

Bài 17. Xác thực mạng

1. OpenLDAP Server

Thư mục (directory) là một dạng CSDL lưu trữ các thông tin theo cấu trúc cây, được gọi là Cây thông tin thư mục (Directory Information Tree - DIT). Trong tài liệu này, thuật ngữ CSDL được sử dụng để chỉ DIT.

LDAP (Lightweight Directory Access Protocol) là một giao thức cho việc truy vấn và sửa đổi DIT dựa vào X.500 chạy trên TCP/IP. Phiên bản LDAP hiện tại là LDAPv3 được định nghĩa trong RFC4510, và được cài đặt trong Ubuntu với tên gọi OpenLDAP.

ĐIPT phù hợp để lưu trữ các mục dữ liệu ngắn, có quan hệ với nhau theo cấu trúc cây, không thường xuyên thay đổi. Sử dụng LDAP và DIT để đạt hiệu năng (tốc độ truy vấn và cập nhật) cao.

Tài liệu này hướng dẫn sử dụng DIT để làm CSDL người dùng và sử dụng LDAP để xác thực người dùng, OpenLDAP làm AAA server (server cung cấp dịch vụ xác thực, phân quyền và kiểm toán – Authentication, Authorization, Accounting).

Các thuật ngữ và khái niệm chính:

- Một mục dữ liệu trong DIT bao gồm một tập các thuộc tính.
- Một thuộc tính bao gồm một kiểu (tên/miêu tả) và một hay nhiều giá trị.
- Mỗi thuộc tính phải được định nghĩa trong ít nhất một objectClass.
- Thuộc tính và objectclass được định nghĩa trong các lược đồ (schemas). Objectclass được xem là một loại thuộc tính đặc biệt.
- Mỗi mục phải có một định danh duy nhất: Distinguished Name (DN hay dn). DN bao gồm một Relative Distinguished Name (RDN) theo sau là DN của mục cha. DN không phải là thuộc tính và cũng không được xem là bộ phận của mục.
- Các thuật ngữ object, container, và node đều có nghĩa là mục (entry).

Ví dụ sau là một mục với 11 thuộc tính:

```
dn: cn=John Doe,dc=example,dc=com
cn: John Doe
givenName: John
sn: Doe
telephoneNumber: +1 888 555 6789
telephoneNumber: +1 888 555 1232
mail: john@example.com
manager: cn=Larry Smith,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

Mục dữ liệu trên theo định dạng LDIF (LDAP Data Interchange Format). Bất kỳ thông tin gì cần đưa vào DIT cũng phải có định dạng như trên. Nó được định nghĩa trong RFC2849.

1.1. Cài đặt

Cài đặt OpenLDAP server daemon và các tiện ích quản lý LDAP bằng các gói slapd và ldap-utils tương ứng. Cài đặt slapd sẽ tạo cấu hình làm việc, Cụ thể, nó sẽ tạo một thể hiện CSDL để lưu trữ dữ liệu. Tuy nhiên, hậu tố (hay là DN cơ sở) của thể hiện CSDL này sẽ được xác định từ tên miền của localhost. Hướng dẫn này sẽ sử dụng hậu tố dc=example,dc=com.

Chỉnh sửa tệp /etc/hosts, thay tên miền bằng dòng sau đây.

```
127.0.1.1 hostname.example.com hostname
```

Từ Terminal, chạy lệnh sau để cài đặt:

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

Trong quá trình cài đặt, bạn được yêu cầu nhập thông tin xác thực cho rootDN. dn của rootDN là “cn=admin,dc=example,dc=com”.

Một số lược đồ như core, cosine, nis, inetorgperson được dựng sẵn với slapd.

1.2. Kiểm tra kết quả cài đặt

Quá trình cài đặt tạo 2 DITs, một cho slapd-config và một cho dữ liệu của người dùng (dc=example,dc=com). DIT cho slapd-config nằm trong thư mục /etc/ldap/slapd.d.

Để cập nhật trực tiếp CSDL này mà không cần khởi động slapd.

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldap:/// -b cn=config dn
```

