Compte rendu technique

Mission 7 : Mise en place du serveur de fichiers NAS
Mission 8 : Automatisation des paramètres grâce aux GPO

Contexte : entreprise RIOCA (groupe 3)

Réalisé par Maxime FOREST et Souhir ZAIMI

Sommaire

1. Introduction aux besoins
2. Étude comparative
3. Mise en place du serveur NAS (mission 7)
4. Automatisation par GPO (mission 8)
5. Tests
6. Difficultés rencontrées
7. Conclusion

1. Introduction aux besoins

L'entreprise RIOCA dispose d'un hyperviseur Hyper-V, d'un contrôleur de domaine Active Directory (srv-ad-rioca, 172.19.100.2) et de postes clients joints au domaine RIOCA.local. Il lui manque un serveur de fichiers pour stocker les dossiers des utilisateurs et des services.

La mission 7 consiste à installer un NAS sur un serveur physique Dell PowerEdge T140 avec un stockage en RAID 1, à le joindre au domaine et à créer quatre partages SMB. La mission 8 automatise ensuite la configuration des postes par GPO : mappage des lecteurs, fond d'écran imposé, blocage du panneau de configuration et déploiement de Firefox et VLC.

Partage	Usage	Droits demandés
Dossiers personnels	Un dossier par utilisateur	Utilisateur propriétaire de son dossier, admins du domaine en contrôle total
Collaboratif	Un dossier par service	Groupe du service en lecture/écriture, admins en contrôle total
Outils	Installeurs des logiciels	Tout le monde en lecture, admins en contrôle total
Sauvegardes	Sauvegardes des systèmes	Admins du domaine uniquement

Machine	Rôle	Adresse IP
srv-ad-rioca	Contrôleur de domaine, DNS, serveur de temps	172.19.100.2
srv-nas-3	Serveur NAS	172.19.100.3/24
PC-USER-GRP3	Poste client (OU ORDINATEURS/PCs, port authentifié en 802.1X)	DHCP (172.19.60.4)

2. Étude comparative

Critère	TrueNAS Community Edition	OpenMediaVault	Windows Server
Licence	Gratuit, open source	Gratuit, open source	Payant (licence serveur + CAL)
Prérequis	8 Go de RAM (ECC conseillée), SSD de boot	Très léger	2 Go de RAM, 32 Go de disque
RAID 1	Miroir ZFS ou RAID matériel	RAID logiciel (mdadm) ou matériel	RAID matériel ou espaces de stockage
Jonction AD	Depuis l'interface web	Manuelle (Samba/winbind)	Native

Critère	TrueNAS Community Edition	OpenMediaVault	Windows Server
Partages et ACL	SMB + éditeur d'ACL type Windows	SMB, ACL limitées	Partages + ACL NTFS
Snapshots	Snapshots ZFS planifiables	Via plugins	VSS, Windows Server Backup

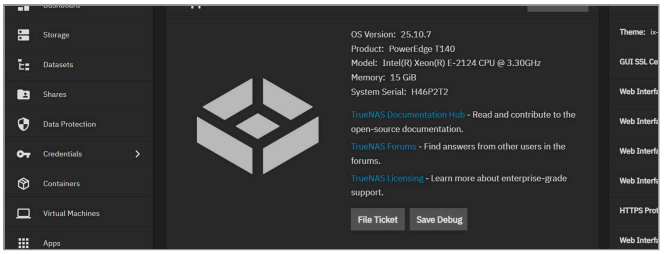
Solution retenue : TrueNAS Community Edition 25.10.7. C'est un système dédié au stockage, gratuit, qui permet de joindre le domaine et de gérer les ACL de type Windows depuis son interface. Le serveur (Xeon E-2124, 15 Go de RAM ECC) dépasse ses prérequis. Windows Server a été écarté car il est payant et généraliste, et OpenMediaVault car sa jonction à l'Active Directory n'est pas intégrée.

Pour le RAID 1, TrueNAS conseille un miroir ZFS. À la demande du professeur, nous avons utilisé le RAID matériel du contrôleur Dell PERC H330 : le miroir est géré par le contrôleur et TrueNAS voit un seul disque.

3. Mise en place du serveur NAS (mission 7)

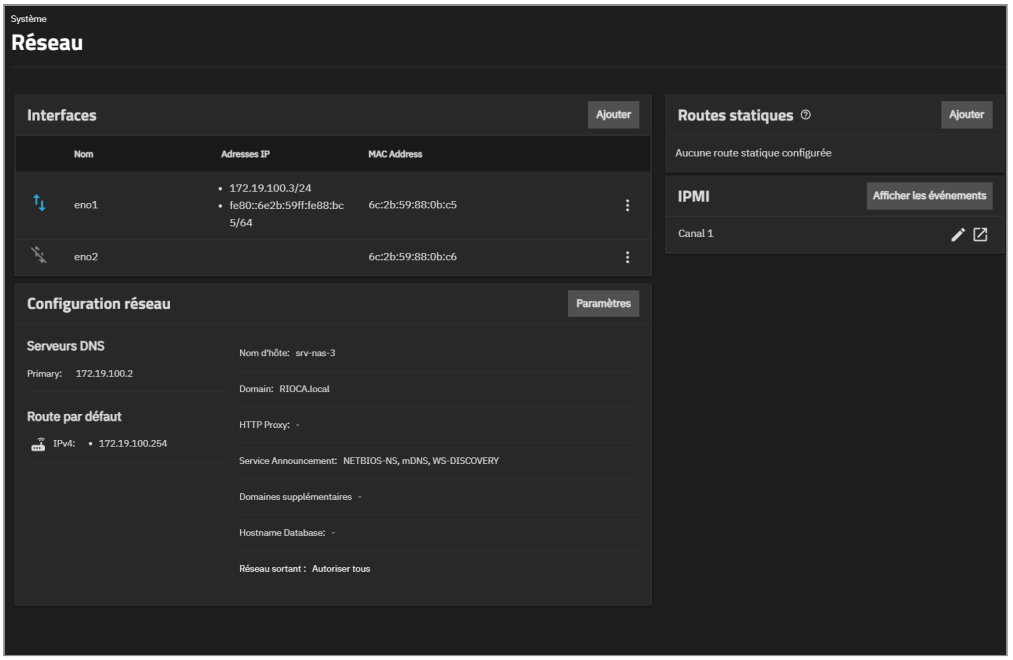
3.1 Installation et configuration réseau

TrueNAS a été installé depuis une clé USB créée avec Rufus (GPT/UEFI) sur le SSD de 240 Go. Le réseau a été configuré depuis la console puis vérifié dans l'interface web.



