

Permissions Linux : la checklist sûre avant d'utiliser chmod ou chown

Avant de modifier un fichier, vérifiez ce qui doit réellement changer : son propriétaire, son groupe ou ses droits d'accès. Cette fiche vous aide à appliquer la commande la plus ciblée, puis à contrôler le résultat.

Au sommaire

1. Vérifier avant toute modification
2. Choisir la bonne commande
3. Lire les droits sans se tromper
4. Repères chmod à utiliser selon le besoin
5. Contrôle final et réflexes de sécurité

1. Vérifier avant toute modification



Se placer dans le bon répertoire avec pwd

Évite de viser un fichier homonyme situé ailleurs.



Afficher l'état actuel avec ls -l fichier

Repérez les droits, le propriétaire et le groupe.



Confirmer le chemin exact et le type d'élément

Un - indique un fichier ordinaire ; un d indique un dossier.



Identifier le problème à corriger

Propriétaire, groupe ou permission : ce sont trois réglages distincts.



Prévoir une vérification avec ls -l après la commande

Modifiez un seul élément à la fois lorsque c'est possible.



LA GESTION RÉCURSIVE SÉCURISÉE DES PERMISSIONS LINUX

Protéger vos données, appliquer les bons droits, éviter les risques.



1



RÉPERTOIRE CIBLE

```
/var/www/html/monsite
```

C'est le répertoire racine de votre site web. Toutes les permissions seront appliquées à son contenu.

2



PERMISSIONS DES DOSSIERS

```
find /var/www/html/monsite -type d -exec chmod 755 {} \;
```

Commande simplifiée : `find -type d chmod 755`

Attribue le droit 755 à tous les dossiers (drwxr-xr-x) :

- Propriétaire : lecture, écriture, exécution
- Groupe : lecture, exécution
- Autres : lecture, exécution

3



PERMISSIONS DES FICHIERS

```
find /var/www/html/monsite -type f -exec chmod 644 {} \;
```

Commande simplifiée : `find -type f chmod 644`

Attribue le droit 644 à tous les fichiers (-rw-r--r-) :

- Propriétaire : lecture, écriture
- Groupe : lecture
- Autres : lecture

4



LE RISQUE À ÉVITER

```
chmod -R 755 /var/www/html/monsite
```

Cette commande rend **TOUS** les fichiers exécutables (drwxr-xr-x), y compris les fichiers PHP, HTML, CSS, JS, etc.

Cela représente un risque de sécurité majeur !



BONNES PRATIQUES

- ✓ Appliquez des permissions strictes et adaptées au besoin.
- ✓ Séparez les droits des dossiers et des fichiers.
- ✓ Évitez les commandes récursives globales comme `chmod -R 755`.
- ✓ Vérifiez régulièrement les permissions de votre site.



Moins de privilèges, plus de sécurité.

INFOGRAPHIE Schéma chmod Linux séparant les permissions des dossiers en 755 et des fichiers en 644.

2. Choisir la bonne commande

Besoin	Commande adaptée	Exemple
Changer le propriétaire	chown	<code>sudo chown olivia manuel.odt</code>
Changer le propriétaire et le groupe	chown utilisateur:groupe	<code>sudo chown olivia:partageur manuel.odt</code>
Changer uniquement le groupe	chgrp	<code>sudo chgrp devs projet.txt</code>
Ajouter ou retirer un droit précis	chmod symbolique	<code>chmod u+x script.sh</code>
Définir tous les droits d'un coup	chmod octal	<code>chmod 644 notes.txt</code>

3. Lire les droits sans se tromper

Les droits sont répartis entre le propriétaire (u), le groupe (g) et les autres utilisateurs (o).

Sur un dossier, x permet de le traverser et d'accéder à son contenu selon les autres droits accordés.

En mode octal, lecture vaut 4, écriture 2 et exécution 1 : chaque chiffre correspond à la somme des droits accordés.

r signifie lecture, w écriture et x exécution.

En mode symbolique, associez une catégorie, un opérateur et un droit : u+x, o-w, g+w ou g=rw.

