Documentation

-

Projet Réseau d'entreprise

Table of Contents

I. Introduction

Ce projet de réseau d'entreprise répond aux besoin actuels de l'entreprise, afin de profiter de toutes les possibilités offertes par internet aujourd'hui, sans pour autant compromettre la sécurité de ses données, ainsi qu'en gardant le contrôle des accès des utilisateurs d'internet dans l'entreprise.
Pouvoir assurer la sauvegarde et la centralisation des données, tout en conservant une politique rigoureuse d'accès aux différentes données.
Avoir la possibilité d'héberger soi-même différents services sur internet, comme un serveur de contenu internet (serveur 'web').

Ce projet a été pensé de facon accepter tout type d'extension par la suite, sans incidences de l'existant, et en utilisant les bases d'authentification existantes si besoin est.

Cette documentation est basée sur une distribution Mandrake 8.1, mais peut tout a fait s'appliquer san modifications à la Redhat 7.2, et avec quelques arrangements à toute distribution de linux récente utilisant PAM pour l'authentification.

A)Authentification centralisée avec LDAP : Fonctionnement général

La plupart des services authentifiée peuvent utiliser LDAP comme base d'authentification, soit de manière native, soit via PAM.
Selon le service, il faudra ou non ajouter des attributs dans la base LDAP, et un schema correspondant sur le serveur OpenLDAP.

Pour le serveur de mail, le format de boites à lettre 'Maildir' a été préféré au standard unix 'mbox', car il permet une meilleure rapidité du service ainsi qu'un meilleur contrôle des quotas de mail. Il est en passe de devenir le nouveau standard et est supporté par la plupart des serveurs.

B)Choix effectués

Les serveurs et services retenus sont :

- Openldap > 2.0.15 (2.0.21 conseillé)
  Ce serveur, outre son statut opensource, présente des bonnes garanties de stabilité et une parfaite compatibité aux standards LDAP et X.500
- Pour PAM : pam_ldap > 136 et nss_ldap > 181
- Samba (version 2.2 cvs ou supérieure à 2.2.2)
  Samba 2.2 a inclus le support LDAP, encore a ses débuts. La vesion 3 sera beaucoup plus intéressante.
- Courier-mta mail server > 0.37.2 (cvs stable conseillé)

Courier-mta est un projet relativement récent, mais comportant plusieurs points très intéressants :
Serveur smtp basé sur qmail
Support ssl
Support du format Maildir
Serveurs imap et pop3
Serveur webmail
Administration web (webadmin)
Compatibilité avec la plupart des applications liées à sendmail
Modularité

- Squid proxy server > 2.4STABLE6 ou cvs stable
  Le serveur proxy Squid a déjà fait ses preuves, cependant le support LDAP n'est que rarement inclus dans les distributions binaires par défaut.
  La seule limitation est que le service d'authentification de squid ne permet pas de différencier les droits selon les utilisateurs/groupes.
- Client LDAP (toujours utile) : ldapbrowser
  Ecrit en java, donc multiplatesformes, ldapbrowser permet de gérer la base LDAP simplement, supporte ssl et permet l'authentification à la base.
  Voir http://www.ldapbrowser.com

II.Le serveur Openldap

A)Choix stratégiques

Le serveur LDAP choisi est OPENLDAP, version 2.0.x (2.0.21 ou supérieur conseillé), utilisant le standard LDAP v.3. Je n'ai pas eu l'occasion d'en essayer d'autres, et celui-ci est parfaitement compatible au standard LDAP, ce qui lui permet d'être accessible à toute application se conformant au standard.
La version v.3 (2.0.x) est stable, bien que quelques mises à jour soient encore à faire. Il ne m'a pas paru raisonnable d'utiliser la version 2 du protocole (OPENLdap-1.2.x).
Cette documentation ne prend pas en compte la possibilité offerte par OpenLdap de réplication de base (slurpd), le standard n'étant lui-même pas encore finalisé.