Kết quả tìm sẽ có dạng

```
dn: cn=config
dn: cn=module{0},cn=config
dn: cn=schema,cn=config
dn: cn={0}core,cn=schema,cn=config
dn: cn={1}cosine,cn=schema,cn=config
dn: cn={2}nis,cn=schema,cn=config
dn: cn={3}inetorgperson,cn=schema,cn=config
dn: olcBackend={0}hdb,cn=config
```

```
dn: olcDatabase={-1}frontend,cn=config
dn: olcDatabase={0}config,cn=config
dn: olcDatabase={1}hdb,cn=config
```

DIT thứ hai có dạng như sau

```
ldapsearch -x -LLL -H ldap:/// -b dc=example,dc=com dn
dn: dc=example,dc=com
dn: cn=admin,dc=example,dc=com
trong đó,
dc=example,dc=com: cơ sở của DIT
cn=admin,dc=example,dc=com: administrator (rootDN) của DIT
```

1.3. Cập nhật/tìm kiếm CSDL LDAP

CSDL sẽ thêm bao gồm:

- Một nút People (để lưu trữ người dùng)
- Một nút Groups (để lưu trữ nhóm)
- Một nhóm tên là miners
- Một người dùng tên là john

Tạo tệp LDIF add_content.ldif với nội dung như sau:

```
dn: ou=People,dc=example,dc=com
objectClass: organizationalUnit
ou: People

dn: ou=Groups,dc=example,dc=com
objectClass: organizationalUnit
ou: Groups

dn: cn=miners,ou=Groups,dc=example,dc=com
objectClass: posixGroup
cn: miners
gidNumber: 5000

dn: uid=john,ou=People,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: john
sn: Doe
givenName: John
cn: John Doe
displayName: John Doe
uidNumber: 10000
gidNumber: 5000
userPassword: johnldap
gecos: John Doe
loginShell: /bin/bash
homeDirectory: /home/john
```

Lưu ý không sử dụng khoảng giá trị lớn, ví dụ từ 5000 trở lên, để tránh đụng độ giữa các giá trị của uid và gid đụng độ với các giá trị cục bộ.

Chạy lệnh ldapadd để thêm dữ liệu LDAP đã được chuẩn bị trong tệp add_content.ldif

```
ldapadd -x -D cn=admin,dc=example,dc=com -W -f add_content.ldif
```

Enter LDAP Password: *****

Có thể kiểm tra lại dữ liệu đã được thêm đúng bằng lệnh ldapsearch:

```
ldapsearch -x -LLL -b dc=example,dc=com 'uid=john' cn gidNumber
```

trong đó, các tham số có ý nghĩa như sau

- x: binding đơn giản
- LLL: không in thông tin mở rộng
- 'uid=john': điều kiện tìm kiếm

cn gidNumber: các trường thông tin được hiển thị trong kết quả.

1.4. Cập nhật CSDL cấu hình slapd

Cũng có thể truy vấn và cập nhật CSDL slapd-config DIT để đọc và thay đổi các lược đồ. Phần này dành cho tự học và nâng cao.

1.5. Ghi nhật ký

Ghi nhật ký là chức năng hết sức cần thiết đối với giải pháp LDAP. OpenLDAP có nhiều hệ thống con để ghi nhật ký, các hệ thống con lồng nhau và hệ thống trong ghi nhật ký chi tiết cho hệ thống ngoài.

Tạo tệp logging.ldif với nội dung như sau:

```
dn: cn=config
changetype: modify
replace: olcLogLevel
olcLogLevel: stats
```

Thay đổi cấu hình log:

```
sudo ldapmodify -Q -Y EXTERNAL -H ldapi:/// -f logging.ldif
```

Kiểu log vừa thiết lập ghi rất chi tiết nhật ký, có thể dẫn nhiều thông báo với tần suất cao. Để mô tơ rsyslog không loại bỏ một số thông báo khi tần suất thông báo vượt quá giới hạn cho phép, hãy thay đổi cấu hình rsyslog. Trong tệp/etc/rsyslog.conf, đặt:

```
# Disable rate limiting
# (default is 200 messages in 5 seconds; below we make the 5 become 0)
$SystemLogRateLimitInterval    0
```

Và khởi động lại hệ rsyslog:

```
sudo systemctl restart syslog.service
```

1.6. Nhân bản

Dịch vụ LDAP trở nên hết sức quan trọng khi nhiều hệ thống mạng sử dụng nó. Do vậy, nhân bản cho LDAP là điều cần thiết.

