

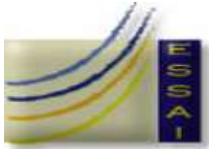


TP 5 Linux

**Gestion des utilisateurs, des groupes
et des droits d'accès sous linux**

Contact : sihemmansour@yahoo.fr

Enseignante: MANSOUR Sihem



Plan du cours



1. Gestion des utilisateurs et des groupes
2. les droits d'accès sous Linux



Gestion des utilisateurs et des groupes



1. Introduction

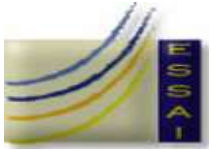
- Linux est un système multi-utilisateurs. Un utilisateur n'est obligatoirement une personne physique. Il peut détenir des fichiers, exécuter des programmes ou encore déclencher automatiquement des fonctions systèmes.
- Un utilisateurs possède un login lui permettant de démarrer une session. À ce login est associé un mot de passe personnel pour accéder au ressource système.



Gestion des utilisateurs et des groupes



- En plus de ce couple, chaque utilisateur est référencé sur le système par une valeur numérique nommée un UID (« User Identifier») unique.
- Les utilisateurs de linux sont définis dans le fichier `/etc/passwd`.
- De même chaque utilisateur est rattaché à au moins un groupe (groupe principal), chaque groupe possédant un identifiant unique, le GID (« Group Identifier»). Les groupes sont définis dans `/etc/group`.



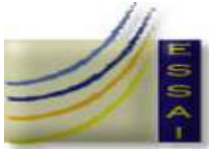
Gestion des utilisateurs et des groupes



2. L'utilisateur root:

- Pour pouvoir utiliser les commandes de ce cours, vous devez être root:
- Sous linux, vous avez deux possibilité pour vous connecter en root:
 - Sudo : devenir root pour un instant

```
administrateur@administrateur-VirtualBox: ~  
administrateur@administrateur-VirtualBox:~$ sudo ls -a /root  
[sudo] password for administrateur:  
. .. .bash_history .bashrc .cache .dbus .profile .pe
```



Gestion des utilisateurs et des groupes



- Sudo su : devenir root et le rester

```
root@admistrateur-VirtualBox:~$ sudo su
[sudo] password for administrateur:
root@admistrateur-VirtualBox:/home/administrateur# cd /root
root@admistrateur-VirtualBox:~#
```

A speech bubble points to the `sudo su` command with the text "passer et rester en root".



Gestion des utilisateurs et des groupes



3. Le fichier /etc/passwd

- Le fichier /etc/passwd contient les informations de tous les utilisateurs du système.
- Ce fichier est composé de plusieurs lignes, chaque ligne est composée des champs séparés par :
- ces champs sont:
 - Login de l'utilisateur
 - Mot de passe de l'utilisateur: ce champ peut prendre plusieurs significations:
 - *: il est impossible de authentifier sur le système avec ce compte



Gestion des utilisateurs et des groupes



- `!!`: le compte est désactivé
- `x` ou `!`: le mot de passe est conservé dans le fichier shadow.
- Champ vide: il n'y a pas de mot de passe pour ce compte.
- UID: par convention l'utilisateur root possède l'UID 0 et les UID inférieurs à 100 sont réservés aux comptes systèmes
- GID: le numéro du groupe de l'utilisateur
- Info utilisateur: informations sur l'utilisateur, chaque information est séparée par une virgule
- Répertoire personnel de l'utilisateur
- Shell: c'est l'interpréteur de commande qui sera lancé après l'authentification.