On utilisera la fonction 'schemacheck' de slapd :

Les schemas
Pour ce qui est des schémas utilisés, on retiendra:

- core.schema
  Obligatoire
- cosine.schema
  Obligatoire
- inetorgperson.schema
  Pour les attributs et objectClass 'person, inetorgperson' ainsi que le carnet d'adresses
- nis.schema
  Pour les attributs systèmes linux/unix
- samba.schema (livré avec samba-2.2.x)
  La définition de l'attribut 'DisplayName' doit être éliminée car elle se trouve déjà dans 'nis.schema' (elle est éliminée dans la version cvs ce jour 28/01/2002)
  Pour le serveur samba bien sur
- courier.schema (livré avec courier-0.37.x)
  Pour les attributs de mail. Si un autre serveur de mail doit accéder à la base LDAP, il peut être intéressant d'ajouter 'rfc822-MailMember.schema', qui définit des attributs mieux standardisés pour les aliases.

Le schema de samba est valable uniquement pour les versions 2.2.x de samba, le future version 3 devrait apporter un certain nombre de modifications à ce schéma, afin d'être compatible avec Active Directory (dans la mesure ou ce dernier respecte les standards bien sûr :).

La base LDAP aura une forme simple :

```
dc=example,dc=com
        o=realink
                ou=People
                        uid=user1
```

```
                                uid=user2
                                ...
                ou=Group
                                cn=group1
                                cn=group2
                                ...
                ou=Aliases
                                mail=postmaster
                                mail=webmaster
                                mail=realink-liste
                                ...
        o=admin
                cn=mailserver
                cn=sambaserver
                ...
```

Le « cn=sambaserver,o=admin,dc=example,dc=com » servira de dn d'authentification pour le serveur samba, ei ainsi pour chaque serveur, permettant ainsi de créer des acl's par serveur.

B)Installation du serveur

Sur un système redhat 7.2, il est conseillé de ne pas installer la version des CD's mais celle mise à jour (2.0.21).
Sur un système Mandrake 8.1, aucune mise à jour n'est actuellement disponible, cependant mes tests ont été effectués avec la version 2.0.14 (patchée par mandrake) livrée dans la distribution.
Par contre, il faut absolument mettre a jour le package glibc (=> 2.2.4-9.1mdk).

Sinon, reste toujours la solution .tar.gz ...
Pour les rpm's, installer : openldap, openldap-servers, openldap-guide, et
sur Mandrake : libldap2 et libldap2-devel
sur Redhat : openldap-devel et openldap-clients

C)Fichiers de configuration

- « /etc/openldap/slapd.conf »
  Fichier de configuration du serveur ldap (slapd).

```
# Les fichiers .schema a utiliser
include     <location des fichiers .schema>/core.schema
include     <location des fichiers .schema>/cosine.schema
include     <location des fichiers .schema>/inetorgperson.schema
include     <location des fichiers .schema>/nis.schema
include     <location des fichiers .schema>/openldap.schema
include     <location des fichiers .schema>/samba.schema
```

```
include      <location des fichiers .schema>/courier.schema
# option de sécurité
schemacheck on

# le type de database (ne pas modifier)
database    ldbm
# emplacement de la base ldap dans le système de fichiers – peut varier
directory    /var/lib/ldap

pidfile      <dépend de la distribution>
argsfile     <idem>

# le 'base dn'
suffix       « dc=example,dc=com »
# le 'root dn' (dn administrateur)
rootdn       « cn=Manager,dc=example,dc=com »
# en clair ou en crypté avec l'utilitaire 'slappasswd' :
rootpw       <pass_du_rootdn>
# options d'index, permettent d'augmenter la vitesse de recherche
index        objectClass,uid,uidNumber,gidNumber          eq
index        cn,mail,sn                                   eq,subinitial

# Si SSL doit être actif, un certificat X500 doit être installé sous
« /etc/openldap/ldap.pem »
# et les options ci-dessous décommentées
#
#TLSCipherSuite         HIGH:MEDIUM:+SSLv2
#TLSCertificateFile     /etc/openldap/ldap.pem
#TLSCertificateKeyFile              /etc/openldap/ldap.pem
#TLSCACertificateFile /etc/openldap/ldap.pem

# Si les acl's ne sont pas dans ce fichier :
include      /etc/openldap/slapd.access.conf
```

