Guide de Dépannage Samba/Zentyal

UAC — Synchronisation LDAP Multi-Sites

Universités Publiques du Bénin — Mars 2026

1. Contexte et Architecture

UAC (Université d'Abomey-Calavi) déploie Zentyal/Samba4 comme Active Directory multi-sites. Chaque site distant dispose d'un DC (Domain Controller) qui réplique la base LDAP centrale depuis le rectorat.

Site	Hostname	IP	Statut
Rectorat (maître)	uacpdc.uac.bj	10.24.112.33	✓ Opérationnel
FSS	fsspdc.uac.bj	10.17.112.33	✓ Opérationnel
IMSP	imsppdc.uac.bj	10.16.112.33	✓ Opérationnel
ENEAM	eneampdc.uac.bj	10.18.112.33	■ À investiguer
ENS Porto-Novo	ensportopdc.uac.bj	-	■ Hors ligne

2. Problèmes Identifiés

2.1 DNS pollué par les interfaces virtuelles

Docker et les interfaces VLAN s'enregistrent automatiquement dans le DNS Samba au démarrage. Chaque DC accumule des dizaines d'IPs parasites pour son propre hostname, ce qui bloque la résolution NetBIOS et fait boucler les commandes samba-tool.

2.2 Base LDAP désynchronisée après restauration

Une restauration de base crée un décalage de numéros USN (Update Sequence Numbers). Les DCs distants peuvent croire être à jour alors qu'ils manquent des milliers de changements. L'erreur typique est WERR_DS_DRA_ACCESS_DENIED ou des timeouts RPC.

2.3 Réplication lente sur liaisons WAN

Samba réplique la partition complète sur tous les DCs. Un --full-sync sur 105k objets via un lien à 600ms de latence provoque systématiquement des timeouts (WERR_SEM_TIMEOUT, Device Timeout).

3. Référence des Outils et Commandes

3.1 wbinfo — Winbind Information

wbinfo est l'outil de diagnostic de Winbind, le service qui fait le pont entre Linux/PAM et le domaine Active Directory. Il permet de tester l'authentification, lister les utilisateurs et vérifier la communication avec le DC.

Commande	Rôle
wbinfo -u	Lister tous les utilisateurs du domaine
wbinfo -g	Lister tous les groupes du domaine
wbinfo -i <user>	Voir les infos d'un utilisateur (UID, GID, shell)

wbinfo -c	Renouveler le mot de passe machine (trust secret) À faire après un domain join ou une restauration
wbinfo -a "dom\\user%pass"	Tester l'authentification d'un utilisateur (plaintext + challenge/response)
wbinfo --ping-dc	Tester la connectivité avec le DC

3.2 samba-tool drs — Directory Replication Services

Outil principal de gestion de la réplication AD. DRS (Directory Replication Service) est le protocole utilisé par les DCs pour synchroniser leurs bases.

Commande	Rôle
samba-tool drs showrepl	Afficher l'état de toutes les réplications (succès, échecs, dernière synchro)
samba-tool drs showrepl <IP>	Afficher l'état de réplication d'un DC distant
samba-tool drs kcc	Forcer le KCC (Knowledge Consistency Checker) à recalculer la topologie de réplication
samba-tool drs replicate <dest> <src> <NC>	Déclencher une réplication d'une partition Exemple : DC=uac,DC=bj
samba-tool drs replicate ... --full-sync	Forcer une réplication complète (ignore les USNs) Attention : très lent sur WAN

3.3 samba-tool dns — Gestion DNS

Commande	Rôle
samba-tool dns query <server> <zone> <name> A	Lister les enregistrements A d'un hostname
samba-tool dns delete <server> <zone> <name> A <IP>	Supprimer un enregistrement A parasite
samba-tool dns add <server> <zone> <name> A <IP>	Ajouter un enregistrement A

3.4 ldbsearch / ldbmodify — Accès direct à la base LDB

LDB est le format de base de données interne de Samba (similaire à LDAP). Ces outils permettent d'accéder et modifier directement sam.ldb sans passer par le protocole réseau.

Commande	Rôle
ldbsearch -H /var/lib/samba/private/sam.ldb -b "CN=Sites,..." "(objectClass=siteLink)" dn replInterval	Rechercher un objet dans la base locale (ici : trouver l'intervalle de réplication)
ldbmodify -H /var/lib/samba/private/sam.ldb /tmp/fichier.ldif	Modifier un objet via un fichier LDIF

