acl

Listes de contrôle d'accès

Tout objet peut être considéré comme étant associé avec une ACL qui gouverne l'accès discrétionnaire de cet objet. Cette ACL est référée à une ACL d'accès. En plus, un répertoire peut avoir une ACL associée qui gouverne l'ACL initial pour les objets créés dans ce répertoire. Cette ACL est référé à l'ACL par défaut.

Une ACL consiste d'un jeu d'entrées d'ACL. Une entrée ACL spécifie les permissions d'accès sur l'objet associé pour un utilisateur ou groupe individuel comme une combinaison de permissions de lecture, écriture et de recherche/exécution.

Une entrée d'ACL contient un type de tag d'entrée, une qualifiant de tag d'entrée, et un jeu de permissions. On utilise le terme qualifier pour dénoter le qualifieur de tag d'entrée d'une entrée d'ACL.

Le qualifieur dénote l'identifiant d'un utilisateur ou un groupe, pour les entrées avec les types de tag d'ACL_USER ou ACL_GROUP, respectivement. Les entrées avec des types de tag autre que ACL_USER ou ACL_GROUP n'ont pas de qualifieur définis.

Les types de tag d'entrée suivant sont définis

ACL_USER_OBJ dénote les droits d'accès pour le propriétaire du fichier

ACL_USER dénote les droits d'accès pour les utilisateurs identifiés par le qualifieur de l'entrée

ACL_GROUP_OBJ dénote les droits d'accès pour le groupe du fichier

ACL_GROUP dénote les droits d'accès pour les groupes identifiés par le qualifieur de l'entrée

ACL_MASK dénote les droits d'accès maximum qui peuvent être donnés par les entrées de type ACL_USER, ACL_GROUP_OBJ ou ACL_GROUP.

ACL_OTHER dénote les droits d'accès pour les processus qui ne matchent aucune autre entrée dans l'acl.

Quand un accès est vérifié, les entrées ACL_USER_OBJ et ACL_USER sont testés avec le user ID effectif. L'ID de groupe effectif, et les IDs de groupe supplémentaire sont testé avec les entrées ACL_GROUP_OBJ et ACL_GROUP.

Une ACL valide contient exactement une entrée avec chaque types de tag ACL_USER_OBJ, ACL_GROUP_OBJ, et ACL_OTHER. Les entrées avec les types de tag ACL_USER et ACL_GROUP peuvent apparaître 0 ou plusieurs fois dans une ACL. Dans une ACL qui contient des entrée de type de tag ACL_USER ou ACL_GROUP doivent contenir exactement une entrée de type de tag ACL_MASK. Si une ACL ne contient pas d'entrées de type de tag ACL_USER ou ACL_GROUP, l'entrée ACL_MASK est optionnel.

Tous les qualifier d'UID doivent être unique dans les entrées du type de tag ACL_USER, et tous les GID doivent être unique dans les entrée de type de tag ACL_GROUP.

La fonction acl_get_file() retourne une ACL avec 0 entrées d'ACL comme ACL par défaut d'un répertoire, si le répertoire n'est pas associé avec une ACL par défaut. La fonction acl_set_file() accepte également une ACL avec 0 entrées d'ACL comme ACL par défaut pour les répertoires, dénotant que le répertoire ne devrait pas être associé avec une ACL par défaut. C'est équivalement à utiliser la fonction acl_delete_def_file().

[SECTION] name="Correspondance entre les entrées d'ACL et les bits de permission de fichier" table="paragraphes" imbrication="0"

Il y a une correspondance entre les permissions du propriétaire du fichier, groupe, et autres et les entrées d'ACL : les permissions du propriétaire correspondent aux permissions de l'entrée ACL_USER_OBJ. Si l'ACL a une entrée ACL_MASK, les permissions du groupe correspondent aux permission de l'entrée ACL_MASK. Sinon, si l'ACL n'a pas d'entrée ACL_MASK, les permissions du groupe correspondent aux permissions de l'entrée ACL_GROUP_OBJ. Les permissions des autres correspondent aux permission de l'entrée ACL_OTHER_OBJ.

Les permissions du propriétaire, du groupe, et des autres match toujours les permissions de l'entrée d'ACL correspondante. Les modification des bits de permission de fichier résultent en la modification des entrées d'ACL correspondantes, et les modification des entrées d'ACL résultent en la modification des bits de permission de fichier.