Pour les « acl » (access control list), elles sont définies dans ce fichier, ou dans « /etc/openldap.slapd.access.con », auquel cas ce dernier fait l'objet d'un 'include' dans slapd.conf.
Elles définissent l'accès aux attributs selon le type d'utilisateur.

```
# Les ACL
# La protection du mot de passe
access to attr=userPassword
            by self write
            by dn 'cn=Manager,dc=example,dc=com' write
            by dn 'cn=mailserver,o=admin,dc=example,dc=com' write
            by anonymous auth
            by * none
```

```
# Pour samba...
access to attr=lmPassword
        by self write
        by dn 'cn=samba,o=admin,dc=example,dc=com' write
        by dn 'cn=Manager,dc=example,dc=com' write
        by * none
access to attr=ntPassword
        by self write
        by dn 'cn=samba,o=admin,dc=example,dc=com' write
        by dn 'cn=Manager,dc=example,dc=com' write
        by * none
access to *
        by dn='cn=samba,o=admin,dc=example,dc=com' write
        by dn='cn=Manager,dc=example,dc=com' write
        by * read
```

D)Initialisation de la base

Il faut maintenant créer l'arborescence de la base ldap. Les exports/imports de la base se font aisément grâce au format de fichiers 'ldif', voici un exemple de fichier ldif créant les principaux dn's de la base :

```
dn: dc=example,dc=com
objectClass: dcObject
dc: example

dn: o=admin, dc=example,dc=com
objectClass: organization
o: admin

dn: cn=samba,o=admin,dc=example,dc=com
objectClass: person
cn: samba
userPassword:: e1NIQX1scFc1c0pJVkRwTG5OODZsSmtwRWFKbTFEeHc9
sn: Serveur Samba

dn: o=realink, dc=example,dc=com
objectClass: organization
o: realink

dn: ou=People,o=realink,dc=example,dc=com
ou: People
objectClass: organizationalUnit

dn: uid=user, ou=People, o=realink,dc=example,dc=com
shadowExpire: 999999
objectClass: top
```

```
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
objectClass: CourierMailAccount
shadowLastChange: 11717
userPassword::
e1NTSEF9WXNGOVdTN1VXMWJVRWQ5WjYwMTErOHNxZm1FSGtKOTY=
uid: user
uidNumber: 500
cn: Utilisateur
shadowFlag: 0
shadowInactive: 0
loginShell: /bin/user
gidNumber: 100
homeDirectory: /home/user
quota: 5000000S,200M
shadowWarning: 7

dn: ou=Group, o=realink, dc=example,dc=com
ou: Group
objectClass: organizationalUnit

dn: cn=users, ou=Group, o=realink, dc=example,dc=com
gidNumber: 100
memberUid: user
userPassword:: e1NIQX1jZmpubDI1TXZFVmh5ZFl2c29Qbjk0Z2dLc3M9
description: Groupe Utilisateurs
objectClass: top
objectClass: posixGroup
cn: users
```

Dans ldapbrowser, utilisez la fonction 'Import' puis indiquez le fichier ldif correspondant.
Sinon, vous pouvez aussi utiliser ldapadd (fourni avec openldap). Bien que mois intuitif, cet outil en ligne de commande est aussi capable d'insérer un fichier LDIF dans la base. Voir « man ldapadd » ou « ldapadd -h »

III.Le client Linux - PAM

ou tout système utilisant PAM (Plugable Authentification Module)

A)Introduction

Le système d'authentification utilisé par les distributions de linux est parfaitement adapté, grâce à sa modularité, aux authentifications sur une base LDAP, via le module 'pam_ldap.so'. La librairie glibc, une des bases du système, contient des composants 'nss'

B)Prérequis

Nécessite les serveurs 'openldap-2.x.x', 'samba-2.2.2' et les packages 'pam_ldap' et 'nss_ldap' qui contiennent le module de PAM pour l'authentification LDAP.

