Utiliser SSL/TLS avec OpenLDAP

Pour éviter que les transactions LDAP circulent en claires sur votre réseau, vous pouvez utiliser les mécanismes TLS/SSL.
TLS/SSL assure la protection du transit des données entre serveurs/clients en créant un tunnel crypté.

Installation des packages supplémentaires

Mandrake	debian
openssl-0.9.7c-3mdk libopenssl0.9.7-0.9.7c-3mdk	openssl_0.9.7d-1_i386.deb libssl0.9.7_0.9.7d-1_i386.deb

Pour utiliser TLS/SSL, vous devez créer un certificat et une clef.
Il faut aussi créer un fichier de configuration Openssl adapté.

Créez le fichier **/etc/ssl/openldap/openssl-ldap.cnf** :

```
[ req ]

default_bits            = 2048
default_keyfile         = server_key.pem
default_md              = sha1
distinguished_name      = req_distinguished_name
x509_extensions         = server_cert
string_mask             = nombstr


[ req_distinguished_name ]

countryName                     = (C) Pays (code à 2 lettres)
countryName_default             = FR
countryName_min                 = 2
countryName_max                 = 2

stateOrProvinceName             = (ST) Etat, region ou departement
stateOrProvinceName_default     = Haute-Savoie

localityName                    = (L) Ville
localityName_default            = Alex

0.organizationName              = (O) Organisation
0.organizationName_default      = Alex

organizationalUnitName          = (OU) Unite organisationnelle
#organizationalUnitName_default =

commonName                      = (CN) FQDN du serveur
commonName_max                  = 64

emailAddress                    = (E) Adresse mail
emailAddress_max                = 64


[ server_cert ]
```

```
basicConstraints       = critical, CA:FALSE
subjectKeyIdentifier   = hash
keyUsage               = digitalSignature, keyEncipherment
extendedKeyUsage       = serverAuth, clientAuth
nsCertType             = server
nsComment              = "Certificat Serveur OpenLDAP"
# Si votre serveur Openldap possède plusieurs noms DNS :
#subjectAltName         = DNS:srv2.alex.fr,DNS:ldap.alex.fr
```

Vous pouvez maintenant générer votre clef et certificat pour un serveur.
Si vous avez un deuxième serveur (replica par exemple) il faudra lui générer une autre clef et certificat, puisqu'il aura un FQDN différent.

```
srv2:/tmp# cd /etc/ssl/openldap
srv2:/etc/ssl/openldap# openssl req -x509 -new -config openssl-ldap.cnf
-out ldap_cert.pem -keyout ldap_key.pem -days 730 -nodes

Generating a 1024 bit RSA private key
......++++++.....++++++
writing new private key to 'ldap_key.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.
-----
(C) Pays (code à 2 lettres) [FR]:
(ST) Etat, region ou departement [Haute-Savoie]:
(L) Ville [Alex]:
(O) Organisation [Alex]:
(OU) Unite organisationnelle []:
# Mettez bien le FQDN de votre serveur sinon le
# certificat ne sera pas valide !
(CN) FQDN du serveur []:srv2.alex.fr
(E) Adresse mail []:root@alex.fr
```

Pour vérifier le bon déroulement de l'opération :

```
srv2:/etc/ssl/openldap# openssl x509 -in ldap_cert.pem -text -noout

Certificate:
 Data:
   Version: 3 (0x2)
   Serial Number: 0 (0x0)
   Signature Algorithm: sha1WithRSAEncryption
   Issuer: C=FR, ST=Haute-Savoie, L=Alex, O=Alex,
CN=srv2.alex.fr/emailAddress=root@alex.fr
   Validity
   Not Before: Dec  9 18:01:46 2004 GMT
   Not After : Dec  9 18:01:46 2006 GMT
   Subject: C=FR, ST=Haute-Savoie, L=Alex, O=Alex,
CN=srv2.alex.fr/emailAddress=root@alex.fr
   Subject Public Key Info:
   Public Key Algorithm: rsaEncryption
   RSA Public Key: (2048 bit)
   Modulus (2048 bit):
...
```

Changez les droits sur la clef :

Mandrake	debian
`[root@srv2 openldap]# chmod 440 ldap_key.pem` `[root@srv2 openldap]# chown root:ldap ldap_key.pem`	`srv2:/etc/ssl/openldap# chmod 400 ldap_key.pem`

Pour activer TLS/SSL sur votre serveur, modifiez :

Mandrake	debian
/etc/openldap/slapd.conf	**/etc/ldap/slapd.conf**

```
...
TLSCertificateFile /etc/ssl/openldap/ldap_cert.pem
TLSCertificateKeyFile /etc/ssl/openldap/ldap_key.pem
# Si vous souhaitez que votre annuaire vérifie si les clients
# possèdent bien un certificat valide :
#TLSVerifyClient demand # ([never]|allow|try|demand)
...
```

debian

Editez **/etc/default/slapd** pour modifier :

```
...
SLAPD_SERVICES="ldap://127.0.0.1:389 ldap://192.168.0.2:389
ldaps://192.168.0.2:636"
...
```

Relancez le serveur Openldap pour qu'il écoute sur le port standard 389 et sécurisé 636.

Sur votre serveur et les clients modifiez la configuration classique :

Mandrake	debian
Dans **/etc/ldap.conf** activez SSL :	Dans **/etc/libnss-ldap.conf** et **/etc/pam_ldap.conf** activez SSL :

```
...
#ssl start_tls
ssl on
...
```

Copiez le (ou les) certificat(s) sur vos clients dans /etc/ssl/openldap/ puis modifiez :

Mandrake	debian
/etc/openldap/ldap.conf :	**/etc/ldap/ldap.conf**

```
# Indiquez le certificat ou le répertoire qui peut en contenir plusieurs.
#TLS_CACERT      /etc/ssl/openldap/ldap_cert.pem
TLS_CACERTDIR  /etc/ssl/openldap
# Pour demander absolument la validité du certificat.
#TLS_REQCERT demand
```

```
# Pour demander la validité du certificat : s'il n'y en à pas ou
# qu'il est mauvais, la session continuera quand même.
TLS_REQCERT allow
#TLS_REQCERT    ([demand],never,allow,try)

# La racine de votre annuaire.
BASE    dc=alex,dc=fr
# L'adresse FQDN de vos (ou votre) serveurs OpenLDAP.
URI     ldaps://srv2.alex.fr ldaps://srv6.alex.fr
```

Vérifiez sur votre serveur si tout c'est bien passé en affichant le contenu de l'annuaire en ldaps :

```
srv2:/etc/ssl/openldap# ldapsearch -x -H ldaps://srv2.alex.fr -D
"cn=Manager,dc=alex,dc=fr" -w mypassword -b "dc=alex,dc=fr"
# extended LDIF
#
# LDAPv3
# base <dc=alex,dc=fr> with scope sub
# filter: (objectclass=*)
# requesting: ALL
#

# search result
search: 2
result: 32 No such object
```

Merci à Christophe et Nico pour leur aide.

Document mis à jour : 05/12/05