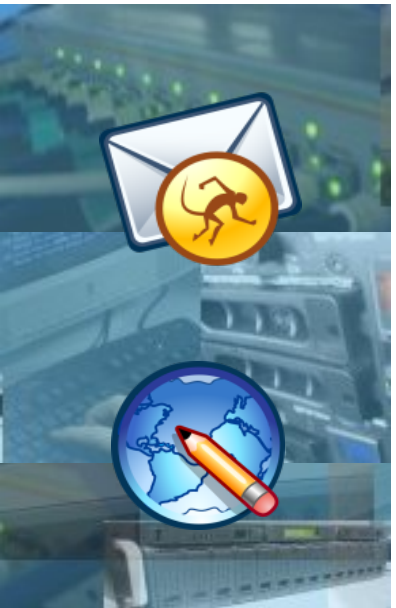
Conférence technique sur Samba

(samedi 6 avril 2006)

Windows dansera la Samba...

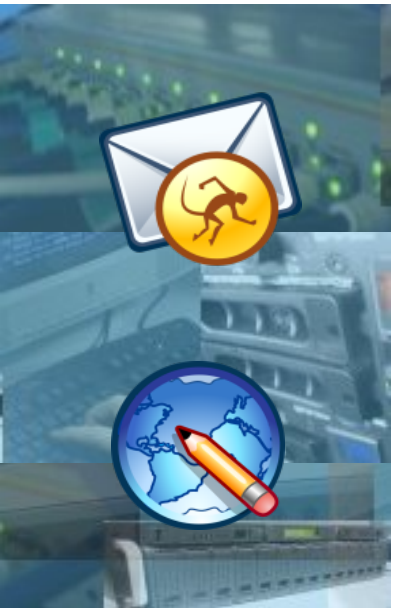
evolix
Informatique et Logiciels Libres



http://linux-azur.org/wiki/wakka.php?wiki=SaMBa

JM2L 2006

evolix
Informatique et Logiciels Libres

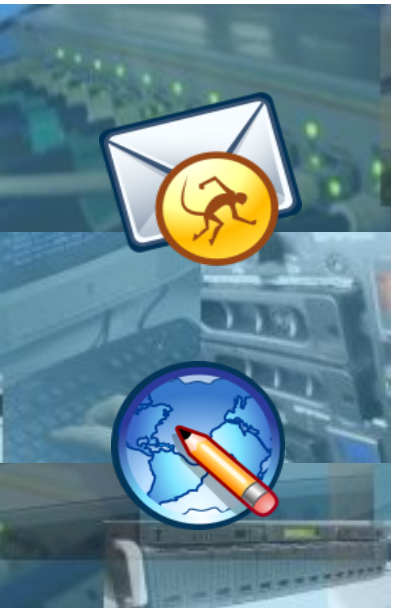


Plan

- Historique de Samba
- Protocoles SMB/CIFS
- Installation
- Serveurs Samba
- Utilisation avec OpenLDAP
- Clients SMB/CIFS pour Linux/Unix
- Connexion à un domaine NT/ADS depuis Linux

JM2L 2006

evolix
Informatique et Logiciels Libres



Samba, en quelques mots...

Samba est un logiciel libre qui met en oeuvre des services de type partage de fichiers ou d'imprimantes pour des clients SMB/CIFS. Il permet une interopérabilité entre les serveurs Linux/Unix et les clients Microsoft Windows.

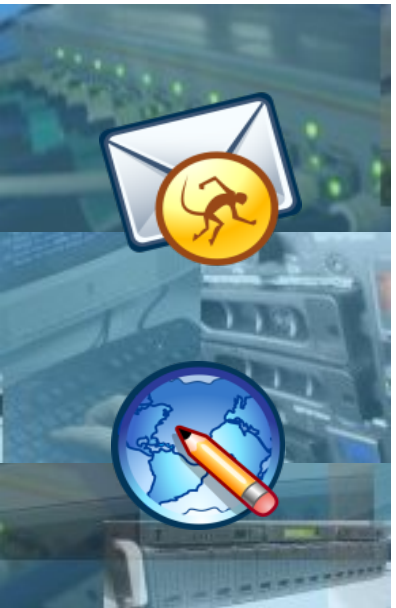
JM2L 2006

Historique

Pourquoi “SaMBa” ?

grep “^s.*m.*b” /usr/dict/words

evolix
Informatique et Logiciels Libres



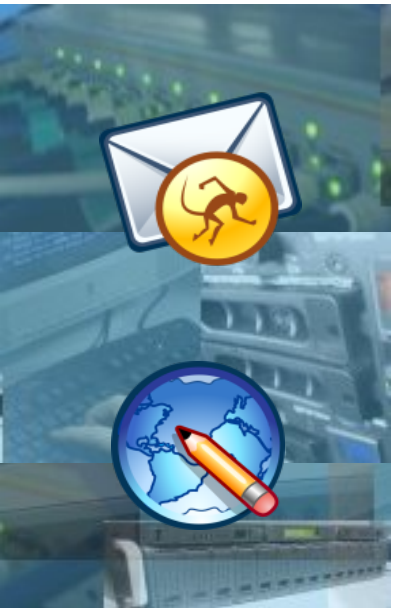
Développé par Andrew Tridgell (Australie) depuis 1991, c'est l'un des exemples le plus célèbre de reverse-engineering parmi les logiciels libres.

