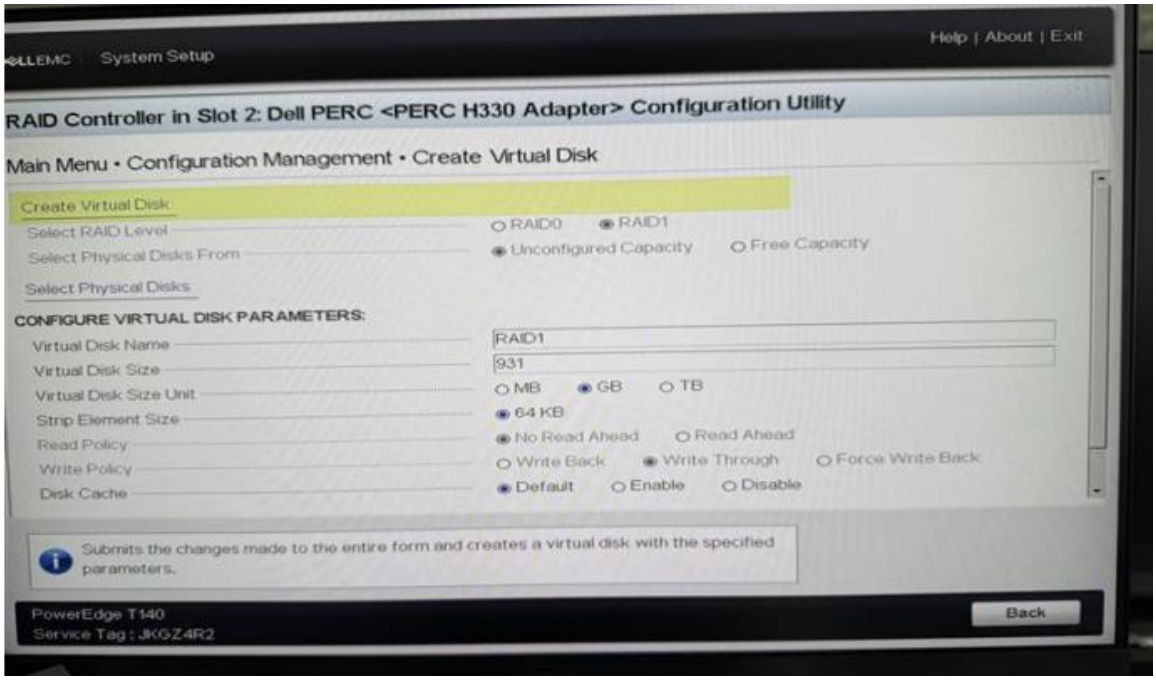
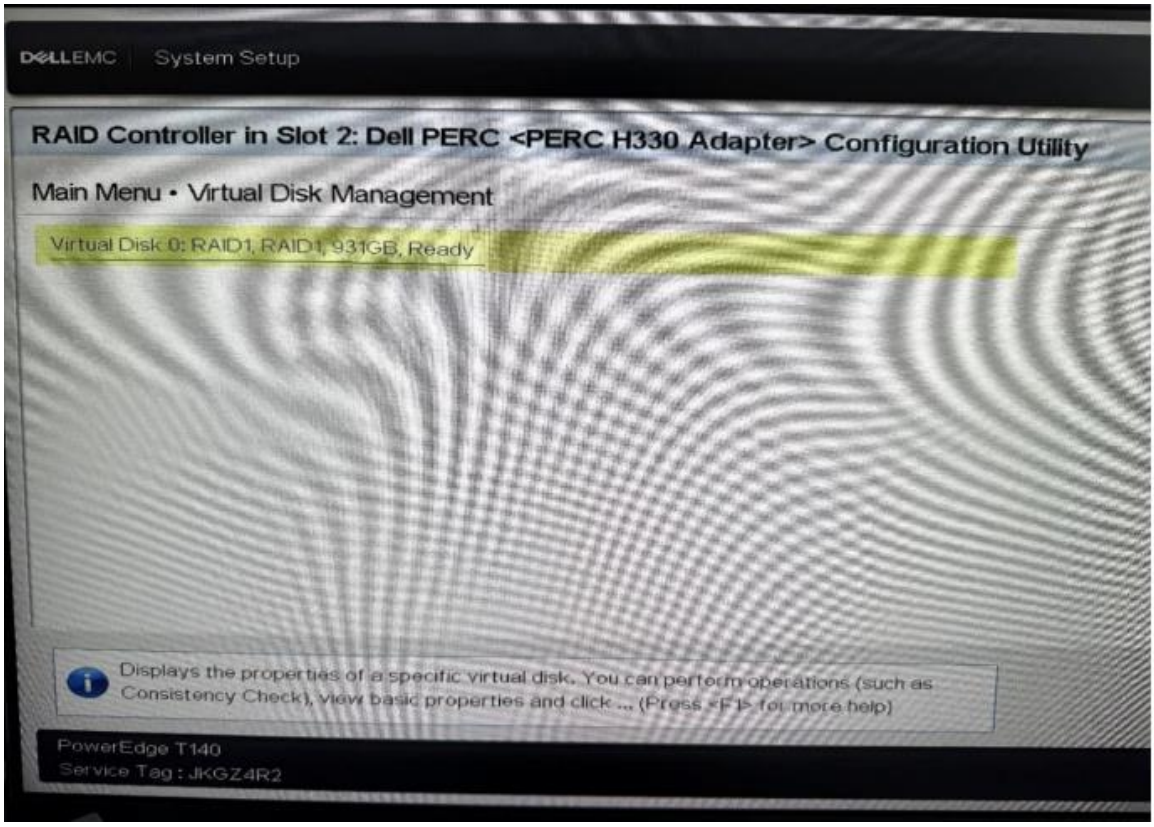
Documentation Mission 7 et 8