C)Configuration

Les fichiers joints dans le répertoire 'exemples/linux/pam' sont de bons exemples :

- nsswitch.conf est le fichier de configuration du module nss, qui permet de stocker un certain nombre d'informations généralement contenus dans des fichiers sur les postes linux dans la base ldap. Ceci dépassant le cadre de cette documentation, reportez-vous au site de 'padl software' http://www.padl.com .
  Pour les options qui nous intéressent, ce sont les lignes 'passwd', 'shadow' et 'group', qui doivent contenir 'ldap' comme paramètre, en plus de 'files' et éventuellement d'autre(s) source's) comme nis, nis+...
  exemple :

```
# extrait de /etc/nsswitch.conf permettant les authentifications système sur une base ldap:
passwd:     files nisplus ldap
shadow:     files nisplus ldap
group:      files nisplus ldap
```

- ldap.conf, a placer également dans /etc, contient la configuration du serveur ldap utilisé par pam, mais aussi par d'autres services. Il peut être accompagné d'un fichier 'ldap.secret' qui contiendra, le cas échéant, le mot de passe d'administration du serveur ldap défini par 'rootdn=...' dans ldap.conf.

```
# extrait de /etc/ldap.conf
# prefixe de recherche
base o=realink,dc=example,dc=com
# IP ou FQDN du serveur LDAP
host 127.0.0.1
# le port du serveur (389 par défaut)
port 389
# on peut aussi utiliser à la place une uri standardisée :
#uri ldaps://127.0.0.1
#uir ldap://127.0.0.1
```

```
#  le dn de l'administrateur ldap
rootbinddn cn=Manager,dc=example,dc=com
# le mot de passe doit alors être contenu dans le fichier /etc/ldap.secret, mode 600.
# Pour plus d'infos, « man ldap.conf »
```

- /etc/pam.d/system-auth (dans le cas d'une distribution Mandrake ou Redhat)
  Les fichiers de configuration de pam sont très sensibles et difficiles à manipuler sans connaissance approfondie de leur fonctionnement.
  Dans le cas d'une Mandrake, le fichier joint devrait suffire, en remplacement du fichier original.
  De manière générale, on peut simplement ajouter une ligne supplémentaire par type (account,auth,password,session) avant celle contenant 'pam_unix.so' ou 'pam_pwdb.so', comportant 'sufficient' comme contrôle, et indiquant le module 'pam_ldap.so'.
  ATTENTION: une mauvaise manipulation entraîne facilement un plantage complet du système à la première tentative de login !!!
  Pour plus d'infos : « man pam »

exemple de system-auth (uniquement sur redhat et mandrake) :

```
#%PAM-1.0
auth       required     /lib/security/pam_env.so
auth       sufficient   /lib/security/pam_unix.so likeauth nullok
auth       sufficient   /lib/security/pam_ldap.so use_first_pass
auth       required     /lib/security/pam_deny.so

account    required     /lib/security/pam_unix.so
account    required     /lib/security/pam_ldap.so

password   required     /lib/security/pam_cracklib.so retry=3 type=
password   sufficient   /lib/security/pam_unix.so nullok use_authtok md5 shadow
password   sufficient   /lib/security/pam_ldap.so use_authtok
password   required     /lib/security/pam_deny.so

session    required     /lib/security/pam_limits.so
session    required     /lib/security/pam_unix.so
session    optional     /lib/security/pam_ldap.so
```

IV.Pour un serveur courier-mta/courier-imap

A)Introduction

Les rpm's joints contiennent la totalité des serveurs courier, pour redhat 7.2 et Mandrake 8.1.
Pour les recompiler, utiliser '#rpm --rebuild --target <votre_architecture> courier-0.37.2-<version>.src.rpm'

- courier: le serveur smtp
- courier-imapd: le serveur imap
- courier-pop3d: serveur pop3
- courier-maildrop: programme de filtrage des mails
- courier-maildrop-wrapper: compatibilité de maildrop avec certains programmes
- courier-sendmail-wrapper: quelques liens pour rendre courier compatible avec sendmail pour les programmes locaux
- courier-smtpauth: module pour utiliser le service smtp authentifié
- courier-webmail: programme de webmail (CGI)
- courier-webadmin: script CGI d'administration de courier
- courier-ldap: module pour utiliser ldap pour les authentifications
- courier-[mysql|pgsql]: modules pour utiliser mysql/pgsql pour les authentifications

