|  |  |
| --- | --- |
| Special Permissions (SetUID, SetGID and Sticky Bit) in Linux - Cyber Sophia | Autorisations spéciales |

# Définitions

**setuid**Ce bit est présent pour les **binaires qui ont des autorisations d’exécution**.   
Le bit setuid indique simplement que lors de l'exécution de binaires, il définira ses **autorisations sur celles de** **l'utilisateur qui l'a créé** (propriétaire), au lieu de le définir sur l'utilisateur qui l'a lancé.   
Cela donne à un **utilisateur le droit d’effectuer une tâche spécifique** qui nécessite des **privilèges root/superuser**, **sans** toutefois vouloir lui **donner un accès sudo ou root** ;

**setgid**  
Le bit setgid affecte à la fois les **fichiers et les répertoires**.   
Lorsqu'il est utilisé sur un **fichier**, il **s'exécute avec les privilèges du groupe de l'utilisateur qui le possède** au lieu de s'exécuter avec ceux du groupe de l'utilisateur qui l'a exécuté.  
Lorsque le bit est défini pour un **répertoire**, l'**ensemble de fichiers dans ce répertoire aura le même groupe que le groupe du répertoire parent**, et non celui de l'utilisateur qui a créé ces fichiers.   
Ceci est utilisé pour le **partage de fichiers** car ils peuvent être **modifiés par tous les utilisateurs qui font partie du groupe** du répertoire parent.

**bit persistant (*sticky bit*)**  
Le bit persistant est seulement **défini pour les répertoires**.  
Le bit persistant **permet au propriétaire ou à root de supprimer des fichiers et des sous‑répertoires**.   
Les autres utilisateurs se voient **refuser le droit de supprimer des fichiers**, quelles que soient les autorisations du répertoire.

# setuid

L'exemple le plus courant sous Linux est sudo.

**>> id  
uid=1000(tux) gid=1000(tux ) groupes=1000(tux) …**

**>> which sudo  
/usr/bin/sudo**

**>> ls -l /usr/bin/sudo  
-rwsr-xr-x 1 root root 136808 Jan 31 13:37 /usr/bin/sudo**

On peut constater que l’autorisation **s** pour les autorisations de l'utilisateur a remplacé le **x** que l’on retrouve normalement.

Cela indique que lorsqu'un utilisateur exécute ce binaire, le système d'exploitation exécute ce fichier, non pas en tant qu'utilisateur **tux**, mais en tant qu'utilisateur **root**.   
En ce qui concerne l'utilisation de la commande sudo, cela permet à un utilisateur normal d'exécuter des fonctions système élevées sans avoir à se connecter en tant que l'utilisateur root.

## Modification du bit suid

La définition de l'autorisation setuid est aussi simple que la définition de toute autre autorisation sous Linux. …  
**>> chmod u+s <Nom du fichier>**  
**>> chmod u+s document.texte**

# setgid

setgid, lorsqu'il est utilisé sur des fichiers, est très similaire à setuid.   
Un binaire, lorsqu'il est exécuté, s'exécutera en tant que groupe propriétaire du fichier.

Un exemple typique d'un fichier qui l'utilise est la commande crontab …  
**>> which crontab  
/usr/bin/crontab**

**>> ls -l /usr/bin/crontab   
-rwxr-sr-x 1 root crontab 43568 22 fév 2021 /usr/bin/crontab**

L'application de l'autorisation setgid sur un **répertoire possède un comportement différent**.

Un répertoire qui possède autorisation setgid fera de sorte que tous les fichiers créés dans ce répertoire appartiendront au groupe du répertoire par opposition au groupe du propriétaire.