1. Recherche du système d'exploitation adapté et comparatif

Une étude comparative a été menée afin d'identifier un système d'exploitation répondant aux besoins de stockage, de partage SMB/CIFS, de gestion simplifiée et d'intégration dans un domaine Active Directory. Trois solutions ont été analysées : TrueNAS CORE, OpenMediaVault, Windows Server Storage Services. TrueNAS a été retenu pour sa stabilité, sa compatibilité SMB native, ses ACL avancées et son intégration simple dans un environnement Windows.



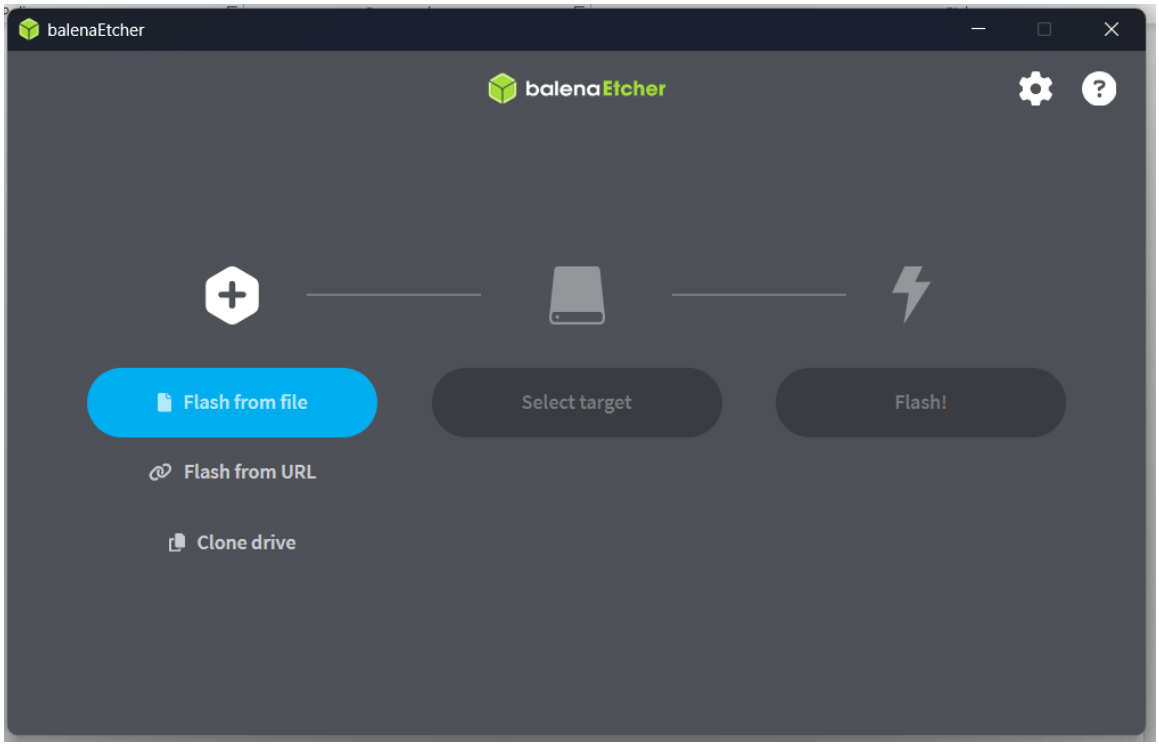


2. Vérification du serveur physique Dell PowerEdge T140 & RAID1

Le serveur fourni a été contrôlé matériellement : présence de deux disques pour le RAID1, vérification des températures et du contrôleur RAID dans le BIOS, confirmation que le RAID1 matériel est actif. Cette étape garantit que la base matérielle est saine.

