LDAP

Grzegorz Bandur
Jakub Stasiński

Historia

W 1980 roku Międzynarodowy Związek Telekomunikacyjny (ITU) w 1980 rok stowrzył specyfikacje X500.

Usługi katalogowania X.500 używały X.500 Directory Access Protocol (DAP), wymagała ona protokołów Open Systems Interconnection (OSI).

LDAP był początkowo lekkim protokołem alternatywnym korzystającym z TCP/IP. Został nazwany lekkim z powodu mniejszych wymagań sieciowych niż jego poprzednicy(DAP).

Wstęp

LDAP to skrót od terminu „Lighweight Directory Access Protocol”, czyli „Lekki Protokół Dostępu do Usług Katalogowych”.

LDAP można potraktować jak zwykłą bazę danych: Są w niej rekordy, w rekordach są pola z danymi, można dopisywać i kasować rekordy oraz wyszukiwać rekordy spełniające podane kryteria. Są jednak spore róznice miedzy zwykłą bazą a LDAPem:

- baza LDAP jest heterogeniczna
- baza LDAP jest hierarchiczna (drzewiasta)

O protokole

Klient łączy się z serwem LDAP Directory System Agend (DSA).

Klient może wykonać następujące operacje:

- *StartTLS*
- *bind*
- *unbind*
- *search*
- *modify*
- *add*
- *delete.*
- *Compare*
- *Abandon*
- *Extended Operation*

Dodatkowo serwer moze zwracać notyfikacje nie bedace odpowiedziami na żądania.

OpenLDAP

OpenLDAP to, należąca do Wolnego Oprogramowania, implementacja protokołu LDAP (wersji 2 i 3). Zawiera serwer usług katalogowych, biblioteki oraz klientów do komunikacji z serwerem. Oprogramowanie przeznaczone jest na Linuksa oraz systemy uniksopodobne, można też używać na Microsoft Windows (2000, XP).
Rozwijany jest przez **OpenLDAP Project** (projekt założony w 1998 roku przez Kurt D. Zeilenga), OpenLDAP wywodzi się z U-M LDAP rozwijanego na początku przez Uniwersytet Michigan.

AD a LDAP

Active Directory jest usługą katalogową (hierarchiczna baza danych) dla systemów Windows.
Zapewnia mozliwość uwierzytelniania, autoryzacji obiektów (np. użytkowników, komputerów), którzy mają prawo lub nie dostępu do innych obiektów *Active Directory* (dowolnych, np. kontenera lub obiektu użytkownika) oraz do zasobów innych, w tym dyskowych, sieciowych itd.

LDAP (Lightweight Directory Access Protocol) jest protokołem używaym przez usługi takie jak AD do komunikacji. LDAP jest znacznie starszy od Active Directory i nie jest rozwiązaniem należącym jakiejkolwiek firmy. Ogromna część Active Directory pochodzi z LDAP.

Adresowanie rekordów

LDAP do wskazania rekordów wykorzystuje ścieżkę do rekordu(distinguished name, DN). W obrębie jednego poziomu hierarchii (jednego rekordu nadrzędnego) stosowany jest skrót, nazwa rekordu (relative distinguished name, RDN).

Przykładowy adres LDAP to np:

„cn=Jarek,ou=People,dc=asl,dc=com”

Adresowanie rekordów

„cn=Jarek,ou=People,dc=asl,dc=com”

Podana nazwa składa się z 4 części, czytanych od prawej do lewej i oddzielonych przecinkami. Każda część ma postać typ=nazwa. Typ określa charakter danej opisanej nazwą:

- cn – nazwa rekordu (od common name) – to jest najbliższe kluczowi głównemu.
- dc – fragment adresu DNS podmiotu opisanego DN, czyli asl.coml staje się dc=asl, dc=com (od directory context)

Możliwe są jeszcze:

- o – nazwa (od organization)
- ou – oddział (od organizational unit)
- c – kraj (od country)
- l – miasto (od locality)

Adresowanie rekordów

Ostatnia część DN, wspólna dla wszystkich rekordów w bazie LDAP to tzw adres bazowy (base distingushed name). Może być konstruowany na kilka sposobów:

- od adresu DNS firmy: dc=asl,dc=com (forma preferowana) bądź o=asl.com (forma przestarzała)
- od nazwy: o=Super asl,c=pl

Przykład

Rozwiązanie z przykładem faktuy VAT.