JM2L 2006

Méthode de développement

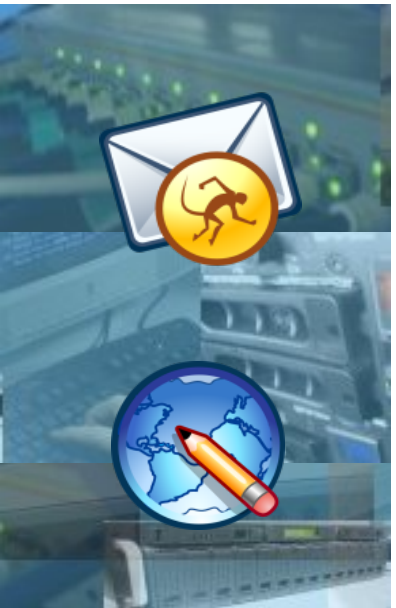
- quelques (rares) documentations
- French Cafe Technique : reverse-engineering (comportement, erreurs, simulation, etc.)

evolix
Informatique et Logiciels Libres



JM2L 2006

evolix
Informatique et Logiciels Libres



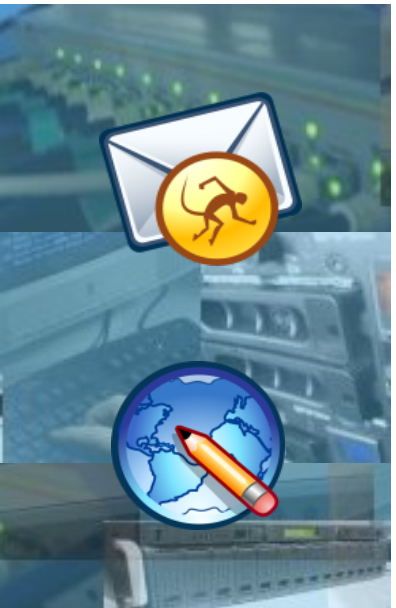
Fonctionnalités

On peut donc installer le logiciel SAMBA sur des machines Linux/Unix. Cela permet de faire passer notre machine pour un serveur SMB/CIFS sur un réseau Microsoft. Concrètement, cela offre aux machines Windows les fonctionnalités suivantes :

- serveur de fichiers
- partage d'imprimantes
- serveur d'authentification
- serveur WINS

JM2L 2006

evolix
Informatique et Logiciels Libres



Protocoles utilisés par Samba

SMB est un protocole réseau pour le partage de fichiers, imprimantes, ports séries entre différentes machines. Inventé à l'origine par IBM, il fut repris et largement modifié par Microsoft. Il est renommé en CIFS en 1998. CIFS est le successeur du protocole réseau SMB apportant son lot de nouvelles fonctionnalités : liens, fichiers de grande taille, etc.

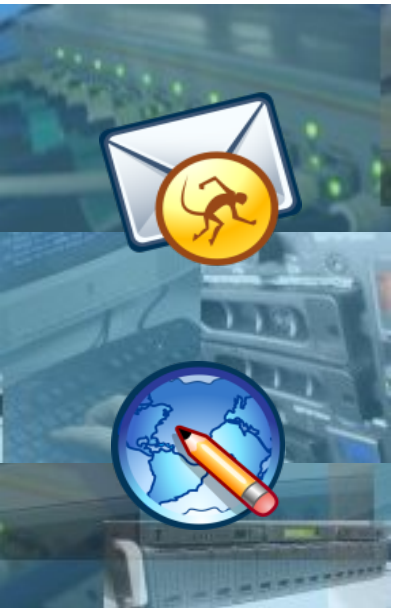
JM2L 2006

Nom NETBIOS, domaine Microsoft...

Chaque serveur SMB/CIFS possède un nom NetBIOS. Les noms NetBIOS sont des noms "human readable" assignés à chaque machine.

D'une longueur maximale de 15 caractères, ils peuvent contenir les caractères suivants : a-z, A-Z, 0-9 et ! @ # $ % ^ & ( ) - ' { } . ~ "

evolix
Informatique et Logiciels Libres



Ce sont ces noms généralement visibles dans le "voisinage réseau" des systèmes Windows. Un service de résolution des noms NetBIOS, comparable au service DNS, permet l'utilisation directe de ces noms.

- Broadcast seulement (B-Node)
- NBNS seulement (P-Node)
- premièrement Broadcast et NBNS seulement si aucune réponse en Broadcast (M-Node)
- NBNS puis Broadcast uniquement si le serveur ne répond pas (H-Node)

JM2L 2006

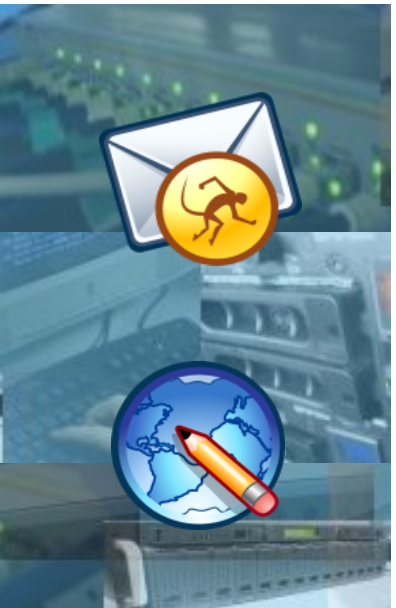
Installation

On peut bien sûr utiliser la méthode classique de recompilation à partir des sources :

$ ./configure [options]

$ make

 # make install



ou bien utiliser le système de (packages|ports) de son système.

JM2L 2006

Focus sur le package Debian (apt-get | aptitude) it !

http://packages.debian.org/samba

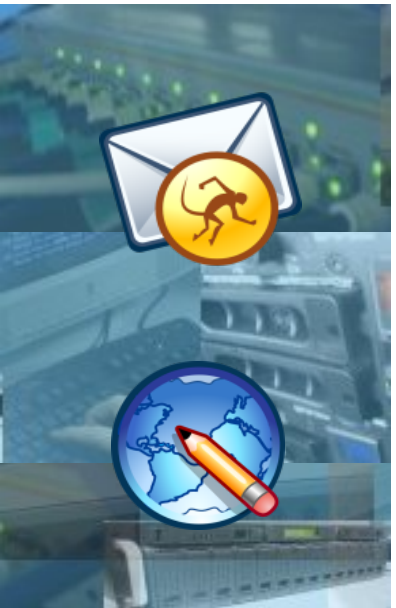
Packagé depuis 1996

Samba 2.2 dans Woody

Samba 3 dans Sarge

Samba 4 dans experimental (pas dans Etch)

evolix
Informatique et Logiciels Libres



Un split des paquets samba3 et samba4 est discuté.