Capture 1 : Version de TrueNAS, modèle et numéro de série du serveur

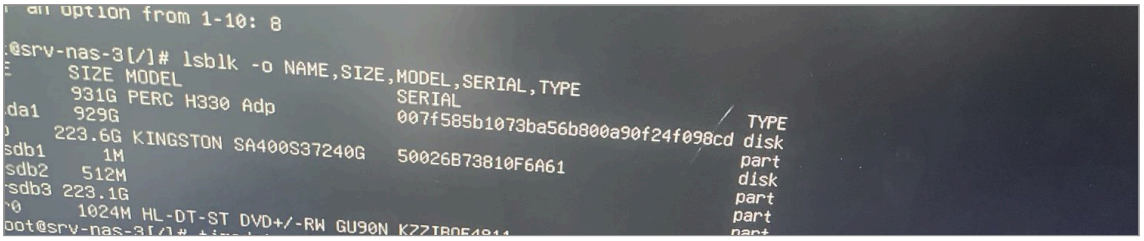
Élément	Valeur
Serveur	Dell PowerEdge T140 (n° de série H46P2T2)
Système	TrueNAS CE 25.10.7 « Goldeye »
Nom d'hôte	srv-nas-3
IP (eno1)	172.19.100.3/24
Passerelle	172.19.100.254
DNS	172.19.100.2 (DC), pas de secondaire
NTP	172.19.100.2 (DC)



Capture 2 : Configuration réseau du NAS : eno1 en 172.19.100.3/24, DNS, passerelle, nom d'hôte et domaine

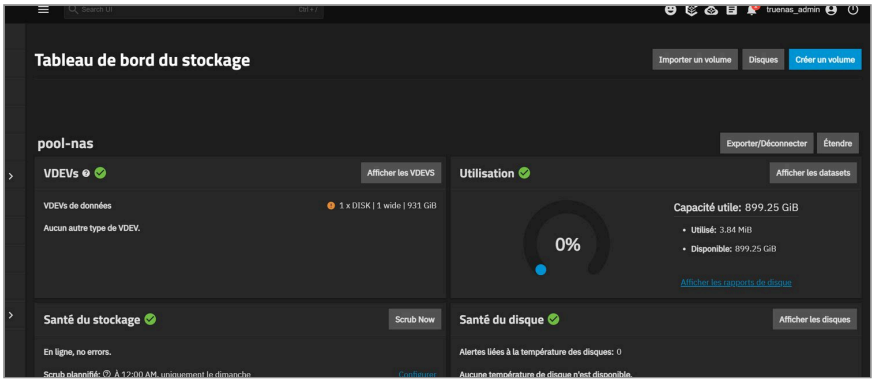
3.2 RAID 1 et pool de stockage

Le serveur contient un SSD Kingston de 240 Go (système) et deux disques SATA de 1 To (HGST HUS722T1TALA600 et Seagate ST1000NM0018). Dans l'utilitaire du contrôleur (F2 → Device Settings → PERC H330), les deux disques ont été regroupés dans un disque virtuel **VD-NAS en RAID 1** de 931 Go. TrueNAS ne voit alors qu'un seul disque « PERC H330 Adp ».



Capture 3 : lsblk : le disque virtuel RAID 1 de 931 Go et le SSD système

Le pool `pool-nas` a été créé sur ce disque en disposition Stripe, puisque la redondance est déjà assurée par le contrôleur. Il offre **899 Go utiles**.

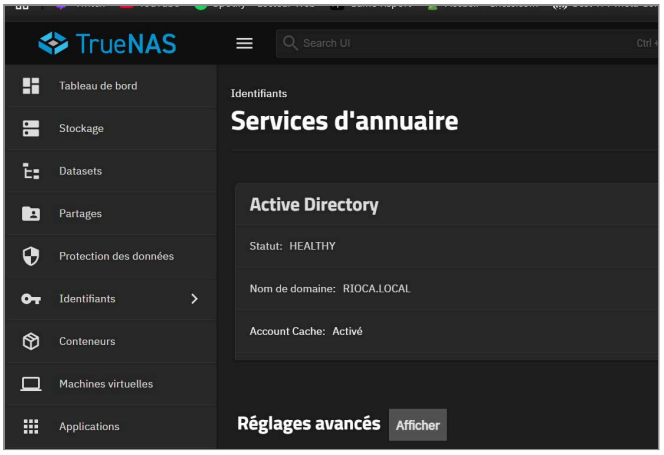


Capture 4 : Pool pool-nas en ligne, 899,25 Gio utiles

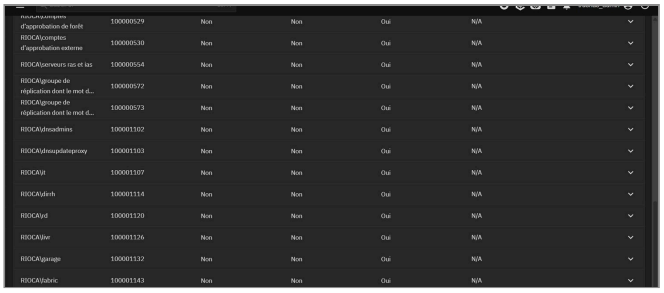
3.3 Jonction au domaine

Dans Identifiants → Services d'annuaire, le NAS a été joint au domaine RIOCA.local avec le compte administrateur du domaine. Les utilisateurs et groupes de l'AD sont ensuite lisibles par TrueNAS, ce qui permet

de les utiliser dans les ACL.



