

Vampiriser un contrôleur NT4



Ce tutoriel présente la migration d'un contrôleur de domaine NT4, en service, vers un contrôleur de domaine OpenLDAP/Samba pour le remplacer.

Tout les comptes et groupes seront entrés puis injectés dans l'annuaire OpenLDAP à l'aide de Samba.

La racine principale de l'annuaire sera nommée : **dc=alex,dc=fr**

dc pour domain controler, **alex** comme nom du domaine et **fr** pour France.

Installation des packages OpenLDAP

	
Pour le <u>Serveur Contrôleur de domaine</u> : openldap2.2-2.2.17-1mdk openldap2.2-clients-2.2.17-1mdk openldap2.2-servers-2.2.17-1mdk libldap2.2_7-2.2.17-1mdk libdb4.2-4.2.52-6mdk pam_ldap-170-3mdk nss_ldap-220-3mdk samba-common-3.0.10-0.1.101mdk samba-server-3.0.10-0.1.101mdk samba-client-3.0.10-0.1.101mdk samba-doc-3.0.10-0.1.101mdk (pour le samba.schema)	Pour le <u>Serveur Contrôleur de domaine</u> : slapd_2.2.23-5_i386.deb ldap-utils_2.2.23-5_i386.deb libldap2_2.1.30-8_i386.deb libdb4.2_4.2.52-18_i386.deb libnss-db_2.2-6.2_i386.deb libdbd-ldap-perl_0.05-1_all.deb libnss-ldap_238-1_i386.deb libpam-ldap_178-1_i386.deb libpam-cracklib_0.76-22_i386.deb samba_3.0.14a-1_i386.deb samba-common_3.0.14a-1_i386.deb samba-doc_3.0.14a-1_all.deb (pour le samba.schema) smbldap-tools_0.8.7-4_all.deb

Configuration d'OpenLDAP

	
Le fichier /etc/openldap2.2/slapd.conf	Le fichier /etc/ldap/slapd.conf

comporte diverses informations telles que la racine supérieure de l'annuaire, l'administrateur principal de l'annuaire LDAP et son mot de passe, les droits d'accès par défaut, les fichiers d'objets et de syntaxe à utiliser ainsi que les règles d'accès (ACL) pour les entrées et les attributs de l'annuaire LDAP.

Compte tenu que ce fichier contient le mot de passe de l'administrateur de l'annuaire, il est impératif de positionner les droits « rw----- » sur le fichier slapd.conf :

```
[root@srv2 user]# chmod 600 /etc/openldap2.2/slapd.conf
```