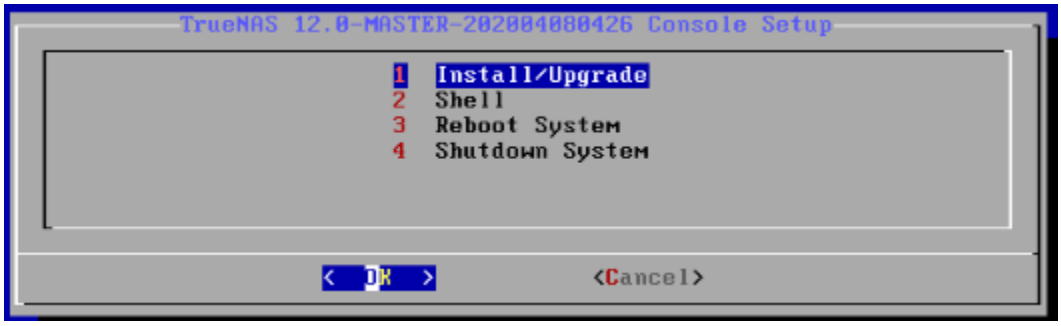
3. Création de la clé USB bootable

L'image ISO de TrueNAS a été téléchargée. La clé USB bootable a été créée avec Balena Etcher (Rufus étant incompatible avec la version de GRUB). L'écriture de l'image a été vérifiée.



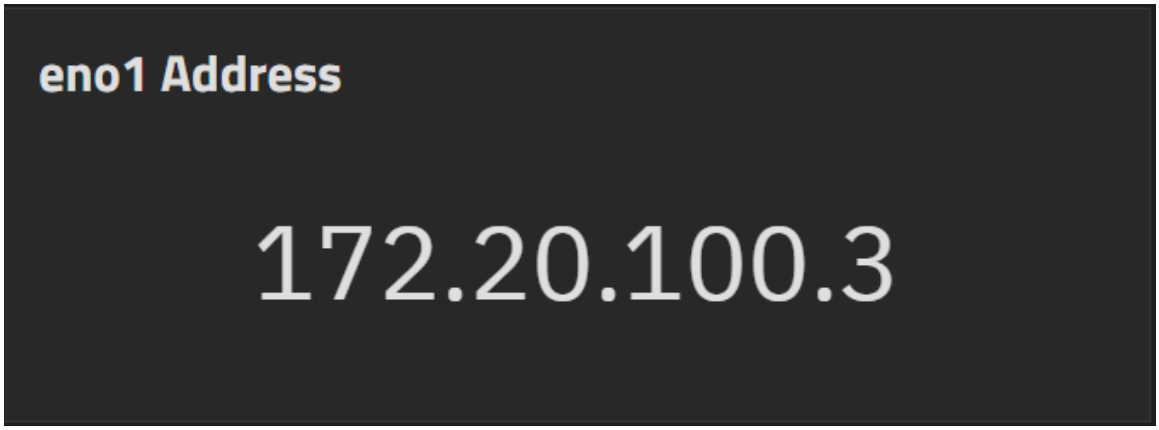
4. Installation de TrueNAS sur le serveur

L'installation a suivi les étapes : boot sur USB, choix Install/Upgrade, sélection du disque système (sans toucher aux disques du RAID1), création du mot de passe root, retrait de la clé USB et redémarrage. Le NAS affiche ensuite l'URL d'administration web.



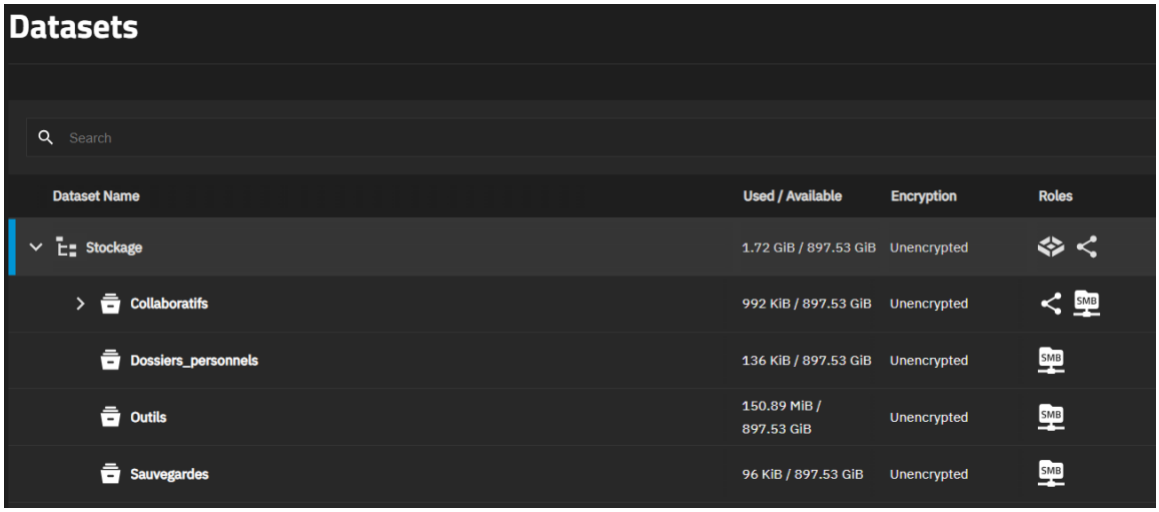
5. Configuration réseau du NAS

La configuration réseau a été réalisée via Network > Interfaces : hostname srv-nas, IP 172.20.100.3, masque 255.255.255.0, passerelle 172.20.100.254, DNS 172.20.100.2. Cette configuration permet l'intégration au domaine Active Directory.