Voici un exemple typique de l’utilisation de l’autorisation setuid pour un répertoire …  
**>> mkdir /tmp/data  
>> ls -ld /tmp/data  
drwxr-xr-x 2 tux tux 4096 2 déc 07:53 /tmp/data**

On grée un groupe nommé gestionnaires …  
**>>** **sudo groupadd gestionnaires   
>> cat /etc/group | grep gestionnaires  
gestionnaires:x:1001:**

Ensuite, on modifie la propriété du groupe du répertoire en utilisant la commande chgrp et on ajouter l'autorisation setgid ...  
**>> sudo chgrp --verbose gestionnaires /tmp/data  
groupe de '/tmp/data' modifié de tux en gestionnaires**

**>> sudo chmod --verbose g+s /tmp/data  
Le mode de '/tmp/data' a été modifié de 0755 (rwxr-xr-x) en 2755 (rwxr-sr-x)**

**>> ls -ld /tmp/data  
drwxr-sr-x 2 tux gestionnaires 4096 2 déc 07:53 /tmp/data**

On crée un nouveau fichier dans le répertoire /tmp/data.  
Puisque le setgid est défini sur le répertoire et qu'il appartient au groupe gestionnaires, ce fichier obtiendra gestionnaires comme groupe …  
**>> touch /tmp/data/document.texte  
>> ls -l /tmp/data/document.texte  
-rw-r--r-- 1 tux gestionnaires 0 2 déc 08:08 /tmp/data/document.texte**

## Modification du bit sgid

La définition de l'autorisation setuid est aussi simple que la définition de toute autre autorisation sous Linux. …  
**>> chmod g+s <Nom du fichier>**  
**>> chmod g+s document.texte**

# Bit persistant

La dernière autorisation spéciale est le bit persistant (*sticky bit*).   
Lorsque ce bit est défini sur un répertoire, les fichiers de ce répertoire ne peuvent être supprimés que par le propriétaire.

Une utilisation typique est le répertoire /tmp/.  
Le répertoire /tmp est accessible en **rwx** par n'importe quel utilisateur, sans toutefois que les autres utilisateurs peuvent supprimer les fichiers des autres …  
**>> ls -ld /tmp  
drwxrwxrwt 11 root root 4096 2 déc 07:53 /tmp**

Notez que /tmp peut être écrit par tout le monde mais a le 't' à la place du 'x' à la fin de la liste des autorisations. Cela signifie qu'il a le bit collant.

Modification du bit persistant

Le bit pesistant est défini avec la commande est aussi simple que la définition de toute autre autorisation sous Linux. …  
**>> chmod +t <Nom du répertoire>**

**>> sudo mkdir --verbose /tmp/documents  
mkdir: création du répertoire '/tmp/documents'  
>> ls -ld /tmp/documents  
drwxr-xr-x 2 tux tux 4096 2 déc 10:34 /tmp/documents**

**>> chmod --verbose -t /tmp/documents  
Le mode de '/tmp/documents' a été modifié de 0755 (rwxr-xr-x) en 1755 (rwxr-xr-t)   
>> ls -ld /tmp/documents  
drwxr-xr-t 2 lsavard lsavard 4096 2 déc 10:34 /tmp/documents**

# Définition d'autorisations spéciales avec la notation numérique

Pour les autorisations spéciales, on ajoute aux autorisations régulières avec un autre nombre où …

* 4 pour le setuid ;
* 2 pour le setgid   
  et
* 1 pour le bit persistant.

Les commandes suivantes sont toutes identiques …

**>> chmod 4755 <Nom du fichier>**  
**>> chmod u+s <Nom du fichier**

**>> chmod 2755 <Nom du répertoire>**  
**>> chmod g+s <Nom du répertoire>**

**>> chmod 1755 <Nom du répertoire>**  
**>> chmod +t <Nom du répertoire>**

# Suppression des autorisations spéciales

Pour supprimer des autorisations spéciales on peut utiliser la commande chmod avec un signe **-** …  
**>> chmod u-s <Nom du fichier>**

**>> chmod g-s <Nom du répertoire>**

**>> chmod -t <Nom du répertoire>**