Modifiez le fichier `/etc/openldap2.2/slapd.conf`

```
# $OpenLDAP: pkg/ldap2.2/servers/slapd/slapd.conf,v 1.8.8.6 2001/04/20
23:32:43 kurt Exp $
```

```
include /usr/share/openldap2.2/schema/core.schema
include /usr/share/openldap2.2/schema/cosine.schema
include /usr/share/openldap2.2/schema/corba.schema
include /usr/share/openldap2.2/schema/inetorgperson.schema
include /usr/share/openldap2.2/schema/java.schema
include /usr/share/openldap2.2/schema/krb5-kdc.schema
include /usr/share/openldap2.2/schema/kerberosobject.schema
include /usr/share/openldap2.2/schema/misc.schema
include /usr/share/openldap2.2/schema/nis.schema
include /usr/share/openldap2.2/schema/openldap.schema
include /usr/share/openldap2.2/schema/autofs.schema
# Pour qu'OpenLDAP utilise les bonnes informations concernant
# la version de Samba, copiez le fichier :
# /usr/share/doc/samba-doc-3.0.10/examples/LDAP/samba.schema
# vers /etc/openldap2.2/schema/samba-3.0.10.schema.
include /etc/openldap2.2/schema/samba-3.0.10.schema
include /usr/share/openldap2.2/schema/kolab.schema
include /usr/share/openldap2.2/schema/evolutionperson.schema
include /usr/share/openldap2.2/schema/calendar.schema
include /usr/share/openldap2.2/schema/sudo.schema
include /usr/share/openldap2.2/schema/dnszone.schema
include /usr/share/openldap2.2/schema/dhcp.schema

#include /usr/share/openldap2.2/schema/rfc822-MailMember.schema
#include /usr/share/openldap2.2/schema/pilot.schema
#include /usr/share/openldap2.2/schema/qmail.schema
#include /usr/share/openldap2.2/schema/mull.schema
#include /usr/share/openldap2.2/schema/netscape-profile.schema
#include /usr/share/openldap2.2/schema/trust.schema
#include /usr/share/openldap2.2/schema/dns.schema
#include /usr/share/openldap2.2/schema/cron.schema

include /etc/openldap2.2/schema/local.schema

# Inclusion du fichier slapd.access.conf contenant les ACLs
include /etc/openldap2.2/slapd.access.conf

# Do not enable referrals until AFTER you have a working directory
# service AND an understanding of referrals.
#referral ldap://root.openldap.org

pidfile /var/run/ldap2.2/slapd.pid
argsfile /var/run/ldap2.2/slapd.args

modulepath /usr/lib/openldap

# SASL config
#sasl-host ldap.example.com
```

```

# To allow TLS-enabled connections.
#TLSRandFile /dev/random
#TLSCipherSuite HIGH:MEDIUM:+SSLv2
#TLSCACertificatePath /etc/ssl/openldap2.2/
#TLSCACertificateFile /etc/ssl/openldap2.2/ldap_cert.pem
# Pour activer ldaps sur votre annuaire, décommenté ces 2 lignes
# et reportez vous au chapitre "SSL/TLS" pour mettre en place ldaps.
#TSLCertificateFile /etc/ssl/openldap2.2/ldap_cert.pem
#TSLCertificateKeyFile /etc/ssl/openldap2.2/ldap_key.pem
# Si vous souhaitez que votre annuaire vérifie si les clients
# possèdent bien un certificat valide :
#TLSVerifyClient demand # ([never]|allow|try|demand)

# Niveau des informations de logs.
loglevel 256

# Vérification de la structure des objectClasses définis
# dans les fichiers .schema inclus plus haut.
schemacheck on

#####
# database definitions
#####

database bdb

# Définition de la racine du serveur.
suffix "dc=alex,dc=fr"

# Définition du compte d'administration ici Manager
# c'est un nom arbitraire et ce n'est pas forcément un
# utilisateur défini dans /etc/passwd du système.
rootdn "cn=Manager,dc=alex,dc=fr"

#mot de passe en clair est « mypassword », voir plus loin comment le crypter
rootpw {crypt}ijFYNcSNctBYg

# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd/tools. Mode 700 recommande.
directory /var/lib/ldap2.2

# Tuning settings, please see the man page for slapd-bdb for more
# information as well as the DB_CONFIG file in the database directory
# commented entries are at their defaults
# In-memory cache size in entries
cachesize 1000
# Checkpoint the bdb database after 256kb of writes or 15 minutes have
# passed since the last checkpoint
checkpoint 256 15

```

```
# Liste des attributs à indexer pour une recherche plus rapide.
```

```
# Ils sont dépendant de la version de samba.schema
```

```
index objectClass,uidNumber,gidNumber,memberUid eq
```

```
index sambaSID,sambaPrimaryGroupSID eq
```

```
index mail,surname,givenname eq,subinitial
```

```
index cn,uid pres,sub,eq
```

```
index default sub
```

```
# Indique le format du cryptage, ici {crypt}
```

```
password-hash {crypt}
```

```
password-crypt-salt-format "$1$%.8s"
```

