Quand samba danse le Mambo

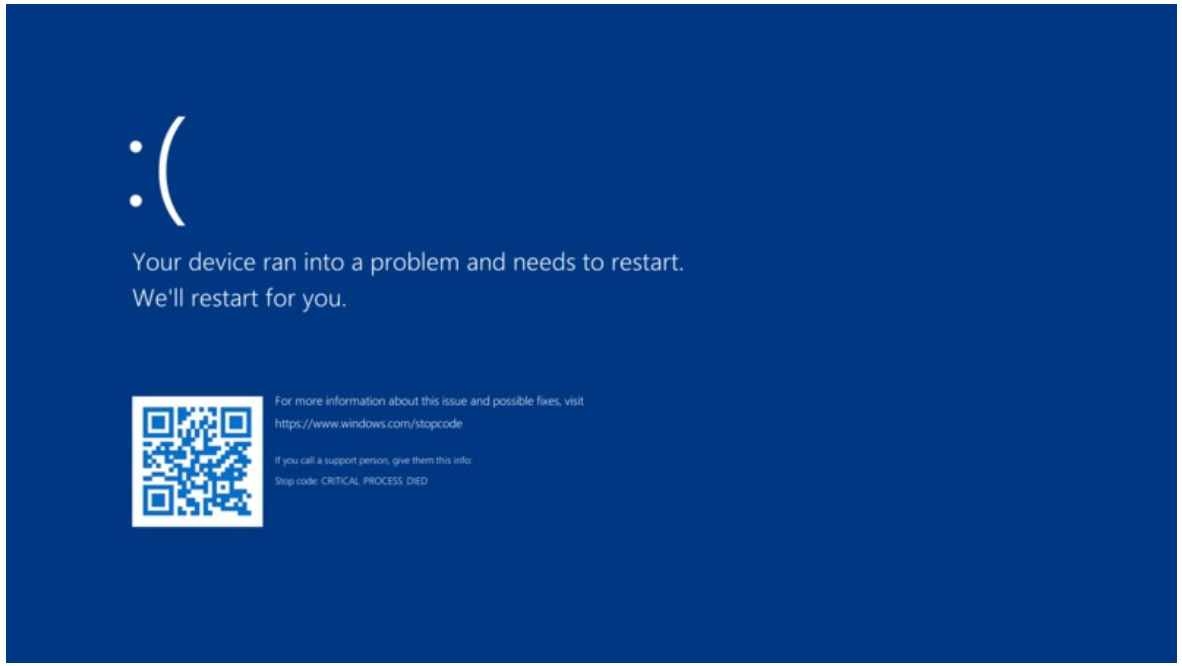
histoire d'une migration vers Samba 4 AD

Centrale Méditerranée

...ou comment passer de

ça

à ça



Centrale Méditerranée

Rappel : NT 4

Apparu en 1996 avec la sortie de Windows NT 4.0, il est composé de :

- Un Primary Domain Controler (rw)
- Un/des Backup Domain Controler (ro)

