SPRINT 2 — Serveur de Fichiers, Partages et Autorisations NTFS

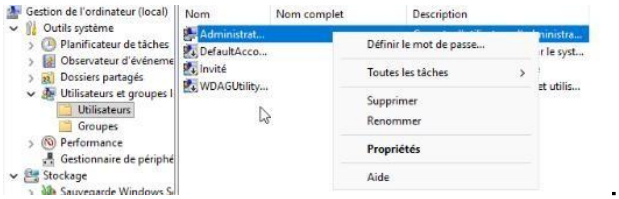
Sprint 2.1 : Joindre le serveur de fichiers SRV-FS au domaine sio.local, préparer le disque de stockage et définir le mot de passe admin local.

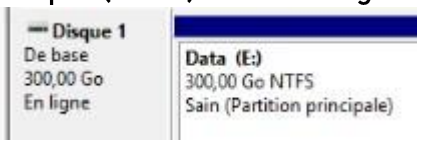
- Besoin :
  - Appartenance au domaine : Joindre la machine membre au domaine sio.local.
  - Espace de stockage dédié : Utiliser un disque virtuel séparé de 300 Go pour stocker les fichiers des utilisateurs et les logiciels
- Sécurisation du compte local : Mettre un mot de passe admin local propre au serveur (différent de celui du domaine).
- Analyse/Etude :
  - IP du serveur de fichiers : 172.16.20.103 /24. ○ Disque de données : Initialiser et formater le volume dédié de 300 Go.

- Paramétrage :
  - Configuration IP et Jonction de domaine (SRV-FS) :
    - Adresse IP fixe : 172.16.20.103 /24, Passerelle : 172.16.20.254, DNS : 172.16.20.100.



    - ○ Configuration du compte Administrateur local :

- 

    - Définition d'un mot de passe fort respectant la politique de complexité Active Directory (stocké de manière sécurisée dans le gestionnaire de mots de passe de l'équipe).
    - Préparation du volume :
      Initialisation du disque de 300 Go en GPT, création du volume simple (DATA) et formatage en NTFS.
      

- Test :
  - 

Figure 1: Confirmation de la jonction du serveur de fichiers SRV-FS au domaine sio.local.

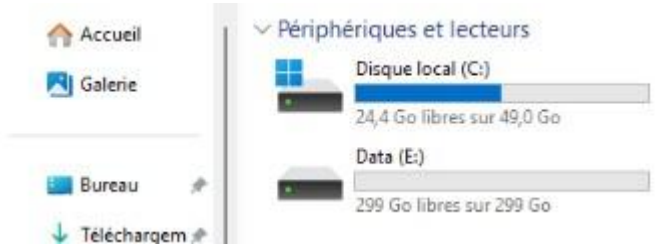
  - 

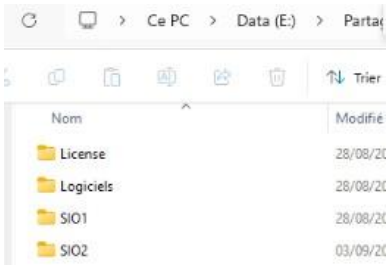
Figure 2: Vérification de la disponibilité du volume de stockage dédié de 300 Go.

Sprint 2.2 : Configurer les partages réseau, désactiver l'héritage des permissions NTFS et appliquer le contrôle d'accès ciblé par groupes de sécurité.

- Besoin :
  - Isolation des données : Empêcher les utilisateurs d'une section (ex: SIO1) d'accéder aux répertoires d'une autre section (SIO2).
  - Déploiement logiciel : Permettre aux machines du domaine de lire le répertoire de déploiement d'applications .msi. ○ Gérer les accès: Appliquer le contrôle d'accès sur le système de fichiers (NTFS) plutôt que sur le partage.
- Analyse/Etude :
  - Permissions de partage : Mettre "Tout le monde" en Contrôle Total sur le partage pour laisser la sécurité entièrement au NTFS. ○ Permissions NTFS : Couper l'héritage NTFS sur les dossiers SIO1 et SIO2, puis retirer les accès attribués par défaut aux utilisateurs classiques.

- Attribution ciblée :
  - Dossier SIO1 : Groupe G_SIO1 (Modification).
  - Dossier SIO2 : Groupe G_SIO2 (Modification).
  - Dossier License : Groupe G_License (Modification).
  - Dossier Logiciels : Groupes Administrateurs du domaine (Contrôle total) et Ordinateurs du domaine (Lecture & Exécution).

- Paramétrage :
  - Création des dossiers et partages sur le disque dédié de SRV-FS :



  - Désactivation de l'héritage NTFS :
    - > Convertir les autorisations héritées en autorisations explicites
    - Supprimer les accès du groupe Utilisateurs. (LES DEUX) ○ Application des autorisations NTFS :
    - Sur SIO1 : Ajout du groupe sio\G_SIO1 (Autorisations : Modification, Lecture, Écriture).
    - Sur SIO2 : Ajout du groupe sio\G_SIO2 (Autorisations : Modification, Lecture, Écriture).
    - Sur License: Ajout du groupe sio\G_License (Autorisations : Modification, Lecture, Écriture).
    - Sur Logiciels : Ajout du groupe sio\Ordinateurs du domaine (Autorisations : Lecture & Exécution, Affichage du contenu).

Entrées d'autorisations :

Principal	Type	Accès	Hérité de	S'applique à
Administrateurs (SRV-FS\Admi...	Auto...	Contrôle total	Aucun	Ce dossier, les sous-dossiers et...
Système	Auto...	Contrôle total	Aucun	Ce dossier, les sous-dossiers et...
CREATEUR PROPRIETAIRE	Auto...	Contrôle total	Aucun	Les sous-dossiers et les fichier...
G_SIO2 (SIO\G_SIO2)	Auto...	Modification	Aucun	Ce dossier, les sous-dossiers et...

Figure 3: attribution du droit de modification au groupe de sécurité correspondant.

- Test :

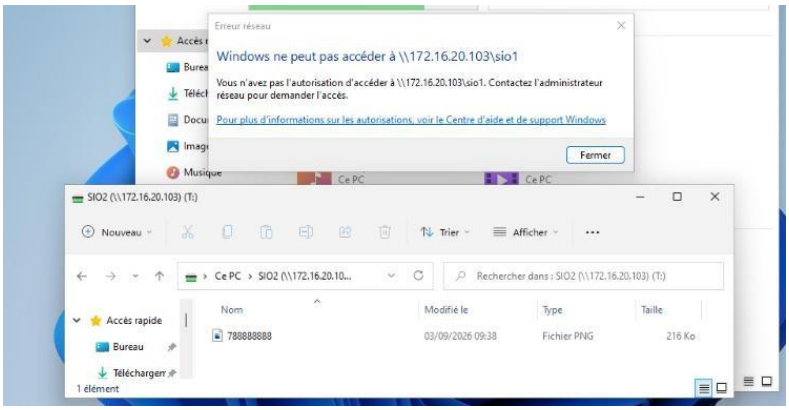
- 

Figure 4:Validation de la sécurité NTFS : l'élève SIO2 accède à son dossier partagé mais se voit refuser l'accès au dossier SIO1.