SSL / TSLによる通信路の保護

概要

LDAPサーバへのアクセスを暗号化するための準備を行う。公開鍵暗号方式で通信を行うので、主に以下の準備を行う。

- 簡易認証局の立ち上げ
- 証明書、秘密鍵の作成
  準備は各サーバでそれぞれ行う。以下例として[ldap1]の場合を記述する。

簡易CA（認証局）の設定

OpenSSLに付属している簡易認証局を使用して証明書を作成する。

```
[root@ldap1 root]# cd /usr/share/ssl/misc
[root@ldap1 misc]# ./CA -newca
CA certificate filename (or enter to create)←Enterキーでcreateする。
Making CA certificate ...
Generating a 1024 bit RSA private key
......++++++
.++++++
writing new private key to './demoCA/private/./cakey.pem'
Enter PEM pass phrase:←証明書のパスフレーズを入力する。
Verifying - Enter PEM pass phrase:←確認のため再入力する。
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:JP←以降、CAの身元情報を入力する。
State or Province Name (full name) [Berkshire]:Kyoto
Locality Name (eg, city) [Newbury]:Kyoto-shi
Organization Name (eg, company) [My Company Ltd]:Kyoto University
Organizational Unit Name (eg, section) []:Faculty of Engineering
Common Name (eg, your name or your server's hostname) []:ldap1
Email Address []:
[root@ldap1 misc]#
```

ここまでで、
/usr/share/ssl/misc/demoCA/cacert.pen：CAの証明書
/usr/share/ssl/misc/private/cakey.pen：CAの秘密鍵
が作成される。

次に、証明書を検証するためのシンボリックリンクを作る。

```
[root@ldap1 misc]# cd demoCA/
[root@ldap1 demoCA]# ls
cacert.pem  certs  crl  index.txt  newcerts  private  serial
[root@ldap1 demoCA]# ln -s cacert.pem `openssl x509 -noout -hash < cacert.pem`.0
[root@ldap1 demoCA]# ll
合計 24
lrwxrwxrwx    1 root     root           10  7月 16 13:35 88f1338b.0 -> cacert.pem
-rw-r--r--    1 root     root         1038  7月 16 11:46 cacert.pem
drwxr-xr-x    2 root     root         4096  7月 16 11:32 certs
drwxr-xr-x    2 root     root         4096  7月 16 11:32 crl
-rw-r--r--    1 root     root            0  7月 16 11:32 index.txt
drwxr-xr-x    2 root     root         4096  7月 16 11:32 newcerts
drwxr-xr-x    2 root     root         4096  7月 16 11:32 private
-rw-r--r--    1 root     root            3  7月 16 11:32 serial
[root@ldap1 demoCA]#
```

簡易CAの設定は以上で完了。

LDAPサーバの証明書発行要求と暗号鍵の作成

LDAPサーバの証明書と秘密鍵を格納する場所を作成する。

```
[root@ldap1 demoCA]# cd /usr/local/etc
[root@ldap1 etc]# mkdir -p openldap/private
[root@ldap1 etc]# ll
合計 4
drwxr-xr-x    3 root     root         4096  7月 16 13:43 openldap
```

```
[root@ldap1 etc]#
```

opensslコマンドでCSR（Certificate Signing Request＝証明書発行要求）と秘密鍵を作成する。

```
[root@ldap1 etc]# cd openldap/
[root@ldap1 openldap]# openssl req -new -nodes -keyout private/ldapsvkey.pem -out ldapsvreq.pem
Generating a 1024 bit RSA private key
........++++++
.................................++++++
writing new private key to 'private/ldapsvkey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:JP
State or Province Name (full name) [Berkshire]:Kyoto
Locality Name (eg, city) [Newbury]:Kyoto-shi
Organization Name (eg, company) [My Company Ltd]:Kyoto University
Organizational Unit Name (eg, section) []:Faculty of Engineering
Common Name (eg, your name or your server's hostname) []:ldap1
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

これで、
/usr/local/etc/openldap/ldapsvreq.pem：証明書発行要求
/usr/local/etc/openldap/private/ldapsvkey.pem：LDAPサーバの秘密鍵
が作成された。

privateディレクトリ配下は保護する必要があるので、以下のようにオーナー、グループ、パーミッションを設定する。