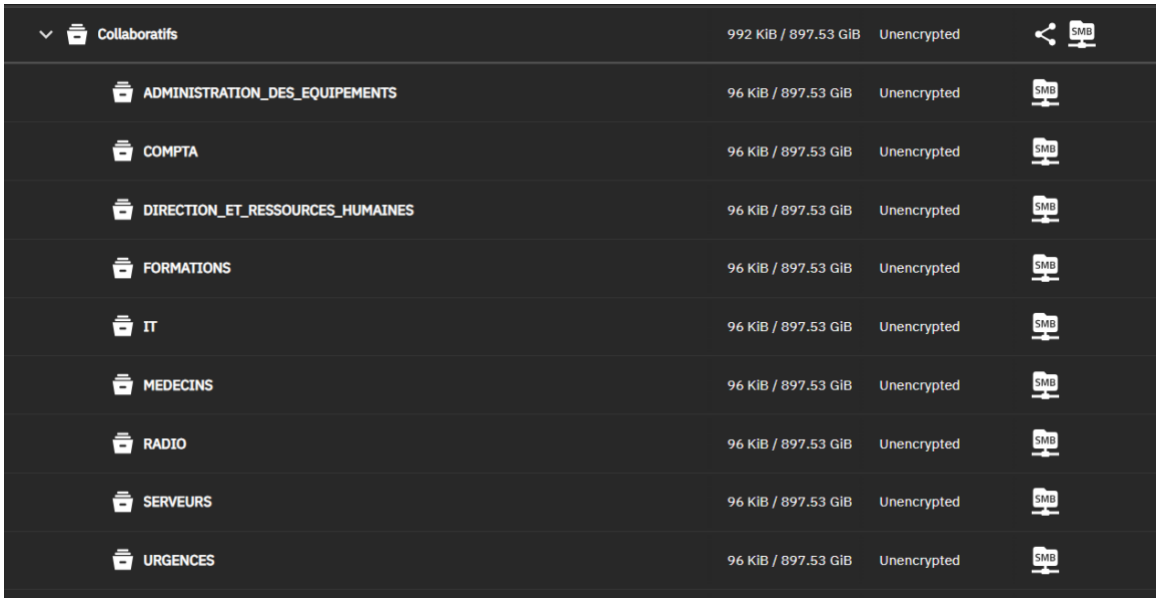
6. Création du dataset Dossiers Personnels

Création du dataset 'Dossiers_Personnels' (preset SMB), activation du partage, activation du mode Home Share. ACL configurées : Domaine Users en traverse, Domain Admins en contrôle total. Chaque utilisateur obtient un dossier personnel automatique et privé.



7. Création du dossier Collaboratif

Un dataset Collaboratif a été créé puis des sous-datasets pour chaque service (ex : Compta, RH, IT). ACL : groupe du service en lecture/écriture, Domain Admins en contrôle total. Ceci permet un partage structuré et sécurisé.



8. Création du dossier Outils

Création du dataset Outils (preset SMB). Droits : tous les utilisateurs en lecture, administrateurs en contrôle total. Ce dossier stocke les fichiers d'installations nécessaires aux déploiements automatisés via GPO.

9. Création du dossier Sauvegardes

Le dataset Sauvegardes permet de stocker les sauvegardes internes. ACL : accès uniquement aux Domain Admins. Aucun autre groupe n'a la permission de lecture ou d'écriture.

MISSION 8 — Automatisation des paramètres grâce aux GPO

---

1. Vérification du bon fonctionnement de la maquette

Avant toute configuration des GPO, il est nécessaire de vérifier que l'infrastructure fonctionne correctement.

Les actions réalisées sont :

- Vérification des paramètres réseau (IP, masque, passerelle, DNS) des postes clients.
- Réalisation d'un ping vers le contrôleur de domaine pour assurer la connectivité :
  → `ping 172.20.100.2`
- Vérification de la résolution DNS du domaine :
  → `ping mondomaine.local`
  Ce test confirme que les postes utilisent bien le serveur DNS du domaine.

Ensuite, un utilisateur existant dans l'Active Directory a été dupliqué puis une connexion a été testée sur une machine cliente afin de valider que l'authentification au domaine fonctionne.

---

2. Vérification / création du dossier partagé "Dossiers personnels" sur le NAS

Si le dossier n'existait pas déjà, un dataset Dossiers_Personnels a été créé sur le serveur NAS.