Nhân bản LDAP được thực hiện bởi chương trình Syncrepl. Việc nhân bản và đồng bộ hóa được thực hiện theo mô hình Consumer - Provider.

Cấu hình Provider

Để OpenLDAP server đóng vai trò Provider, thực hiện các bước cấu hình sau.

Tạo tệp provider_sync.ldif có nội dung như sau:

```
# Add indexes to the frontend db.
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: entryCSN eq
-
add: olcDbIndex
olcDbIndex: entryUUID eq

#Load the syncprov and accesslog modules.
dn: cn=module{0},cn=config
changetype: modify
add: olcModuleLoad
olcModuleLoad: syncprov
-
add: olcModuleLoad
olcModuleLoad: accesslog

# Accesslog database definitions
dn: olcDatabase={2}hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {2}hdb
olcDbDirectory: /var/lib/ldap/accesslog
olcSuffix: cn=accesslog
olcRootDN: cn=admin,dc=example,dc=com
olcDbIndex: default eq
olcDbIndex: entryCSN,objectClass,reqEnd,reqResult,reqStart

# Accesslog db syncprov.
dn: olcOverlay=syncprov,olcDatabase={2}hdb,cn=config
```

```

changetype: add
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
olcSpNoPresent: TRUE
olcSpReloadHint: TRUE

# syncrepl Provider for primary db
dn: olcOverlay=syncprov,olcDatabase={1}hdb,cn=config
changetype: add
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
olcSpNoPresent: TRUE

# accesslog overlay definitions for primary db
dn: olcOverlay=accesslog,olcDatabase={1}hdb,cn=config
objectClass: olcOverlayConfig
objectClass: olcAccessLogConfig
olcOverlay: accesslog
olcAccessLogDB: cn=accesslog
olcAccessLogOps: writes
olcAccessLogSuccess: TRUE
# scan the accesslog DB every day, and purge entries older than 7 days
olcAccessLogPurge: 07+00:00 01+00:00

```

Tạo một thư mục, thiết lập tệp cấu hình, và tải lại hồ sơ apparmor:

```

sudo -u openldap mkdir /var/lib/ldap/accesslog
sudo -u openldap cp /var/lib/ldap/DB_CONFIG /var/lib/ldap/accesslog
sudo systemctl reload apparmor.service

```

Thêm nội dung mới và khởi động lại daemon:

```

sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f provider_sync.ldif
sudo systemctl restart slapd.service

```

Cấu hình Consumer

Trên máy tính khác (máy nhân bản), cài đặt OpenLDAP server, cấu hình sldap-config DIT giống như Provider. Cụ thể, cần cấu hình các lược đồ và hậu tố giống với sldap-config DIT của Provider.

Tạo tệp consumer_sync.ldif có nội dung như sau:

```

dn: cn=module{0},cn=config
changetype: modify
add: olcModuleLoad
olcModuleLoad: syncprov

dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: entryUUID eq
-
add: olcSyncRepl
olcSyncRepl: rid=0 provider=ldap://ldap01.example.com bindmethod=simple binddn="cn=admin,dc=example,dc=com"
credentials=secret searchbase="dc=example,dc=com" logbase="cn=accesslog"
logfilter="(&(objectClass=auditWriteObject)(reqResult=0))" schemachecking=on
type=refreshAndPersist retry="60 +" syncdata=accesslog
-
add: olcUpdateRef
olcUpdateRef: ldap://ldap01.example.com

```

Cần đảm bảo các thuộc tính sau đây nhận giá trị đúng:

- provider (tên miền hay địa chỉ IP của Provider server -- ldap01.example.com trong ví dụ này)
- binddn (DN của admin)
- credentials (mật khẩu của admin)

- searchbase (hậu tố của CSDL)
- olcUpdateRef (tên miền hoặc địa chỉ IP của Provider server)
- rid (Replica ID, 3 chữ số duy nhất định danh Consumer)

Chạy lệnh sau để thêm nội dung:

```
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f consumer_sync.ldif
```

Kiểm thử

Chạy cùng truy vấn trên cả Provider và Consumer để thấy kết quả trả về là như nhau.

```
ldapsearch -z1 -LLLQY EXTERNAL -H ldapi:/// -s base -b dc=example,dc=com contextCSN
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b dc=example,dc=com dn
```

Nếu kết quả trả trên Consumer khác trên Provider thì cần xem lại cấu hình Comsumer.