Ils possèdent tous un partage ***netlogon*** pour les logon scripts

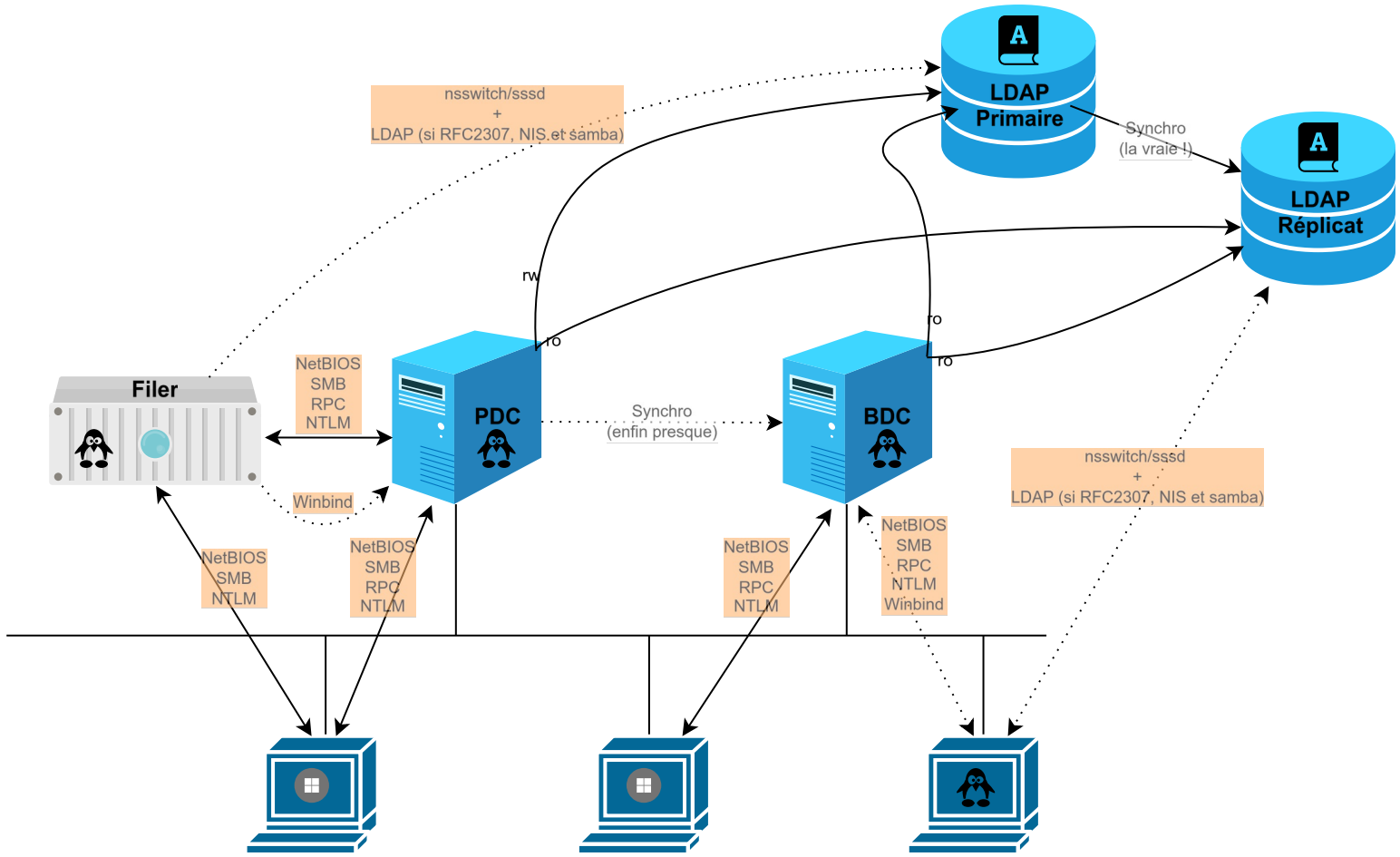
Il s'appuie entre autre sur :

- La base **SAM**, un fichier local que seul le PDC peut écrire
- **WINS** (1994) qui gère la résolution NetBIOS
- **SMB** (CIFS 1996) pour le partage de fichiers
- **NT NetLogon** pour l'authentification (v2 1998)

Pas de **LDAP** jusqu'à la sortie de Windows 2000 et samba 3.0 (2003)

Centrale Méditerranée

Rappel : Samba NT 4



Centrale Méditerranée

Samba 4 AD

Sorti en le 11 décembre 2012, enfin une compatibilité avec Active Directory, il se compose de :

- Contrôleurs de Domaine tous en rw* avec

En plus du partage ***netlogon*** le partage ***sysvol*** fait son apparition pour les stratégies de groupe