La configuration réalisée est :

- Utilisation d'un preset SMB pour permettre le partage Windows.
- Activation du mode Home Share, permettant à chaque utilisateur d'obtenir automatiquement son propre dossier personnel.
- Configuration des ACL :
    - Les utilisateurs possèdent les droits sur leur propre dossier (owner).
    - Les Domain Admins ont un contrôle total.
    - Les autres utilisateurs n'ont aucune visibilité.

Ce dossier servira à monter automatiquement les lecteurs personnels via GPO.

---

3. Vérification / création du dossier partagé "Collaboratif" sur le NAS

Si le dossier n'existait pas encore, un dataset Collaboratif a été créé.

Ensuite :

- Création d'un dataset pour chaque service de l'entreprise (ex : Compta, RH, Informatique…).
- Activation des partages SMB pour permettre l'accès aux utilisateurs.
- Application des ACL adaptées :
    - Les membres du service obtiennent lecture/écriture.
    - Les Domain Admins ont un contrôle total.

Ces dossiers serviront au mappage automatique des lecteurs collaboratifs via GPO.

---

4. Création des GPO de mappage automatique des lecteurs

Plusieurs GPO ont été créées pour automatiser le montage des lecteurs réseau lors de la connexion de l'utilisateur.

Deux types de lecteurs ont été automatisés :

✔ Lecteur personnel

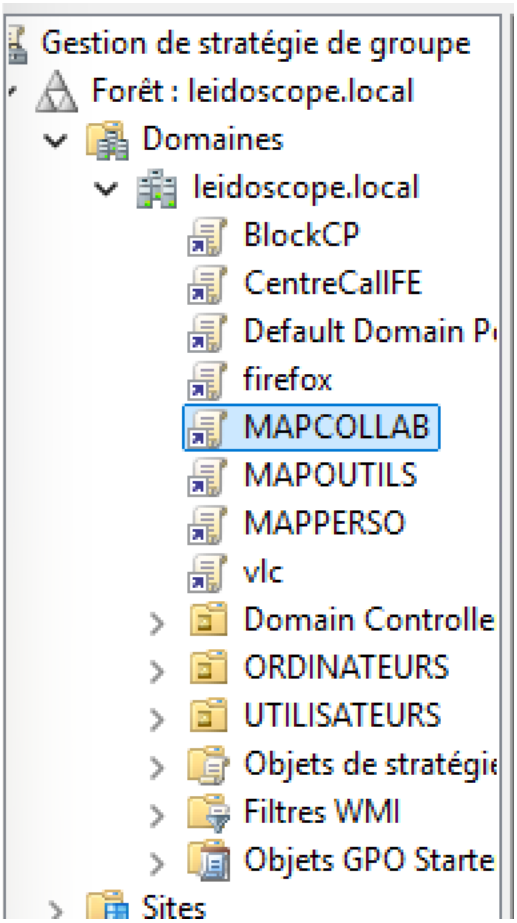
Une GPO dédiée a été créée pour attribuer :