LDAP

- jest drzewo ogólnych danych firmy dc=Firma,dc=pl
- jest tam poddrzewo ‚faktury' ou=faktury,dc=Firma,dc=pl
- każda faktura jest rekordem zawierającym dane faktury – datę, numer, dane kontrahenta, itd. cn=FV01/13,ou=faktury,dc=Firma,dc=pl
- szczegóły faktury są podrekordami danej faktury: zawierają towar, ilość, cenę, podatek cn=1,cn=FV01/13,ou=faktury,dc=Firma,dc=pl

Instalacja

Instalujemy:
apt-get install slapd
Konfiguracja:
dpkg-reconfigure -plow slapd

Omit OpenLDAP server configuration? **No**
DNS domain name: ***asl.com***
Organization name? ***asl.com***
Administrator password: ***password***
Confirm password: ***password***
Database backend to use: **HDB**
Do you want the database to be removed when slapd is purged? **yes**
Move old database:**yes, wazne jesli istnieje juz backup całość sie nie powiedzie**
Allow LDAPv2 protocol? **No - już przestarzałe**

Instalacja

Ldap-utils zawiera szereg narzędzi, które mogą być używane do wykonywania zapytań na serwerze LDAP.

apt-get install ldap-utils

Podstawowe komendy:

ldapsearch - wyszukiwanie i wyświetlanie wpisów

manipulować wpisy

ldapmodify - zmodyfikować wpis

ldapadd - dodać nowy wpis

ldapdelete - usuń i wejście

ldapmodrdn - zmień wpis

ldappasswd - zmienić hasło do wejścia * Uwaga: To nie jest zamiennikiem dla passwd

Inne operacje

ldapwhoami: wyświetlacz z którym wpis jestem związany z serwerem

ldapcompare porównanie pola w wejściu do pewnej wartości

Instalacja

Modyfikacja " /etc/ldap/ldap.conf"
"

ldap_version 3
URI ldap://localhost:389
SIZELIMIT 0
TIMELIMIT 0
DEREF never
BASE dc=asl, dc=com

"

Przykład search:

ldapsearch -b'dc=asl,dc=com’ -x

Dodanie organizationalUnit

W pliku /var/tmp/ou.ldif :

"

dn: ou=People,dc=asl,dc=com
ou: People
objectClass: organizationalUnit

dn: ou=Group,dc=asl,dc=com
ou: Group
objectClass: organizationalUnit

"

```
invoke-rc.d slapd stop
slapadd -c -v -l /var/tmp/ou.ldif
invoke-rc.d slapd start
```

ldapsearch -b'ou=people,dc=asl,dc=com' -x

Tworzenie użytkownika

tworzymy plik: /var/tmp/user1.ldif plik

Wgrywamy do bazy poleceniem:

```
ldapadd -c -x -D cn=admin,dc=asl,dc=com -W -f /var/tmp/user1.ldif
```

Wybieramy Hasło dla Jarka

```
ldappasswd -x -D cn=admin,dc=asl,dc=com -W -S uid=Jarek,ou=people,
dc=asl,dc=com
```

Szukanie nowo utworzonego użytkownika

```
ldapsearch -b'dc=grzegorz,dc=jakub' -x 'uid=jarek'
```

Konfiguracja NSS

Gdy mamy utworzonego użytkownika w LDAP, powinniśmy pozwolić, aby system go zobaczył. Na przykład, załóżmy przetestujmy czy istnieje Jarek.

```
id root
uid=0(root) gid=0(root) groups=0(root)

id Jarek
id: Jarek: No such user
```

Konfiguracja NSS

Aby system zobaczył konta LDAP, należy zainstalować i skonfigurować libnss-ldap.

```
apt-get install libnss-ldap nscd
```

Odpowiedzi na debconf

LDAP server Uniform Resource Identifier: **ldap://*localhost*/** (Note the "ldap://", NOT "ldapi://"!)
Distinguished name of the search base: ***dc=asl,dc=com***
LDAP version to use: **3**
Does the LDAP database require login? **No**
Special LDAP privileges for root? **No**
Make the configuration file readable/writeable by its owner only? **No**
Make local root Database admin. **No**
Does the LDAP database require login? **No**
Local crypt to use when changing passwords. **crypt**

Konfiguracja NSS

W pliku :/etc/libnss-ldap.conf.

base dc=asl,dc=com
uri ldap:///*localhost/*

Oraz w /etc/nsswitch.conf podmieniamy na:

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

hosts:          files dns ldap
networks:       files ldap
```

Zatrzymaj nscd, demona buforowania Name Service, ale zostaw uruchamianie przy następnym starcie systemu:

sudo invoke-rc.d nscd stop

W końcu Jarek jest widoczny:

id jarek

uid=10000(jarek) gid=20000(students) groups=20000(students)

Dziękujemy za uwagę