořit heslo pro nového uživatele (jinak se uživatel nebude moci přihlásit ke svému účtu). Nezapomeňte také kliknout na kartu **Unix**, kde můžete nastavit uživatelské jméno, domovský adresář, primární skupinu, přihlašovací shell a další. Jakmile zadáte potřebné informace o uživateli, klikněte na **Uložit** a uživatelský účet pak najdete ve stromu adresářů LDAP.

Správce účtů LDAP zcela jasně usnadňuje práci s OpenLDAP. Bez použití tohoto nástroje strávíte zadáváním uživatelů do stromu LDAP více času, než byste pravděpodobně chtěli.

V další části bude provedena konfigurace desktopu Linux tak, aby se mohl ověřovat vůči serveru OpenLDAP.

3. Ověření Linux Desktopu vůči OpenLDAP serveru

Konečným cílem použití LDAP (v mnoha případech) je umožnění autentizace desktopových zařízení. S tímto nastavením mohou administrátoři lépe spravovat a ovládat uživatelské účty a přihlášení.

S OpenLDAP můžete spravovat své uživatele na centralizovaném adresářovém serveru a připojit k tomuto serveru ověřování každého linuxového desktopu ve vaší síti.

Instalace

Na všech stolních počítačích, které vyžadují ověření pomocí serveru LDAP, je nutné nainstalovat potřebný klientský software. Otevřete okno terminálu na jednom z desktopů a zadejte následující příkaz:

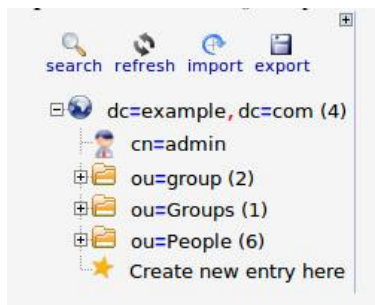
```
sudo apt install libnss-ldap libpam-ldap ldap-utils nscd
```

Během instalace budete požádáni o zadání URI (Uniform Resource Identifier) serveru LDAP.

LDAP URI je adresa OpenLDAP serveru ve tvaru `ldap://SERVER_IP` (kde `SERVER_IP` je IP adresa OpenLDAP serveru).

V dalším okně musíte zadat rozlišovací název (Distinguished name) serveru OpenLDAP. Bude to ve tvaru `dc=example,dc=com`.

Pokud si nejste jisti, jaké je vaše DN OpenLDAP, přihlaste se do Správce účtů LDAP, klikněte na stromové zobrazení a v levém podokně uvidíte DN.



Následujících několik konfiguračních oken bude vyžadovat následující informace:

- Specifikovat verzi LDAP (vyberte 3)
- Vytvořit místní kořenovou admin databázi (vyberte Ano)
- Požadování přihlášení k LDAP databázi (vyberte Ne)
- Zadejte, že postačí účet správce LDAP (bude ve tvaru `cn=admin,dc=example,dc=com`)
- Zadání heslo správce LDAP

Po zodpovězení otázek se instalace dokončí.

Konfigurace klienta LDAP

Každý desktop, který chceme mít zařazení pod správou LDAP, je třeba nakonfigurovat tak, aby se ověřoval vůči serveru OpenLDAP.

Nejprve provedeme konfiguraci souboru `/etc/hosts` tak, aby v něm byly uvedeny IP adresy jako klientského počítače, tak počítače se serverem LDAP.

```
sudo vi /etc/hosts
```


Do souboru vložíme údaje ve tvaru IP_adresa FQDN_název počítače (LDAP server + klient)

```
Klient_IP Klient_FQDN
Server_LDAP_IP Server_LDAP_FQDN
```

FQDN počítače zjistíme např. příkazem

```
hostname -f
```

Uložte a zavřete tento soubor.

Dále si ověříme funkčnost zadaných údajů.

```
ping server_FQDN
```

V dalším kroku nakonfigurujeme nsswitch. Tento konfigurační soubor otevřeme příkazem:

```
sudo vi /etc/nsswitch.conf
```

U položek *passwd*, *group* a *shadow* nahradíme údaj *files* názvem *compat* a přidáme *ldap* na konec řádků:

```
passwd: compat systemd ldap
group: compat systemd ldap
shadow: compat ldap
```

Pokud zde není, tak na konec celé této sekce přidejte řádek:

```
gshadow files
```

Takže celé by to mělo vypadat např. takto:

```
passwd: compat systemd ldap
group: compat systemd ldap
shadow: compat ldap
gshadow files
```

Uložte a zavřete tento soubor.

Dále musíme nakonfigurovat PAM pro ověřování LDAP. Zadejte příkaz:

```
sudo vi /etc/pam.d/common-password
```

Odeberte položku *use_authtok* z následujícího řádku:

```
password [success=1 user_unknown=ignore default=die] pam_ldap.so use_authtok
try_first_pass
```

Uložte a zavřete tento soubor.

Je tu ještě jedna konfigurace PAM, kterou musíme upravit. Zadejte příkaz:

```
sudo vi /etc/pam.d/common-session
```

Na konec tohoto souboru přidejte následující:

```
session optional pam_mkhomedir.so skel=/etc/skel umask=077
```

Výše uvedený řádek vytvoří výchozí domovský adresář (při prvním přihlášení) na ploše Linuxu pro každého uživatele LDAP, který nemá na počítači místní účet.

Uložte a zavřete tento soubor.

Pro aplikování změn potřebujeme restartovat a trvale zapnout službu pracující s nastavenými parametry ldap klienta:

```
sudo systemctl restart nscd
```

```
sudo systemctl enable nscd
```

nscd je démon, který ukládá do mezipaměti dotazy pro různé jmenné služby, včetně passwd, group a hosts.

Testování konfigurace

Než budeme testovat funkčnost konfigurace, musíme na počítači ldap_server povolit na firewallu komunikaci pro službu ldap.

```
sudo ufw allow ldap
```

K otestování správnosti konfigurace použijeme např. příkaz ldapsearch:

```
ldapsearch -x -H ldap://IP_ldap_server -b "dc=example,dc=com"
```

Další možností otestování správnosti konfigurace je přihlášení jako uživatel, který má na ldap serveru založený účet.

```
su - ldap_login
```

Při prvním přihlášení systém oznámí, že vytvořil uživatelský domovský adresář.

Přihlášení

Restartujte klientský počítač. Po zobrazení přihlašovacího jména se pokuste přihlásit pomocí uživatele na vašem serveru OpenLDAP. Uživatelský účet by se měl ověřit proti LDAP serveru a spustit pracovní plochu na přihlašovaném desktopu.

Závěr

Máte spuštěný server OpenLDAP s nainstalovaným správcem účtů LDAP pro snadnou správu účtů. Každý uživatel zapsaný v LDAP adresáři se může přihlásit k libovolnému nakonfigurovanému desktopu Linux v síti.