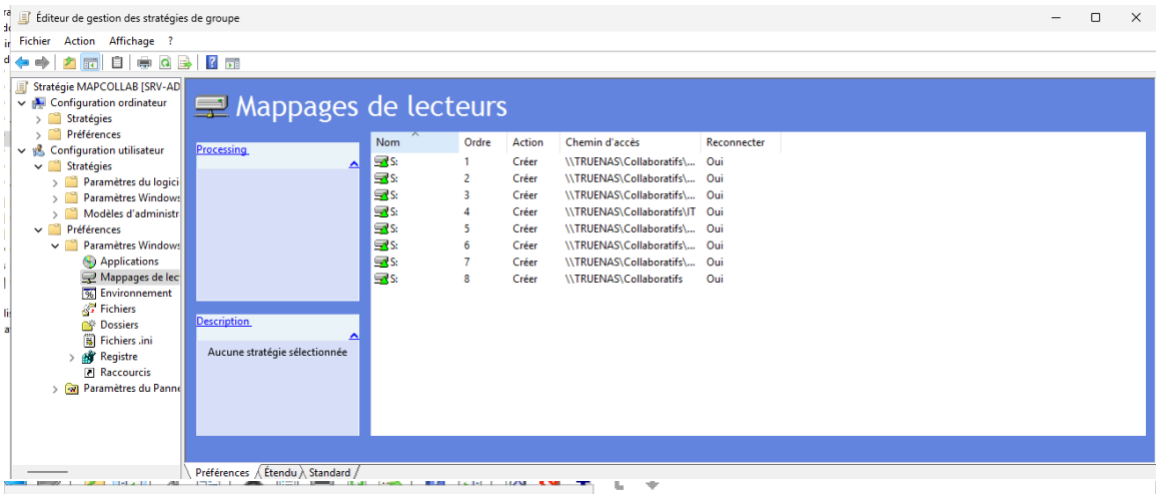
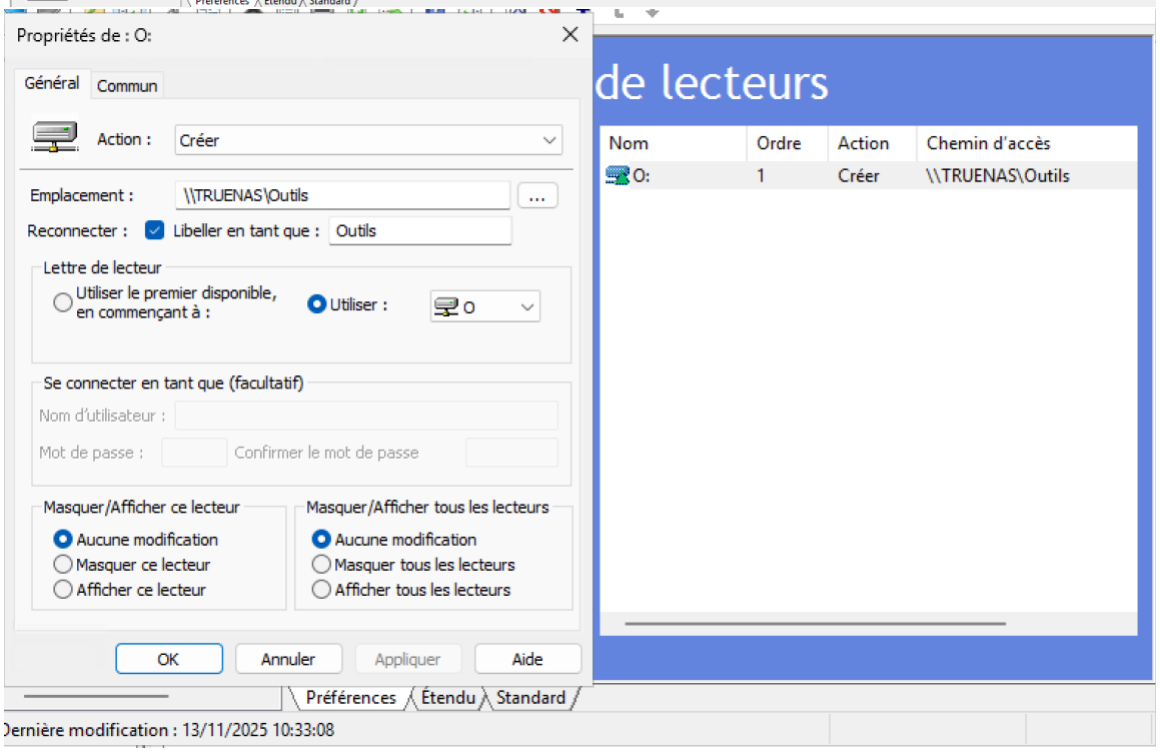
- Le lecteur P: ou H: (selon la convention choisie).
- Le chemin UNC pointant vers le Home Share du NAS.
- Le mappage se fait via Preferences → Windows Settings → Drive Maps.