Interactions avec la Samba Team (suivi du BTS, co-maintenance, etc.)

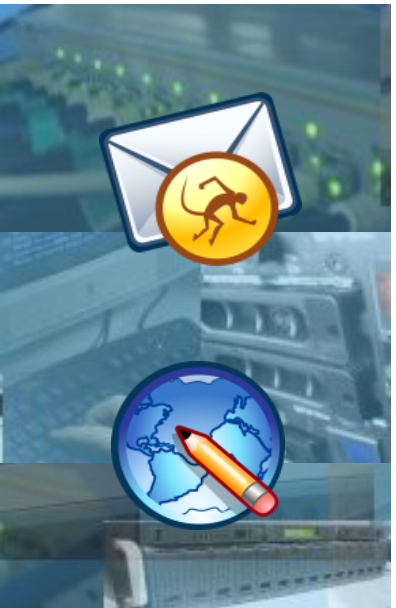
JM2L 2006

Configuration d'un serveur Samba

Plusieurs modes d'utilisation :

- serveur de fichiers
- serveur d'impression
- serveur PDC
- serveur PDC avec profils itinérants
- serveur BDC
- serveur membre d'un domaine Microsoft

evolix
Informatique et Logiciels Libres



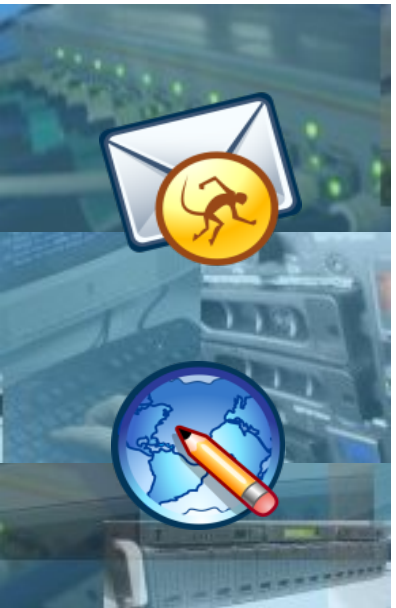
JM2L 2006

Configurer Samba

Toute la configuration se déroule dans le fichier smb.conf.

evolix
Informatique et Logiciels Libres

editor smb.conf



[global]

; configuration

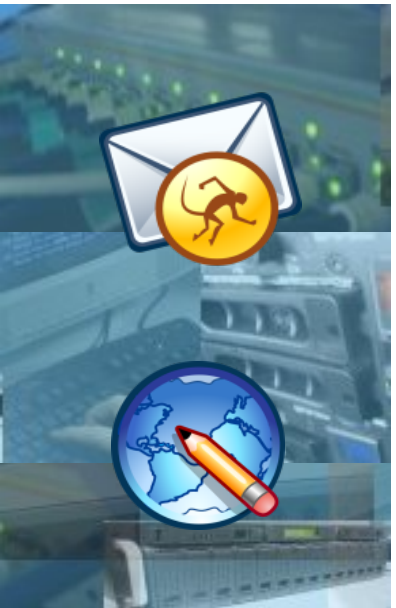
[shares]

JM2L 2006

Outils de configuration

- module Samba de Webmin
- Outil du projet Samba : SWAT (Samba Web Administration Tool)