4. Procédures Opérationnelles

4.1 Nettoyer les IPs parasites dans le DNS Samba

À faire après chaque redémarrage de Samba jusqu'à mise en place du cron. Remplacer par le nom du DC (ex: uacpdc, imsppdc, fsspdc).

```
# 1. Lister les IPs enregistrées
samba-tool dns query 127.0.0.1 uac.bj <HOSTNAME> A -U administrator

# 2. Supprimer les IPs parasites (garder uniquement l'IP WAN légitime)
for IP in 10.xx.0.2 10.xx.64.2 172.17.0.1 172.18.0.1; do
  samba-tool dns delete 127.0.0.1 uac.bj <HOSTNAME> A $IP -U administrator%<PASSWORD>
done

# 3. Vérifier — doit retourner une seule IP
samba-tool dns query 127.0.0.1 uac.bj <HOSTNAME> A -U administrator
```

4.2 Fixer le template smb.conf.mas (permanent)

Zentyal régénère smb.conf à chaque redémarrage depuis son template. Il faut modifier le template natif pour exclure les interfaces Docker et virtuelles.

```
# Éditer le template natif
nano /usr/share/zentyal/stubs/samba/smb.conf.mas

# Trouver le bloc suivant et modifier :
% if ($ifaces) {
    interfaces = lo bond1 bond0 vlan101 vlan102 vlan103 vlan111 vlan112 vlan113
#interfaces = <% $ifaces %>     # commenter la ligne originale     bind
interfaces only = yes % }

# Adapter la liste des interfaces selon le site :
# - Rectorat : bond1 bond0 + vlan101 à vlan114
# - IMSP     : bond1 bond0 + vlan101 vlan102 vlan103 vlan111 vlan112 vlan113
# - FSS      : bond1 bond0 + vlan101 vlan102 vlan103 vlan111 vlan112 vlan113
# NE PAS inclure : eth0 eth1 eth2 eth3 virbr0 docker0 172.x.x.x

# Régénérer et redémarrer
systemctl restart zentyal
systemctl restart samba-ad-dc
```

■ Ne pas créer de fichier stub dans /etc/zentyal/stubs/samba/smb.conf.mas avec seulement quelques lignes — il remplacerait complètement le template natif et générerait un smb.conf tronqué (Server role: ROLE_STANDALONE).

4.3 Resynchroniser un DC distant — Domain Join propre

C'est la méthode recommandée pour resynchroniser un DC dont la base est corrompue ou désynchronisée. Elle reconstruit une identité DC propre sans conflit USN.

```
# Sur le DC distant (SSH)
systemctl stop samba-ad-dc

# Sauvegarder l'ancienne base
mv /var/lib/samba/private /var/lib/samba/private.bak.$(date +%Y%m%d)
rm -rf /var/lib/samba/private

# Rejoindre le domaine depuis le rectorat samba-
tool domain join uac.bj DC \   --
server=10.24.112.33 \
  -U administrator \   --dns-
backend=SAMBA_INTERNAL

# Démarrer Samba
systemctl start samba-ad-dc
systemctl status samba-ad-dc
```

```
# Resynchroniser le mot de passe machine
wbinfo -c

# Tester l'authentification
wbinfo -a "uac\\administrator%<PASSWORD>"
```

Après le join, le showrepl peut ne pas encore afficher UACPDC en voisin — le KCC prend quelques minutes pour recalculer la topologie.

4.4 Réduire l'intervalle de réplication

Par défaut à 180 minutes (3h). Réduire à 15 minutes (minimum Samba) pour une synchronisation plus réactive.

```
# Vérifier l'intervalle actuel
ldbsearch -H /var/lib/samba/private/sam.ldb \
-b "CN=Sites,CN=Configuration,DC=uac,DC=bj" \
  "(objectClass=siteLink)" dn replInterval

# Créer le fichier de modification LDIF
cat > /tmp/replinterval.ldif << EOF
dn: CN=DEFAULTIPSITELINK,CN=IP,CN=Inter-Site Transports,CN=Sites,CN=Configuration,DC=uac,DC=bj
changetype: modify replace: replInterval replInterval: 15 EOF

# Appliquer
ldbmodify -H /var/lib/samba/private/sam.ldb /tmp/replinterval.ldif
```

4.5 Vérifier et réparer l'intégrité de la base

```
# Vérification (lecture seule, sans modifier) samba-
tool dbcheck --cross-ncs

# Réparation automatique
samba-tool dbcheck --cross-ncs --fix --yes

# Résultat normal : "Checked X objects (0 errors)"
```