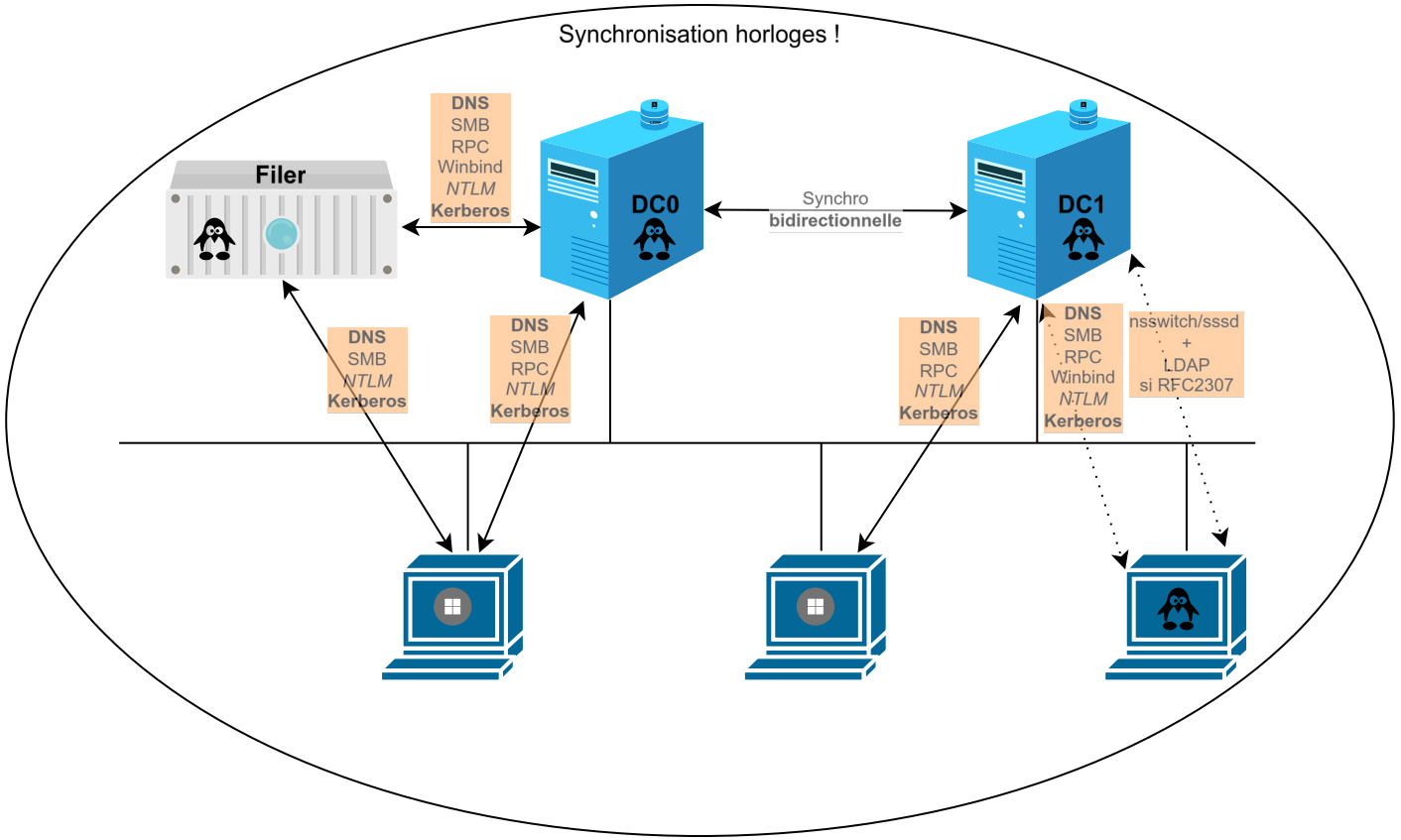
Il s'appuie entre autre sur :

- **LDAP** intégré aux DCs
- Le **DNS** qui « remplace » **NetBIOS**
- **SMB** pour le partage de fichiers
- **NTLM** toujours présent
- **Kerberos** devient le système d'authentification principal

La synchronisation des horloges devient essentielle !