1.7. Điều khiển truy cập

Điều khiển truy cập LDAP được thực hiện bằng ACL. Khi cài đặt slapd, nhiều ACL sẽ được cài đặt mặc định.

Các lệnh sau đây cho biết ACLs của CSDL pdb ("dc=example,dc=com") và CSDL frontend.

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b \
cn=config '(olcDatabase={1}hdb)' olcAccess
```

```
dn: olcDatabase={1}hdb,cn=config
olcAccess: {0}to attrs=userPassword,shadowLastChange by self write by anonymous
          auth by dn="cn=admin,dc=example,dc=com" write by * none
olcAccess: {1}to dn.base="" by * read
olcAccess: {2}to * by self write by dn="cn=admin,dc=example,dc=com" write by *
          read
```

rootDN luôn có đủ quyền trên CSDL.

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b \
cn=config '(olcDatabase={-1}frontend)' olcAccess
```

```
dn: olcDatabase={-1}frontend,cn=config
olcAccess: {0}to * by dn.exact=gidNumber=0+uidNumber=0,cn=peercred,
          cn=external,cn=auth manage by * break
olcAccess: {1}to dn.exact="" by * read
olcAccess: {2}to dn.base="cn=Subschema" by * read
```

Xét ACL thứ nhất. Đây là ACL thiết yếu:

```
olcAccess: {0}to attrs=userPassword,shadowLastChange by self write by anonymous auth by dn="cn=admin,dc=example,dc=com" write by * none
```

hay viết lại cho dễ đọc

```
to attrs=userPassword
  by self write
  by anonymous auth
  by dn="cn=admin,dc=example,dc=com" write
  by * none

to attrs=shadowLastChange
  by self write
  by anonymous auth
  by dn="cn=admin,dc=example,dc=com" write
  by * none
```

Quyền truy cập 'auth' được cấp cho Anonymous trên thuộc tính userPassword. Điều này cho phép thực hiện các kết nối. Để người dùng thay đổi mật khẩu của họ, sử dụng lệnh passwd hoặc tiện ích nào đó, người dùng cần được truy cập thuộc tính shadowLastChange.

ACL sau cho biết mọi người dùng đều có quyền đọc DIT.

```
olcAccess: {2}to * by self write by dn="cn=admin,dc=example,dc=com" write by *
  read
```

Định danh SASL có toàn quyền. Định danh này đại diện cho superuser (root/sudo) của localhost. Định danh này là

```
dn.exact=gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
```

Lệnh sau đây cho biết các ACLs của slapd-config DIT:

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b \
```

```
cn=config '(olcDatabase={0}config)' olcAccess
dn: olcDatabase={0}config,cn=config
olcAccess: {0}to * by dn.exact=gidNumber=0+uidNumber=0,cn=peercred,
           cn=external,cn=auth manage * break
```

Có thể xem tất cả ACLs bằng lệnh:

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldap:// -b \
cn=config '(olcAccess=*)' olcAccess olcSuffix
```

1.8. TLS

Phần này hướng dẫn sử dụng OpenLDAP trên Transport Layer Security (TLS). Hướng dẫn sẽ sử dụng chứng thư tự ký và CA riêng.

Cài đặt các gói gnutls-bin và ssl-cert:

```
sudo apt install gnutls-bin ssl-cert
```

Tạo khóa bí mật cho CA:

```
sudo sh -c "certtool --generate-privkey > /etc/ssl/private/cakey.pem"
```

Tạo tệp mẫu /file /etc/ssl/ca.info cho CA với nội dung như sau:

```
cn = Example Company
ca
cert_signing_key
```

Tạo chứng thư CA tự ký:

```
sudo certtool --generate-self-signed \
--load-privkey /etc/ssl/private/cakey.pem \
--template /etc/ssl/ca.info \
--outfile /etc/ssl/certs/cacert.pem
```

Tạo khóa bí mật cho server, hãy thay ldap01 bằng hostname của server:

```
sudo certtool --generate-privkey \
--bits 1024 \
--outfile /etc/ssl/private/ldap01_slapd_key.pem
```

