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 pączątkowo 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:

Otóż klasyczne bazy danych (Relational Database, RDB) mają dwie podstawowe cechy:

- baza jest homogeniczna, czyli wszystkie rekordy mają tą samą strukturę (kolejność, nazwy i typy pól)
- baza jest płaska czyli można ją zapisać rekord za rekordem jako tablicę – wszystkie rekordy są równorzędne i w podejściu klasycznym nieuporządkowane.

- baza LDAP jest heterogeniczna, czyli każdy rekord może mieć inną strukturę – co więcej, budowa rekordu może się zmieniać w czasie
- baza LDAP jest hierarchiczna (drzewiasta), czyli jedne rekordy mogą być rekordami podrzędnymi dla innych. Dodatkowo zamiast rekodu można umieścić odnośnik do zupełnie innego miejsca w drzewie.

O protokole

Client startuje sesje z LDAPem łączą się z servem LDAP Directory System Agent (DSA), bazowo na porcie TCP port 389. Zwykle klient nie musi czekać na odpowiedzi miedzy kolejnymi żądaniami do serwera, a serwer moze zwracac wyniki w dowolnej kolejnosci.

Wszystkie informacje są transmitowane użwyając BER(Basic Encoding Rules).

Klient może wykonać następujące operacje:

- StartTLS —Używać LDAPv3 Transport LAyer Security (TLS) dla bezpiecznego połączenia.
- *bind* – uwierzytelnienie użytkownika, czyli powiązanie jego tożsamości (i obiektu LDAP) z połączeniem sieciowym i sesją. Wymaga potwierdzenia odbioru od serwera, w którym znajduje status żądania klienta. Operacja ta może też przestawić sesję w stan „anonimowy" jeśli podany zostanie pusty *DN* i hasło. W ramach jednej sesji można wielokrotnie dokonywać operacji *bind*, zmieniając w ten sposób kontekst uwierzytelniania.
- *unbind* – zakończenie sesji i połączenia sieciowego LDAP. Nie potrzebuje potwierdzenia. Nie jest (wbrew popularnemu przekonaniu) odwrotnością operacji *bind*.
- *search* – zgłoszenie żądania poszukiwanego zasobu, które będzie realizowane przez serwer, co pozwala na pobieranie oraz wyszukiwanie informacji
- *modify* – umożliwia klientowi modyfikowanie, wprowadzanie nowych pozycji oraz ich usuwanie z bazy danych znajdującej się na serwerze
- *add* – daje klientowi możliwość zgłoszenia żądania dodania wpisów do katalogu, zmiany istniejącego wpisu oraz zmiany nazwy wpisu.
- *delete* – umożliwia klientowi żądanie usunięcia wpisów z katalogu.
- Compare — testuje czy wpis o podanej nazwie posiada atrybut o danej wartości
- Abandon — abortowanie poprzedniego żądania
- Extended Operation — operacja służąca do definiowanie innych operacji
-

Dodatkowo serwer moze zwracać notyfikacje nie bedace odpowiedziami na żądania.

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

W LDAP tak jak w klasycznych bazach można zasymulować klucz główny: Można zrobić pole rekordu z unikalnym numerem i według niego szukać.

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).
Bardziej obrazowo: LDAP zachowuje się jak dysk: rekordy to pliki, DN to absolutna ścieżka do pliku a RDN to względna ścieżka do pliku. Adresy rekordów LDAP są dłuższe od kluczy RDB, jednak sa bardziej obrazowe: „cn=Jarek,ou=People,dc=asl,dc=com”

Podana zazwa składa się tutaj 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 firma.pl staje się dc=asl,dc=com (od directory context)
- o – nazwa firmy (od organization)
- ou – oddział firmy (od organizational unit)
- c – kraj (od country)
- l – miasto (od locality)

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=com

Przykład

Rozwiązanie z przykładem faktuy VAT.

- 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**

Instalujemy ldap-utils:

apt-get install ldap-utils

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

Podstawowe komendy:

ldapsearch - wyszukiwanie i wyświetlanie wpisów

ldapmodify - zmodyfikować wpis

ldapadd - dodać nowy wpis

ldapdelete - usuń wpis

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-cd

Dodać następujące linie do " /etc/ldap/ldap.conf"

tworząc plik jesli nie istnieje:

"

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

"

Jeśli chcemy postawić LDAP nie na localhost, wpisujemy inny adres należy wtedy również skonfigurować dnsa.

Sprawdzenie czy działa:
Przykład search:
ldapsearch -b'dc=asl,dc=com' -x powinieśmy dostać zwrot w stylu:

```
# extended LDIF
#
# LDAPv3
# base <dc=asl,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# asl.com
dn: dc=asl,dc=com
objectClass: top
objectClass: dcObject
```

objectClass: organization
o: asl.com
dc: asl

admin, asl.com
dn: cn=admin,dc=asl,dc=com
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

search result
search: 2
result: 0 Success

numResponses: 3
numEntries: 2

w przypadku błednego działania warto spróbowac:
Restart ldapa:
/etc/init.d/slapd restar lub
Stopuje serwer ldapa:
/etc/init.d/slapd stop
Startuje serwer ldapa:
/etc/init.d/slapd star

Tworzymy organization unit:

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.ld
invoke-rc.d slapd star

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

Pierwszy użytkownik

/var/tmp/user1.ldif plik:

dn: cn=students,ou=group,dc=asl,dc=com
cn: students
gidNumber: 20000
objectClass: top
objectClass: posixGroup

dn: uid=Jarek,ou=people,dc=asl,dc=com
uid:Jarek
uidNumber: 10000
gidNumber: 20000
cn: Jarek
sn: Jarek
objectClass: top
objectClass: person
objectClass: posixAccount
objectClass: shadowAccount
loginShell: /bin/bash
homeDirectory: /home/Jarek

dn: uid=Zbyszek,ou=people,dc=asl,dc=com
uid:Zbyszek
uidNumber: 10001
gidNumber: 20000
cn: Zbyszek
sn: Zbyszek
objectClass: top
objectClass: person
objectClass: posixAccount
objectClass: shadowAccount
loginShell: /bin/bash
homeDirectory: /home/Zbyszek
"

Wgrywamy do bazy poleceniem:

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

Wybieramy Hasło dla Jarka

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

Sprawdzenie, czy jest z nami Jarek?

```
ldapsearch -b'dc=asl,dc=com' -x 'uid=Jarek
```

tak samo zbyszek.

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

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

```
apt-get install libnss-ldap nsc
```

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**

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:

```
invoke-rc.d nscd stop
```

W końcu Jarek jest widoczny:

id jarek

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