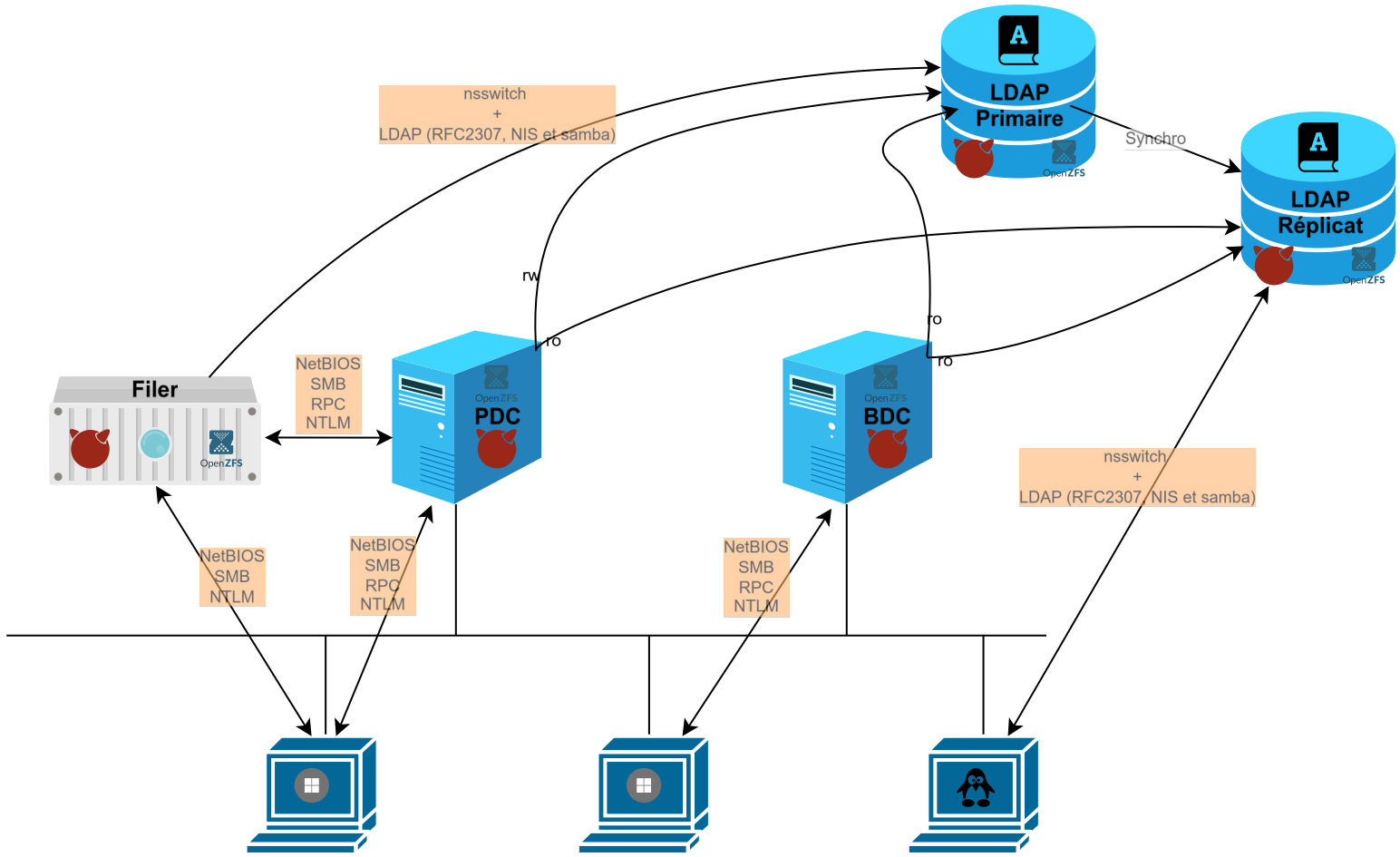
Centrale Méditerranée

Samba 4 AD



Centrale Méditerranée

Samba NT4 à Centrale



Centrale Méditerranée

Objectifs migration

- Migration transparente pour les utilisateurs :
  - méthode « classicupgrade »
  - Ansible
  - tester, retester et retester encore...