Capture 5 : Active Directory à l'état HEALTHY



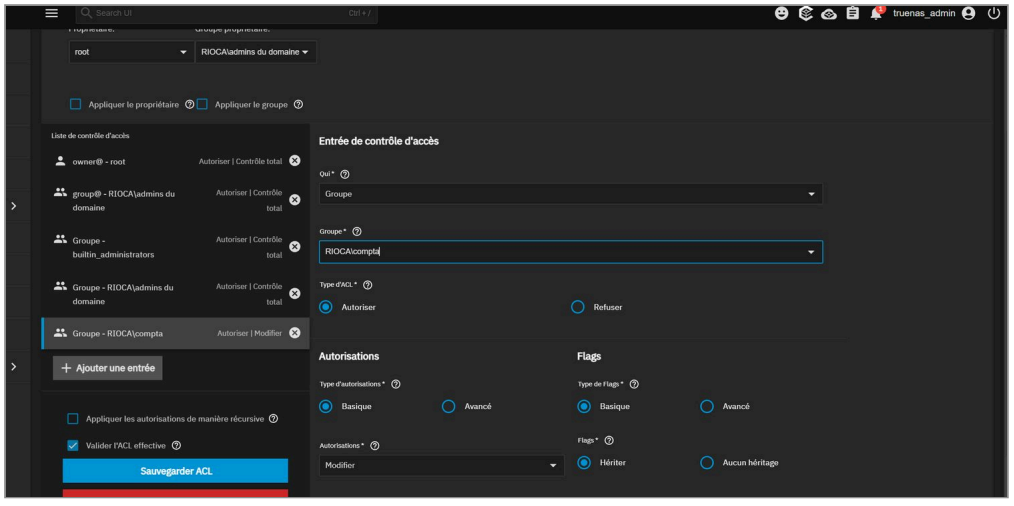
Capture 6 : Groupes de service de l'AD visibles dans TrueNAS

3.4 Datasets, droits et partages

Un dataset a été créé pour chaque partage avec le préréglage SMB, et un sous-dataset par service dans collaboratif (compta, dirrh, fabric, garage, it, livr, rd). Les droits suivants ont été appliqués dans l'éditeur d'ACL :

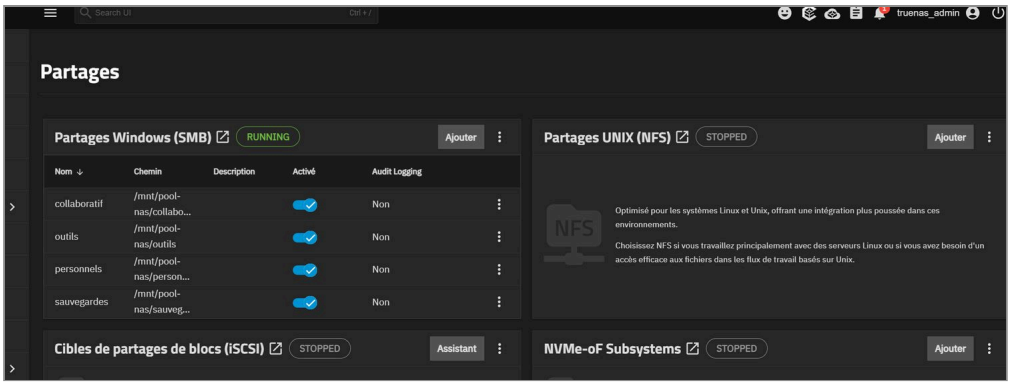
Dataset	Admins du domaine	Autres droits
sauvegardes	Contrôle total	Aucun
outils	Contrôle total	Utilisateurs et ordinateurs du domaine : lecture
collaboratif	Contrôle total	Utilisateurs du domaine : lecture, sans héritage
collaboratif/<service>	Contrôle total	Groupe du service : modifier (lecture/écriture)
personnels	Contrôle total	Utilisateurs du domaine : lecture, sans héritage
personnels/<utilisateur>	Contrôle total	L'utilisateur : propriétaire, contrôle total

Les utilisateurs ont la lecture sans héritage à la racine de collaboratif et personnels pour pouvoir ouvrir le partage, sans obtenir de droits dans les sous-dossiers. Les ordinateurs du domaine lisent outils car l'installation des logiciels par GPO se fait avec le compte de l'ordinateur. L'ACL du dossier compta est donnée en exemple ; la même a été appliquée aux six autres services avec leur groupe.



Capture 7 : ACL de collaboratif/compta : groupe RIOCA\compta en « Modifier »

Les quatre partages SMB ont été créés avec l'option **Access Based Share Enumeration**, qui n'affiche à un utilisateur que les dossiers auxquels il a accès.



Capture 8 : Les quatre partages SMB actifs

3.5 Dossiers personnels

Dans Utilisateurs et ordinateurs Active Directory, le dossier de base des utilisateurs de chaque OU a été défini sur `\\srv-nas-3\personnels\%username%`, ce qui crée automatiquement leur dossier. Chaque utilisateur a ensuite été rendu propriétaire de son dossier depuis le shell du NAS :

```
for d in /mnt/pool-nas/personnels/*/; do sudo chown "RIOCA\\$(basename "$d")" "$d"; done
```

```
total 374
drwxrwx--- 2 RIOCA\abdel      RIOCA\admins du domaine 2 Oct 15 13:43 abdel
drwxrwx--- 2 RIOCA\achille    RIOCA\admins du domaine 2 Oct 15 13:43 achille
drwxrwx--- 2 RIOCA\angel      RIOCA\admins du domaine 2 Oct 15 13:44 angel
drwxrwx--- 2 RIOCA\aymen      RIOCA\admins du domaine 2 Oct 15 13:43 aymen
drwxrwx--- 2 RIOCA\bilel      RIOCA\admins du domaine 2 Oct 15 13:43 bilel
drwxrwx--- 2 RIOCA\burger     RIOCA\admins du domaine 2 Oct 15 13:43 burger
drwxrwx--- 2 RIOCA\carole     RIOCA\admins du domaine 2 Oct 15 13:44 carole
drwxrwx--- 2 RIOCA\chaise     RIOCA\admins du domaine 2 Oct 15 13:43 chaise
drwxrwx--- 2 RIOCA\decevant   RIOCA\admins du domaine 2 Oct 15 13:42 decevant
```

Capture 9 : Chaque dossier appartient à son utilisateur, groupe admins du domaine

