SYSINT_7.2

Verfasser: **Leonhard Stransky, 4AHIT**

Datum: **10.10.2023**

Einführung

Das Lightweight Directory Access Protocol (LDAP) ist ein Protokoll um ein X.500-basiertes Directory Service verwenden zu können. In Ubuntu gibt es die Implementierung OpenLDAP.

Ziele

Diese Übung ist eine einfache Einführung in die Verwendung von LDAP. Besonderes Augenmerk wird auf LDAP als Authentifizierungsquelle beim Login, sowie Ausfallsicherheit gelegt. Es soll mittels virtuellen Maschinen also ein Directory Service angeboten und ausgetestet werden.

Vorrausetzungen

- Linux Grundlagen
- Grundlegende Kenntnis über Directory Services
- betriebsbereites Linux (bevorzugt Ubuntu LTS Server oder Debian Stable) mit funktionierender Netzwerkverbindung und SSH Zugang (ohne grafische Oberfläche), bevorzugt als virtuelle Maschine (=> Snapshot zu Übungsbeginn nicht vergessen)

Aufgaben:

Installiere und Konfiguriere einen OpenLDAP Server. Du kannst dabei dem Ubuntu Server Guide folgen.

Bei der Installation auf debian/ubuntu wird standardmäßig "nodomain" als Root-Objekt im Verzeichnisdienst angelegt. Mittels dpkg-reconfigure slapd lässt sich der Dienst nach der Installation neu und umfangreicher konfigurieren.

Folgende Schritte sind durchzuführen:

Installation des OpenLDAP Servers (slapd) und weiterer Hilfsmittel (ldap-utils) Konfiguration des OpenLDAP Servers für die Domain "syt.tgm.ac.at" (dpkg-reconfigure slapd) Hinzufügen von Benutzern (mindestens 2, verwende deine persönlichen Daten) Konfiguriere dein System (Client), sodass es LDAP als Authentifizierungsquelle beim Login verwendet (Server Guide: Legitimation; Stichworte: libnss-ldap, libpam-ldap, ldap-auth-config)

Commands:

Konfigurieren des OpenLDAP Servers:

```
sudo apt-get update
sudo apt-get upgrade
sudo apt install slapd ldap-utils
```

```
sudo dpkg-reconfigure slapd
sudo nano /etc/ldap/ldap.conf
```

Bearbeiten von ldap.conf:

ldap.conf:

```
BASE    dc=syt,dc=tgm,dc=ac,dc=at
URI     ldap://ldap01.tgm.ac.at
```

Testen der Änderungen:

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=config dn
sudo ldapsearch -x -LLL -H ldap:/// -b dc=syt,dc=tgm,dc=ac,dc=at dn
# Output: dn: dc=syt,dc=tgm,dc=ac,dc=at
sudo ldapwhoami -x
# Output: cannot contact LDAP server
```

DNS ldap01.tgm.ac.at existiert nicht, daher wird die IP-Adresse verwendet:

ldap.conf:

```
BASE    dc=syt,dc=tgm,dc=ac,dc=at
URI     ldap://localhost ldap://127.0.0.1
```

Checken ob es funktioniert:

```
sudo ldapwhoami -x
# Output: anonymous
sudo ldapwhoami -x -D cn=admin,dc=syt,dc=tgm,dc=ac,dc=at -W
# Output: dn:cn=admin,dc=syt,dc=tgm,dc=ac,dc=at
sudo ldapsearch -x -H ldap://127.0.0.1
# Output: ...
cd /etc/ldap
sudo nano add_content.ldif
```

Erstellen der .ldif Datei:

add_content.ldif:

```
dn: ou=People,dc=syt,dc=tgm,dc=ac,dc=at
objectClass: organizationalUnit
ou: People
```

```
dn: uid=leo,ou=People,dc=syt,dc=tgm,dc=ac,dc=at
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: leo
sn: Stransky
givenName: Leo
cn: Leo Stransky
displayName: Leo Stransky
uidNumber: 10001
gidNumber: 5001
userPassword: {CRYPT}x
gecos: Leo Stransky
loginShell: /bin/bash
homeDirectory: /home/leo

dn: uid=julian,ou=People,dc=syt,dc=tgm,dc=ac,dc=at
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: julian
sn: Neuwirth
givenName: Julian
cn: Julian Neuwirth
displayName: Julian Neuwirth
uidNumber: 10002
gidNumber: 5002
userPassword: {CRYPT}x
gecos: Julian Neuwirth
loginShell: /bin/bash
homeDirectory: /home/julian
```

`modify_content.ldif`:

```
dn: uid=leo,ou=People,dc=syt,dc=tgm,dc=ac,dc=at
changetype: add
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: leo
sn: Stransky
givenName: Leo
cn: Leo Stransky
displayName: Leo Stransky
uidNumber: 10001
gidNumber: 5001
userPassword: {CRYPT}x
gecos: Leo Stransky
loginShell: /bin/bash
homeDirectory: /home/leo
```

```
dn: uid=julian,ou=People,dc=syt,dc=tgm,dc=ac,dc=at
changetype: add
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: julian
sn: Neuwirth
givenName: Julian
cn: Julian Neuwirth
displayName: Julian Neuwirth
uidNumber: 10002
gidNumber: 5002
userPassword: {CRYPT}x
gecos: Julian Neuwirth
loginShell: /bin/bash
homeDirectory: /home/julian
```

Hinzuügen der Benutzer u. passwort ändern:

```
ldapadd -x -D cn=admin,dc=syt,dc=tgm,dc=ac,dc=at -W -f add_content.ldif
ldapmodify -x -D cn=admin,dc=syt,dc=tgm,dc=ac,dc=at -W -f modify_content.ldif
# Output:
# adding new entry "uid=leo,ou=People,dc=syt,dc=tgm,dc=ac,dc=at"
# adding new entry "uid=julian,ou=People,dc=syt,dc=tgm,dc=ac,dc=at"
ldapsearch -x -LLL -H ldap://localhost -b "dc=syt,dc=tgm,dc=ac,dc=at" # "
(uid=Name)"
ldappasswd -x -D cn=admin,dc=syt,dc=tgm,dc=ac,dc=at -W -S
uid=leo,ou=people,dc=syt,dc=tgm,dc=ac,dc=at
```

Aktivieren der Authentifizierung:

```
sudo apt install libnss-ldap libpam-ldap ldap-auth-config
sudo dpkg-reconfigure ldap-auth-config
sudo nano /etc/nsswitch.conf
```

`nsswitch.conf`:

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

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

```
hosts:          files dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

Services neustarten:

```
sudo systemctl restart systemd-resolved
sudo systemctl restart nscd
```

Testen der Authentifizierung:

```
getent passwd
```

```
su - leo
# su: user leo does not exist or the user entry does not contain all the required
fields
```

Aufgaben (EK):

Lege zusätzlich eine Gruppe für die Benutzer im LDAP an. Erstelle einen zweiten OpenLDAP Server und repliziere die Daten automatisch zwischen den beiden Servern.

Quellen:

[1] releases.ubuntu.com 2023. [online] Available at: https://releases.ubuntu.com/22.04.3/ubuntu-22.04.3-live-server-amd64.iso [Accessed 12 Oktober 2023].

[2] ubuntu.com 2023. [online] Available at: https://ubuntu.com/server/docs/service-ldap [Accessed 12 Oktober 2023].