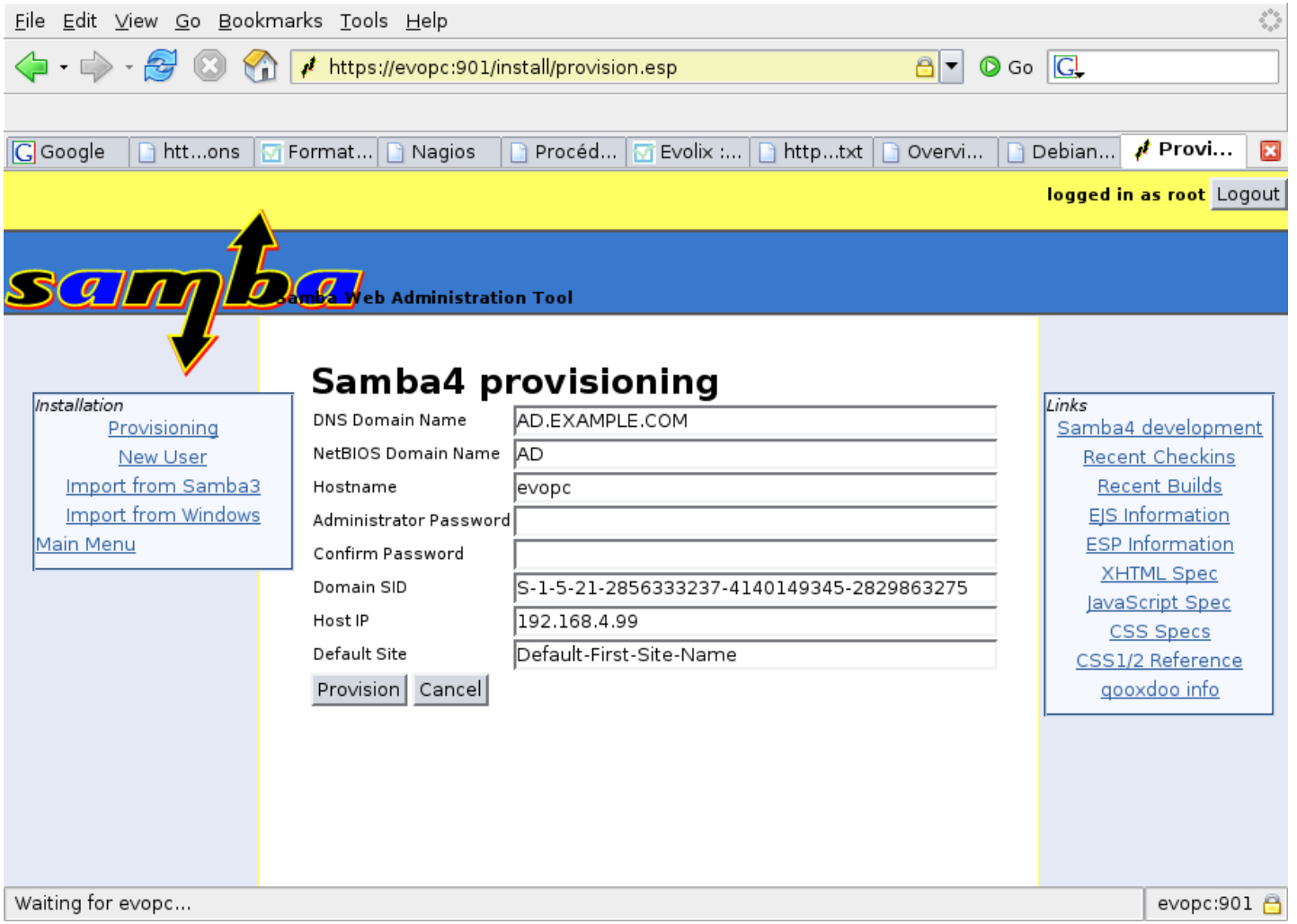
evolix
Informatique et Logiciels Libres



Manque (?) d'outils conviviaux pour la configuration pour la configuration de Samba (surtout pour la partie [shares]). Problème du backend...

JM2L 2006

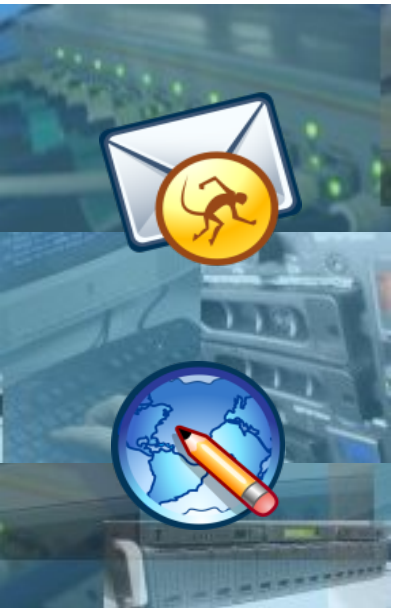
Screenshot de SWAT



evolix
Informatique et Logiciels Libres

JM2L 2006

evolix
Informatique et Logiciels Libres



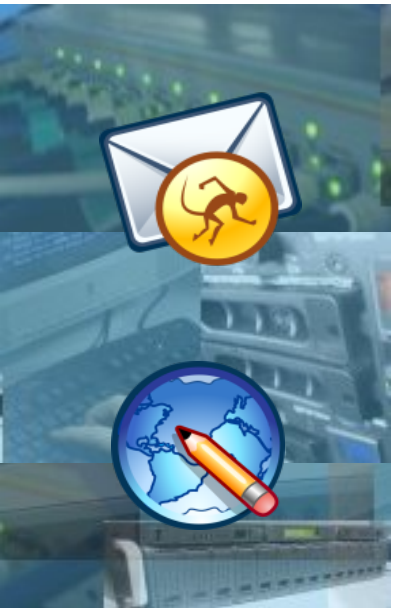
« Simple » serveur de fichier

Exemple d'un smb.conf

[global]
workgroup = NOM_DOMAINE
netbios name = NOM_MACHINE
server string = Mon ptit serveur
security = user
guest account = nobody
[public]
comment = Partage public
path = /samba/tmp
public = yes
browseable = yes
writable = yes

JM2L 2006

evolix
Informatique et Logiciels Libres



contrôleur de domaine primaire (PDC)

security = USER

[security = SHARE peu utilisé sur un serveur]

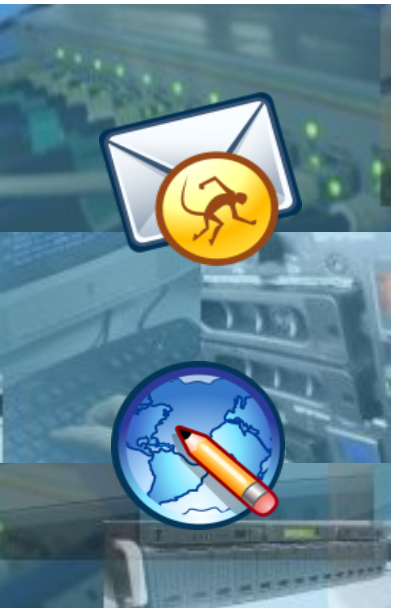
[global]
workgroup = SAMBATEST2
netbios name = MACHINE2
server string = bla
security = user
guest account = nobody
domain logons = yes
domain master = yes
preferred master = yes
os level = 35
logon path =
logon home =

JM2L 2006

contrôleur de domaine secondaire (BDC)

=> Uniquement si le PDC est Samba !!