4. Automatisation par GPO (mission 8)

4.1 Vérification de la maquette

Le poste PC-USER-GRP3 est joint au domaine dans l'OU ORDINATEURS/PCs. Il obtient son adresse par DHCP (172.19.60.4/24, passerelle 172.19.60.254) et utilise le contrôleur de domaine 172.19.100.2 comme serveur DNS. Le contrôleur de domaine répond au ping par son adresse et par le nom du domaine, ce qui confirme la résolution DNS.

```
C:\Users\souhir.RIOCA>ipconfig /all

Configuration IP de Windows

   Nom de l'hôte . . . . . . . . . . . . : pc-user-grp3
   Suffixe DNS principal . . . . . . . . : RIOCA.local
   Type de noeud. . . . . . . . . . . . . : Hybride
   Routage IP activé . . . . . . . . . . : Non
   Proxy WINS activé . . . . . . . . . . : Non
   Liste de recherche du suffixe DNS.: RIOCA.local

Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . :
   Description. . . . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Adresse physique . . . . . . . . . . . : FC-34-97-80-54-1D
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::5fbd:b79d:dcf4:2f58%3(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 172.19.60.4(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Bail obtenu. . . . . . . . . . . . . . : jeudi 12 novembre 2026 17:27:49
   Bail expirant. . . . . . . . . . . . . : samedi 14 novembre 2026 09:29:23
   Passerelle par défaut. . . . . . . . . : 172.19.60.254
   Serveur DHCP . . . . . . . . . . . . . : 172.19.60.254
   IAID DHCPv6 . . . . . . . . . . . . . : 284963991
   DUID de client DHCPv6. . . . . . . . . : 00-01-01-00-32-34-44-C5-FC-34-97-80-54-1D
   Serveurs DNS. . . . . . . . . . . . . : 172.19.100.2
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé
```

Capture 10 : ipconfig /all sur le poste client

```
C:\Users\souhir.RIOCA>ping 172.19.100.2

Envoi d'une requête 'Ping'  172.19.100.2 avec 32 octets de données :
Réponse de 172.19.100.2 : octets=32 temps=2 ms TTL=127
Réponse de 172.19.100.2 : octets=32 temps=3 ms TTL=127
Réponse de 172.19.100.2 : octets=32 temps=2 ms TTL=127
Réponse de 172.19.100.2 : octets=32 temps=3 ms TTL=127

Statistiques Ping pour 172.19.100.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 3ms, Moyenne = 2ms

C:\Users\souhir.RIOCA>ping rioca.local

Envoi d'une requête 'ping' sur rioca.local [172.19.100.2] avec 32 octets de données :
Réponse de 172.19.100.2 : octets=32 temps=2 ms TTL=127
Réponse de 172.19.100.2 : octets=32 temps=3 ms TTL=127
Réponse de 172.19.100.2 : octets=32 temps=3 ms TTL=127
Réponse de 172.19.100.2 : octets=32 temps=2 ms TTL=127

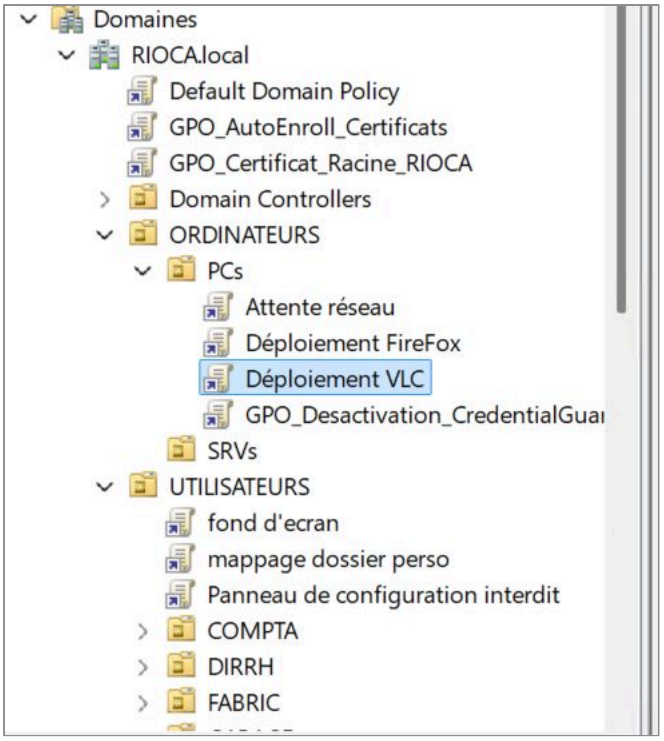
Statistiques Ping pour 172.19.100.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 3ms, Moyenne = 2ms
```

Capture 11 : Ping du contrôleur de domaine par son adresse et par le nom du domaine

L'utilisateur deniz a été créé par copie d'un utilisateur existant du domaine. Il se connecte sur le poste et reçoit bien les stratégies du contrôleur de domaine :

```
C:\Users\deniz> gpresult /r /scope user
Données RSOP pour RIOCA\deniz sur PC-USER-GRP3
    CN=deniz,OU=COMPTA,OU=UTILISATEURS,DC=RIOCA,DC=local
    Stratégie de groupe appliquée depuis :      srv-ad-rioca.RIOCA.local
    L'utilisateur fait partie des groupes de sécurité suivants
        Utilisateurs du domaine
        COMPTA
```

4.2 GPO créées



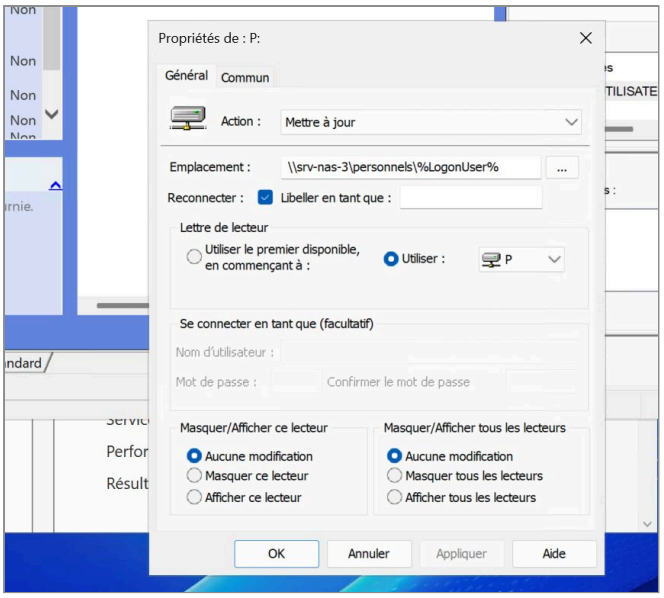
Capture 12 : GPO liées aux OU PCs et UTILISATEURS

