
setfacl

Définis les listes de contrôle d'accès des fichiers

Cet utilitaire définit les ACL des fichiers et répertoires. Sur la ligne de commande, une séquence de commande est suivie par une séquence de fichiers (qui peut être suivis par une autre séquence de commandes, ...).

Les options `-m` et `-x` s'attendent à une ACL sur la ligne de commande. Plusieurs entrées d'ACL sont séparés par des `,`. Les options `-M` et `-X` lisent une ACL depuis un fichier ou l'entrée standard.

Les options `-set` et `-set-file` définissent l'ACL d'un fichier ou un répertoire. L'ACL précédente est remplacée. Les entrées d'ACL pour cette opération doivent inclure les permissions.

Les options `-m` (`--modify`) et `-M` (`--modify-file`) modifient l'ACL d'un fichier ou répertoire. Les entrées d'ACL pour cette opération doivent inclure les permissions.

les options `-x` (`--remove`) et `-X` (`--remove-file`) suppriment les entrée d'ACL. Ce n'est pas une erreur de supprimer une entrée qui n'existe pas. Seules les entrées d'ACL dans le champ perms sont acceptés, sauf si `POSIXLY_CORRECT` est définis.

En lisant les fichiers avec les options `-M` et `-X`, setfacl accepte les productions de getfacl. Il y a plus d'une entrée d'ACL par ligne.

Si setfacl est utilisé dans un système de fichier qui ne supporte pas les ACL, setfacl opère sur les bits de permission des fichiers. Si l'ACL ne contient pas tous les bits de permission, setfacl modifie les bits de permission pour refléter les ACL le plus proche possible, écrit un message sur stderr, et retourne avec un status supérieur à 0.

Permissions

Le propriétaire du fichier et les processus capable de `CAP_FOWNER` ont le droit de modifier les ACL d'un fichier. C'est analogue aux permissions requises pour accéder au mode de fichier. (dans les système Linux, root est le seul utilisateur avec la capacité `CAP_FOWNER`)

OPTIONS

- b, --remove-all** Supprime toutes les entrée d'ACL étendues. Les entrées d'ACL de base du propriétaire, groupe et autre sont conservés.
- k, --remove-default** Supprime toutes les ACL par défaut.
- n, --no-mask** Ne recalcule pas le masque de permissions effectives
- mask** Recalcule le masque de permissions effectives, même si une entrée de mask a été explicitement donné.
- d, --default** Toutes les opérations s'appliquent sur l'ACL par défaut. Les entrées d'ACL régulières dans le jeu d'entrée sont transformés en entrée d'ACL par défaut.
- restore-file** Restaure un backup de permissions créé par getfacl -R ou similaire. Toutes les permissions de l'arborescence sont restaurés en utilisant ce mécanisme. Si l'entrée contient le propriétaire et le groupe, setfacl tente de restaurer le propriétaire et le groupe. Si l'entrée contient des flags (qui définissent le setuid, setgid, et sticky bits), setfacl définit ces 3 bits en fonction ; sinon il est supprime.
- test** Mode simulation. Liste les ACL résultantes.

-
- R, -recursive** Applique les opérations à tous les fichiers et répertoires récursivement. Cette option ne peut pas être mixé avec `-restore`.
 - L, -logical** Mode logique, traverse les liens symboliques. Seulement avec `-R`. ne peut pas être utilisé avec `-restore`.
 - P, -physical** Mode physique, ne traverse pas les liens symboliques. Seulement avec `-R`. ne peut pas être utilisé avec `-restore`.
 - Fin des options de la ligne de commande
 - Si un paramètre est un `'-'`, lis depuis l'entrée standard

Entrées d'ACL

L'utilitaire `setfacl` reconnaît les formats d'entrée d'ACL suivantes (de blanc ont été inséré pour plus de clarté) :

Permissions d'un utilisateur nommé. Permissions du propriétaire du fichier si l'uid est vide

[d[efault] :] [u[ser] :]uid [:perms]

Permissions du groupe nommé. Permissions du groupe propriétaire si gid est vide

[d[efault] :] g[roup] :gid [:perms]

Masque de droits effectifs

[d[efault] :] m[ask][:] [:perms]

Permissions pour les autres

[d[efault] :] o[ther][:] [:perms]

Les espaces blanc entre les caractères de délimitation sont ignorés. Les entrée d'ACL propre incluant les permissions sont utilisées dans les opérations `modify` et `set`. (les options `-m`, `-M`, `-set` et `-set-file`). Les entrées sans le champ `perms` sont utilisé pour la suppression des entrées (options `-x` et `-X`).

Pour `uid` et `gid`, vous pouvez spécifier soit un nom, soit un nombre.

Le champ `perms` est une combinaison des caractères qui indiquent les permissions : `read` (`r`), `write` (`w`), `execute` (`x`). `perms` peut également être un chiffre octal.

Entrées créées automatiquement

Initialement, les fichiers et répertoires ne contiennent que les 3 entrées d'ACL de base. Il y a certaines règles qui doivent être satisfaites pour une ACL soit valide :

- Les 3 entrées de base ne peuvent pas être supprimés.
- Quand une ACL contient des entrées d'utilisateurs nommés ou des groupes nommés, elle doit également contenir un masque de droits effectifs.
- Quand une ACL contient des entrées d'ACL par défaut, les 3 entrées de base doivent également exister.
- Quand une ACL par défaut contient des entrées `user` et `group` nommés, elle doit également contenir un masque de droits effectifs.

Pour aider l'utilisateur à s'assurer de ses règles, `setfacl` créé des entrées des entrées existantes sous certaines conditions.

- Si une ACL contient des entrées `user` et `group` nommés, et qu'aucun `mask` n'existe, une entrée `mask` contient les même permission que l'entrée `group` créé. Sauf si `-n` est donné, les permission de l'entrée `mask` sont ensuite ajustés pour inclure l'union de toutes les permissions affectées par l'entrée de `mask`.
- Si une ACL par défaut est créé, et qu'elle ne contient pas de propriétaire, groupe, ou `other`, une copie de l'ACL sont ajoutés à l'ACL par défaut.
- Si une ACL par défaut contient des entrées utilisateur ou groupes nommés, et qu'aucun `mask` n'existe, une entrée `mask` contenant les même permissions que que l'entrée de groupe de l'ACL par défaut est ajouté. Sauf si `-n` est donné, les permission de l'entrée `mask` sont ensuite ajustés pour inclure l'union de toutes les permissions affectées par l'entrée de `mask`.

Exemples

Ajouter un droit de lecture à un utilisateur

setfacl -m u :lisa :r file

révoquer l'accès en écriture à tous les groupes et tous les utilisateurs nommés en utilisant le masque de droits effectifs

setfacl -m m : :rx file

Supprimer une entrée de groupe nommé de l'ACL du fichier

setfacl -x g :staff file

Copier l'ACL d'un fichier dans un autre

getfacl file1 | setfacl --set-file=- file2

copier l'ACL d'accès dans l'ACL par défaut

getfacl --access dir | setfacl -d -M- dir