

Activité B1B – Droits et habilitations SNP-SHARE

PARTIE 3

Description générale

Propriétés	Description
Intitulé long	Configuration des droits et des habilitations des utilisateurs dans un système Linux
Matière	Bloc 1 Support et mise à disposition de services informatiques
Présentation	Ce contexte introduit les notions d'habilitations et de privilèges des utilisateurs et des groupes dans un système d'exploitation libre.
Transversalité	CEJMA
Auteur(es)	Steeve CHANSAY
Version	1.1.1
Date maj doc	17/11/2022
Date publication	11/11/2022
A propos du contexte	Ce contexte se base sur des éléments réels et fictifs.

Évolutions du document

VERSION	DATE	NATURE DES MODIFICATIONS
1.0.0	11/11/2022	Nouvelle version de départ
1.1.0	13/11/2022	Modification de la partie permissions
1.1.1	17/11/2022	Modification de la partie Utilisateurs et Groupes

Description activité B1B - 3

Propriétés	Description
Période indicative	Du 14 au 15 Novembre 2022
Savoirs	<ul style="list-style-type: none">Le système d'exploitation Linux, utilisateurs & groupes
Compétences	B1.1 Gérer un patrimoine informatique <ul style="list-style-type: none">Mettre en place et vérifier les niveaux d'habilitation associés à un service sous Linux
Mots-clés	Mise en réseau, configuration, OS, utilisateurs, groupes
Durée indicative	2 séances x 2h
Condition de réalisation	Toutes les réponses devront se trouver <u>dans votre cahier</u> ou dans un <u>document numérique sauvegardé</u> dans votre espace Drive accessible de n'importe quel endroit du globe... Toujours faire une COPIE de chaque document d'activité et <u>travailler</u> dessus !

Le contexte



Les fichiers (documents, images, audio, video...) stockés sur une machine est accessible en lecture et en écriture par leurs **propriétaires** ou par tout **utilisateur** du système. La configuration **des droits d'accès** est nécessaire pour respecter les critères de sécurité **DIC** (**D**isponibilité, **I**ntégrité, **C**onfidentialité).

L'**accès aux ressources** du nouveau **serveur SNP-SHARE** doit être configuré pour permettre aux utilisateurs et aux groupes d'utilisateurs d'accéder aux données.

Les missions

Pour permettre aux salariés d'exploiter leurs ressources, les fichiers devront être stockés sur le nouveau serveur SNP-SHARE et rendu disponible sur le réseau. Les droits d'accès devront être configurés pour des raisons de sécurité.

Les fichiers et les répertoires sous Linux

Les documents et les répertoires situés sur le **serveur d'origine WINDOWS SNP-SHARE** seront déplacés sur le **serveur de DESTINATION SNP-SHARE**. L'arborescence des dossiers devront être identiques au serveur d'origine.

1. **Rappelez l'arborescence des répertoires du serveur d'origine à créer.**
2. **Authentifiez-vous sur Linux et exécutez les commandes Shell suivantes**

```
bts@pxx-snp-share:~$ sudo ls /home/
```

3. **Donnez le résultat de la commande et qu'en déduisez-vous ?**

Le dossier **/home/** est le répertoire **par défaut** après vous être authentifié !

Le dossier **/home/** contient aussi **TOUS LES DOSSIERS** des utilisateurs créés ou qui seront créés !

Les créations des répertoires

Les administrateurs et les techniciens ont besoin de stocker des fichiers pour la maintenance et l'installation de mises-à-jour: pour placer leurs fichiers sur



Un dossier « DOWNLOAD » est donc nécessaire

4. **Créez un dossier « DOWNLOAD » dans /home/bts/**

```
bts@pxx-snp-share:~$ cd /home/bts/  
bts@pxx-snp-share:~$ sudo mkdir DOWNLOAD
```

