

EOLE AD DC - T che #37308

Sc nario # 37288 (Nouveau): Traitement express MEN en cours (sc nario de remplacement)

Suggestions d'am liorations smb.conf

28/01/2026 05:17 - Laurent Brillard

Statut:	En cours	D�but:	28/01/2026
Priorit�:	Normal	Ech�ance:	
Assign� �:	Klaas TJEBBES	% r�alis�:	0%
Version cible:	Carnet MENSr	Temps estim�:	0.00 heure
		Temps pass�:	0.00 heure
Description Bonjour � tous, Sur un Scribe 2.8 / Seth 2.8 d'un lyc�e, les ouvertures de sessions sont souvent tr�s longues (plusieurs minutes). Un administrateur nous fait une suggestion de modification du fichier smb.conf dans lequel il y a peut-�tre des param�tres pertinents. Nous restons � votre disposition pour �changer sur ce sujet. <pre>##### # # CONFIGURATION SAMBA - EOLE 2.8 # # OBJECTIFS : # 1. Corriger les erreurs de configuration existantes # 2. R�duire significativement le temps de logon # 3. Maintenir la compatibilit� avec l'infrastructure existante # # STRUCTURE : # [FIX] = Correction critique (appliquer imm�diatement) # [OPT] = Optimisation (tester avant d�ploiement complet) # [INFO] = Information / contexte # ##### [global] # ===== IDENTIFICATION ===== realm = 974NNNNX.AD.IN.AC-REUNION.FR netbios name = S-LYC-NNNNX workgroup = 974NNNNX server string = Serveur Scribe - EOLE 2.8 # ===== PROTOCOLE RESEAU ===== disable netbios = yes ; [FIX] NetBIOS obsol�te et lent smb ports = 445 ; [INFO] SMB direct over TCP # ===== ACTIVE DIRECTORY ===== security = ADS ; [INFO] Int�gration Active Directory # Mapping Windows SID � Linux UID/GID idmap config *:backend = tdb ; [INFO] Backend par d�faut idmap config *:range = 2000-9999 ; [INFO] Plage locale idmap config 974NNNNX:backend = rid ; [FIX] Mapping d�terministe (RID) idmap config 974NNNNX:range = 10000-999999 ; [INFO] Plage pour 1400 comptes # ===== WINBIND (INT�GRATION AD) ===== winbind use default domain = yes # CORRECTION CRITIQUE - Gain majeur de performance winbind enum users = no ; [FIX] �vite l'�num�ration compl�te de l'AD</pre>			

```

winbind enum groups = no ; [FIX] Réduction charge CPU de 60-80%

winbind refresh tickets = yes ; [INFO] Actualisation des tickets Kerberos
template homedir = /home/adhomes/%U ; [INFO] Chemin des répertoires utilisateurs

# ===== PROTOCOLE SMB =====
# FORCER SMB2/SMB3 - Sécurité + Performance
server min protocol = SMB2_02 ; [FIX] Bloque SMB1 obsolète
server max protocol = SMB3 ; [FIX] Force protocole moderne

# ===== AUDIT ET LOGS =====
# Audit des connexions Samba
vfs objects = full_audit recycle ; [FIX] Suppression du doublon
full_audit:prefix = %T|%u|%h|%U|%I ; [INFO] Format du préfixe de log
full_audit:success = connect ; [INFO] Logue les connexions réussies
full_audit:failure = none ; [INFO] Pas de log pour les échecs
full_audit:priority = NOTICE ; [INFO] Niveau de priorité

# ===== IMPRESSION =====
printing = cups
printcap name = cups
load printers = yes
show add printer wizard = yes
cups server = localhost:631 ; [FIX] Correction syntaxe (ancien: socket:port)

# ===== GESTION DES SESSIONS =====
time server = yes ; [INFO] Serveur de temps pour les clients
deadtime = 30 ; [FIX] 30min au lieu de 15 (évite déco en pause)

# ===== SÉCURITÉ ET PERMISSIONS =====
usershare max shares = 0 ; [INFO] Désactive les partages utilisateurs
unix extensions = no ; [INFO] Compatibilité Windows
nt acl support = yes ; [INFO] Support des ACL Windows
wide links = yes ; [INFO] Autorise les liens symboliques
acl allow execute always = True ; [INFO] Permet l'exécution via ACL

# ===== ATTRIBUTS DOS/WINDOWS =====
# Essentiel pour la cohérence des profils itinérants
ea support = no ; [FIX] Désactive les attributs étendus Linux
store dos attributes = yes ; [FIX] Stocke hidden/system/archive
map archive = no ; [FIX] Windows gère nativement
map hidden = no ; [FIX] Windows gère nativement
map system = no ; [FIX] Windows gère nativement
map readonly = no ; [FIX] Complément pour cohérence

# ===== FICHIERS SYSTÈME WINDOWS =====
hide files = /desktop.ini/ ; [INFO] Masque les fichiers système Windows
delete veto files = yes ; [INFO] Supprime les fichiers interdits
veto files = /$RECYCLE.BIN/ ; [INFO] Bloque la corbeille Windows

# ===== ADMINISTRATION =====
admin users = @"Domain Admins" ; [INFO] Administrateurs du domaine
interfaces = lo ens3 ; [INFO] Interfaces réseau à écouter

# ===== FICHIERS INCLUS =====
include = /etc/samba/recycle.conf ; [INFO] Configuration de la corbeille Samba

[printers]
# ===== PARTAGE IMPRIMANTES =====
comment = All Printers
path = /var/spool/samba
printable = yes
browseable = yes
available = yes

[print$]
# ===== DRIVERS IMPRIMANTES =====