Tạo tệp mẫu /etc/ssl/ldap01.info có nội dung:

```
organization = Example Company
cn = ldap01.example.com
tls_www_server
encryption_key
signing_key
expiration_days = 3650
```

Tạo chứng thư cho server:

```
sudo certtool --generate-certificate \
--load-privkey /etc/ssl/private/ldap01_slapd_key.pem \
--load-ca-certificate /etc/ssl/certs/cacert.pem \
--load-ca-privkey /etc/ssl/private/cakey.pem \
--template /etc/ssl/ldap01.info \
--outfile /etc/ssl/certs/ldap01_slapd_cert.pem
```

Tạo tệp certinfo.ldif với nội dung như sau:

```
dn: cn=config
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ssl/certs/cacert.pem
-
add: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ssl/certs/ldap01_slapd_cert.pem
-
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ssl/private/ldap01_slapd_key.pem
```

Sử dụng ldapmodify để cấu hình slapd làm việc trên TLS.

```
sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f /etc/ssl/certinfo.ldif
```

Thêm thông tin sau vào tệp /etc/default/slapd:

```
SLAPD_SERVICES="ldap:/// ldapi:///"
```

Cập nhật lại các quyền truy cập:

```
sudo adduser openldap ssl-cert
sudo chgrp ssl-cert /etc/ssl/private/ldap01_slapd_key.pem
sudo chmod g+r /etc/ssl/private/ldap01_slapd_key.pem
sudo chmod o-r /etc/ssl/private/ldap01_slapd_key.pem
```

Khởi động lại OpenLDAP:

```
sudo systemctl restart slapd.service
```

1.9. Nhân bản và TLS

Giả sử đã cấu hình nhân bản giữa Provider và Consumer, đồng thời đã thiết lập TLS trên Provider.

Trên Consumer, thiết lập TLS cho chứng thực cũng cần được thiết lập. Hơn nữa, truyền dữ liệu giữa Provider và Consumer cũng cần được thực hiện trên TLS.

Trên Provider,

Tạo khóa bí mật cho Consumer

```
mkdir ldap02-ssl
cd ldap02-ssl
sudo certtool --generate-privkey \
--bits 1024 \
--outfile ldap02_slapd_key.pem
```

Tạo tệp thông tin cho Consumer server:

```
organization = Example Company
cn = ldap02.example.com
tls_www_server
encryption_key
signing_key
expiration_days = 3650
```

Tạo chứng thư cho Consumer:

```
sudo certtool --generate-certificate \
--load-privkey ldap02_slapd_key.pem \
--load-ca-certificate /etc/ssl/certs/cacert.pem \
--load-ca-privkey /etc/ssl/private/cakey.pem \
--template ldap02.info \
--outfile ldap02_slapd_cert.pem
```

Sao chép chứng thư của CA:

```
cp /etc/ssl/certs/cacert.pem .
```

Sao chép chứng thư CA và chứng thư cho Consumer, trong thư mục ldap02-ss; sang Consumer.

```
cd ..
```

```
scp -r ldap02-ssl user@consumer:
```

Trên Consumer,

Cấu hình chứng thực TLS

```
sudo apt install ssl-cert
sudo adduser openldap ssl-cert
sudo cp ldap02_slapd_cert.pem cacert.pem /etc/ssl/certs
sudo cp ldap02_slapd_key.pem /etc/ssl/private
sudo chgrp ssl-cert /etc/ssl/private/ldap02_slapd_key.pem
sudo chmod g+r /etc/ssl/private/ldap02_slapd_key.pem
sudo chmod o-r /etc/ssl/private/ldap02_slapd_key.pem
```

Tạo tệp /etc/ssl/certinfo.ldif với nội dung như sau:

```
dn: cn=config
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ssl/certs/cacert.pem
-
add: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ssl/certs/ldap02_slapd_cert.pem
-
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ssl/private/ldap02_slapd_key.pem
```

Cập nhật slapd-config DIT:

```
sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f certinfo.ldif
```

Cấu hình /etc/default/slapd với SLAPD_SERVICES như trên Provider.

Trên Consumer,

Cấu hình TLS cho nhận bản.

