

C1.3 : Mettre en place et vérifier les niveaux d'habilitation associés à un service

Durant cette année au sein du GRETA, nous avons pu mettre en place une bonne quantité de services. Prenons le cas, par exemple, d'un TP que nous avons effectué sur le thème du « Support système des utilisateurs » et plus particulièrement sur la virtualisation d'un NAS Synology. Durant la phase de configuration de notre NAS, nous avons pu définir les règles des accès utilisateurs. Pour ce faire, nous avons pu créer, pour chaque utilisateur de notre service, un « **Dossier partagé** » et par exemple masquer les sous-dossiers et les fichiers des utilisateurs n'ayant pas d'autorisations de déposer des documents dans l'espace de stockage dédié :

Création d'un dossier partagé – extrait de la documentation sur le NAS Synology

Afin de gérer au mieux les niveaux d'habilitation des utilisateurs de notre service, nous pouvons créer des « **catégories** » afin de leur attribuer des droits personnalisés. Par exemple, dans le TP nous avons créé une catégorie d'utilisateurs « test », faisant partie des « **groupes par défaut** » et qui avait accès aux dossiers **en lecture et en écriture**.

Service	Utilisateur					
	Nom	Aperçu	Permissions de...	<input type="checkbox"/> Pas d'accès	<input checked="" type="checkbox"/> Lecture/éc...	<input type="checkbox"/> Lecture se...
	partage	Lecture/écriture	-	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Configuration des droits utilisateurs – extrait de la documentation sur le NAS Synology

Afin de contrôler au maximum les actions des utilisateurs de notre service, nous avons mis une **sécurité sur le quota de données** qu'il était possible pour eux de déposer. Nous avons fixé la limite ici à 1Mo.

Volume/Share	Quota effectif	Quota de groupe	Quota	Unité
Volume 1	1.00 MB	Sans limite	1	Mo

Limitation des données déposées – extrait de la documentation sur le NAS Synology

Pour rendre les choses un peu plus « réalistes », nous avons créé un autre groupe, les « SIO ». Ce groupe n'avait accès **qu'aux droits de lecture** pour l'ensemble des documents présents sur le NAS. Nous avons fait le test de déposer un fichier.

Éditeur de permission

Utilisateur ou groupe:

Hériter de:

Type:

Appliquer à:

Permission

- ☐ **Administration**
 - ☐ Changer les permissions
 - ☐ Prendre possession
- ☐ **Lire**
 - ☐ Traverser les dossiers/Exécuter les fichiers
 - ☐ Lister les dossiers/Lire les données
 - ☐ Lire les attributs
 - ☐ Lire les attributs étendus
 - ☐ Lire les permissions
- ☒ **Écrire**
 - ☒ Créer des fichiers/Écrire des données
 - ☒ Créer des dossiers/Ajout de données

Désolé, ce compte utilisateur ne dispose pas des droits nécessaires pour accomplir cette action.

Permissions insuffisantes en écriture – extrait de la documentation sur le NAS Synology

Enfin, nous avons créé un dossier nommé « Secret », qu'il serait impossible de voir pour le groupe « SIO ». Cela peut refléter, par exemple, des dossiers administratifs comme la comptabilité en entreprise, que ne devrait pas être visible pour tous les utilisateurs de la plateforme. Pour ce faire, nous avons **limité au maximum leurs droits** sur cet espace.

Éditeur de permission

Utilisateur ou groupe:



Hériter de:

Type:

Appliquer à:

Permission

- ▼ ☒ **Administration**
 - ☒ Changer les permissions
 - ☒ Prendre possession
- ▼ ☒ **Lire**
 - ☒ Traverser les dossiers/Exécuter les fichiers
 - ☒ Lister les dossiers/Lire les données
 - ☒ Lire les attributs
 - ☒ Lire les attributs étendus
 - ☒ Lire les permissions
- ▼ ☒ **Écrire**
 - ☒ Créer des fichiers/Écrire des données
 - ☒ Créer des dossiers/Ajouter de données

Nom	Taille	Type de fichier	Date de modification
 Public		Dossier	2021-10-13 19:43:46
 Test.txt	0 bytes	TXT Fichier	2021-10-08 13:56:30

Dossier caché pour un groupe donné – extrait de la documentation sur le NAS Synology