Modifiez le fichier **/etc/ldap/slapd.conf**

```
#####
# Global Directives:

# Schema and objectClass definitions
include          /etc/ldap/schema/core.schema
include          /etc/ldap/schema/cosine.schema
include          /etc/ldap/schema/nis.schema
include          /etc/ldap/schema/inetorgperson.schema
# Pour qu'OpenLDAP utilise les bonnes informations concernant
# la version de Samba, extraire le fichier :
# /usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz
# vers /etc/ldap/schema/samba-3.0.10-1.schema.
include          /etc/ldap/schema/samba-3.0.10-1.schema

# Inclusion du fichier slapd.access.conf contenant les ACLs
include          /etc/ldap/slapd.access.conf

# Schema check allows for forcing entries to
# match schemas for their objectClasses's
schemacheck      on

# Where the pid file is put. The init.d script
# will not stop the server if you change this.
pidfile          /var/run/slapd/slapd.pid

# List of arguments that were passed to the server
argsfile         /var/run/slapd.args

# To allow TLS-enabled connections.
# et reportez vous au chapitre "SSL/TLS" pour mettre en place ldaps.
#TLSCertificateFile /etc/ssl/openldap/ldap_cert.pem
#TLSCertificateKeyFile /etc/ssl/openldap/ldap_cert.pem
# Si vous souhaitez que votre annuaire vérifie si les clients
# possèdent bien un certificat valide :
#TLSVerifyClient demand # ([never]|allow|try|demand)

# Read slapd.conf(5) for possible values
loglevel         256

# Where the dynamically loaded modules are stored
modulepath       /usr/lib/ldap
moduleload       back_bdb

#####
# Specific Backend Directives for bdb:
# Backend specific directives apply to this backend until another
# 'backend' directive occurs
backend bdb
checkpoint 512 30
```

```

# Définition de la racine du serveur.
suffix "dc=alex,dc=fr"

# Définition du compte d'administration ici Manager
# c'est un nom arbitraire et ce n'est pas forcément un
# utilisateur défini dans /etc/passwd du système
rootdn "cn=Manager,dc=alex,dc=fr"

# mot de passe en clair est « mypassword », voir plus loin comment le crypter
rootpw {crypt}ijFYNcSNctBYg

# Where the database file are physically stored for database #1
directory "/var/lib/ldap"

#####
# Specific Directives for database #1, of type bdb:
# Database specific directives apply to this database until another
# 'database' directive occurs
database bdb

# Liste des attributs à indexer pour une recherche plus rapide.
# Ils sont dépendant de la version de samba.schema
index objectClass,uidNumber,gidNumber,memberUid eq
index sambaSID,sambaPrimaryGroupSID eq
index mail,surname,givenname eq,subinitial
index cn,uid pres,sub,eq
index default sub

# Indique le format du cryptage, ici {crypt}
password-hash {crypt}
password-crypt-salt-format "$1$%.8s"

# Save the time that the entry gets modified, for database #1
#lastmod on

```

Le mot de passe de l'administrateur est «mypassword» en clair, pour le crypter au format {CRYPT}, il faudra taper (exemple avec mypassword) :

```

[root@pc user]# slappasswd -v -s mypassword -h {CRYPT}
{CRYPT}G.H5krNMMw0cc

```



Modifiez le fichier
/etc/openldap2.2/slapd.access.conf

Créez le fichier
/etc/ldap/slapd.access.conf

ACLs authentication **PDC POSIX/SAMBA**

Respectez les tabulations, elles font parties de la syntaxe !

La racine DIT doit être accessible pour tout les clients.

access to dn.exact="" by * read

Protection de l'attribut userPassword dans tout l'annuaire.

access to attribute=userPassword
by self write
by dn="cn=admin,dc=alex,dc=fr" write
by anonymous auth
by * none

Protection des passwords et informations Samba dans la branche

"ou=People,dc=alex,dc=fr".

access to dn.children="ou=People,dc=alex,dc=fr"
attrs=sambaLMPassword,sambaNTPassword,sambaPwdLastSet,
sambaPwdMustChange,sambaPasswordHistory
by self write
by dn="cn=admin,dc=alex,dc=fr" write
by group="cn=Domain Controllers,ou=Group,dc=alex,dc=fr" write
by anonymous auth
by * none

ACL permettant à l'admin de l'annuaire et au groupe

Domain Controllers d'ajouter des utilisateurs dans cette branche.

access to dn.children="ou=People,dc=alex,dc=fr"
attrs=entry,children,posixAccount,sambaSamAccount
by dn="cn=admin,dc=alex,dc=fr" write
by group="cn=Domain Controllers,ou=Group,dc=alex,dc=fr" write
by users read
by anonymous read

ACL permettant à l'admin de l'annuaire et au groupe

Domain Controllers d'ajouter des groupes dans cette branche.

access to dn.children="ou=Group,dc=alex,dc=fr"
attrs=entry,children,posixGroup,sambaGroupMapping
by dn="cn=admin,dc=alex,dc=fr" write
by group="cn=Domain Controllers,ou=Group,dc=alex,dc=fr" write
by users read
by anonymous read