B)Prerequis

- La configuration OpenLdap fonctionelle
- Les comptes unix déjà gérés pas LDAP (même s'ils sont invalidés)
- Un utilisateur Openldap avec des droits d'écriture dans 'ou=People'

C)Installation

rpm -i courier-<version>.i686.rpm
rpm -i courier-<version>-ldap.i686.rpm
rpm -i courier-<version>-imapd.i686.rpm
rpm -i courier-<version>-sendmail-wrapper.i686.rpm
rpm -i courier-<version>-courier-maildrop-*
rpm -i courier-<version>-imapd.i686.rpm

rpm -i courier-<version>-pop3d.i686.rpm

D)Fichiers de configuration

- Edition de /etc/courier/authdaemonrc :

```
authmodulelist="authcustom authcram authldap authpam"
version=authdaemond.ldap
```

- Edition de /etc/courier/authldaprc :

```
LDAP_SERVER         ldap.example.com
LDAP_PORT           389
LDAP_BASEDN         dc=example,dc=com
#Commenter BINDPW et BINDDN, sauf si le serveur LDAP requiert une
authentification
BINDDN              cn=mailserver,o=admin,dc=example,dc=com
BINDPW              <mot_de_passe_ldap>
LDAP_MAIL           mail
LDAP_HOMEDIR        homeDirectory
LDAP_MAILDIR        mailDir
LDAP_FULLNAME       cn
LDAP_UID            uidNumber
LDAP_GID            gidNumber
# Pour les quotas :
LDAP_MAILDIRQUOTA           maildirQuota
```

- Edition de /etc/courier/courierd :

```
DEFAULTDELIVERY="| /usr/lib/courier/bin/maildrop"
```

- Edition de /etc/courier/esmtpd :

```
ESMTPDSTART=YES
```

- Edition de /etc/courier/ldapaliasrc :

```
# /etc/courier/ldapaliasrc
LDAP_ALIAS          1
LDAP_SERVER         ldap.example.com
LDAP_PORT           389

LDAP_NUMPROCS       5
# Le baseDN des aliases
LDAP_BASEDN         ou=Aliases,o=realink,dc=example,dc=com

# Facultatif si l'accès anonyme est autorisé en lmecture:
```

```
#LDAP_BINDDN        cn=mailaliases,o=admin,dc=example,dc=com
#LDAP_BINDPW        <passwd_dn_ci_dessus>

LDAP_TIMEOUT        5

# Les attributs à chercher :
# L'attribut du(des) mail(s) de l'alias
LDAP_MAIL           mail
# Le(s) adresse(s) de destination
LDAP_MAILDROP       maildrop
# Facultatif, pour restreindre l'accès à un alias selon la provenance
# LDAP_SOURCE       source
# Pour les domaines virtuels
LDAP_VDOMAIN        virtualdomain
LDAP_VUSER          virtualdomainuser
```

- Edition de /etc/courier/esmtpacceptmailfor.dir/<domaine>
  Entrer ici les noms de domaines dont la redirection est gérée par ce serveur :

exemple:

```
localdomain
mail.example.com
domainevirtuel.com
```

- Edition de /etc/courier/hosteddomains/<domain_local>
  Entrer ici le(s) nom(s) de domaine(s) local(locaux), c'est à dire hébergés localement (tous les noms d'utilisateurs seront les mêmes sur tous ces domaines)
  Inutile si un seul domaine est géré

exemple:

```
example.com
```

- Edition de /etc/courier/me
  Entrer ici le nom du serveur
- Edition de /etc/courier/locals
  Entrer ici le nom de domaine du serveur
- Edition de /etc/courier/defaultdomain
  Entrez ici le nom du domaine par défault (ajouté à tout nom d'utilisateur sans domaine)

Activation de la configuration :
makehosteddomains
makealiases
/usr/lib/courier/sbin/makeacceptmailfor

Votre serveur Courier devrait être opérationnel à présent.
ATTENTION: le serveur avec cette configuration ne permet pas au système du serveur d'envoyer des mails : C'est à vous de définir les aliases pour « root », « postmaster », etc... dans la base LDAP.