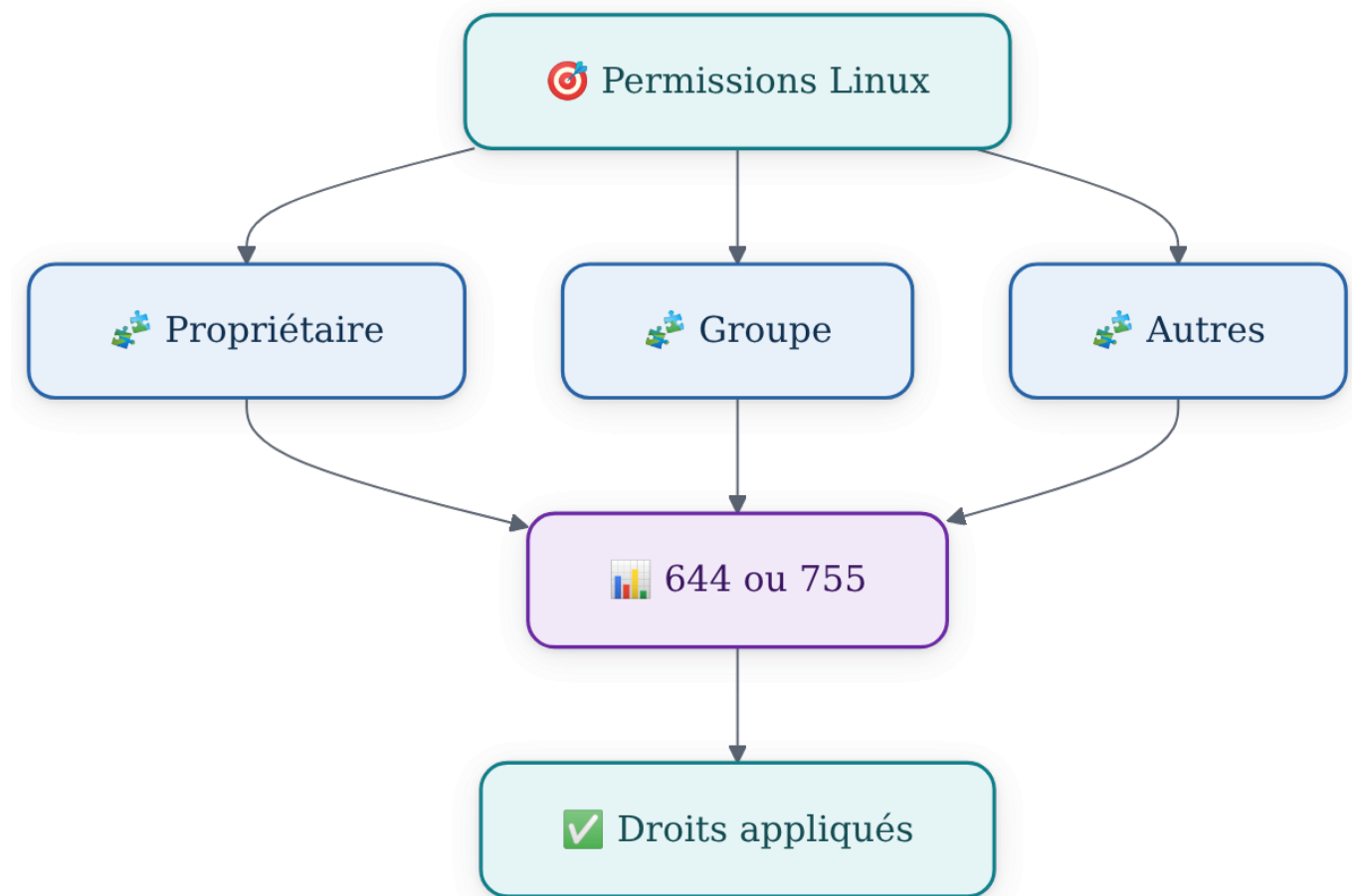


SCHÉMA Repère visuel : propriétaire, groupe, autres utilisateurs et valeurs chmod courantes.

4. Repères chmod à utiliser selon le besoin

Valeur	Droits	Usage indiqué
644	Propriétaire : lecture/écriture ; groupe et autres : lecture	Fichier texte, document ou fichier web non exécutable
755	Propriétaire : tous droits ; groupe et autres : lecture/exécution	Dossier accessible ou script à exécuter
700	Propriétaire : tous droits ; aucun droit pour groupe et autres	Dossier ou script strictement privé
775	Propriétaire et groupe : tous droits ; autres : lecture/exécution	Dossier de travail partagé par un groupe identifié

5. Contrôle final et réflexes de sécurité

- Relancer ls -l après chaque changement**
Vérifiez le propriétaire, le groupe et la chaîne de droits obtenue.
- Utiliser sudo seulement lorsque nécessaire**
Il est souvent requis pour modifier un fichier appartenant à un autre utilisateur ou à un compte système.
- Préférer chmod symbolique pour une correction limitée**
Exemple : `chmod o-w fichier.conf` retire uniquement l'écriture aux autres utilisateurs.
- Adapter les droits au service et à l'usage réel**
Un fichier ordinaire et un dossier n'ont pas nécessairement besoin des mêmes permissions.

Éviter chmod 777 comme solution automatique

Accorder tous les droits à tous les utilisateurs n'est pas un correctif sûr.

Être particulièrement prudent avant une commande récursive

Contrôlez d'abord le chemin et le résultat sur un élément précis.

✓ Le principe à retenir

Accordez uniquement les droits nécessaires : chown règle la propriété, chgrp règle le groupe et chmod règle l'accès. Changer l'un ne corrige pas automatiquement les autres.

Avant toute modification étendue ou récursive, vérifiez le chemin ciblé et testez la commande sur un fichier ou dossier précis.