Gestion des utilisateurs et des groupes

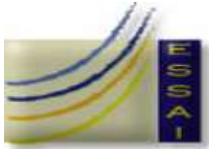


```
administrateur@administrateur-VirtualBox: ~  
administrateur@administrateur-VirtualBox:~$ cat /etc/passwd
```

le fichier qui contient les informations sur les utilisateurs

```
usbmux:x:108:46:usbmux daemon,,,:/home/usbmux:/bin/false  
kernoops:x:109:65534:Kernel Oops Tracking Daemon,,,:/bin/false  
pulse:x:110:119:PulseAudio daemon,,,:/var/run/pulse:/bin/false  
rtkit:x:111:122:RealtimeKit,,,:/proc:/bin/false  
speech-dispatcher:x:112:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false  
hplip:x:113:7:HPLIP system user,,,:/bin/false  
saned:x:114:123:,,,:/home/saned:/bin/false  
administrateur:x:1000:1000:administrateur,,,:/home/administrateur:/bin/bash
```

les différents champs qui composent le fichier /etc/passwd



Gestion des utilisateurs et des groupes



4. Le fichier /etc/group

- Sur les systèmes linux, les groupes permettent de classer les utilisateurs. Les informations concernant les groupes sont stockées dans le fichier /etc/group. Les lignes de ce fichier sont structurées de cette façon:

groupe*:GID:utilisateurs



- groupe: le nom du groupe
- *: aucune signification
- GID: c'est l'identifiant unique du groupe sous forme numérique.
- Utilisateurs: il s'agit de la liste des utilisateurs secondaires appartenant au groupe



Gestion des utilisateurs et des groupes



- Pour un utilisateur, un groupe peut être de deux types:
 - Principal: c'est le groupe auquel appartiendront par défaut tous les fichiers de l'utilisateur
 - Secondaire :les groupes secondaires sont utilisés pour gérer plus facilement les permissions d'accès au système.



Gestion des utilisateurs et des groupes



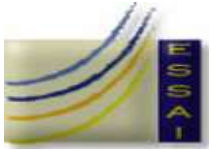
5. Les commandes de gestion des utilisateurs

a) Création d'un utilisateur:

- la commande `useradd` permet de créer un utilisateur:

`#useradd [option] <login>`

- Parmi les options de cette commande, on peut trouver :
 - `-m` pour créer le répertoire personnel . Exemple:
 - `-c <commentaire>`: avec cette option, on peut donner des informations sur l'utilisateur
 - `-s /bin/bash`



Gestion des utilisateurs et des groupes



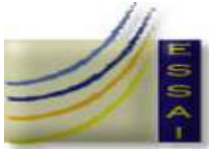
b) Modification de mot passe de l'utilisateur

#passwd [login]

```
root@admistrateur-VirtualBox: ~  
root@admistrateur-VirtualBox:~# passwd admistrateur  
Entrez le nouveau mot de passe UNIX :  
Retapez le nouveau mot de passe UNIX :  
passwd : le mot de passe a été mis à jour avec succès
```

Changer le mot de passe de l'utilisateur

- Si l'argument login n'est pas spécifié, le changement de mot de passe s'applique à l'utilisateur actuellement connecté



Gestion des utilisateurs et des groupes



b) Suppression de l'utilisateur

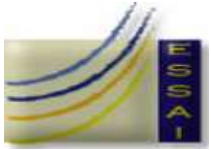
deluser nom_utilisateur

```
root@admistrateur-VirtualBox: ~  
root@admistrateur-VirtualBox:~# deluser tt  
Suppression de l'utilisateur « tt »...  
Attention ! Le groupe « tt » ne contient plus aucun membre.  
Fait.
```

- Toutefois, cette commande seule ne supprime pas le répertoire personnel de l'utilisateur **tt**. Si vous voulez supprimer aussi son home et tous ses fichiers personnels, utilisez le paramètre **--**

remove-home

```
root@admistrateur-VirtualBox: ~  
root@admistrateur-VirtualBox:~# deluser --remove-home tt  
Recherche des fichiers à sauvegarder ou à supprimer...  
Suppression des fichiers...  
Suppression de l'utilisateur « tt »...  
Attention ! Le groupe « tt » ne contient plus aucun membre.  
Fait.
```



