Distribution EOLE - Tâche #37468

Scénario # 37402 (Terminé (Sprint)): Porter Seth en 2.11

Etude samba

19/05/2026 14:27 - Ludwig Seys

Statut:	Fermé	**Début:**	01/10/2022
Priorité:	Normal	**Echéance:**	
Assigné à:	Ludwig Seys	**% réalisé:**	100%
Version cible:	Livraison Cadoles - MEN 30/04/2026 (30)	**Temps estimé:**	0.00 heure

Description

Historique

#1 - 19/05/2026 14:27 - Ludwig Seys

- Statut changé de Nouveau à En cours

#2 - 19/05/2026 14:37 - Ludwig Seys

Après lecture des release notes Samba 4.23 et 4.24 et comparaison avec les templates smb.conf dc1,dc2 et dc3, aucune adaptation obligatoire n'a été identifiée pour le passage à Samba 4.23.
Pour Samba 4.24, aucune incompatibilité directe n'a été identifiée, mais plusieurs nouveaux paramètres KDC/sécurité apparaissent.
Les défauts restent compatibles CEPENDANT un choix est à faire si on souhaite forcer les recommandations Samba 4.24, notamment ```kdc require canonicalization = yes.```
Point de vigilance : Samba 4.23 active smb3 unix extensions par défaut. Aucun changement requis pour les DC purs, mais un test rapide serait pertinent sur les partages fichiers homes/profiles exposés par DC3.

impact 4.23

Changement 4.23	Impact sur tes templates
`smb3 unix extensions` activé par défaut	Pas bloquant. À surveiller seulement pour les partages fichiers, surtout `homes` / `profiles` sur DC3
SMB3 over QUIC	Aucun impact, sauf si on veut l'activer
timestamp `last_write_time` mis à jour immédiatement	Changement de comportement, pas de template à adapter
nouveaux paramètres `client smb transports`, `server smb transports`, `smbd profiling share`, `winbind varlink service`	Rien à ajouter, réglé par défaut

Samba 4.24 introduit plusieurs paramètres KDC/PKINIT/certificats :

```
strong certificate binding enforcement = full
certificate backdating compensation = 0
kdc always include pac = yes
kdc require canonicalization = no
kdc name match implicit dollar without canonicalization = yes
```

Il change aussi la valeur par défaut de :

```
kdc default domain supported enctypes
```

qui passe vers les types AES par défaut si le niveau fonctionnel du domaine le permet.

Dans notre cas, le domaine est en niveau fonctionnel 2008 R2 d'après dc1, un changement peut être pertinent, et provoquerait un changement de comportement Kerberos/chiffrement.

Samba recommande notamment :

```
strong certificate binding enforcement = full
kdc always include pac = yes
kdc require canonicalization = yes
```

Mais kdc require canonicalization reste à no par défaut pour compatibilité, et ubuntu 26 passe en samba 23 candidate.

Donc à décider. (pour aide cf : https://www.samba.org/samba/history/samba-4.24.0.html)

#3 - 21/05/2026 12:25 - Gilles Grandgérard

Bonjour Ludwig

Je suis d'accord avec tes commentaires.
Nous devons chercher à fournir un module Seth 2.11 le plus à jour possible avec les recommandations.

Il n'y a que le "kdc default domain supported enctypes" qui pourrait être sensible...

Donc, tu as mon Go.

#4 - 05/06/2026 11:56 - Ludwig Seys

- Statut changé de En cours à À valider

#5 - 05/06/2026 16:11 - Ludwig Seys

- Statut changé de À valider à Résolu

#6 - 17/08/2026 09:52 - Joël Cuissinat

- Statut changé de Résolu à Fermé

- % réalisé changé de 0 à 100

- Restant à faire (heures) mis à 0.0