- Les mondes Unix et Windows restent « séparés » mais compatibles
  - les Unix se réfèrent à OpenLDAP
  - les Windows à Samba AD

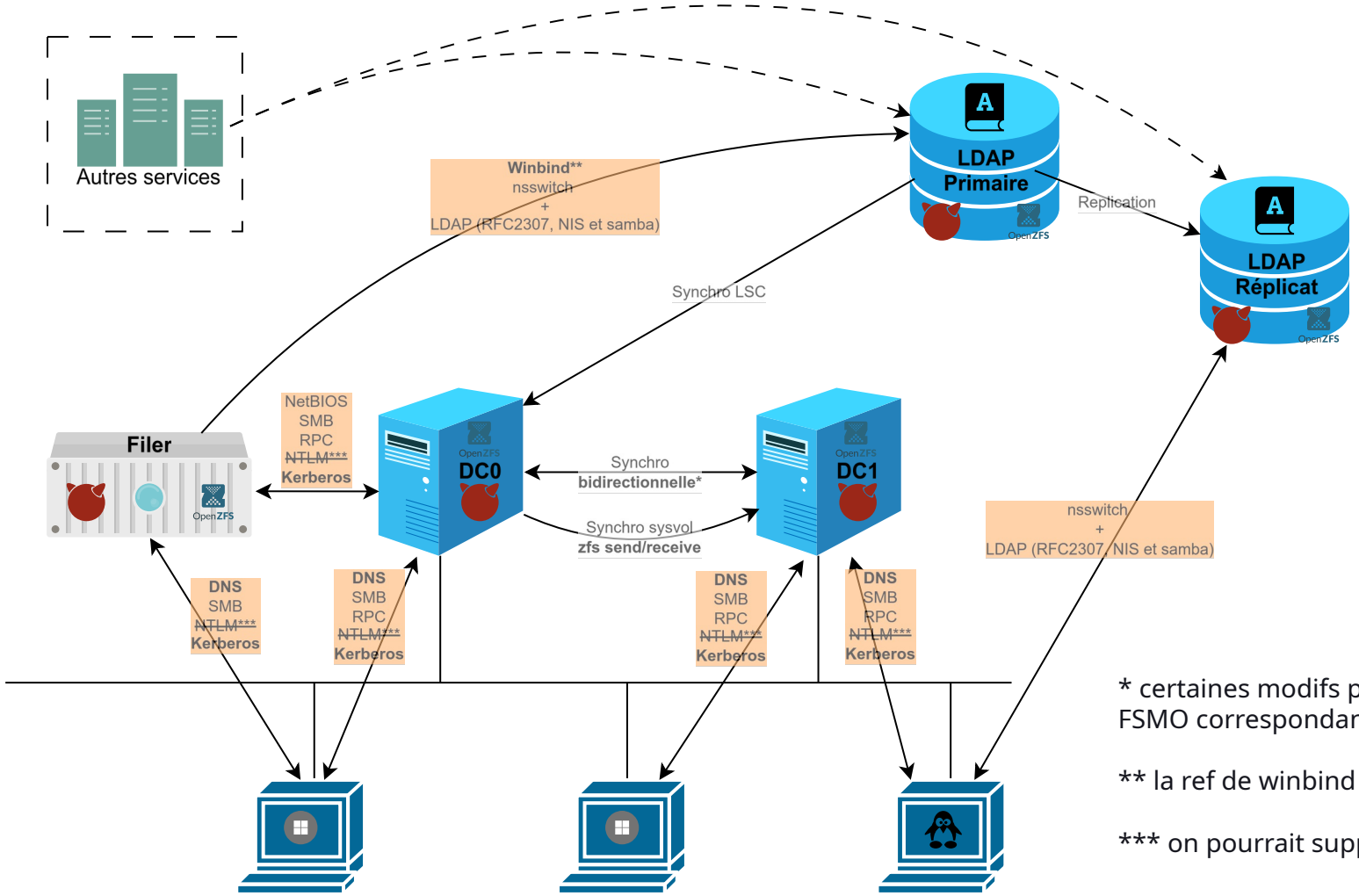
- Les serveurs OpenLDAP sont la référence (users et groupes)
  - synchro OpenLDAP -> Samba AD (LSC)
  - les filers : se réfèrent à OpenLDAP avec idmap nss** (winbind ??)