Tạo tệp có nội dung như sau:

```
dn: olcDatabase={1}hdb,cn=config
replace: olcSyncRepl
olcSyncRepl: rid=0 provider=ldap://ldap01.example.com bindmethod=simple
binddn="cn=admin,dc=example,dc=com" credentials=secret searchbase="dc=example,dc=com"
logbase="cn=accesslog" logfilter="(&(objectClass=auditWriteObject)(reqResult=0))"
schemachecking=on type=refreshAndPersist retry="60 +" syncdata=accesslog
starttls=critical tls_reqcert=demand
```

Thuộc tính olcSyncRepl được thay đổi, cho biết Consumer phải sử dụng StartTLS và CA để thực hiện đồng bộ với Provider.

Cập nhật thay đổi

```
sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f consumer_sync_tls.ldif
```

Khởi động lại slapd:

```
sudo systemctl restart slapd.service
```

Trên Provider,

Kiểm tra phiên TLS đã được thiết lập hay chưa bằng việc xem nội dung log /var/log/syslog. Log của phiên TLS có dạng như sau:

```
slapd[3620]: conn=1047 fd=20 ACCEPT from IP=10.153.107.229:57922 (IP=0.0.0.0:389)
slapd[3620]: conn=1047 op=0 EXT oid=1.3.6.1.4.1.1466.20037
slapd[3620]: conn=1047 op=0 STARTTLS
slapd[3620]: conn=1047 op=0 RESULT oid= err=0 text=
slapd[3620]: conn=1047 fd=20 TLS established tls_ssf=128 ssf=128
slapd[3620]: conn=1047 op=1 BIND dn="cn=admin,dc=example,dc=com" method=128
slapd[3620]: conn=1047 op=1 BIND dn="cn=admin,dc=example,dc=com" mech=SIMPLE ssf=0
slapd[3620]: conn=1047 op=1 RESULT tag=97 err=0 text=
```

1.10. Quản lý người dùng và nhóm

Gói ldap-utils có đủ tiện ích để quản lý thư mục nhưng khó sử dụng. Ldapscripts là bao gói lên nó và sử dụng dễ dàng hơn.

Cài đặt ldapscripts:

```
sudo apt install ldapscripts
```

Cấu hình /etc/ldapscripts/ldapscripts.conf với nội dung tương tự sau:

```
SERVER=localhost
BINDDN='cn=admin,dc=example,dc=com'
BINDPWDFILE="/etc/ldapscripts/ldapscripts.passwd"
SUFFIX='dc=example,dc=com'
GSUFFIX='ou=Groups'
USUFFIX='ou=People'
MSUFFIX='ou=Computers'
```

```
GIDSTART=10000
UIDSTART=10000
MIDSTART=10000
```

Tạo tệp ldapscripts.passwd để cho phép rootDN truy cập. Thay secret bằng mật khẩu thật của rootDN:

```
sudo sh -c "echo -n 'secret' > /etc/ldapscripts/ldapscripts.passwd"
sudo chmod 400 /etc/ldapscripts/ldapscripts.passwd
```

Để tạo người dùng, chạy lệnh:

```
sudo ldapadduser george examplegroup
```

Để thay đổi mật khẩu của người dùng, chạy lệnh:

```
sudo ldapsetpasswd george
```

Để xóa người dùng chạy lệnh:

```
sudo ldapdeleteuser george
```

Để thêm nhóm, chạy lệnh:

```
sudo ldapaddgroup qa
```

Để xóa nhóm, chạy lệnh:

```
sudo ldapdeletegroup qa
```

Để thêm người dùng vào nhóm, chạy lệnh:

```
sudo ldapaddusertogroup george qa
```

Để bỏ người dùng khỏi nhóm, chạy lệnh:

```
sudo ldapdeleteuserfromgroup george qa
```

Để thay đổi thông tin người dùng, chạy lệnh ldapmodifyuser rồi nhập thông tin thay đổi. Ví dụ thay đổi tên hiển thị của người dùng george như sau:

```
sudo ldapmodifyuser george

# About to modify the following entry :
dn: uid=george,ou=People,dc=example,dc=com
objectClass: account
objectClass: posixAccount
cn: george
uid: george
uidNumber: 1001
gidNumber: 1001
homeDirectory: /home/george
loginShell: /bin/bash
gecos: george
description: User account
userPassword:: e1NTSEF9eXFstFcylWhwWkF1eGUybVdFWHZKRzJVMjFTSG9vcHk=

# Enter your modifications here, end with CTRL-D.
dn: uid=george,ou=People,dc=example,dc=com
replace: gecos
gecos: George Carlin
```