Gestion des utilisateurs et des groupes



d) Changement d'utilisateur

su nom_utilisateur

```
administrateur@administrateur-VirtualBox:/home/tt$ su tt
Mot de passe :
```




Gestion des utilisateurs et des groupes



- la commande `addgroup` permet créer un nouveau groupe

`addgroup [option] groupe`

Exemple:

```
root@administrateur-VirtualBox: ~  
root@administrateur-VirtualBox:~# addgroup amis  
Ajout du groupe « amis » (GID 1001)...  
Fait.
```




Gestion des utilisateurs et des groupes



b) Suppression d'un groupe

- Si vous voulez supprimer un groupe, utilisez cette commande:

```
#delgroup nom_groupe
```



- avec cette commande, vous ne pouvez pas supprimer un groupe primaire.

```
root@administrateur-VirtualBox:~# delgroup administrateur
/usr/sbin/delgroup: « administrateur » possèdent toujours « administrateur » en tant
que groupe primaire !
```



Gestion des utilisateurs et des groupes



c) Modification d'un utilisateur

- La commande usermod permet d'éditer un utilisateur. Elle possède plusieurs paramètres ; nous allons en retenir deux :
- -l : renomme l'utilisateur (le nom de son répertoire personnel ne sera pas chang é par contre) ;
- -g : change de groupe.



Gestion des utilisateurs et des groupes



- Exemple :

si on veut changer le groupe primaire de l'utilisateur administrateur , taper la commande suivante:

```
root@administrateur-VirtualBox: ~  
root@administrateur-VirtualBox:~# usermod -g amis administrateur  
root@administrateur-VirtualBox:~# ls -l /home  
total 4  
drwxr-xr-x 21 administrateur amis 4096 oct.  6 22 149 administrateur
```

Changer le groupe primaire de l'utilisateur

- Si vous voulez attribuer des nouveaux groupes secondaires à un utilisateur, taper la commande: **#usermod -G gp1,gp2,...,gpn utilisateur**

```
root@administrateur-VirtualBox: ~  
root@administrateur-VirtualBox:~# usermod -G saned,amis,pulse tt
```



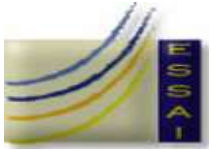
Gestion des utilisateurs et des groupes



- si vous voulez ajouter des groupes secondaires à un utilisateur sans supprimer ses autres groupes . Utilisez la commande:

: #usermod -aG gp1,gp2,...,gpn utilisateur

```
root@administrateur-VirtualBox:~# usermod -aG colord tt
```



Gestion des utilisateurs et des groupes



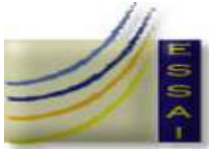
d) Affichage les groupes d'un utilisateur

- La commande qui permet d'afficher les groupes d'un utilisateur déterminé

groups nom_utilisateur

```
VirtualBox: ~  
root@administrateur-VirtualBox:~# groups tt  
tt : tt colord ssh pulse saned amis
```

A speech bubble points to the word 'Groupe primaire' in the terminal output.



Gestion des utilisateurs et des groupes



7. Changer le propriétaire et le groupe des fichiers

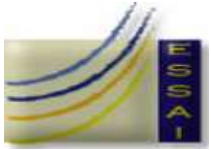
a) Changer le propriétaire d'un fichier

- Pour savoir le propriétaire d'un fichier, taper `ls -l nom_fichier`
- Supposons que votre utilisateur possède un fichier intitulé `text`:

```
administrateur@ubuntu:~$ ls -l text
-rw-rw-r-- 1 administrateur administrateur 12 oct.  7 07:08 text
```

A speech bubble with the text "le propriétaire du fichier" points to the word "administrateur" in the output line.