- On s’appuie sur les technos utilisées et maîtrisées (ZFS...) :
  - synchro sysvol avec ZFS send/receive

- On génère les logon scripts à la connexion :
  - Pas de synchro de netlogon > netlogon séparé

Centrale Méditerranée

Samba 4 AD à Centrale



* certaines modifs passent par le DC ayant le rôle FSMO correspondant

** la ref de winbind c'est ldap !

*** on pourrait supprimer NTLM !

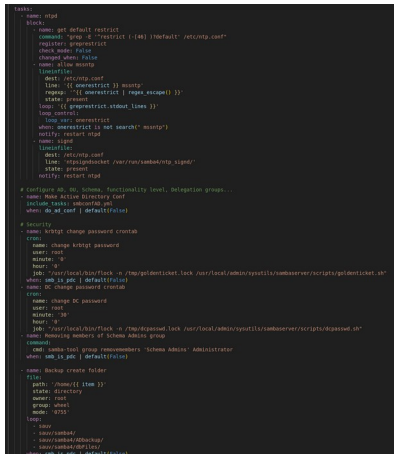
Centrale Méditerranée

Ça se passe comment la migration ?

```python
#!/usr/bin/python
# A quick and dirty python script that checks for duplicate SID's using slapcat.
import os

data = os.popen("slapcat 2>&1 | grep sambaSID", 'r')
line = []

def anydup(thelist):
        dups = list(set([x for x in thelist if thelist.count(x) > 1]))
        for i in dups:
                print("Duplicate id: ", i)

for each_line in data:
        line.append(each_line.strip())

anydup(line)
```

1. traquer et résoudre les collisions de SID
2. redirection DNS
3. un playbook ansible de préparation :
   - mettre les *.tdb nécessaires au classicupgrade dans un dossier temporaire
   - mettre smb.conf dans un autre dossier temporaire
4. le classicupgrade
5. définir mdp Administrateur
6. placer krb5.conf
7. ACL sur le netlogon : getfacl <sysvol> | setfacl -d -M- <netlogon>
8. on lance samba et on teste un peu
9. on lance un playbook pour configurer notre samba et connecter l'autre DC
10. synchro de idmap.ldb puis tests sur l'autre DC
11. les filers et cups sont toujours ok mais on adapte la conf : playbook ! Et on teste
12. déplacement des objets dans les bonnes OU
13. mise en place des délégations de droits et création des users admins et exploit
14. ssp : playbook encore, on teste (hashes pour kerberos !)
15. première synchro LSC (forcée)... on teste !
16. Restaurer les GPO créées dans l'infra test, les adapter... tester
17. nettoyer les comptes admin
18. bières ou lexomil ???

```
samba-tool domain classicupgrade  --dbdir=/root/migrationtmp/dbdir/ \
--realm={{ samba.domain|upper }} --dns-backend=SAMBA_INTERNAL \
/root/migrationtmp/etc/smb4.conf
```