5. Listez le contenu du dossier /home/bts/

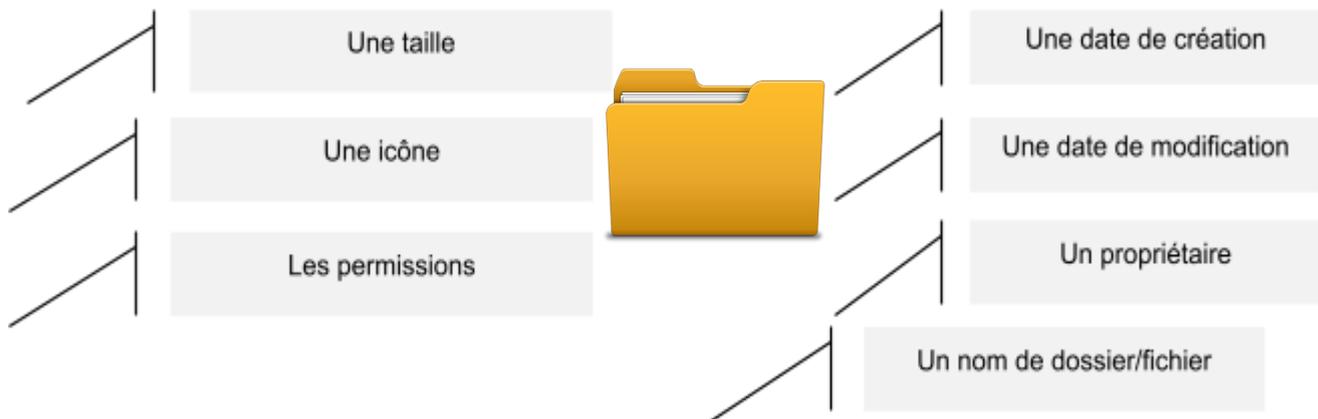
```
bts@pxx-snp-share:~$ ls -l /home/bts/
```

6. Donnez le résultat de la commande

7. Comparez les commandes `ls` et `ls -l`

Les caractéristiques d'un répertoire

Peu importe le système d'exploitation, les dossiers et les fichiers possèdent des **propriétés** qu'on peut exploiter :



Après l'exécution de la commande Shell `ls -l` sur le dossier /home/bts/, nous obtenons le résultat suivant :

```
bts@pxx-snp-share:~$ ls -l /home/bts/  
drwxr-xr-x 1 root root 4096 nov 15 07:43 DOWNLOAD
```

8. Repérez les caractéristiques d'un répertoire à partir du résultat ci-dessus

9. Vérifiez que le répertoire **DOWNLOAD** a bien été créé à la bonne heure

*Pour changer le fuseau horaire du serveur

```
bts@pxx-snp-share:~$ sudo timedatectl set-timezone Pacific/Tahiti
```

Les droits d'accès à une ressource

Source :

https://dane.ac-lyon.fr/spip/IMG/scenari/ubuntuavance/co/afficher_droits_fichiers.html

Source : <https://www.linuxtricks.fr/wiki/droits-sous-linux-utilisateurs-groupes-permissions>

Dans un serveur, le système d'exploitation **organise**, manipule et gère plusieurs types de fichiers grâce à son/ses **systèmes de fichiers** (FS – FileSystem) : NTFS (pour Windows), FAT32 (pour la plupart des OS mais vieillissant), Ext4 (pour Linux, Android) et APFS (pour Apple)...