GPO	Lien	Type
Attente réseau	PCs	Ordinateur
Déploiement FireFox	PCs	Ordinateur
Déploiement VLC	PCs	Ordinateur
mappage dossier perso	UTILISATEURS	Utilisateur
fond d'ecran	UTILISATEURS	Utilisateur
Panneau de configuration interdit	UTILISATEURS	Utilisateur
Une GPO par service (Dossier Compta...)	OU du service	Utilisateur

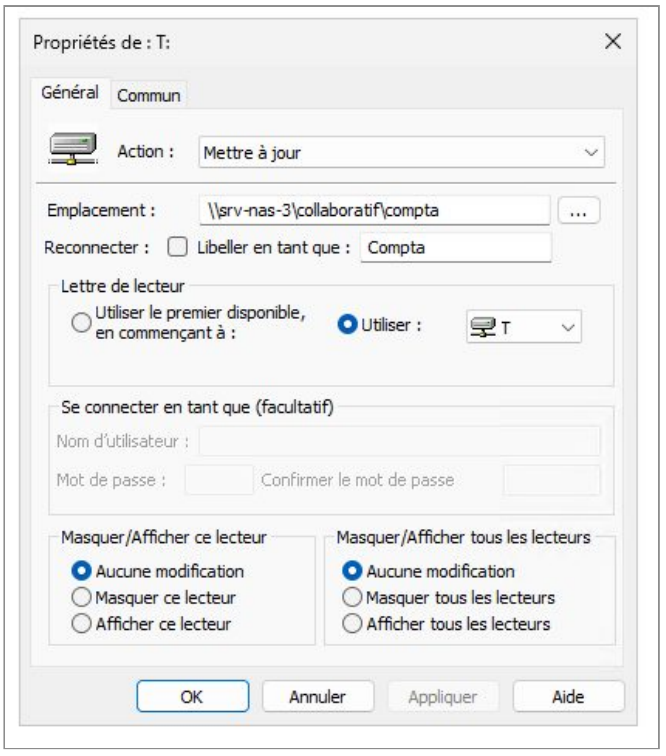
GPO	Chemin du paramètre
Mappage Dossiers personnels	Config. utilisateur → Préférences → Paramètres Windows → Mappages de lecteurs : P: vers `\\srv-nas-3\personnels\%LogonUser%`
Mappage Collaboratif	Même emplacement : T: vers `\\srv-nas-3\collaboratif\<service>`, une GPO liée à l'OU de chaque service
Fond d'écran	Préférences → Paramètres Windows → Fichiers (copie de l'image) et Stratégies → Modèles d'administration → Bureau → Bureau → Papier peint du Bureau
Panneau de configuration	Config. utilisateur → Stratégies → Modèles d'administration → Panneau de configuration → Interdire l'accès au Panneau de configuration et à l'application Paramètres du PC
Firefox et VLC	Config. ordinateur → Stratégies → Paramètres du logiciel → Installation de logiciel (package attribué)
Attente réseau	Config. ordinateur → Modèles d'administration → Système → Ouverture de session → Toujours attendre le réseau lors du démarrage et de l'ouverture de session

Mappage des lecteurs

Le lecteur P: utilise la variable `%LogonUser%` : une seule GPO donne à chacun son propre dossier. Le lecteur T: dépend du service, il y a donc une GPO par service, liée à l'OU du service. Celle de COMPTA est présentée ; la même logique a été appliquée aux autres services (DIRRH, FABRIC, GARAGE, IT, LIVR, RD), chacun vers son dossier.



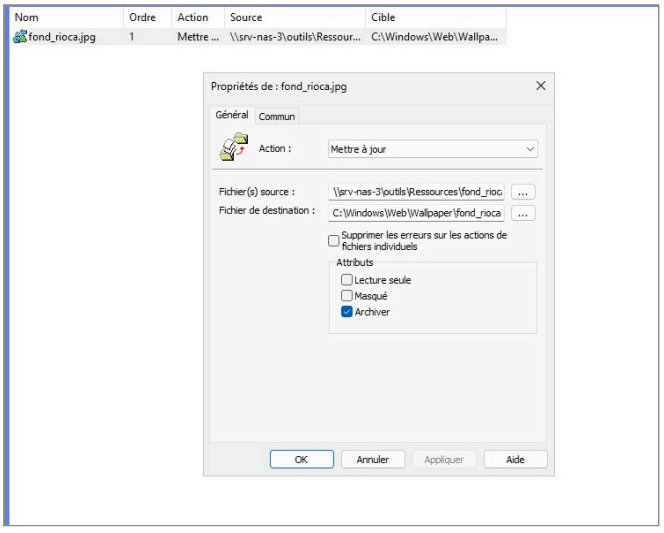
Capture 13 : Lecteur P: vers le dossier personnel



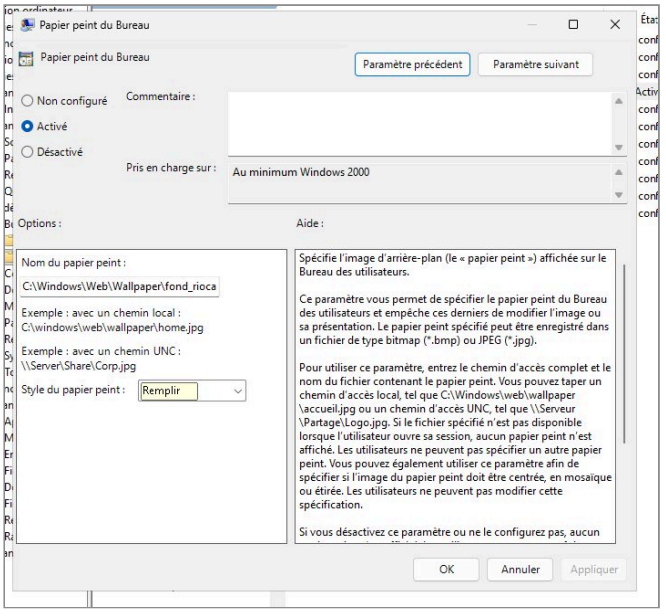
Capture 14 : Lecteur T: vers le dossier du service COMPTA

Fond d'écran

L'image `fond_rioca.jpg` est stockée dans `\\srv-nas-3\outils\Ressources`. Une préférence Fichiers la copie sur le poste dans `C:\Windows\Web\Wallpaper`, puis le paramètre Papier peint du Bureau l'applique depuis cette copie locale. Ce paramètre empêche aussi l'utilisateur de changer de fond.