- Pour changer le propriétaire de ce fichier, il faut que vous connecter en mode root et taper la commande suivante:



Gestion des utilisateurs et des groupes

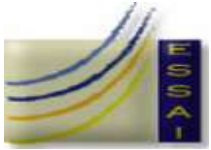


chown nom_utilisateur fichiers

```
root@admistrateur-VirtualBox:/home/admistrateur# chown tt text  
root@admistrateur-VirtualBox:/home/admistrateur# ls -l text
```

vous pouvez vérifier maintenant que le propriétaire du fichier a changé

```
root@admistrateur-VirtualBox:/home/admistrateur# ls -l text  
-rw-rw-r-- 1 tt admistrateur 12 oct.  7 07:08 text
```



Gestion des utilisateurs et des groupes



b) Changer le groupe propriétaire d'un fichier

- Pour savoir le groupe propriétaire d'un fichier, taper la commande :

`ls -l nom_fichier`

```
root@administrateur-VirtualBox: /home/administrateur# ls -l text
-rw-rw-r-- 1 tt administrateur 12 oct.  7 07:08 text
```

le groupe primaire de ce fichier

Pour changer le groupe d'un fichier, taper la commande:

`chgrp groupe nom_fichier`

```
root@administrateur-VirtualBox: /home/administrateur# chgrp amis text
root@administrateur-VirtualBox: /home/administrateur# ls -l text
-rw-rw-r-- 1 tt amis 12 oct.  7 07:08 text
```




Gestion des utilisateurs et des groupes



c) chown peut aussi changer le groupe propriétaire d'un fichier et de répertoire

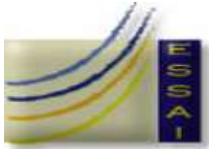
- Pour changer l'utilisateur et le groupe d'un fichier ou répertoire

chown utilisateur:groupe fichier

- **-R : affecter récursivement les sous-dossiers:**

- Très utile aussi, l'option -R de chown. Elle modifie tous les sous-dossiers et fichiers contenus dans un dossier pour y affecter un nouvel utilisateur. Exemple:

chown -R tt:tt /home/administrateur/



Les droits d'accès sous Linux

1. Présentation des droits d'accès sous Linux

- Pour consulter les droits d'accès des fichiers des répertoires, taper la commande suivante: `ls -l`

```
administrateur@administrateur-VirtualBox: ~  
administrateur@administrateur-VirtualBox:~$ ls -l  
total 56  
drwxr-xr-x 2 administrateur administrateur 4096 sept. 1 20:03 Bureau  
drwxr-xr-x 2 administrateur administrateur 4096 sept. 1 20:03 Documents  
-rw-rw-r-- 1 administrateur administrateur 46 oct. 4 00:05 doublons  
-rw-r--r-- 1 administrateur administrateur 8445 sept. 1 19:29 exemples.desktop  
drwxr-xr-x 2 administrateur administrateur 4096 sept. 1 20:03 Images  
drwxr-xr-x 2 administrateur administrateur 4096 sept. 1 20:03 Modèles
```

- Si vous appliquez la commande `ls -l` sur:
 - un fichier, elle vous donne les caractéristiques de ce dernier
 - Un répertoire, elle vous donne les caractéristique de son contenu





Les droits d'accès sous Linux

- **Explication:**
- Chaque (fichier/rep) Unix a 3 types de permissions qui déterminent ce que l'on peut faire avec :
 - Lecture : **r**
 - Fichier : l'utilisateur peut lire le contenu du fichier
 - Répertoire : l'utilisateur peut avoir la liste des fichiers du répertoire
 - Ecriture : **w**
 - Fichier : l'utilisateur peut modifier le contenu du fichier
 - Répertoire : l'utilisateur peut créer,renommer et/ou supprimer des fichiers du répertoire (indépendamment des autorisations d'accès aux fichiers)



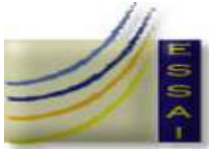
Les droits d'accès sous Linux

- Exécution :
 - Fichier : l'utilisateur peut exécuter le fichier
 - Répertoire : l'utilisateur peut se déplacer dans le répertoire,
Avec uniquement ce droit les fichiers et répertoires inclus dans celui-ci peuvent être accédés mais il faut alors obligatoirement connaître leur nom.