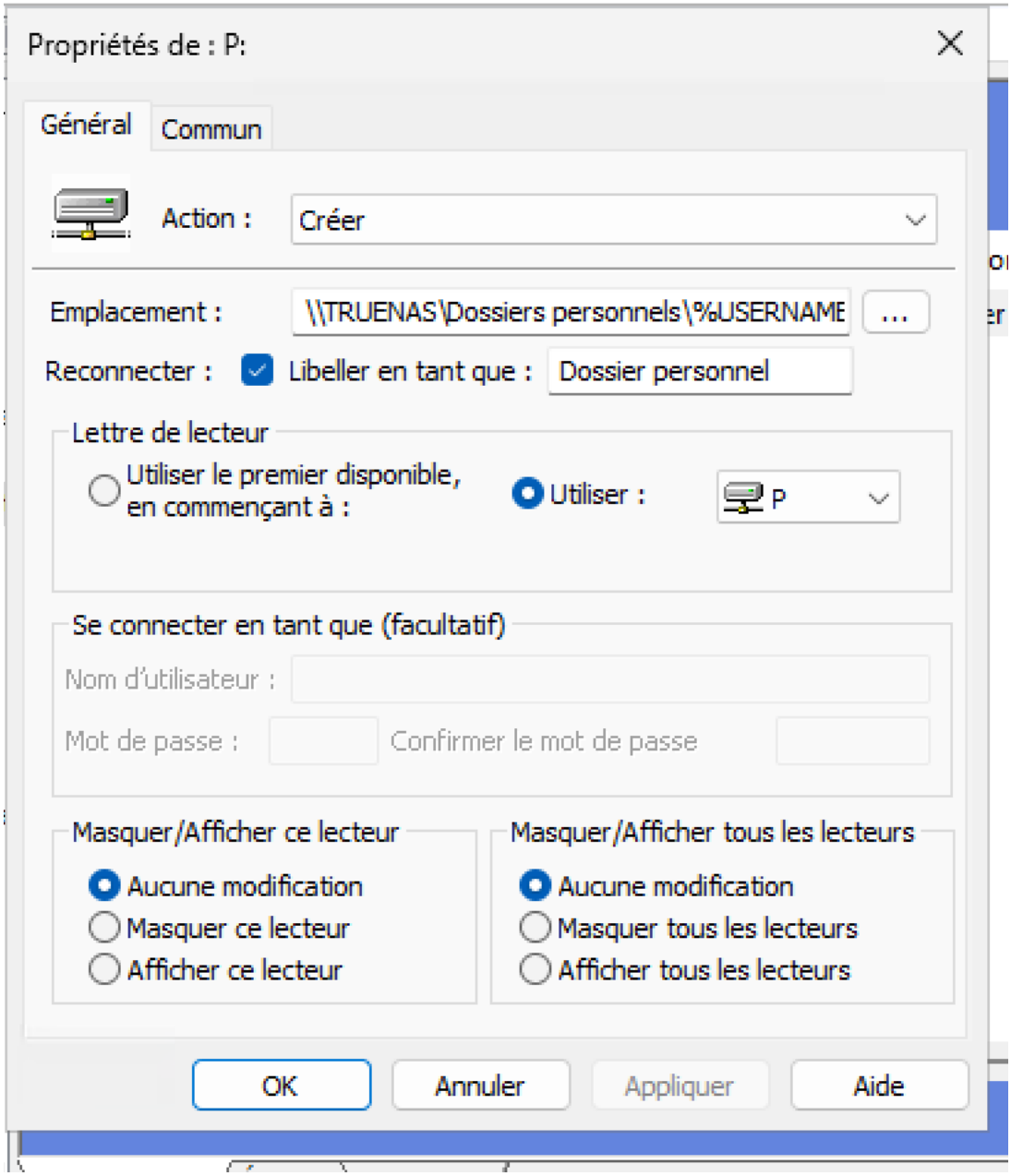
✔ Lecteurs collaboratifs

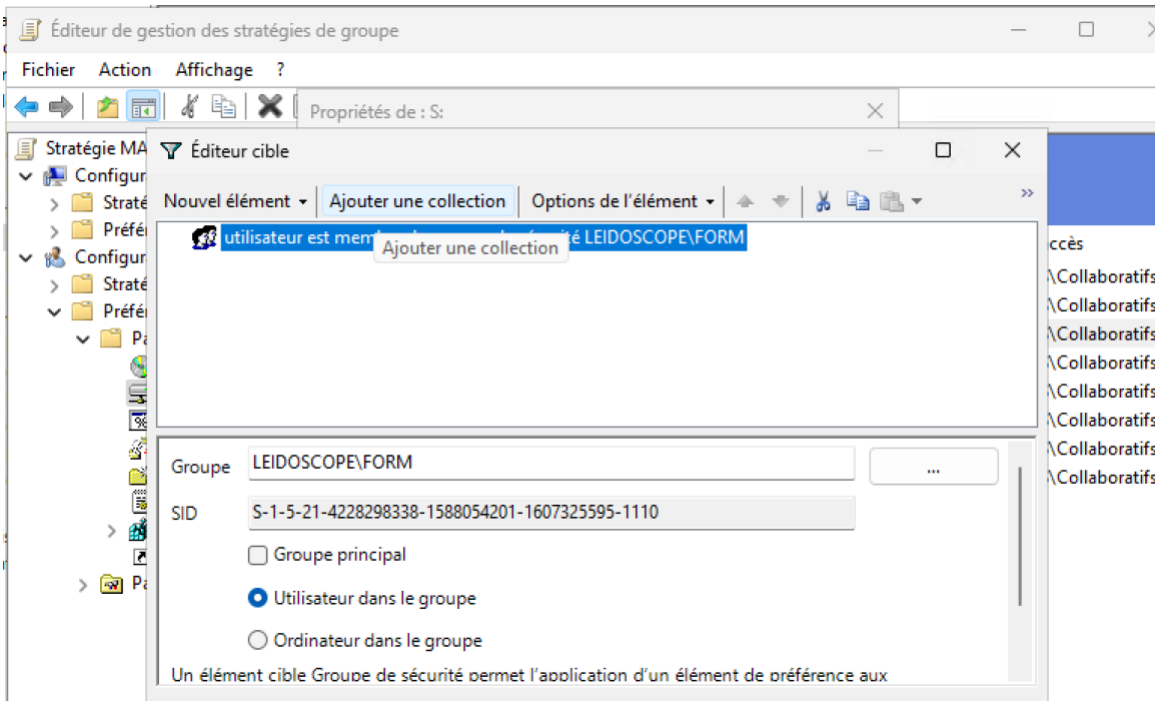
Une GPO par service a été créée pour attribuer :

- Le lecteur du département concerné (ex : S:, R:, C:).
- Le chemin UNC du dataset du service.
- La GPO est filtrée par groupe de sécurité pour que seuls les membres du service montent ce lecteur.