Centrale Méditerranée

Focus sur : les difficultés

- Des filers qui se réfèrent à ldap : « backend = nss »

```
Oct 31 14:11:31 fou winbindd[36328]:   tdb(/var/db/samba4/winbindd_idmap.tdb): tdb_transaction_commit: transaction error pending
Oct 31 14:11:31 fou winbindd[36328]:   Error allocating a new GID
Oct 31 14:11:31 fou winbindd[36328]:   tdb(/var/db/samba4/winbindd_idmap.tdb): tdb_transaction_commit: transaction error pending
Oct 31 14:11:31 fou winbindd[36328]:   Error allocating a new GID
Oct 31 14:11:31 fou winbindd[36328]:   tdb(/var/db/samba4/winbindd_idmap.tdb): tdb_transaction_commit: transaction error pending
Oct 31 14:11:31 fou winbindd[36328]:   Error allocating a new GID
```

- ZFS et les ACL
  - La configuration du zfs pour sysvol :
    - aclmode: passthrough
    - aclinherit: passthrough
    - acltype: nfsv4
  - la configuration de samba
    - "winbind enum users = 'yes'" dans la section [global]
    - "nfs4:acedup = merge" dans les sections [sysvol] et [netloggon]
    - "nfs4:chown = 'yes'" dans les sections [sysvol] et [netloggon]

- idmap.tdb : refaire le mappage, re-mapper Administrator à 0, sysvolreset

- Doucement sur le hardening : les GPO

Stratégie	Paramètre
Sécurité réseau : Configurer les types de chiffrement autorisés pour Kerberos	Activé
DES_CBC_CRC	Désactivé
DES_CBC_MD5	Désactivé
RC4_HMAC_MD5	Désactivé
AES128_HMAC_SHA1	Activé
AES256_HMAC_SHA1	Activé
Futurs types de chiffrement	Activé

- Le bug qui tue sysvol (Bugzilla 15733) : Attention à « include » !

Focus sur : la synchronisation

LDAP Synchronisation Connector (https://lsc-project.org/)

- Un outils qui permet de synchroniser des objets et attributs entre des bases ldap
- On synchronise les users et les groups
- On transforme certains attributs
- On ne peut pas synchroniser les mots de passe !

Self Service Password (https://ltb-project.org)

Il modifie le mot de passe sur l'OpenLDAP et via un prehook script celui de l'AD

Centrale Méditerranée

Focus sur : la sécurité

Les sources Wiki Samba Hardening Samba Tranquil IT Fonctionnalités avancées

- Classicupgrade : seul les HashNT (unicodePwd) -> RC4_HMAC_MD5 pour Kerberos
- Délégations : segmenter les droits de manière fine !
- Les GPO pour la sécurité
- Les hashes et protocoles faibles (NetLogon, NTLM1, SMB1...)
- Supprimer NTLM2 : c’est possible !

Centrale Méditerranée

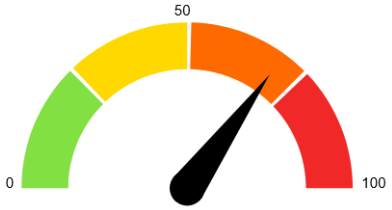
PingCastle

Quoi ?? 70 !!!

Active Directory Indicators

This section focuses on the core security indicators.
Locate the sub-process determining the score and fix some rules in that area to get a score improvement.