4.6 Cron de nettoyage DNS automatique (à mettre en place)

À appliquer sur chaque DC pour éviter l'accumulation d'IPs parasites après chaque redémarrage de Samba.

```
# Créer le script de nettoyage
cat > /usr/local/bin/clean-samba-dns.sh << 'EOF'
#!/bin/bash
PASS="<PASSWORD>"
HOSTNAME="uacpdc"        # adapter : uacpdc / imsppdc / fsspdc / eneam
LEGIT="10.24.112.33"     # adapter : IP WAN légitime du DC
ZONE="uac.bj"

for IP in $(samba-tool dns query 127.0.0.1 $ZONE $HOSTNAME A \             -U
administrator%$PASS 2>/dev/null | grep "^    A:" | awk '{print $2}'); do   if [ "$IP"
!= "$LEGIT" ]; then
    samba-tool dns delete 127.0.0.1 $ZONE $HOSTNAME A $IP -U administrator%$PASS
fi done EOF

chmod +x /usr/local/bin/clean-samba-dns.sh

# Ajouter au cron
cat > /etc/cron.d/samba-dns-clean << EOF # Nettoyage DNS
Samba — toutes les 30 minutes et au démarrage
@reboot root sleep 30 && /usr/local/bin/clean-samba-dns.sh
*/30 * * * * root /usr/local/bin/clean-samba-dns.sh
EOF
```

5. Codes d'Erreur Courants

Code	Signification	Solution
WERR_SEM_TIMEOUT (121)	Timeout réseau — le DC distant ne répond pas dans le délai	Vérifier ping + ports 135/389 Vérifier si le serveur est allumé
WERR_DS_DRA_ACCESS_DE	NIED (8453)Réplication refusée Base corrompue ou permissions cassées	samba-tool dbcheck --fix sur le DC source Puis redémarrer samba-ad-dc
WERR_DS_DRA_INTERNAL_E	RROR (8442)Erreur interne DRS Service de réplication cassé	dbcheck --fix + restart samba-ad-dc
NT_STATUS_WRONG_PASS	ORDMauvais mot de passe ou trust secret désynchronisé	wbinfo -c pour resync le trust Ou samba-tool user setpassword
LDAP_INVALID_CREDENTIAL	(49)Credentials incorrects Compte verrouillé ou mot de passe expiré	Vérifier le compte avec samba-tool user show Réinitialiser le mot de passe
Device Timeout	I/O timeout sur lien WAN lent Typique avec --full-sync sur 100k+ objets	Utiliser domain join au lieu de drs replicate Ou lancer depuis le DC distant (pull)
Server role: ROLE_STANDALO	Nsmb.conf tronqué Le template .mas est incomplet	Supprimer /etc/zentyal/stubs/samba/smb.conf.mas puis restart zentyal

6. Checklist — Nouveau DC ou DC à Resynchroniser

Étape 1 — Vérifier la connectivité réseau

```
ping <IP_DC> nc -
zv <IP_DC> 389
nc -zv <IP_DC> 135
```

Étape 2 — Vérifier le DNS du DC (ne doit avoir qu'une seule IP)

```
samba-tool dns query 127.0.0.1 uac.bj <hostname> A -U administrator
```

Étape 3 — Nettoyer les IPs parasites si nécessaire

```
Voir procédure 4.1
```

Étape 4 — Lancer le domain join depuis le DC distant

```
Voir procédure 4.3
```

Étape 5 — Fixer smb.conf.mas pour éviter le retour des IPs parasites

```
Voir procédure 4.2
```

Étape 6 — Resynchroniser le mot de passe machine

```
wbinfo -c
```

Étape 7 — Tester l'authentification

```
wbinfo -a "uac\administrator%<PASSWORD>"
```

Étape 8 — Vérifier la réplication

```
samba-tool drs showrepl
```

Étape 9 — Installer le cron de nettoyage DNS

```
Voir procédure 4.6
```

7. Concepts Clés

7.1 USN — Update Sequence Number

Compteur entier incrémenté localement sur chaque DC à chaque modification (création, suppression, changement d'attribut). Lors de la réplication, un DC demande : 'donne-moi tout ce qui a changé depuis mon USN X'. Après une restauration, les USNs sont désynchronisés — un DC peut croire être à jour alors qu'il manque des milliers de changements. Le domain join résout ce problème en repartant de zéro avec un USN initial cohérent.

7.2 KCC — Knowledge Consistency Checker

Service Samba qui calcule automatiquement la topologie de réplication entre DCs. Il crée et maintient les objets de connexion (Connection Objects) qui définissent quels DCs répliquent depuis quels autres DCs. La commande 'samba-tool drs kcc' force un recalcul immédiat.

7.3 Partitions AD répliquées

Partition	Contenu
DC=uac,DC=bj	Objets du domaine : utilisateurs, groupes, ordinateurs La plus volumineuse — 122k+ objets pour UAC
CN=Configuration,DC=uac,DC=bj	Configuration de la forêt : sites, services, schéma de réplication
CN=Schema,CN=Configuration,DC=uac,	C=bjDéfinition des classes et attributs LDAP
DC=DomainDnsZones,DC=uac,DC=bj	Enregistrements DNS spécifiques au domaine
DC=ForestDnsZones,DC=uac,DC=bj	Enregistrements DNS de la forêt entière