```

```

comment = Printer Drivers
path = /var/lib/samba/printers
browseable = yes
read only = yes
valid users = @"Print Operators" @"Authenticated Users" @"Domain Users"
write list = @"Print Operators" @"Domain Admins"
create mask = 0664
directory mask = 0775
force group = "root"
vfs objects =                                ; [INFO] Écrase vfs global pour ce partage

[homes]
# ===== RÉPERTOIRES PERSONNELS =====
comment = Répertoire personnel
path = /home/adhomes/%U                      ; [INFO] Variable %U = nom d'utilisateur
browseable = no                              ; [INFO] Non visible dans l'explorateur
read only = no                               ; [INFO] Accès en écriture
valid users = %U                             ; [INFO] Seul l'utilisateur concerné

# Création automatique du répertoire
root preexec = /usr/share/eole/sbin/create_adhome "%U" "/home/adhomes"

# Héritage des permissions
inherit permissions = yes
inherit acls = yes
create mask = 0664
directory mask = 0775

# Désactivation du cache client (CRITIQUE pour profils itinérants)
csc policy = disable                          ; [FIX] Évite la mise en cache locale

# Masquage des fichiers système
hide files = /desktop.ini/config_eole/

# ===== OPTIMISATIONS PROFILS ITINÉRANTS =====
# CORRECTION : Oplocks désactivé uniquement sur [homes]
# Anciennement en [global], cela pénalisait tous les partages
oplocks = no                                ; [FIX] Conflits avec NTUSER.DAT
kernel oplocks = no                         ; [FIX] Verrous noyau
level2 oplocks = no                         ; [FIX] Verrous niveau 2

# ===== OPTIMISATIONS AVANCÉES (À TESTER) =====
# DÉCOMMENTER SEULEMENT APRÈS MESURE DE BASELINE
#
# strict locking = no                        ; [OPT] Gain: 10-40% logon
# posix locking = no                        ; [OPT] Windows gère ses propres verrous
# aio read size = 0                         ; [OPT] Active AIO pour tous les fichiers
# aio write size = 0                       ; [OPT] Améliore les E/S asynchrones
# read raw = yes                           ; [OPT] Pas de buffering Samba
# write raw = yes                           ; [OPT] Réduction latence
# dos filetime resolution = yes             ; [OPT] Granularité 2s (Windows)
# dos filemode = yes                       ; [OPT] Permet modif permissions depuis Windows

# ===== PARTAGES SPÉCIFIQUES =====
include = /etc/samba/conf.d/partage-linux.conf
include = /etc/samba/conf.d/eole.conf
include = /etc/samba/conf.d/nextcloud.conf

#####
# PROCÉDURE PRÉPARATION
#####

# ÉTAPE 1 : PRÉPARATION (5 minutes)
# -----
# 1. Backup de l'ancienne configuration :
#   cp /etc/samba/smb.conf /etc/samba/smb.conf.backup_$(date +%Y%m%d_%H%M%S)
#