Les droits d'accès sous Linux

- **Le classement des utilisateurs:**
 - les systèmes linux reconnaissent trois catégories d'utilisateurs pour définir les droits sur les fichiers:
 - Le propriétaire ou user
 - Membre du groupe propriétaire ou group
 - Les autres, qui ne sont ni propriétaire ni membre du groupe autrement dit la catégorie others



Les droits d'accès sous Linux

- **Exemple:**

```
root@admistrateur-VirtualBox: /home/admistrateur
root@admistrateur-VirtualBox:/home/admistrateur# ls -l text
-rw-rw-r-- 1 admistrateur admistrateur 12 oct. 14 10:10 text
```

- Interprétation du résultat de la commande

- Le premier caractère du résultat est


- : si text est un fichier
 - d, s'il s'agit d'un répertoire
 - l: si text est un lien



il y a d'autres lettres qui ont d'autres significations



Les droits d'accès sous Linux

- Le fichier text appartient à l'utilisateur administrateur et au groupe administrateur
- L'utilisateur administrateur peut lire et modifier le fichier text
- Les utilisateurs du groupe administrateur peuvent lire et modifier le fichier text
- Les autres utilisateurs ne peuvent que lire le fichier text
-  • Seul le propriétaire d'un fichier ou l'administrateur peut modifier les droits



Les droits d'accès sous Linux

2. Comment changer les droits d'accès d'un fichier sous linux

- la commande **chmod** (change mode) permet modifier les droits sur un fichier sous Linux
- Avec cette commande, on peut utiliser deux méthodes pour modifier les droits d'accès : la forme symbolique et la forme octale.



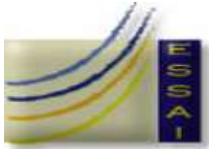
Les droits d'accès sous Linux

a. **Présentation octale:**

- A chaque droit correspond une valeur octale c'est à dire de zéro (0) à sept (7), positionnelle et cumulable.

Propriétaire			Groupe			Reste du monde		
r	w	x	r	w	x	r	w	x
400	200	100	40	20	10	4	2	1

- Pour obtenir le droit final il suffit d'additionner les valeurs.



Les droits d'accès sous Linux

Exemple

- si on veut appliquer les droits d'accès suivant sur le fichier text :

- **rwxrw-rw-** alors on fera le calcul suivant:

$$400+200+100+40+20+4+2=766$$

```
root@admistrateur-VirtualBox: /home/admistrateur
root@admistrateur-VirtualBox: /home/admistrateur# chmod 766 text
root@admistrateur-VirtualBox: /home/admistrateur# ls -l text
-rwxrw-rw- 1 admistrateur admistrateur 12 oct. 14 10:10 text
```

- **rw-r--r--** alors on fera le calcul suivant:

$$400+200+40+4=644.$$

```
root@admistrateur-VirtualBox: /home/admistrateur
root@admistrateur-VirtualBox: /home/admistrateur# chmod 644 text
root@admistrateur-VirtualBox: /home/admistrateur# ls -l text
-rw-r--r-- 1 admistrateur admistrateur 12 oct. 14 10:10 text
```



Les droits d'accès sous Linux

b. **Présentation symbolique:**

- Il existe un autre moyen de modifier les droits d'un fichier. Avec cette présentation, vous devez utiliser les symboles suivants:
 - u = user (propriétaire) ;
 - g = group (groupe) ;
 - o = other (autres).
 - ... et que :
 - + signifie : « Ajouter le droit » ;
 - - signifie : « Supprimer le droit » ;
 - = signifie : « Affecter le droit ».