- 
Éditeur de gestion des stratégies de groupe
Fichier Action Affichage ?
Stratégie MAPCOLLAB [SRV-AD
Configuration ordinateur
Stratégies
Préférences
Configuration utilisateur
Stratégies
Paramètres du logici
Paramètres Windows
Modèles d'administr
Préférences
Paramètres Windows
Applications
Mappages de lec
Environnement
Fichiers
Dossiers
Fichiers .ini
Registre
Raccourcis
Paramètres du Panne
Mappages de lecteurs
Processing
Description
Aucune stratégie sélectionnée
Nom Ordre Action Chemin d'accès Reconnecter
S: 1 Créer \\TRUENAS\Collaboratifs\... Oui
S: 2 Créer \\TRUENAS\Collaboratifs\... Oui
S: 3 Créer \\TRUENAS\Collaboratifs\... Oui
S: 4 Créer \\TRUENAS\Collaboratifs\IT Oui
S: 5 Créer \\TRUENAS\Collaboratifs\... Oui
S: 6 Créer \\TRUENAS\Collaboratifs\... Oui
S: 7 Créer \\TRUENAS\Collaboratifs\... Oui
S: 8 Créer \\TRUENAS\Collaboratifs Oui
Préférences Étendu Standard
- 
Propriétés de : O:
Général Commun
Action : Créer
Emplacement : \\TRUENAS\Outils
Reconnecter : Libeller en tant que : Outils
Lettre de lecteur
Utiliser le premier disponible, en commençant à :
Utiliser : O
Se connecter en tant que (facultatif)
Nom d'utilisateur :
Mot de passe : Confirmer le mot de passe
Masquer/Afficher ce lecteur
Aucune modification
Masquer ce lecteur
Afficher ce lecteur
Masquer/Afficher tous les lecteurs
Aucune modification
Masquer tous les lecteurs
Afficher tous les lecteurs
OK Annuler Appliquer Aide
de lecteurs
Nom Ordre Action Chemin d'accès
O: 1 Créer \\TRUENAS\Outils
Préférences Étendu Standard
Dernière modification : 13/11/2025 10:33:08

- 
Propriétés de : P:
Général
Commun
Action :
Créer
Emplacement :
\\TRUENAS\Dossiers personnels\%USERNAME
...
Reconnecter :
Libeller en tant que :
Dossier personnel
Lettre de lecteur
Utiliser le premier disponible, en commençant à :
Utiliser :
P
Se connecter en tant que (facultatif)
Nom d'utilisateur :
Mot de passe :
Confirmer le mot de passe
Masquer/Afficher ce lecteur
Aucune modification
Masquer ce lecteur
Afficher ce lecteur
Masquer/Afficher tous les lecteurs
Aucune modification
Masquer tous les lecteurs
Afficher tous les lecteurs
OK
Annuler
Appliquer
Aide

- 

---

5. GPO pour déployer le fond d'écran CentreCall

Une GPO a été créée pour imposer un fond d'écran unique à tous les utilisateurs du domaine.

Les actions réalisées :

- Le fichier `.jpg` ou `.png` du fond d'écran a été déposé dans le dossier Outils du NAS.
- Dans la GPO :
  → User Configuration > Administrative Templates > Desktop > Desktop
  → Paramètre Desktop Wallpaper
  → Indication du chemin UNC du fichier dans le NAS
  → Mode : Fill
- Le paramètre a été verrouillé pour empêcher la modification par l'utilisateur.

Cette GPO garantit une identité visuelle homogène sur tous les postes.

---

6. GPO pour bloquer l'accès au panneau de configuration

Une GPO a été construite afin de renforcer la sécurité des postes clients.

Configuration effectuée :

- User Configuration > Administrative Templates > Control Panel
- Activation du paramètre Prohibit access to Control Panel and PC Settings

La GPO a été appliquée à tous les utilisateurs non administrateurs (filtrage via groupe de sécurité).
Cela empêche les utilisateurs standards de modifier des paramètres sensibles du système.

---

7. GPO pour déployer Mozilla Firefox sur les machines clientes

Pour permettre une installation automatique du navigateur :

1. Le fichier d'installation `.msi` de Firefox a été déposé dans le dossier Outils du NAS.
2. Une GPO a été créée :
    - Computer Configuration > Policies > Software Settings > Software Installation
    - Ajout d'un nouveau package → sélection du fichier `.msi` via son chemin UNC.
3. Mode d'installation : Assigned.

Ainsi, Firefox est installé automatiquement lors du prochain redémarrage de chaque poste du domaine.

---

8. GPO pour déployer VLC sur les machines clientes

Le même type de GPO que pour Firefox a été créé afin d'automatiser le déploiement de VLC.

Procédure identique :

- Dépôt du fichier `.msi` de VLC dans le dossier Outils.
- GPO en mode Assigned, appliquée à tous les ordinateurs du domaine.

Chaque client installe VLC automatiquement au démarrage ou lors de la mise à jour de la stratégie.