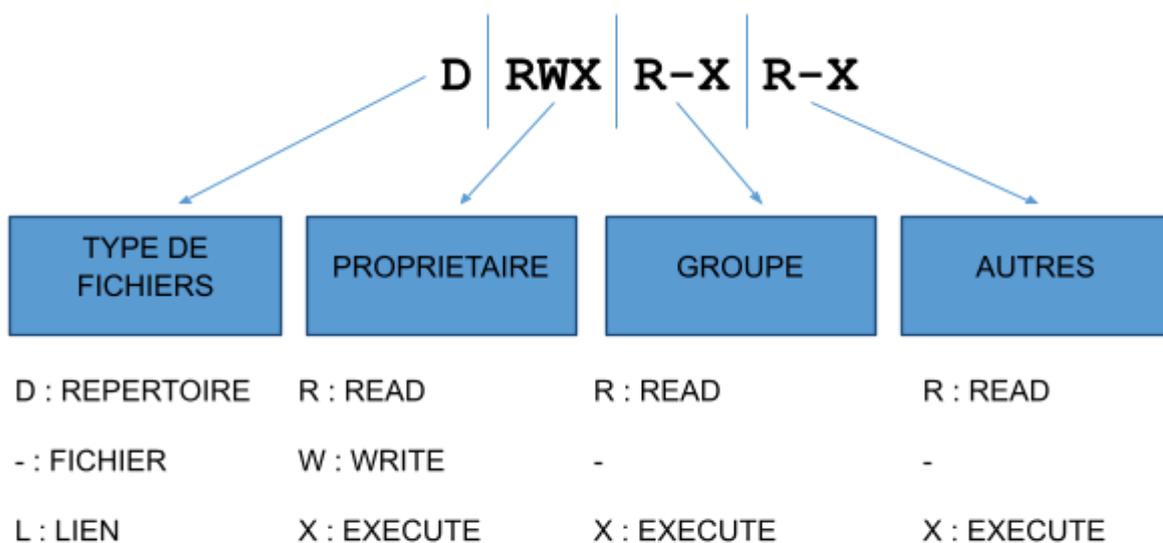
Les ressources sont identifiées sous Linux comme étant un **TYPE DE RESSOURCE** (dossiers, fichiers, liens, périphériques, socket, tube) et appartient à **UN PROPRIETAIRE (USER u)** qui possède les droits :

- DE LECTURE (READ - R)
- D'ECRITURE (WRITE - W)
- D'EXECUTION (EXECUTE - X)

Ces droits sont élargis à d'autres entités c'est-à-dire à un **GROUPE d'utilisateurs (GROUP g)** et **aux AUTRES (OTHER o)** !

```
drwxr-xr-x 1 root root DOSSIERTEST
```

Nous avons créé un dossier « Test » pour illustrer les permissions et nous obtenons celles-ci :



Explications sur les droits du dossier DOSSIERTEST :

Le PROPRIETAIRE « ROOT » a le droit de « tout faire » dans son dossier c'est-à-dire qu'il a le droit de Lire / Écrire / Exécuter.

Le GROUPE « ROOT » n'a le droit que de Lire / Exécuter

Les AUTRES n'ont le droit que de Lire / Exécuter.

UN MOT SUR L'EXECUTION

Ça veut dire que je peux exécuter un répertoire ?

La permission « eXecute » a deux significations pour les fichiers ou pour les répertoires :

Pour les fichiers

« Execute » permet d'exécuter des fichiers que l'on appelle des exécutables (file.exe Windows).

Pour les répertoires

« Execute » permet d'explorer un répertoire (aller dans les sous dossiers) ou d'ouvrir un fichier d'un répertoire (pour lire un fichier, il faut avoir la permission READ (r))



10. Analysons les attributs des répertoires suivants :

```
drwxr-xr-x 1 root root DOWNLOAD
drwxr-xr-x 1 clara clara CLARA
-rwxr----- 1 joey compta BULLETIN_DE_PAIE_CLARA_0822
Lrwxrwxrwx 1 bts bts scanpdf -> /usr/share/scanpdf
```

11. Décrivez chacune des lignes ci-dessus

Parlons de points

Et si nous donnons une valeur pour chacune des permissions :