Les droits d'accès sous Linux

Exemple

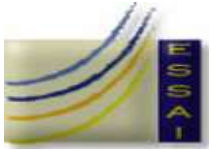
- Supposons que le fichier text possède les droits d'accès suivants:

```
root@administrateur-VirtualBox:/home/administrateur# ls -l text  
-rw-r--r-- 1 administrateur administrateur 12 oct. 14 10:10 text
```

- On veut ajouter le droit d'exécution au membres de son groupes

Pour se faire , utiliser la commande:

```
root@administrateur-VirtualBox:/home/administrateur# chmod g+x text  
root@administrateur-VirtualBox:/home/administrateur# ls -l text  
-rw-r-xr-- 1 administrateur administrateur 12 oct. 14 10:10 text
```



Les droits d'accès sous Linux

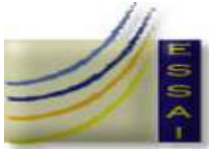
Exemple

- On veut attribuer aux others tous les droits d'accès sur le fichier text

```
root@admistrateur-VirtualBox: /home/admistrateur
root@admistrateur-VirtualBox:/home/admistrateur# chmod o=rwx text
root@admistrateur-VirtualBox:/home/admistrateur# ls -l text
-rw-r-xrwx 1 admistrateur admistrateur 12 oct. 14 10:10 text
```

- Maintenant, on veut retirer le droit d'exécution à tous les membres de groupes de fichier text

```
root@admistrateur-VirtualBox: /home/admistrateur
root@admistrateur-VirtualBox:/home/admistrateur# chmod g-x text
root@admistrateur-VirtualBox:/home/admistrateur# ls -l text
-rw-r--rwx 1 admistrateur admistrateur 12 oct. 14 10:10 text
```



Les droits d'accès sous Linux

- On peut rassembler des catégories des utilisateurs et les attribuer les mêmes droits pour un fichier donné.

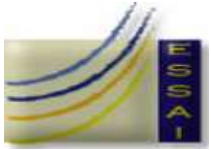
Exemple: **#chmod go+r text**

- on peut rassembler aussi les permissions

Exemple: **#chmod o+rw text**

- on peut attribuer des permissions pour chaque catégories d'utilisateurs dans une même ligne de commande

Exemple: **#chmod g-w,o+r text**



Les droits d'accès sous Linux

3. Les grandes famille de droits

- Sous linux, on trouve trois types de protections:
 - **Les droits permissifs:** le propriétaire possède tous les droits, et a suffisamment confiance pour laisser confiance aux autres (group et others) l'accès en consultation et exécution sur ses fichiers(exécutable) et ses dossiers. Les droits sont `rwxr-xr-x` en notation symbolique et `755` en notation octale ».



Les droits d'accès sous Linux

- **Les droits protecteurs:** la confiance de propriétaire est limitée aux seuls membres de son groupe. Il a tout les droits, le groupe possède le droit de lire et d'exécuter, les autres n'ont aucun droit. Les droits sont `rwxr-x---` en notation symbolique et `750` en notation octale
- **Les droits paranoïaques:** le propriétaire n'a la confiance qu'en lui-même, les autres n'ont aucun droit sur son fichier. Les droits sont `rwx-----` en notation symbolique et `700` en notation octale



Les droits d'accès sous Linux

4. Droit par défaut et umask

- Lors de la création d'un fichier ou d'un répertoire, des droits par défaut sont appliqués.
- ces droits sont inscrits dans le système et ne peuvent pas être changés.
- Par défaut, les valeurs sont les suivants(selon la représentation octale):



Les droits d'accès sous Linux

- 666: pour les fichier ordinaire
- 777: pour les dossier et fichier exécutable.
- Le système permet d'appliquer un filtre de droit lors de la création d'un fichier ou d'un dossier. Ce filtre est une valeur numérique qui sera soustraite aux droits par défaut afin de définir les droits attribués à un fichier.
- ce filtre se nomme **umask**, et est par défaut configuré à 022. il est possible de changer la valeur de umask.