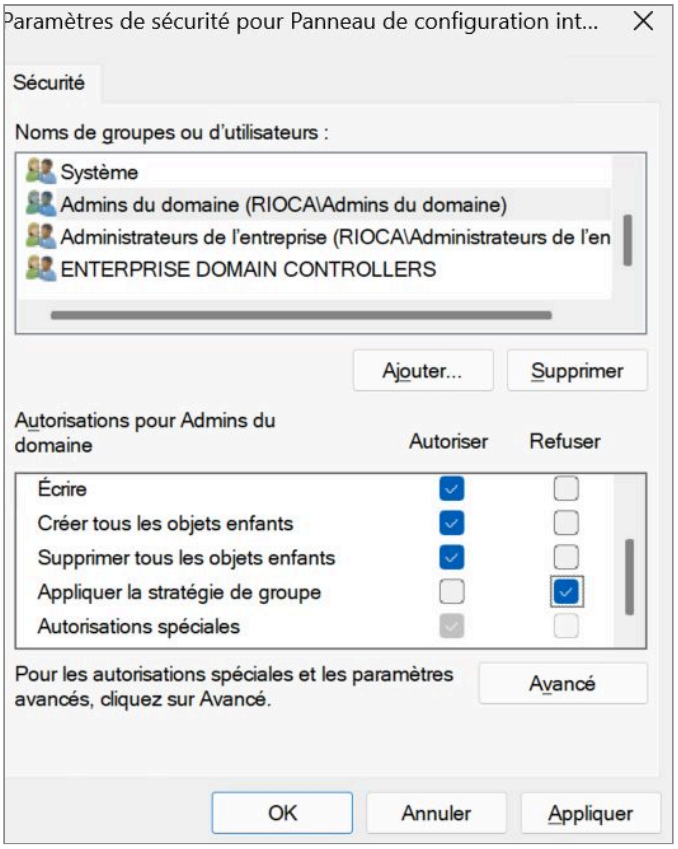
Capture 15 : Copie de l'image du NAS vers le poste



Capture 16 : Paramètre Papier peint du Bureau

Blocage du panneau de configuration

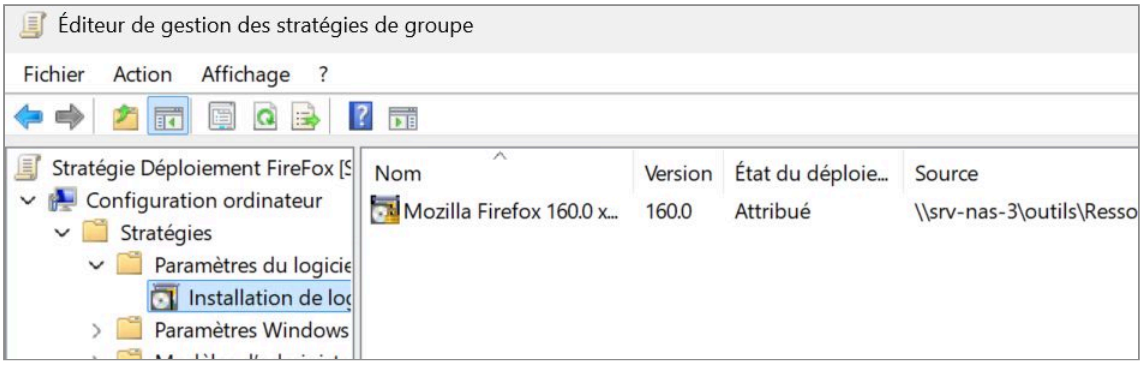
Pour que la GPO ne s'applique qu'aux utilisateurs non administrateurs, l'autorisation « Appliquer la stratégie de groupe » est refusée aux Admins du domaine dans l'onglet Délégation de la GPO.



Capture 17 : Admins du domaine exclus de la GPO

Déploiement de Firefox et VLC

Les installeurs MSI (`Firefox-Setup-160.0.msi` et `vlc-3.0.24-win64.msi`) sont placés dans `\\srv-nas-3\outils\Ressources` et attribués aux ordinateurs par leur chemin UNC. L'installation se fait au démarrage du poste. La GPO Attente réseau oblige Windows à attendre le réseau avant d'appliquer les stratégies, ce qui est nécessaire à l'installation. La GPO de VLC est identique à celle de Firefox.



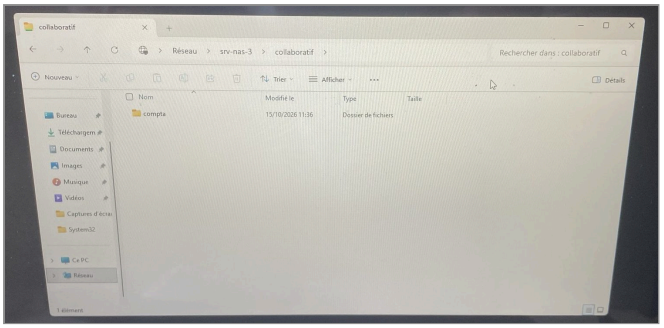
Capture 18 : Package Firefox attribué depuis le partage Outils

5. Tests

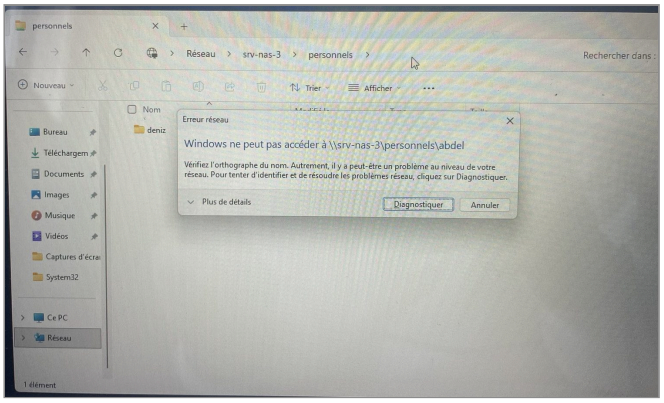
Les tests ont été faits sur PC-USER-GRP3 avec deniz, utilisateur standard du service COMPTA, et avec un compte admin du domaine.