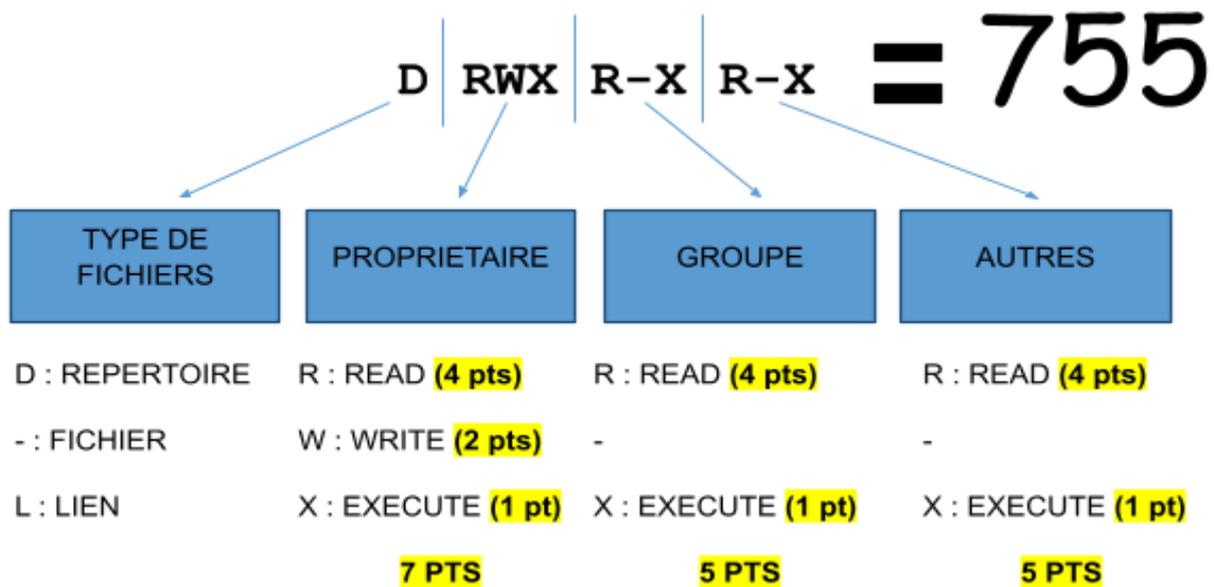
READ vaut 4 pts

WRITE vaut 2 pts

EXECUTE vaut 1 pt

Soit un total de 7 points

Cela nous donne la représentation suivante :



12. Que vaut les permissions suivantes :

- drwxr--r--
- drwxr-xr-x
- -rwxrwxrwx
- -rwxr-----
- Lrwxrwxrwx
- drwx-----

Un nouveau stagiaire dans le service marketing

Source :

https://doc.ubuntu-fr.org/tutoriel/gestion_utilisateurs_et_groupes_en_ligne_de_commande

La société **SNP** vient d'accueillir dans le **service Marketing** 2 nouveaux stagiaires. On nous demande de créer les utilisateurs.

Stagiaire : 1 Nom : ROMAGNI Prénom : Romain Identifiant / mot de passe : romain / romain	Stagiaire : 2 Nom : ARDAN Prénom : Alain Identifiant / mot de passe : alain / alain
---	--

Lorsque le système crée un utilisateur, il utilise 3 fichiers.

Le fichier PASSWD
Le fichier SHADOW
Le fichier GROUP



13. Listez le contenu du fichier /etc/passwd et /etc/group. Donnez les commandes.

Nous allons créer le groupe MARKETING. Il existe 2 fonctions qui permettent de créer des groupes sur Linux mais elles ont la même syntaxe.

```
bts@p50-snp-share:~$ sudo groupadd marketing
ou
bts@p50-snp-share:~$ sudo addgroup marketing
```

14. Vérifiez que le groupe « marketing » a bien été créé. Donnez son numéro GUID/GID.

Nous allons maintenant créer l'utilisateur ROMAIN puis le rajouter dans le service MARKETING.

```
bts@p50-snp-share:~$ sudo adduser romain
Adding user 'romain'...
Adding new group 'romain' (1005) ...
Adding new user 'romain' (1003) with group 'romain' ...
Creating home directory '/home/romain' ...
Copying files from '/etc/skel' ...
New password: _
```

15. Analysez le résultat ci-dessus. Détaillez chacune des lignes exécutées.

16. Vérifiez que l'utilisateur « romain » a bien été créé. Donnez son numéro GID ?

A la création des utilisateurs, le système intègre automatiquement les utilisateurs dans un groupe qui porte leur nom (appelé le **groupe primaire**) ainsi l'utilisateur *Romain* est membre du groupe *Romain* par défaut.

Les systèmes d'exploitation (Windows, Apple Linux) utilisent tous des « utilisateurs » appelés des **utilisateurs système**.

Les utilisateurs systèmes sont des profils qui réalisent des tâches bien précises.

Il est important de vérifier que l'utilisateur **romain** est bien dans le groupe **marketing** et de donner son numéro **UUID**.