Les droits d'accès sous Linux

- 666: pour les fichier ordinaire
- 777: pour les dossier et fichier exécutable.
- Le système permet d'appliquer un filtre de droit lors de la création d'un fichier ou d'un dossier. Ce filtre est une valeur numérique qui sera soustraite aux droits par défaut afin de définir les droits attribués à un fichier.
- ce filtre se nomme **umask**, et est par défaut configuré à 022. il est possible de changer la valeur de umask.



Les droits d'accès sous Linux

- 666: pour les fichier ordinaire
- 777: pour les dossier et fichier exécutable.
- Le système permet d'appliquer un filtre de droit lors de la création d'un fichier ou d'un dossier. Ce filtre est une valeur numérique qui sera soustraite aux droits par défaut afin de définir les droits attribués à un fichier.
- ce filtre se nomme **umask**, et est par défaut configuré à 022. il est possible de changer la valeur de umask.



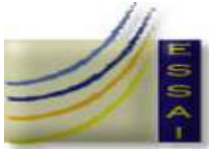
Les droits d'accès sous Linux

Exemple

```
root@admistrateur-VirtualBox: /home/admistrateur
root@admistrateur-VirtualBox:/home/admistrateur# umask
0022
root@admistrateur-VirtualBox:/home/admistrateur# touch f1
root@admistrateur-VirtualBox:/home/admistrateur# ls -l f1
-rw-r--r-- 1 root root 0 oct. 18 06:37 f1
```

A chaque création d'un fichier ordinaire, ses droits d'accès attribués par défaut sont 666: rw-rw-rw-. si applique le masque 0022 => $666 - 22 = 644$. cad le fichier créé aura comme droit **rw- r--r--**
le même principe s'applique sur les dossier qui vont être créé avec les droits 755. en appliquant le masque: $777 - 22 = 755$: **rw-x r-x r-x**

On va voir le masque installé par défaut



Les droits d'accès sous Linux

- si on crée un nouveau masque ayant la valeur 26, donc
- chaque fichier ordinaire non exécutable, il va avoir comme droits d'accès: $666-026 = 640(\text{rw-r-----})$
- Chaque répertoire ou un fichier exécutable, il va avoir comme droits d'accès: $777-026=751 (\text{rwxr-x--x})$
- Les grandes famille de masques
 - Les masques permissifs: 022
 - Les masques protecteurs: 027
 - Les masques paranoïaque: 077

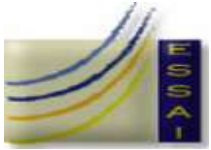




Les droits d'accès sous Linux

5. Le sticky bit

- Le sticky-bit est représenté par la lettre t en notation symbolique pour 1000 en notation octale.
- Il sert principalement à contrôler la destruction des fichiers dans un répertoire donné, en limitant cette action seulement au propriétaire de fichier.
- Exemple:
 - Le repertoire /tmp est un répertoire du travail à tous les utilisateurs (u,g et o ont tous le droit w). Sans le droit sticky-bit tout le monde peut supprimer des fichiers même ceux qui ne l'appartient.

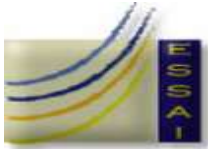


Les droits d'accès sous Linux

- Avec le droit déjà indiqué, chaque utilisateur ne peut supprimer que ses fichiers

Exemple

```
root@admistrateur-VirtualBox: /home/admistrateur
root@admistrateur-VirtualBox:/home/admistrateur# chmod +t /tmp
root@admistrateur-VirtualBox:/home/admistrateur# ls -ld /tmp
drwxrwxrwt 8 root root 4096 oct. 18 07:17 /tmp
root@admistrateur-VirtualBox:/home/admistrateur#
```

MERCI POUR VOTRE ATTENTION

Ens: MANSOUR Sihem