```

```

# 2. Copier cette configuration :
#   nano /etc/samba/smb.conf
#   (coller le contenu ci-dessus)
#
# 3. Valider la syntaxe :
#   testparm -s
#   (DOIT retourner "Load smb config files from /etc/samba/smb.conf" sans erreur)

# ÉTAPE 2 : VÉRIFICATIONS (5 minutes)
# -----
# 4. Vérifier les paramètres critiques :
#   testparm -s | grep -E "winbind enum|server min|oplocks|deadtime|cups server"
#
# RÉSULTATS ATTENDUS :
#   winbind enum users = No
#   winbind enum groups = No
#   server min protocol = SMB2_02
#   server max protocol = SMB3
#   deadtime = 30
#   cups server = localhost:631
#   oplocks = No      (uniquement dans [homes])
#
# 5. Vérifier les inclusions existent :
#   ls -la /etc/samba/conf.d/*.conf
#   ls -la /etc/samba/recycle.conf

# ÉTAPE 3 : DÉPLOIEMENT (2 minutes)
# -----
# 6. Redémarrer Samba :
#   systemctl restart smbd
#   (nmbd n'est plus nécessaire avec disable netbios = yes)
#
# 7. Vérifier le statut :
#   systemctl status smbd
#   journalctl -u smbd -n 20

# ÉTAPE 4 : SURVEILLANCE (30 minutes)
# -----
# 8. Surveiller les logs en temps réel :
#   tail -f /var/log/samba/log.smbd | grep -E "(connect|failed|error)"
#
# 9. Vérifier la charge serveur :
#   top -b -n 1 | grep winbindd
#   (La charge CPU doit être significativement réduite)
#
# 10. Tester la connexion (sur un poste client) :
#   net use \\S-LYC-NNNNX\IPC$ /user:VotreUtilisateur
#   (DOIT fonctionner sans erreur)

# ÉTAPE 5 : TESTS UTILISATEURS (1 jour)
# -----
# 11. Sélectionner 5 utilisateurs tests :
#   - 1 administrateur
#   - 2 enseignants
#   - 2 élèves
#
# 12. Mesurer le temps de logon AVANT/APRÈS :
#   Sur Windows : Event Viewer → Windows Logs → Security
#   Chercher EventID 4624 (Logon réussi) et noter l'heure
#
# 13. Vérifier :
#   - Aucun profil temporaire créé
#   - Les fichiers personnels accessibles
#   - Les impressions fonctionnent

#####
# MESURE DES PERFORMANCES

```

```
#####
# MÉTHODE DE MESURE SIMPLIFIÉE :
#
# 1. AVANT déploiement (baseline) :
#   Sur 3 postes tests, chronométrer manuellement :
#   - Du clic sur "OK" après mot de passe
#   - Jusqu'au bureau complètement chargé
#   Notez les 3 temps, calculez la moyenne : X secondes
#
# 2. APRÈS déploiement (mêmes postes) :
#   Refaites la mesure : Y secondes
#
# 3. CALCUL du gain :
#   Gain = ((X - Y) / X) * 100
#
#   RÉSULTATS ATTENDUS :
#   - Minimum : -10% (amélioration légère)
#   - Typique : -30% à -50%
#   - Exceptionnel : -60% à -80%
#
#####
# OPTIMISATIONS AVANCÉES (PHASE 2)
#####
# UNIQUEMENT SI :
# 1. Les corrections [FIX] sont déployées
# 2. Le gain est inférieur à -30%
# 3. La charge serveur est toujours élevée
#
# PROCÉDURE :
# 1. Dans [homes], décommenter les 8 lignes [OPT]
# 2. Redémarrer : systemctl restart smbd
# 3. Mesurer à nouveau pendant 3 jours
# 4. Analyser :
#   - Si gain supplémentaire > 25% → Garder
#   - Si gain faible (< 10%) → Recommander
#
#####
# DÉPANNAGE RAPIDE
#####
# PROBLÈME : "Accès refusé" sur homes
# SOLUTION : Vérifier les permissions sur /home/adhomes/
#   chmod 755 /home/adhomes
#   chown root:root /home/adhomes
#
# PROBLÈME : Impression ne fonctionne pas
# SOLUTION : Vérifier CUPS
#   systemctl status cups
#   lpstat -t
#
# PROBLÈME : Temps de logon toujours long
# SOLUTION : Investiguer autre cause
#   - GPO Windows (gpresult /h)
#   - Scripts de logon (Event Viewer)
#   - DNS (nslookup S-LYC-NNNNX)
#   - Taille des profils (> 500MB = problème)
#
# PROBLÈME : Rollback nécessaire
# SOLUTION :
#   cp /etc/samba/smb.conf.backup_* /etc/samba/smb.conf
#   systemctl restart smbd
#
#####
# CONTACTS ET RESSOURCES
#####
```

```
# En cas de problème :
# 1. Consulter les logs : /var/log/samba/log.smbd
# 2. Documentation EOLE : https://wiki.eole.education/
# 3. Forum Samba : https://lists.samba.org/
```

```
# Suivi des modifications :
# Date : [Date]
# Modifications : [Liste des changements]
# Responsable : [Nom]
# Résultats : [Gain mesuré]
```

```
#####
# NOTES FINALES
#####
```

```
# Cette configuration apporte :
# 1. Corrections immédiates (gain garanti)
# 2. Organisation claire (maintenance facile)
# 3. Procédures documentées (reproductible)
# 4. Mesures concrètes (décision basée sur les données)
```

```
# Temps estimé pour le déploiement complet :
# - Phase 1 (corrections) : 15-30 minutes
# - Phase 2 (optimisations) : 3-5 jours de tests
```