Pour la création de l'utilisateur « ALAIN », vous tapez la commande suivante :

```
bts@p50-snp-share:~$ sudo useradd alain
```

À l'aide de la source :

17. **Quelle est la différence entre les commandes adduser et useradd ?**
18. **Donnez le groupe d'Alain.**
19. **Mettez Alain dans le groupe Marketing**

UUID et GUID

L'User ID (identifiant utilisateur) et le Group ID (Identifiant de groupe) sont des valeurs que le système utilise pour identifier un utilisateur. La numérotation commence par 1000.

20. **Listez le contenu du fichier /etc/passwd et /etc/group.**

Les utilisateurs créés possèdent un dossier par défaut dans **/home/**.

21. **Listez les dossiers de /home/**
22. **Que remarquez-vous ?**

Source : <https://www.malekal.com/quest-ce-que-etc-shadow-et-son-role/>

Source : <https://www.it-connect.fr/fichier-etc-shadow-a-quoi-sert-ce-fichier-sous-linux/>

Et le fichier /etc/shadow sert à quoi ?
Quel est le rôle de ce fichier dans tout cela ?
Comment est stocké le mot de passe dans ce fichier SHADOW ?



Lorsque l'administrateur crée un utilisateur, il stocke le mot de passe dans /etc/passwd et dans /etc/group. Chaque utilisateur possède un mot de passe qui est stocké dans le fichier /etc/shadow.

Voici un extrait du fichier Shadow :

```
test:$6$PNkLwU7L$2Hm8YRMGgRoxxt4srAzGBZJFxU7SnlDbauwb6APg5dyXSiQvQwSxHY1j0i5t2eMkZ1PwBzY1aHAvZu29wSBpJ0:16735:0:99999:7:::
```

linux-audit.com

23. À l'aide des sources, repérez dans l'extrait ci-dessus les éléments suivants :

- Nom
- Mot de passe chiffré
- Date du dernier changement de son mot de passe
- Nombre de changement de mot de passe minimum
- Nombre de changement de mot de passe maximum
- Période d'avertissement

Changement de droit d'accès et de propriétaire d'un dossier

Le technicien a créé un dossier « clients » pour Alain et a exécuter les commandes suivantes :

```
bts@p50-snp-share:~$ cd /home/alain
bts@p50-snp-share:~$ sudo mkdir clients
bts@p50-snp-share:~$ ls -l
drwxr-xr-x 1 root root 4096 Nov 13 23:00 clients
```

24. Que pouvez-vous dire du dossier clients ?

Le dossier client est un dossier qui appartient à Alain et au service Marketing et personne d'autres ne doit y accéder. Pour répondre à cette question, nous allons donc réaliser les actions suivantes :

- Modifier le propriétaire
- Modifier le groupe
- Modifier l'accès aux autres groupes (en lecture seul)

Voici les commandes réalisées :

```
f) sudo chmod 774 clients
g) sudo chown Alain clients
h) sudo chgrp Marketing clients
```

25. Liez les actions et les commandes

Il s'avère que la permission de lecture du dossier Client pour les autres groupes ne répond pas à la demande de la **SNP**.

26. **Il faudrait retirer l'accès en lecture du dossier clients pour les autres groupes. Donnez la commande**

Evolution du service Marketing

L'activité WEB de la société **SNP** est de plus en plus importante. Le conseil d'administration souhaite créer un service supplémentaire dédié à la communication Web et lié au service Marketing appelé Web Marketing. Pour ce nouveau service, un nouveau salarié vient d'être embauché pour une durée déterminée.

Services: Web Marketing ET Marketing Nom : ENINSTAN Prénom : Marc Identifiant / mot de passe : marc / marc

27. **Veillez créer l'employé MARC du service Marketing et du service Web Marketing.**
28. **Donnez les commandes Shell**
29. **Le mot de passe de Marc est trop simple. Veuillez modifier par 123456. Donnez la commande Shell.**
30. **Testez les modifications.**

Complétez le tableau de synthèse

MOTS CLES
CARTE HEURISTIQUE
<i>Collez ici votre carte faite à partir de l'application FreeMind.</i>



QUIZZ Code :
(à venir)



Easy

Il est temps de faire un petit test de connaissance !

Cela s'appelle Le QUIZZ (Questions Uniques Individuelles Zéro Zéro fautes)