[global]
guest account = nobody
domain logons = yes
domain master = no
os level = 33



=> Redondance (tolérance de panne, répartition de charge)

Partages

Configuration dans smb.conf

Exemple, partage d'un lecteur CD-ROM :

[cdrom]

comment = Samba server's CD-ROM

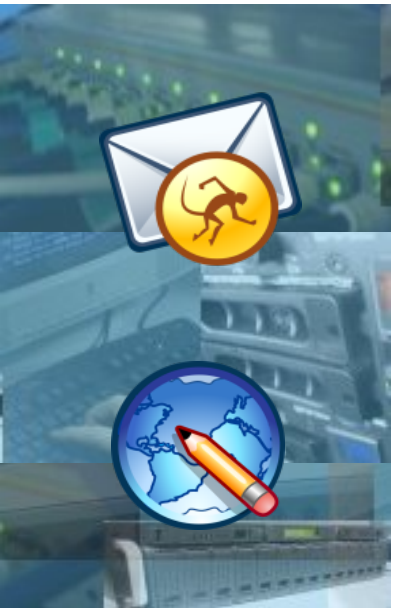
writable = no

locking = no

path = /media/cdrom0

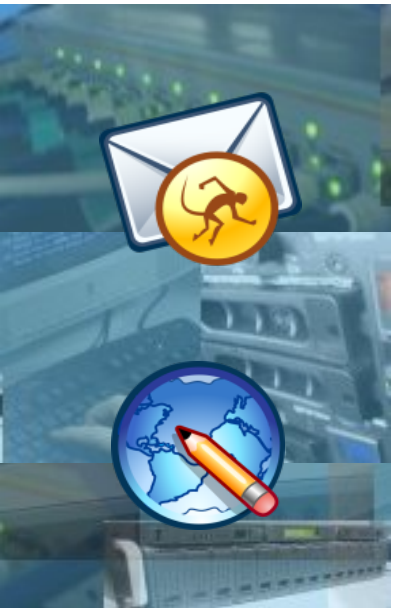
public = yes

evolix
Informatique et Logiciels Libres



JM2L 2006

evolix
Informatique et Logiciels Libres

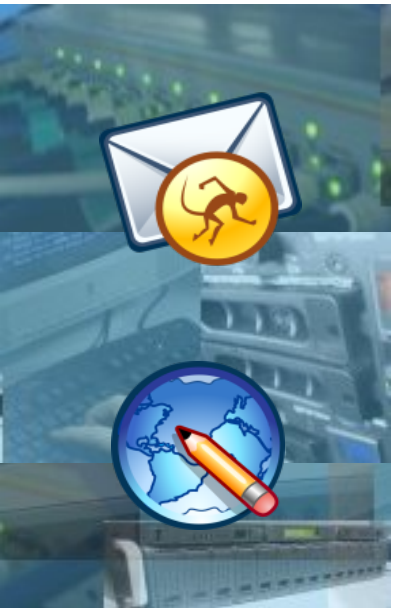


Profils itinérants

```
[global]
workgroup = SAMBATEST2
netbios name = MACHINE2
server string = bla
security = user
guest account = nobody
domain logons = yes
preferred master = yes
logon path = \\%L\ntprofiles
logon home = \\%L\9xprofiles
logon script = %U.bat
```

JM2L 2006

evolix
Informatique et Logiciels Libres



Partages pour les profils

```
[netlogon]
        comment = Repertoires scripts
        path = /samba/netlogon
        browseable = No
[9xprofiles]
        comment = Profils Windows 9x
        path = /samba/9xprofiles/%U
        browseable = No
        read only = No
[ntprofiles]
        comment = Profils Windows NT
        path = /samba/ntprofiles/%U
        browseable = No
       hide files = /desktop.ini/ntuser.ini/NTUSER.*/
```

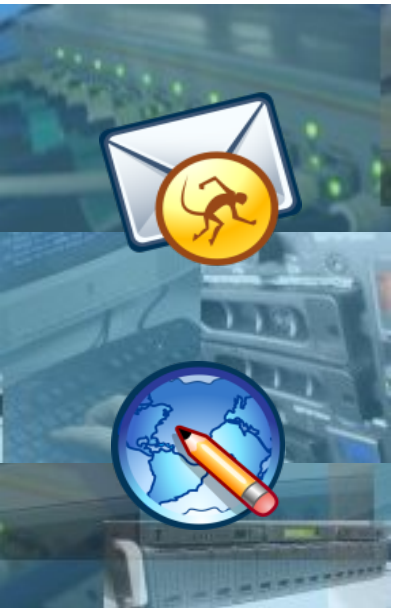
JM2L 2006

Gestion des utilisateurs

Backend : smbpasswd, stockage TDB, serveur MySQL, annuaire LDAP, NIS+, etc.

smbpasswd -a user

pdbedit -L -v user



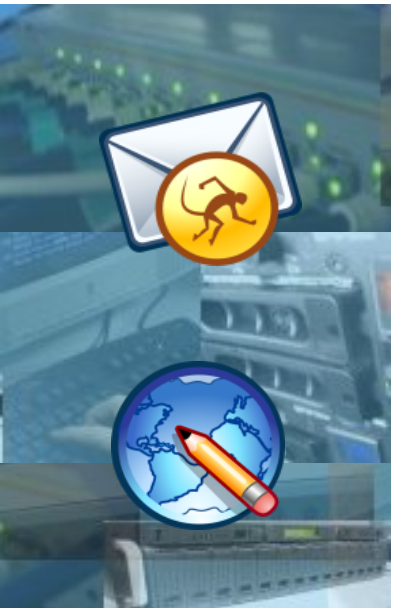
Exemple de *smbpasswd* :

Administrator:0:01FC5A6BE7BC6929AAD3B435B514
04EE:0CB6948805F797BF2A82807973B89537:[U
]:LCT-42B1A64E:

Gestion des machines

Toute machine devant être intégrée au domaine doit être ajoutée. La machine sera gérée comme un utilisateur spécial : elle sera donc stockée de la même façon que les utilisateurs. Il suffit tout simplement de préciser qu'il s'agit d'une machine.