5.1 Partages du NAS

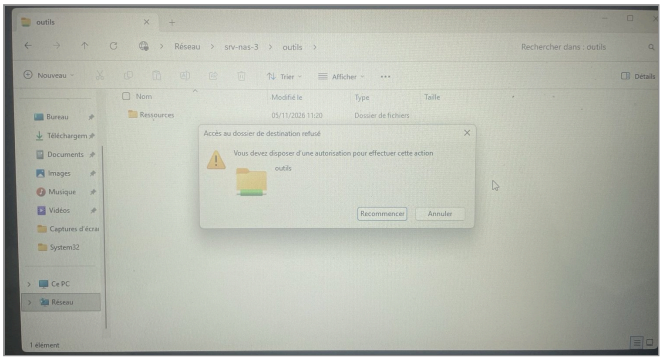
Test	Résultat attendu	Résultat obtenu	Capture
deniz ouvre collaboratif	Seul le dossier compta est visible	Conforme	19
deniz crée un fichier dans collaboratif\compta	Écriture autorisée	Conforme	-
deniz ouvre le dossier personnel d'abdel	Accès refusé	Conforme	20
deniz crée un fichier dans outils	Écriture refusée (lecture seule)	Conforme	21
deniz ouvre sauvegardes	Accès refusé	Conforme	22
Un admin du domaine ouvre collaboratif	Les 7 dossiers de service visibles	Conforme	-



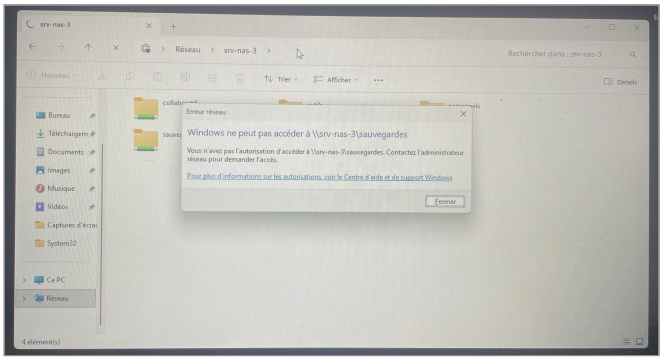
Capture 19 : deniz ne voit que le dossier de son service



Capture 20 : Dossier personnel d'un autre utilisateur inaccessible



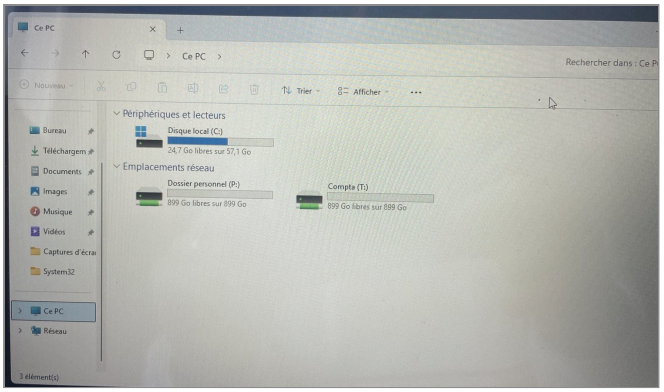
Capture 21 : Écriture refusée dans outils



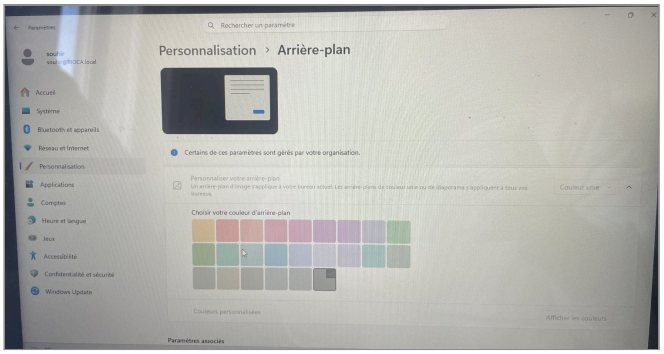
Capture 22 : Accès refusé à sauvegardes

5.2 GPO

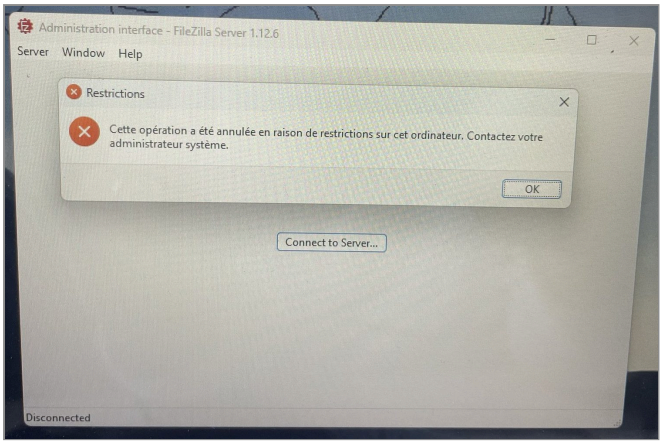
Test réalisé depuis le poste client	Résultat observé	Capture
Lecteurs réseau montés à l'ouverture de session	deniz obtient P: (Dossier personnel) et T: (Compta)	23
Un utilisateur d'un autre service voit-il le même lecteur ?	Non, un utilisateur de l'OU IT reçoit la GPO Dossier IT et non Dossier Compta	-
Fond d'écran appliqué et non modifiable	Fond RIOCA affiché, réglage de l'arrière-plan grisé	24
Panneau de configuration inaccessible pour un utilisateur standard	Message « Restrictions » pour deniz, accès conservé pour un admin	25
Firefox et VLC installés après redémarrage	Installés automatiquement au démarrage	26