```
[root@ldap1 openldap]# chmod 750 private
[root@ldap1 openldap]# chown .ldap private
[root@ldap1 openldap]# ls -ld private
drwxr-x---  2 root ldap 4096  9月  8 15:59 private
```

続いて、証明書発行要求に対してCA側で署名して、証明書を完成させる。

CSRへ署名した証明書を発行

CA側の操作により、CSRに対して署名を行って、LDAPサーバとしての証明書を作成する。

```
[root@ldap1 openldap]# cd /usr/share/ssl/misc
[root@ldap1 misc]# openssl ca -out /usr/local/etc/openldap/ldapsvcert.pem -infiles /usr/local/etc/openldap/ldapsvreq.pem
Using configuration from /usr/share/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/cakey.pem:←CA証明書のパスフレーズを入力する。
パスフレーズを入力させることで、勝手に自CAで署名された証明書が作成されるのを防ぐ。
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
            Not Before: Jul 16 04:56:21 2004 GMT
            Not After : Jul 16 04:56:21 2005 GMT
        Subject:
            countryName               = JP
            stateOrProvinceName       = Kyoto
            organizationName          = Kyoto University
            organizationalUnitName    = Faculty of Engineering
            commonName                = ldap1
        X509v3 extensions:
            X509v3 Basic Constraints:
            CA:FALSE
            Netscape Comment:
            OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
            47:63:77:75:AD:F1:E5:65:1A:CC:88:3A:DE:68:48:8B:B7:1A:AA:23
            X509v3 Authority Key Identifier:
            keyid:33:4F:BC:8A:8D:D0:55:7B:3F:99:58:E2:15:A8:7E:70:FC:72:69:80
            DirName:/C=JP/ST=Kyoto/L=Newbury/O=KYOTO-UNIV/CN=ldap1
            serial:00
Certificate is to be certified until Jul 16 04:56:21 2005 GMT                  (365 days)
Sign the certificate? [y/n]:y← 「y」
1 out of 1 certificate requests certified, commit? [y/n]y← 「y」
Write out database with 1 new entries
```

```
Data Base Updated
[root@ldap1 misc]# cp -p demoCA/cacert.pem /usr/local/etc/openldap/ ←CAの証明書をLDAP側にコピーしておく。
[root@ldap1 misc]#
```

これで
/usr/local/etc/openldap/ldapsvcert.pem：LDAPサーバの証明書
が作成された。

LDAPサーバの設定

LDAPサーバでセキュア通信のための設定を行う。/etc/openldap/slapd.confに以下のように設定する。（変更点のみ）

```
TLSCertificateFile /usr/local/etc/openldap/ldapsvcert.pem
↑LDAPサーバの証明書ファイルパス
TLSCertificateKeyFile /usr/local/etc/openldap/private/ldapsvkey.pem
↑LDAPサーバの秘密鍵ファイルパス
TLSCACertificateFile /usr/local/etc/openldap/cacert.pem
↑CAの証明書ファイルパス
```

LDAPサーバ(slapd)を立ち上げる。

Fedoraの場合は、
/sbin/service ldap start
でldap://（ポート389）、ldaps://（ポート636）の両方とも立ち上がる。
（slapd.conf内をgrepして「TLS」から始まる設定文字列があればldapsでも待ちうけするようになっている）

slapd起動時の-hオプションでこれらの立ち上げ有無を指定できる。以下のように起動スクリプトを編集し、ldapsのみで待ちうけするように設定を行う。
/etc/rc.d/init.d/ldap（/sbin/serviceコマンド用の起動スクリプト）を以下のように変更する。
変更前：

```
daemon ${slapd} -u ldap -h '"ldap:/// ldaps:///"' $OPTIONS $SLAPD_OPTIONS
```

変更後：