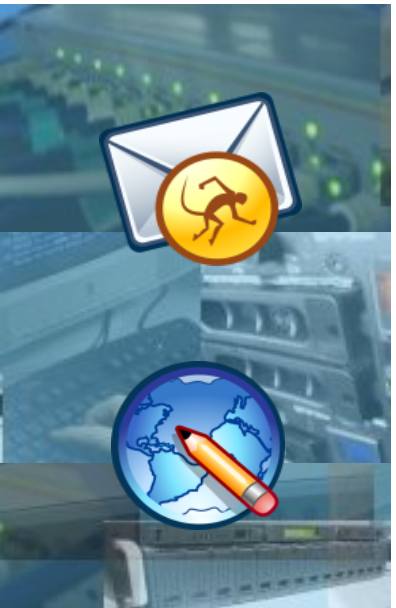
evolix
Informatique et Logiciels Libres



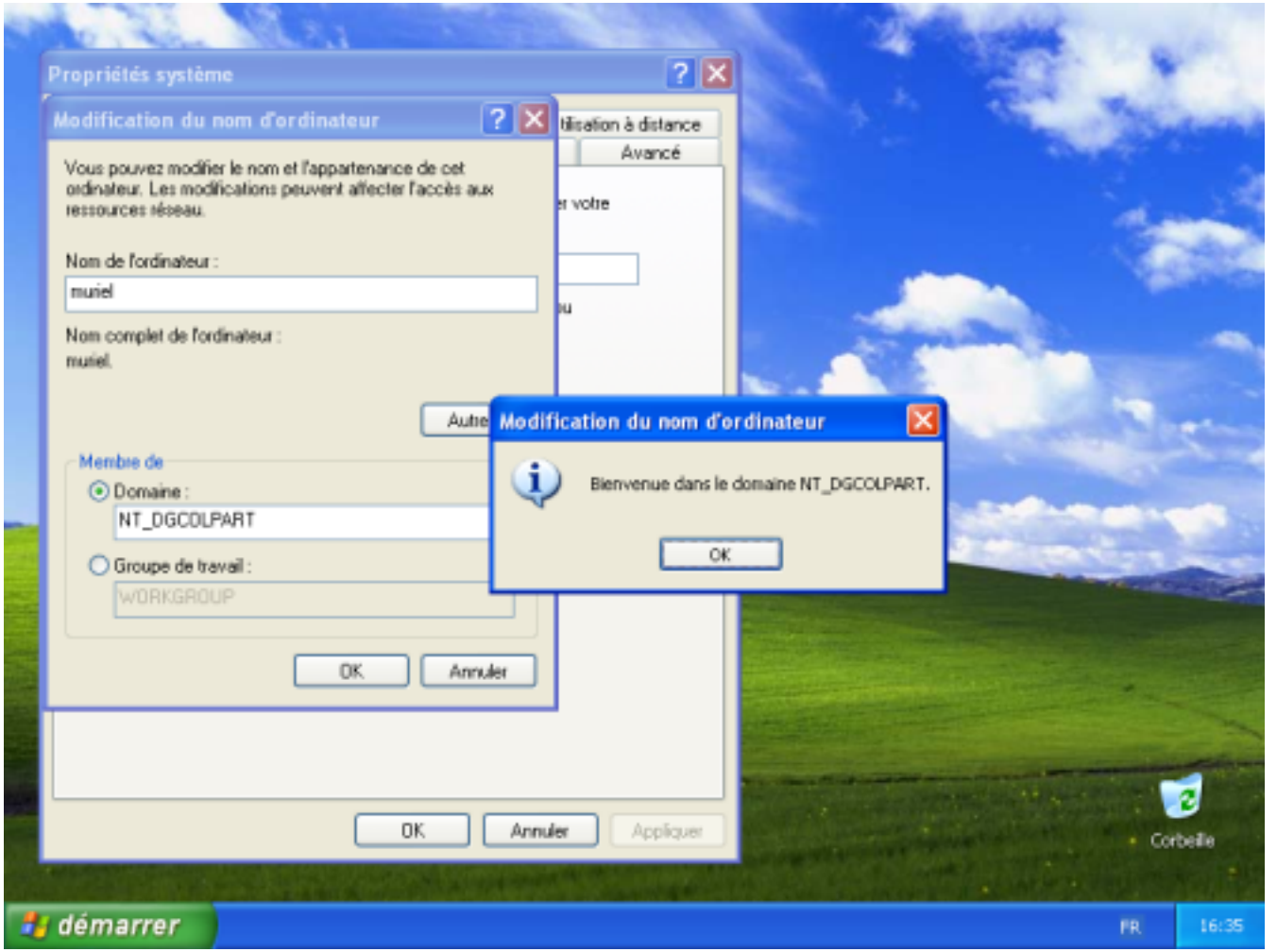
```
# addgroup pcwin
# adduser --ingroup pcwin --shell /dev/false \
--no-create-home --force-badname nom_client$
# smbpasswd -m -a nom_client$
```

JM2L 2006

evolix
Informatique et Logiciels Libres



Joindre les machines au domaine



JM2L 2006

Serveur d'impression

Imprimante classique :

print command = lpr -h -P'%p' %s

Utilisation avec CUPS :

printing = cups

printcap name = cups

[printers]

comment = All printers

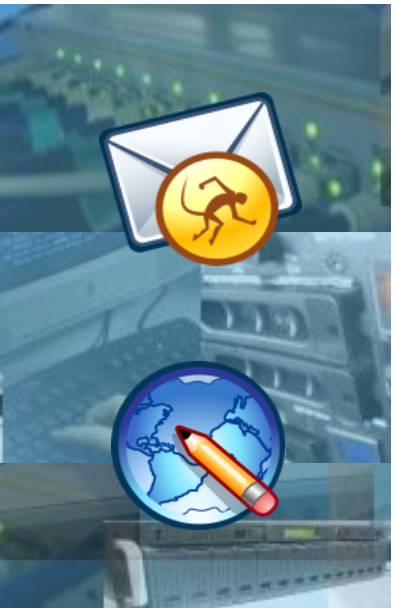
path = /var/spool/samba

printable = Yes

[print$]