Historique

#1 - 09/02/2026 15:12 - Klaas TJEBBES

```
# CORRECTION CRITIQUE - Gain majeur de performance
winbind enum users = no ; [FIX] Évite l'énumération complète de l'AD
winbind enum groups = no ; [FIX] Réduction charge CPU de 60-80%
```

Il y a une variable dans `gen_config` "`%%ad_enum_users_groups`"

Sur DC1 elle est à "non"
Sur File elle est à "oui"

Placé à "yes", cela peut effectivement entraîner des lenteurs.

```
deadtime = 30 ; [FIX] 30min au lieu de 15 (évite déco en pause)
```

Il y a une variable dans `gen_config` "`%%ad_deadtime`"

On peut éventuellement revoir la valeur par défaut dans la mesure où une récréation d'établissement scolaire dure 20 minutes. 30 minutes semble une durée adaptée car elle intègre les 20 minutes de récréation + 5 minutes avant et 5 minutes après.

```
ea support = no ; [FIX] Désactive les attributs étendus Linux
```

Non, "ea support" indique que les attributs étendus sont pris en charge au niveau du protocole SMB. Que l'option soit "yes" ou "no", le backend utilise les attributs étendus "xattr" de toutes façons.

<https://lists.samba.org/archive/samba-technical/2020-November/136053.html>

De nos jours, ce paramètre configure uniquement le comportement au niveau SMB, c'est-à-dire si le protocole prend en charge les attributs étendus (EA). Il existe différentes manières pour un client d'obtenir la liste, de lire et de définir des EA via SMB. En définissant « `ea support = no` », toutes ces opérations échoueront avec une erreur, probablement `NT_STATUS_NOT_SUPPORTED`.

Cependant, même avec « ea support = no » défini, Samba utilisera toujours xattr en arrière-plan comme espace de stockage pour diverses données telles que les attributs DOS, la date de création, les listes de contrôle d'accès (ACL), etc.

Je n'ai trouvé aucune information indiquant que la désactivation de cette option apporte un gain en performance.

```
store dos attributes = yes ; [FIX] Stocke hidden/system/archive
```

C'est déjà la valeur par défaut

```
map archive = no ; [FIX] Windows gère nativement
map hidden = no ; [FIX] Windows gère nativement
map system = no ; [FIX] Windows gère nativement
map readonly = no ; [FIX] Complément pour cohérence
```

La page MAN SMB.CONF dit : Note that this parameter will be ignored if the store dos attributes parameter is set.

Comme "store dos attributes" est à "yes" par défaut, les 3 options "map *" sont ignorées.

```
# ===== OPTIMISATIONS PROFILS ITINÉRANTS =====
# CORRECTION : Oplocks désactivé uniquement sur [homes]
# Anciennement en [global], cela pénalisait tous les partages
oplocks = no ; [FIX] Conflits avec NTUSER.DAT
kernel oplocks = no ; [FIX] Verrous noyau
level2 oplocks = no ; [FIX] Verrous niveau 2
```

"oplocks" sur "/home" pourrait être à étudier.

Selon <https://lists.samba.org/archive/samba/2017-January/206133.html>

il est même possible que :

Having roaming profiles (defined in the user object in LDB)...

Seemingly at random smbd keeps locks on NTUSER.DAT and ntuser.ini for a random time (from minutes to over 2 hours).

In this time it is not possible for the user affected to login any more (from any machine).

Error is: "The User Profile Service failed the sign-in"

The only solution is to call me and I kill then the process on the server.

À noter qu'il parle de Windows 7 et 8.1, et que depuis Microsoft a peut-être corrigé le problème "quand on arrête/éteint Windows, la procédure de logoff n'est pas correctement terminée".

#2 - 10/02/2026 09:25 - Joël Cuissinat

- *Tracker changé de Demande à Tâche*
- *Statut changé de Nouveau à En cours*
- *Assigné à mis à Klaas TJEBBES*
- *Tâche parente mis à #37288*