ACL permettant aux utilisateurs de modifier leurs attributs mail et

telephoneNumber.

access to dn.children="ou=People,dc=alex,dc=fr"
attrs=mail,telephoneNumber
by self write
by dn="cn=admin,dc=alex,dc=fr" write
by users read
by anonymous read

ACL permettant à l'admin de l'annuaire d'ajouter des hôtes dans cette branche.

```
access to dn.children="ou=Hosts,dc=alex,dc=fr"  
  attrs=entry,children,ipHost,device  
  by dn="cn=admin,dc=alex,dc=fr" write  
  by users read  
  by anonymous read
```

Configurez les autres fichiers du serveur PDC selon les explications du chapitre "[Mappage de l'annuaire LDAP avec les modules d'authentification Unix](#)".

smb.conf

Dans cet exemple je crée un répertoire **/home/samba** sur le PDC.

Il contiendra 3 sous répertoires :

/home/samba/netlogon (répertoire pour les différents fichiers de logon)

/home/samba/partage (répertoire Public réservé au groupe users)

/home/samba/profiles (ou seront stocké les profiles des utilisateurs windows)

Dans un premier temps il faut configurer Samba comme serveur membre du domaine NT4.

Ensuite nous pourrons vampiriser le controleur NT4.

Informations sur le controleur NT4 :

- Nom NetBIOS = wint4

- Nom du domaine NT4 = WINALEXNT4

Créez votre fichier smb.conf dans le répertoire /etc/samba/

Il devra ressembler à celui ci :

```
#===== Global Settings =====  
[global]
```

```
# Nom du domaine Windows NT4 existant que nous allons vampiriser.  
workgroup = WINALEXNT4
```

```
# Nom netbios de notre futur controleur de domaine Samba.  
netbios name = PDC-LINUX
```

```
server string = Samba Server %v
```

```
log file = /var/log/samba/log.%m
```

```
max log size = 5
```

```
# Security and Domain Membership Options:
```

```
hosts allow = 127.0.0.1 192.168.0.0/24
```

```
hosts deny = 0.0.0.0/0
```

```
interfaces = eth* lo
```

```
bind interfaces only = yes
```

```
security = user
```

```
encrypt passwords = yes
```

```
passwd program = /usr/bin/passwd %u
```

```
passwd chat = *New*UNIX*password* %n\n *ReType*new*UNIX*password* %n\n
```

```
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
```

```
local master = yes
```

```
os level = 64
```

```
# Pour vampiriser le controleur NT4 il ne faut pas etre "domain master".
```

```
# Une fois les comptes importés, éteindre le controleur NT4 et
```

```
# passer domain master et preferred master à yes. Puis relancez Samba.
# domain master = yes
# preferred master = yes
  domain master = no
  preferred master = no

domain logons = yes

# Le logon script est stocké sur notre serveur Samba.
# %L remplace le nom NetBIOS de Samba.
  logon script = \\%L\netlogon\logon.bat

# Le Profile des utilisateurs est stocké sur notre serveur Samba.
# %U pour remplacer les nom de l'utilisateur.
  logon path = \\%L\Profiles\%U
  logon home = \\%L\%U
  logon drive = U:
```



```
# Scripts de gestion des comptes du domaine entre Samba et OpenLDAP.
# Configurez le fichier : /etc/samba/smbldap_conf.pm
```



```
# Scripts de gestion des comptes du domaine entre Samba et OpenLDAP.
# Configurez les fichiers : /etc/smbldap-tools/smbldap.conf et
# /etc/smbldap-tools/smbldap_bind.conf
```

```
add machine script = /usr/sbin/smbldap-useradd -w -d /dev/null -c 'Machine
Account' -s /bin/false %u
add user script = /usr/sbin/smbldap-useradd -a -m '%u'
delete user script = /usr/sbin/smbldap-userdel -r '%u'
; ldap delete dn = Yes
add group script = /usr/sbin/smbldap-groupadd -g '%g'
delete group script = /usr/sbin/smbldap-groupdel '%g'
add user to group script = /usr/sbin/smbldap-groupmod -m '%u' '%g'
delete user from group script = /usr/sbin/smbldap-groupmod -x '%u' '%g'
set primary group script = /usr/sbin/smbldap-usermod -g '%g' '%u'
```

```
# LDAP configuration for Domain Controlling:
# Lancez cette commande pour que Samba puisse lire et écrire
# dans l'annuaire : smbpasswd -w mypassword
```

```
ldap admin dn = cn=Manager,dc=alex,dc=fr
ldap suffix = dc=alex,dc=fr
ldap passwd sync = yes
```

```
ldap user suffix = ou=People
ldap group suffix = ou=Group
ldap machine suffix = ou=People
ldap idmap suffix = ou=People
```

```

# Connexion à l'annuaire en localhost, puisque
# Samba est sur la même machine que OpenLDAP.
    passdb backend = ldapsam:ldap://localhost
    idmap backend = ldap:ldap://localhost

# DNS Proxy - tells Samba whether or not to try to resolve
# NetBIOS names via DNS nslookups.
    dns proxy = no

#===== Share Definitions =====

[homes]
    comment = Home Directories
    browseable = no
    writable = yes
    valid users = %S

# N'oubliez pas de donner les droits en écriture sur ces
# répertoires, sinon vous aurez un message depuis les stations
# Windows$ "Impossible d'écrire le profil ..."
# Vous pouvez ajouter chaque utilisateurs au groupe "users" dans
# l'annuaire LDAP et changer le groupe des répertoires :
# drwxr--r--  2 root root  4096 aoû  3 09:23 netlogon/
# drwxrwxr--  2 root users 4096 aoû  3 11:41 partage/
# drwxrwxr--  3 root users 4096 aoû  6 10:59 profiles/

[netlogon]
    comment = Network Logon Service
    path = /home/samba/netlogon
    writeable = no
    share modes = no
    read only = yes
    write list = @adm

[Profiles]
    path = /home/samba/profiles
    browseable = no
    writeable = yes
    create mask = 0600
    directory mask = 0700

[public]
    comment = Répertoire Commun Users
    path = /home/samba/partage
    public = yes
    writable = yes
    printable = no
    write list = @users