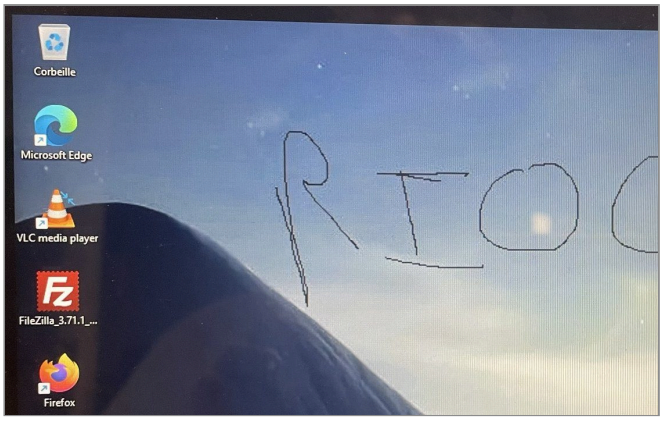
Capture 23 : Lecteurs P: et T: montés pour deniz



Capture 24 : Arrière-plan géré par l'organisation



Capture 25 : Panneau de configuration bloqué



Capture 26 : Firefox et VLC installés par GPO

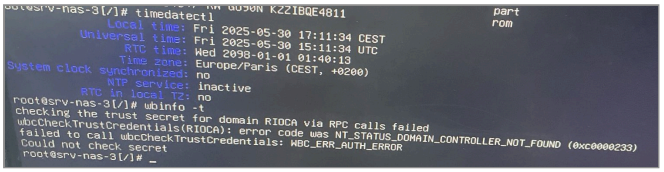
5.3 Question C1

La commande `gpupdate /force` réapplique immédiatement les stratégies sans attendre le cycle de rafraîchissement (environ 90 minutes). Sa limite pour le déploiement de logiciels est que l'installation ne peut se faire qu'au démarrage de l'ordinateur (ou à l'ouverture de session pour un logiciel attribué à l'utilisateur) : `gpupdate /force` ne l'installe pas et demande de redémarrer le poste.

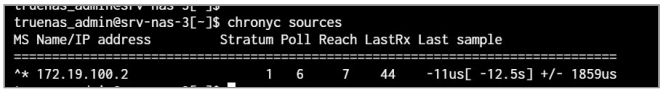
6. Difficultés rencontrées

Heure du NAS et jonction au domaine

La jonction était refusée car l'horloge du NAS indiquait 2025 (horloge matérielle en 2098). Kerberos refuse un écart de plus de 5 minutes avec le contrôleur de domaine. Nous avons corrigé l'heure dans le BIOS du serveur (en UTC) et configuré le NAS pour se synchroniser sur le DC. Côté DC, le service de temps a été déclaré source fiable (`w32tm /config /reliable:yes`), le port UDP 123 ouvert et la synchronisation sur l'hôte Hyper-V désactivée pour qu'il réponde correctement.



Capture 27 : Heure du NAS en 2025, jonction au DC impossible



Capture 28 : Après correction : NAS synchronisé sur le DC

Disques non détectés

TrueNAS ne voyait au départ que le SSD : les deux disques de données étaient bloqués par une ancienne configuration du contrôleur PERC. Ils ont été réinitialisés dans l'utilitaire du contrôleur avant la création du disque virtuel RAID 1.

Droits à la racine des partages

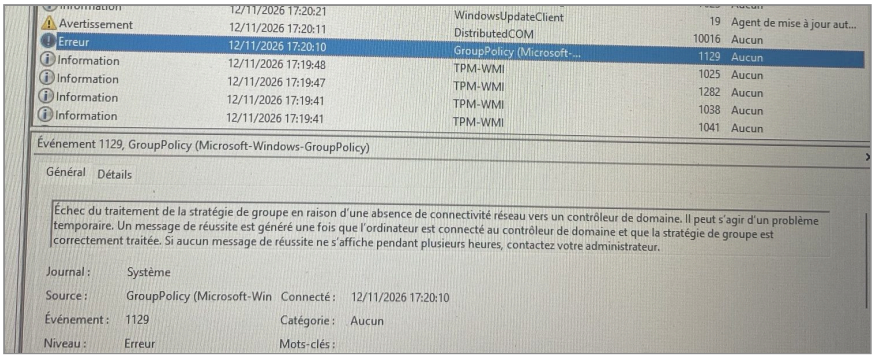
Avec le seul droit « Traverser » à la racine de collaboratif et personnels, Windows refusait d'ouvrir le partage et le lecteur P: ne se montait pas (accès refusé dans le journal Application). Le passage en « Lire » sans héritage a réglé le problème sans donner accès aux dossiers des autres.

GPO non appliquée

La GPO de mappage du dossier personnel n'apparaissait pas dans `gpresult` : sa version utilisateur était à 0 dans l'Active Directory et à 4 dans SYSVOL. Une nouvelle modification de la GPO a resynchronisé les deux versions.

Installation de Firefox et VLC

Les logiciels ne s'installaient pas et Windows demandait un redémarrage à chaque fois. Le journal Système montrait au démarrage l'événement 1129 : pas de connexion au contrôleur de domaine. Le port du poste client utilise l'authentification 802.1X (RADIUS) de l'utilisateur : il reste fermé tant que personne ne s'est connecté, alors que l'installation se fait justement avant l'ouverture de session. Pour ne pas modifier la configuration RADIUS, l'installation a été réalisée en branchant le poste sur un port sans 802.1X. En production, il faudrait activer l'authentification 802.1X des ordinateurs pour que le poste ait le réseau dès le démarrage.



Capture 29 : Événement 1129 au démarrage du poste client

7. Conclusion

Le serveur srv-nas-3 est opérationnel : TrueNAS fonctionne sur un RAID 1 matériel avec 899 Go utiles, il est joint au domaine RIOCA.local et synchronisé sur le contrôleur de domaine. Les quatre partages respectent les droits demandés, comme le montrent les tests d'accès autorisés et refusés. Les GPO montent automatiquement les lecteurs, imposent le fond d'écran, bloquent le panneau de configuration pour les utilisateurs standard et installent Firefox et VLC.

Ce projet nous a permis de comprendre l'importance de l'heure et du DNS dans un domaine Active Directory, de travailler les ACL d'un serveur de fichiers et d'utiliser les journaux Windows pour diagnostiquer les GPO. Comme améliorations, il faudrait activer l'authentification 802.1X des ordinateurs et planifier des snapshots et des sauvegardes vers le partage Sauvegardes.