path = /var/lib/samba/printers/

evolix
Informatique et Logiciels Libres



JM2L 2006

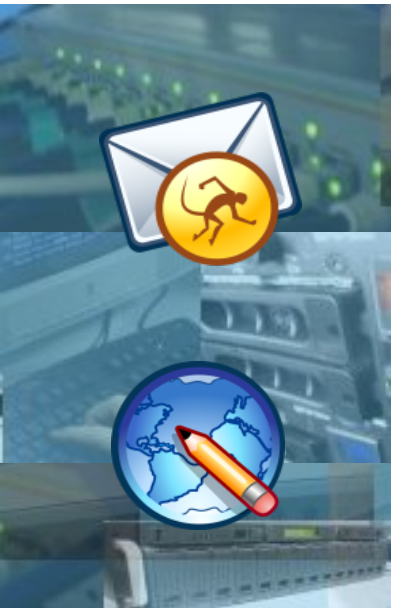
OpenLDAP

LDAP (Lightweight Directory Access Protocol) protocole pour accéder à un service d'annuaire.

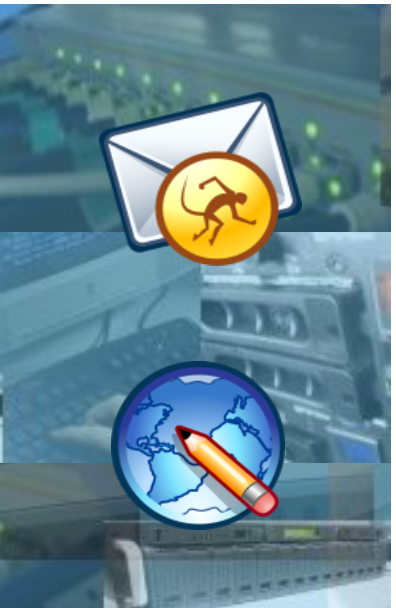
Annuaires :

- Permettent de partager des informations, telles que des coordonnées d'entités ou personnes ou encore des données système.
- Base de données spécifique structurée dans une arborescence hiérarchique.
- Plus performant en consultation qu'un système de gestion de bases de données classiques.

Pour gérer des coordonnées, pour servir des applications (SMTP, Groupware, etc.) ou pour gérer l'authentification (UNIX, Apache, IMAP, etc.).



evolix
Informatique et Logiciels Libres



Utilisation avec OpenLDAP

Modification slapd.conf :

```
include         /etc/ldap/schema/samba.schema
index cn                        pres,sub,eq
index sn                        pres,sub,eq
index uid pres,sub,eq
index sambaSID                  eq
index sambaPrimaryGroupSID eq
index sambaDomainName       eq
index default                   sub
```

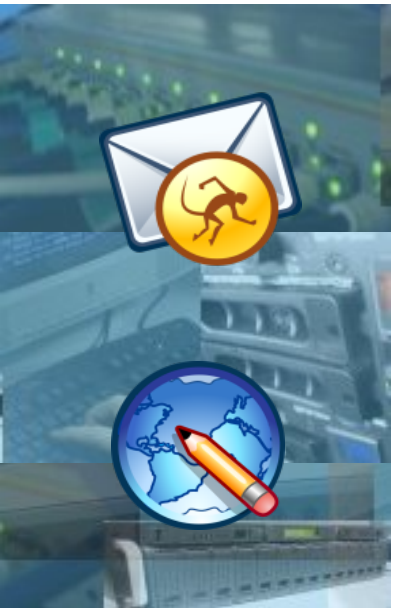
JM2L 2006

Configuration avec OpenLDAP

smb.conf :

passdb backend = ldapsam:ldap://127.0.0.1
ldap admin dn = "cn=Manager,dc=evolix,dc=net"
ldap suffix = dc=evolix,dc=net
ldap filter = (uid=%u)
ldap delete dn = no
ldap user suffix = ou=People
ldap group suffix = ou=Groups
ldap machine suffix = ou=Computers
ldap passwd sync = yes
obey pam restrictions = no

evolix
Informatique et Logiciels Libres

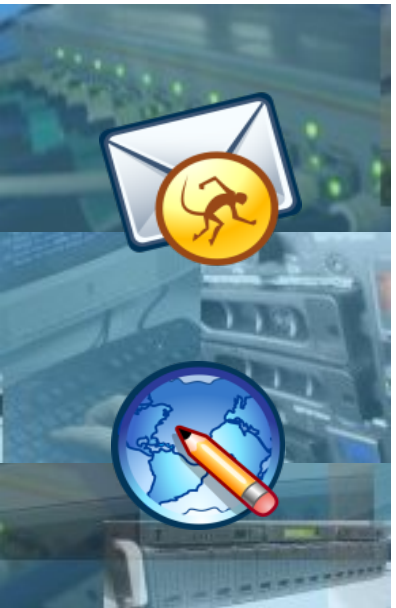


On stocke le mot de passe pour LDAP :