```

Le logon script dans cet exemple permet de monter un lecteur réseau appelé Public sous la lettre P:

Voici son contenu :

```
net use P: \\pdc-linux\public
```

Il faut donner le mot de passe du Manager LDAP à Samba pour qu'il puisse écrire dans l'annuaire :

```
pdg:/home/user# smbpasswd -w mypassword
Setting stored password for "cn=Manager,dc=alex,dc=fr" in secrets.tdb
```

Vampirisation du controleur NT4

Créez un fichier appelé initial.ldif sur le PDC qui contiendra les informations nécessaires au fonctionnement de votre annuaire LDAP.

Vous disposez aussi d'outils avec le package **smbldap-tools** (voir [Smbldap-tools](#)) pour créer les informations initiales dans votre annuaire LDAP et administrer facilement la création, modification et l'effacement de comptes.

Sinon pour des consoles graphiques, utilisez **une interface de gestion** comme GQ, web avec [LAM](#) et [phpLDAPadmin](#) ou java comme [Xplorer](#).

```
dn: dc=alex,dc=fr
dc: alex
objectClass: top
objectClass: dcObject
objectClass: domain
objectClass: domainRelatedObject
associatedDomain: alex.fr
description: Serveur OpenLDAP alex

# admin, alex.fr
dn: cn=admin,dc=alex,dc=fr
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: administrateur annuaire LDAP
userPassword:: e2NyeXB01ga57VElZN2h3cmM=

dn: ou=People,dc=alex,dc=fr
ou: People
objectClass: top
objectClass: organizationalUnit
objectClass: domainRelatedObject
associatedDomain: alex.fr
description: Utilisateurs du Domaine

dn: ou=Group,dc=alex,dc=fr
ou: Group
objectClass: top
objectClass: organizationalUnit
objectClass: domainRelatedObject
associatedDomain: alex.fr
description: Groupes du Domaine

dn: ou=Hosts,dc=alex,dc=fr
ou: Hosts
objectClass: top
objectClass: organizationalUnit
objectClass: domainRelatedObject
associatedDomain: alex.fr
description: Hosts du Domaine
```