Indicators

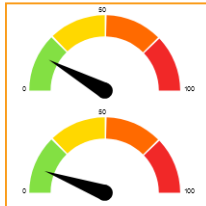


Domain Risk Level: 70 / 100

It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better

Compare with statistics

Privacy notice

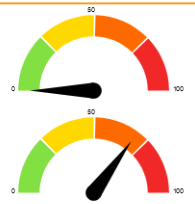


Stale Object : 16 /100 — 9 rules matched

It is about operations related to user or computer objects

Privileged Accounts : 11 /100 — 3 rules matched

It is about administrators of the Active Directory



Trusts : 0 /100 — 0 rules matched

It is about connections between two Active Directories

Anomalies : 70 /100 — 11 rules matched

It is about specific security control points

Anomalies analysis

Anomalies : 70 /100

It is about specific security control points

Anomalies rule details [11 rules matched on a total of 72]

[redacted]	[redacted]
[redacted]	[redacted]
~~Last AD backup has been performed 235 day(s) ago~~	*+ 15 Point(s)*
~~The audit policy on domain controllers does not collect key events~~	*+ 10 Point(s)*

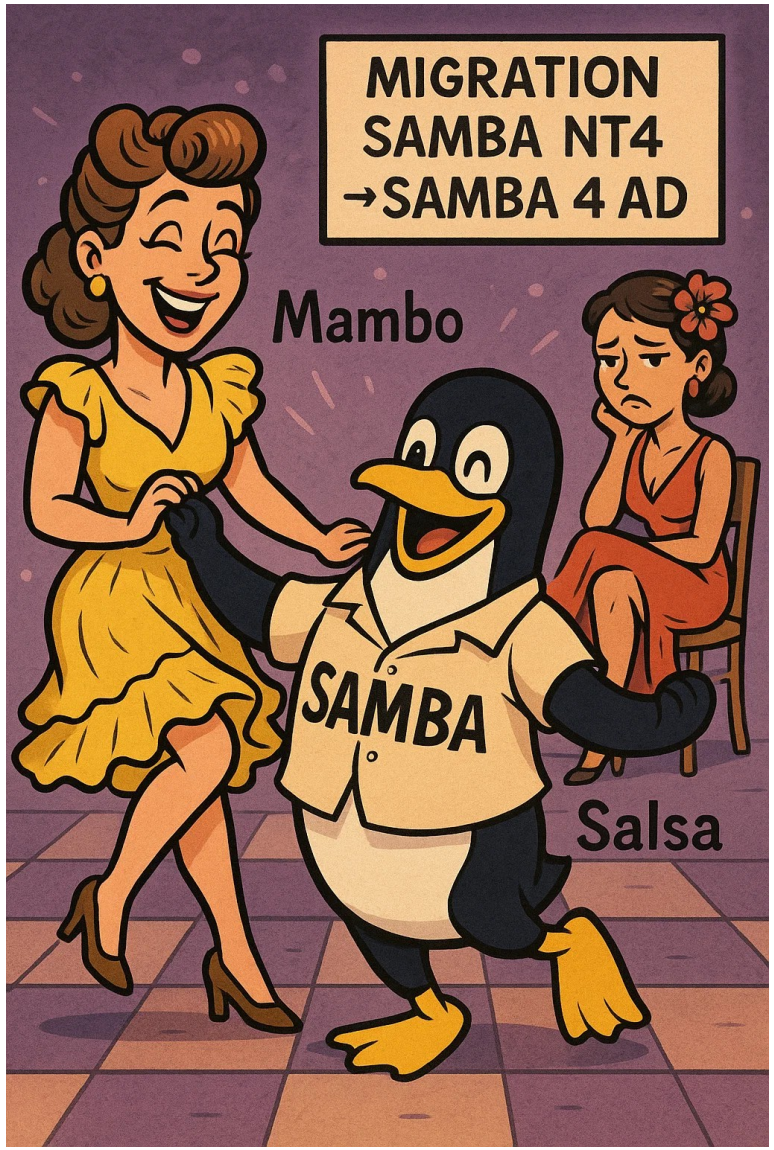
Mais c'est samba !
Les backups sont fait : -15
Audit Policy sur DC : -10

45 !

Vous me faites confiance !

Centrale Méditerranée

Bienvenu sur MAMBO



Vous n’avez rien compris ?
Relisez la prés, relisez-la encore une dernière fois...
puis contactez-moi, ;-)

Merci...

Centrale Méditerranée