Utilisation

Pour insérer des utilisateurs, et/ou des aliases

V.Serveur Samba et LDAP

A)Introduction

Le support de LDAP dans Samba en est à ses balbutiements, comparé à toutes les options offertes par la gestion de réseau windows 2000. Cependant Samba-2.2.x supporte LDAP pour la gestion des utilisateurs et des groupes. (sans utiliser l'ensemble des fonctionnalités de Windows toutefois)

Cette documentation s'appuie sur samba 2.2.x (> 2.2.2)
La package samba fourni d'origine avec les distributions est à proscrire; il ne comporte pas de support pour ldap, qui doit être inclus dans samba au stade de la compilation.
Des packages pour Redhat et Mandrake sont fournis avec cette documentation.

Si vous voulez le recompiler, utilisez la version cvs avec le tag 'SAMBA_2_2'. Ne pas oublier l'option '–with-ldapsam' lors de la compilation.
Pour créer des rpm's, éditez le fichier 'samba2.spec' inclus dans les sources (packaging/<distribution>/samba2.spec) pour y ajouter le support LDAP.

B)Prérequis

- La configuration OpenLdap fonctionelle
- Les comptes unix déjà gérés pas LDAP (même s'ils sont invalidés)
- Un utilisateur Openldap avec des droits d'écriture dans 'ou=People'
- Un script d'ajout d'utilisateurs fonctionnant sur le même principe que 'useradd', permettant de créer des utilisateurs unix à la volée, pour les comptes machine au moins.

C)Configuration

Une fois le package installé, il faut activer LDAP, et éventuellement le support PDC (Primary Domain Controler):

Editer '/etc/samba/smb.conf' :
Exemple pour un PDC du domaine 'EXAMPLEDOMAIN' avec LDAP :

```
# extrait de /etc/samba/smb.conf
[global]
workgroup = EXAMPLEDOMAIN
server string = Samba LDAP PDC

# Options LDAP
# Serveur ldap et port
ldap server = ldap.example.com
```

```
ldap port = 389
# support SSL ldap
ldap ssl = off
# dn d'administration (doit avoir des droits d'écriture)
ldap admin dn = cn=samba,o=admin,dc=example,dc=com
# préfixe de recherche
ldap suffix = ou=People,o=realink,dc=example,dc=com

# options de PDC
security = domain
encrypt passwords = yes
domain logons = yes
# groupe(s) administrateurs des postes windows (groupes ou utilisateurs linux)
domain admin group = root, @ntadmin
```

Ensuite, lancer la commande 'smbpasswd -w sambapassword' ou sambapassword est le mot de passe attribué au dn admin (voir exemple de configuration)

ATTENTION : Une acl doit exister dans Openldap pour autoriser ce dn à écrire dans ou=People et dans ou=Group.

D)Utilisation

Pour ajouter un utilisateur samba correspondant à un compte LDAP existant, lancer : « smbpasswd -a user » ou 'user' est le login de l'utilisateur, tapez ensuite deux fois son mot de passe. Ceci a pour effet d'ajouter dans le dn de l'utilisateur visé l'objectClass 'SambaAccount' ainsi que tous les attributs nécéssaires.
Pour les comptes machine, la sytaxe est la même, sauf que l'on ajoute « -m » comma argument à smbpasswd, et que le login DOIT finir par « $ ».

En PDC, samba DOIT avoir un compte « machine » pour chaque machine du réseau. Si ce n'est pas le cas, la machine se verra refuser l'accès au serveur. Ce compte est un compte système désactivé (home=/dev/null,shell=/bin/false) sans groupe précis (il est conseillé de créer un groupe 'Machines') dont le login est constitué du nom NetBios de la machine suivi de '$'. Le mot de passe n'est pas utilisé, mais doit être présent.