1.11. Backup và Restore

Tự học

2. Sử dụng xác thực LDAP cho Ubuntu client

Once you have a working LDAP server, you will need to install libraries on the client that will know how and when to contact it. On Ubuntu, this has been traditionally accomplished by installing the libnss-ldap package. This package will bring in other tools that will assist you in the configuration step. Install this package now:

```
sudo apt install libnss-ldap
```

You will be prompted for details of your LDAP server. If you make a mistake you can try again using:

```
sudo dpkg-reconfigure ldap-auth-config
```

The results of the dialog can be seen in /etc/ldap.conf. If your server requires options not covered in the menu edit this file accordingly.

Now configure the LDAP profile for NSS:

```
sudo auth-client-config -t nss -p lac_ldap
```

Configure the system to use LDAP for authentication:

```
sudo pam-auth-update
```

From the menu, choose LDAP and any other authentication mechanisms you need.

You should now be able to log in using LDAP-based credentials.

LDAP clients will need to refer to multiple servers if replication is in use. In /etc/ldap.conf you would have something like:

```
uri ldap://ldap01.example.com ldap://ldap02.example.com
```

The request will time out and the Consumer (ldap02) will attempt to be reached if the Provider (ldap01) becomes unresponsive.

If you are going to use LDAP to store Samba users you will need to configure the Samba server to authenticate using LDAP. See [Samba and LDAP](#) for details.

An alternative to the libnss-ldap package is the libnss-ldapd package. This, however, will bring in the nsed package which is probably not wanted. Simply remove it afterwards.

3. Sử dụng xác thực LDAP cho ứng dụng

Một trong những ứng dụng phổ biến của LDAP là dùng LDAP server để lưu trữ tài khoản người dùng chung. Các ứng dụng không có CSDL người dùng riêng mà sử dụng người dùng LDAP. Ví dụ, ứng dụng web với PHP có thể cài đặt chức năng đăng nhập như sau:

<http://php.net/manual/en/book.ldap.php>

<https://www.exchangecore.com/blog/how-use-ldap-active-directory-authentication-php/>

```
<?php
/*
 * Created by Joe of ExchangeCore.com
 */
if(isset($_POST['username']) && isset($_POST['password'])) {
    $adServer = "ldap://domaincontroller.mydomain.com";

    $ldap = ldap_connect($adServer);
    $username = $_POST['username'];
    $password = $_POST['password'];

    $ldapRdn = 'mydomain' . "\\" . $username;

    ldap_set_option($ldap, LDAP_OPT_PROTOCOL_VERSION, 3);
    ldap_set_option($ldap, LDAP_OPT_REFERRALS, 0);

    $bind = @ldap_bind($ldap, $ldapRdn, $password);

    if ($bind) {
        $filter="(sAMAccountName=$username)";
        $result = ldap_search($ldap,"dc=MYDOMAIN,dc=COM",$filter);
        ldap_sort($ldap,$result,"sn");
        $info = ldap_get_entries($ldap, $result);
        for ($i=0; $i<$info["count"]; $i++) {
            if($info['count'] > 1)
                break;
            echo "<p>You are accessing <strong> ". $info[$i]["sn"][0] .", " . $info[$i]["givenname"][0] ."</strong><br /> (" .
            $info[$i]["samaccountname"][0] .")</p>\n";
            echo '<pre>';
            var_dump($info);
            echo '</pre>';
            $userDn = $info[$i]["distinguishedname"][0];
        }
        @ldap_close($ldap);
    } else {
        $msg = "Invalid email address / password";
        echo $msg;
    }
}

else{
?>
<form action="#" method="POST">
    <label for="username">Username: </label><input id="username" type="text" name="username" />
    <label for="password">Password: </label><input id="password" type="password" name="password" />
    <input type="submit" name="submit" value="Submit" />
</form>
<?php } ?>
```

4. Tham khảo

- www.openldap.org

5. Đọc thêm

- [Samba and LDAP](#)
- [Kerberos](#)
- [Kerberos and LDAP](#)
- [SSSD and Active Directory](#)