```
daemon ${slapd} -u ldap -h '"ldaps:///"' $OPTIONS $SLAPD_OPTIONS
```

変更後に
/sbin/service ldap start
として起動すると、ldapsのみでのLISTENとなる。

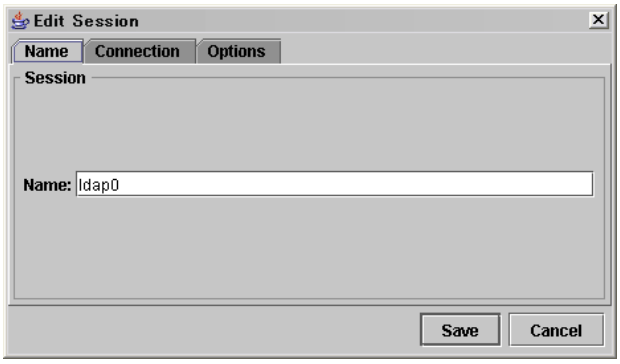
```
[root@ldap1 init.d]# /sbin/service ldap start
slapdを起動中:                                             [  OK  ]
[root@ldap1 init.d]# netstat -a | grep ldap
tcp        0      0 *:ldaps                 *:*                     LISTEN
```

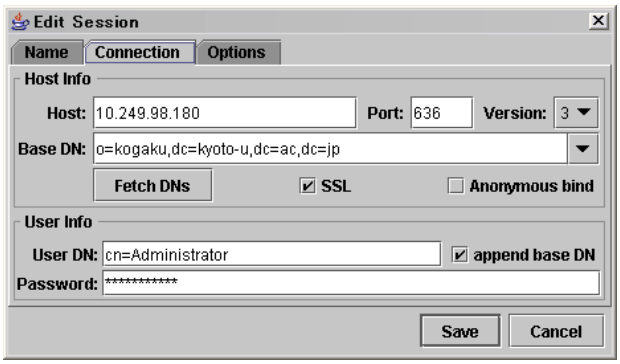
なお、このようにしてldapsのみのLISTENとした場合、ldapaddなどのツールが使用できなくなる。
この場合は、一時的にldapを有効にするか、stunnelの設定を行ったうえ、トンネリングを活用する。

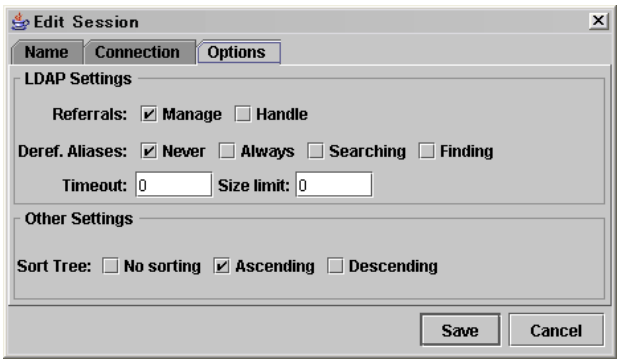
LDAP Browser/Editorのインストールと設定

LDAP Browser/Editorを使用してLDAPサーバに接続する。LDAP BrowserはJavaで動作するので、Javaの動作環境もインストールする。
LDAP Browser本体のインストールと基本設定については、事務サーバの管理者マニュアルを参照すること。
以下では、Java動作環境のSSL対応版インストール方法、およびSSLでの接続方法について記述する。

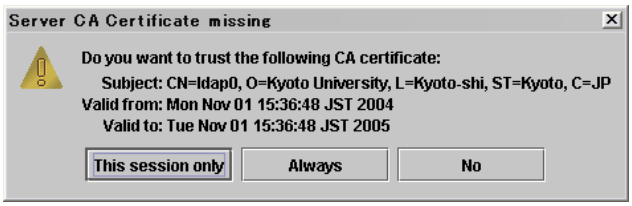
- Java実行環境のダウンロードとインストール
  http://java.sun.com/j2se/1.4.2/ja/download.htmlから「J2SE v 1.4.2_05 SDK JVMテクノロジを含む」（2004.7.16時点での最新版）をダウンロードする。SSLで接続を行う際は、SSLをサポートしている「JSSE」が必要となる。上記SDKにはこれが含まれているが、JRE（ランタイム）版には含まれていないので注意する。。一括ダウンロードでインストールするか、ネットワーク経由でインストールする。インストールオプションはデフォルトとする。一通りインストール作業が完了して、パソコンを再起動すれば完了。
- セッションの接続設定
  LDAPサーバへの接続先設定を以下のようにする。（ただし、例はldap1と異なる）







設定をSaveして接続する。すると証明書を受け入れるかどうかの確認画面が表示される。



ここで「Always」を選択して、LDAP Browserにこの証明書を信用させることとする。
なお、LDAP BrowserにはIEのようにいくつか一般的な認証局の証明書があらかじめインストールされているので、それらの認証局の証明書を使用する場合はこのような確認画面は表示されない。

View Edit