 # smbpasswd -w <pass-bind-LDAP>

JM2L 2006

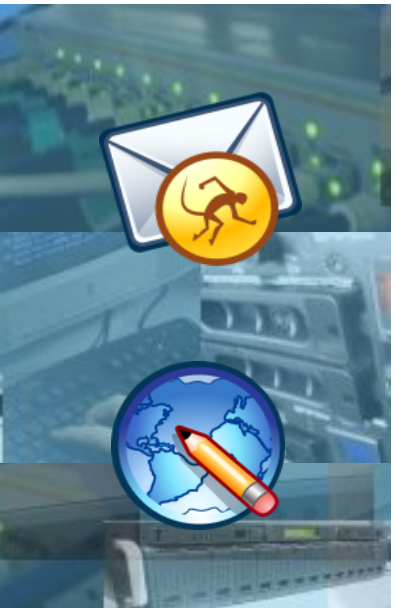
evolix
Informatique et Logiciels Libres



Utilisateurs dans OpenLDAP

dn: uid=gcolpart,ou=people,dc=evolix,dc=net
uid: gcolpart
shadowMin: 1
shadowMax: 365
shadowWarning: 10
shadowInactive: 10
shadowExpire: 21915
objectClass: shadowAccount
objectClass: inetOrgPerson
objectClass: sambaSamAccount
objectClass: posixAccount
displayName: Gregory Colpart
givenName: Colpart
sn: Colpart
cn: Gregory Colpart
sambaSID: S-1-5-21-112706504-53005086-128231200-21078
sambaLMPassword: F7BA8D4CA54E8524AAD3B435B51404EE
sambaNTPassword: AD8BB03DC2AFBE0696058C27093FF62E
sambaPwdLastSet: 1141759951
sambaKickoffTime: 1893488400
sambaAcctFlags: [XU]
sambaHomeDrive: Z:
sambaPrimaryGroupSID: S-1-5-21-112706504-53005086-128231200-513
sambaDomainName: NT_DOMAINE
uidNumber: 10039
gidNumber: 10000
homeDirectory: /home/gcolpart
loginShell: /bin/bash
userPassword:: {SSHA}xxxxxxx

JM2L 2006



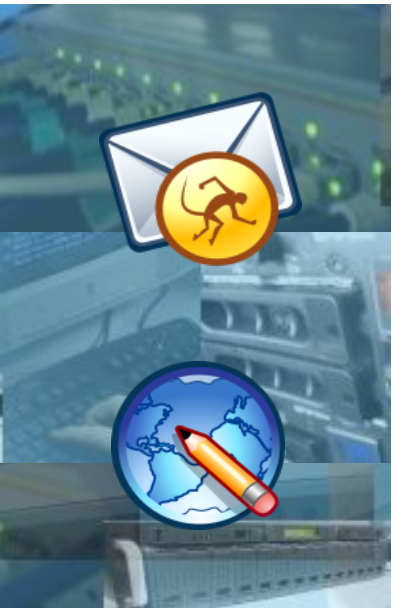
Clients SMB/CIFS pour Linux/Unix

Accès à un serveur SMB/CIFS depuis un client Unix/Linux :

```
# smbclient -L MY-PC -U Administrateur
# smbclient //MY-PC/blabla -U Administrateur
# /usr/bin/net -I 192.168.4.109 -U \
Administrateur rpc SHUTDOWN
# mount -t smbfs //MY-PC/blabla /mnt/partage \
-o username=Administrateur
# mount -t cifs //192.168.50.13/zob /mnt/zob -o \
username=XXX,password=PASS,iocharset=utf8
```

Autres : xsmbrower, linneighborhood, etc.

evolix
Informatique et Logiciels Libres



Connexion à un domaine NT

netbios name = TEST2
workgroup = AD
wins server = 192.168.4.58
security = DOMAIN

idmap uid = 15000-20000
idmap gid = 15000-20000
winbind use default domain = Yes
client schannel = no
winbind separator = +
winbind cache time = 10
template shell = /bin/bash
template homedir = /home/%U
winbind uid = 10000-20000
winbind gid = 10000-20000
winbind enum users = yes
winbind enum groups = yes

JM2L 2006

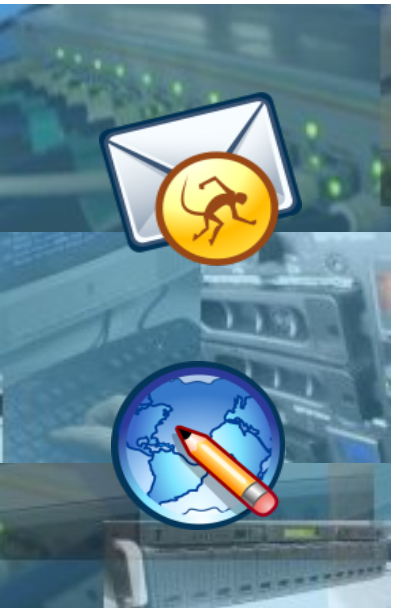
Configuration libnss + PAM

nsswitch.conf :

passwd: *compat ldap winbind*
group: *compat ldap winbind*
shadow: *compat ldap winbind*

pam.d/XXX :

auth *sufficient* *pam_ldap.so*
auth *sufficient* *pam_winbind.so use_first_pass*
auth *required* *pam_unix_auth.so use_first_pass*
account *sufficient* *pam_ldap.so*
account *sufficient* *pam_winbind.so*
account *required* *pam_unix.so*
session required */lib/security/pam_mkhomedir.so skel=/etc/skel*



winbind

 # net rpc join -UAdministrator%PASS

 # wbinfo -t

 # wbinfo -u

 # wbinfo -g

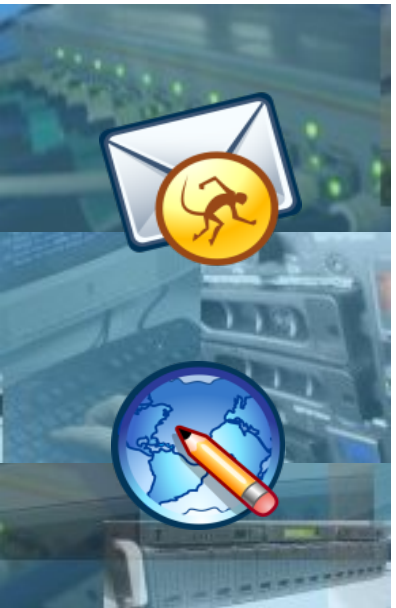
Éventuellement :

 # wbinfo --set-auth-user=Administrator%PASS

Si tout se passe bien :

 # getent passwd

 # getent group



Connexion ADS

smb.conf :

security = ADS

realm = evolix.net

password server = krb.evolix.net

Kerberos (/etc/krb5.conf)

=> Utilisation de pam_krb5