Ajoutez le dans l'annuaire OpenLDAP :

```
pdc:/home/user# slapadd -v -l initial.ldif
added: "dc=alex,dc=fr" (00000001)
```

```
added: "cn=admin,dc=alex,dc=fr" (00000002)
added: "ou=People,dc=alex,dc=fr" (00000003)
added: "ou=Group,dc=alex,dc=fr" (00000004)
added: "ou=Hosts,dc=alex,dc=fr" (00000005)
```

Sous **Mandrake** vérifiez les droits sur les fichiers dans /var/lib/ldap/ :
[root@pdc root]# chown ldap:ldap -R /var/lib/ldap

Démarrez OpenLDAP et Samba :

```
pdc:/home/user# /etc/init.d/slaped start
Starting OpenLDAP: slapd.
```

```
pdc:/home/user# /etc/init.d/samba start
Starting Samba daemons: nmbd smbd.
```

Vérifiez que vous résolvez bien le nom NetBIOS du contrôleur de domaine NT4 :

```
pdc:/home/user# ping -c 2 wint4
PING wint4 (192.168.0.x) 56(84) bytes of data.
64 bytes from wint4 (192.168.0.x): icmp_seq=1 ttl=128 time=0.264 ms
```

On importe le SID du domaine WINALEXNT4 dans Samba :

```
pdc:/home/user# net rpc getsid -S wint4 -W winalexnt4
Storing SID S-1-5-21-2119976258-140979070-1538882281 for Domain WINALEXNT4
in secrets.tdb
```

Copiez le SID dans **/etc/smbldap-tools/smbldap.conf** pour Debian ou **/etc/samba/smbldap_conf.pm** pour Mandrake.

On rejoint le domaine WINALEXNT4 :

```
pdc:/home/user# net rpc join -S wint4 -W winalexnt4 -U
administrateur%mot2passeNT4
Joined domain WINALEXNT4.
```

On vampirise le contrôleur NT4 :

```
pdc:/home/user# net rpc vampire -S wint4
Fetching DOMAIN database
SAM_DELTA_DOMAIN_INFO not handled
Creating unix group: 'Admins du domaine'
Creating unix group: 'Utilisa. du domaine'
Creating unix group: 'Invités du domaine'
Creating account: Administrateur
Creating account: Invité
Use of uninitialized value in pattern match (m//) at
/usr/sbin/smbldap_tools.pm line 677, <DATA> line 283.
/usr/sbin/smbldap-usermod.pl: group Invit\C3\A9s du domaine doesn't exist
Creating account: WINT4$
Creating account: user1
Creating account: user2
Creating account: pdc-linux$
Group members of Admins du domaine: Administrateur,
adding user Administrateur to group Admins du domaine
```

```
Group members of Utilisa. du domaine: Administrateur(primary),WINT4$(primary),user1(primary),user2(primary),pdc-linux$(primary),
Group members of Invit\C3\A9s du domaine: Invite,
/usr/sbin/smbldap-groupmod.pl: group Invit\C3\A9s du domaine not found!
Fetching BUILTIN database
SAM_DELTA_DOMAIN_INFO not handled
Creating unix group: 'Administrateurs'
Creating unix group: 'Duplicateurs'
Creating unix group: 'Invités'
Creating unix group: 'Opérateurs d'impression'
Creating unix group: 'Opérateurs de compte'
Creating unix group: 'Opérateurs de sauvegarde'
Creating unix group: 'Opérateurs de serveur'
Creating unix group: 'Utilisateurs'
pdc:/home/user#
```

Comme vous pouvez le voir dans l'exemple ci-dessus, il peut y avoir quelques bugs ...

Affichez le résultat de la vampirisation :

```
pdc:/home/user# ldapsearch -x -D "cn=Manager,dc=alex,dc=fr" -w mypassword
-b "dc=alex,dc=fr"
```

Il faut maintenant éteindre le contrôleur NT4 et passer Samba comme contrôleur principal. Modifiez /etc/smb.conf en mettant :
domain master et preferred master à yes.

Relancez Samba.

Créez un compte POSIX (avec un UID=0) et validez le dans Samba pour que vos stations Windows puissent rejoindre le domaine. (voir "[Un utilisateur \(UID=0\) pour rejoindre votre domaine](#)")

Samba-3.0.* vous permet de réaliser un mappage entre les groupes UNIX et les groupes Windows. (voir "[Mappage des groupes](#)").

Document mis à jour : 07/05/07