Création d'objet et ACL par défaut

L'ACL d'accès à un objet fichier est initialisé quand l'objet est créé avec une des fonctions creat(), mkdir(), mknod(), mkfifo() ou open(). Si une ACL par défaut est associée avec un répertoire, le paramètre mode des fonctions créant les objets fichier et l'ACL par défaut du répertoire sont utilisés pour déterminer l'ACL du nouvel objet :

1. Le nouvel objet hérite de l'ACL par défaut du répertoire correspondant comme son ACL d'accès
2. Les entrées d'ACL correspondant aux bits de permission de fichier sont modifiés pour qu'elles ne contiennent pas de permission qui ne sont pas contenus dans les permissions spécifiées par le paramètre mode.

Si aucune ACL par défaut n'est associé avec un répertoire, le paramètre mode sont utilisés pour déterminer l'ACL du nouvel objet :

1. Le nouvel objet se voit assigner une ACL d'accès contenant des entrées de type de tag ACL_USER_OBJ, ACL_GROUP_OBJ, et ACL_OTHER. Les permission de ces entrées sont définie aux permissions spécifiées par le masque de création de fichier.
2. Les entrées d'ACL d'accès correspondant au bits de permission de fichier sont modifié pour qu'ils ne contiennent pas de permission qui ne soient pas contenus dans les permissions spécifiées par le paramètre mode.

Algorithme de vérification d'accès

Un processus peut demander un accès en lecture, écriture ou exécution/recherche sur un objet fichier protégé par une ACL. L'algorithme de vérification d'accès détermine si l'accès à l'objet est autorisé.

1. Si le User ID effectif du processus correspond au User ID du propriétaire du fichier, alors
   - Si l'entrée ACL_USER_OBJ contient les permissions demandées, l'accès est donné,
   - Sinon l'accès est refusé
2. Sinon si le User ID effectif du processus correspond au qualifier d'une entrée de type ACL_USER, alors
   - Si l'entrée ACL_USER correspondant et l'entrée ACL_MASK contiennent les permissions requises, l'accès est donné
   - Sinon l'accès est refusé
3. Sinon si le GID effectif d'un ID de groupe supplémentaire du processus correspond au groupe du fichier ou le qualifier d'une entrée du type ACL_GROUP, alord
   - Si l'ACL contient une entrée ACL_MASK, alors
     . Si l'entrée ACL_MASK et une des entrées ACL_GROUP_OBJ ou ACL_GROUP correspondant contient les permissions requises, l'accès est donné
     . Sinon l'accès est refusé
   - Sinon (noter qu'il ne peut pas y avoir d'entrée ACL_GROUP sans entrée ACL_MASK)
     . Si l'entrée ACL_GROUP_OBJ contient les permissions requises, l'accès est donné,
     . Sinon l'accès est refusé
4. Sinon si l'entrée ACL_OTHER contient les permissions requises, l'accès est donné
5. Sinon l'accès est refusé.

Forme de texte d'ACL

Une forme de texte long et cours pour représenter les ACL sont définis. Dans les 2 formes, les entrées d'ACL sont représenté en 3 champs séparés : le type de tag de l'entrée de l'ACL, le qualifier de l'entrée de l'ACL, et les permissions d'accès discrétionnaires. Le premier champ contient un des mots clé de type de tag suivant :

user Une entrée ACL user spécifie que l'accès est donné soit au propriétaire du fichier (type de tag d'entrée ACL_USER_OBJ) ou un utilisateur spécifique (type de tag d'entrée ACL_USER).

group Une entrée ACL group spécifie que l'accès est donné soit au groupe du fichier (type de tag d'entrée ACL_GROUP_OBJ), ou un groupe spécifique (type de tag d'entrée ACL_GROUP).

mask Une entrée ACL mask spécifie l'accès maximum qui peut être donné à toute entrée d'ACL excepté l'entrée utilisateur pour le propriétaire du fichier et l'entrée other (type de tag d'entrée ACL_MASK).

other Une entrée ACL other spécifie l'accès donné à tout processus qui ne correspond à aucune entrée d'ACL user et group (type de tag d'entrée ACL_OTHER).

Le second champ contient l'identifiant d'utilisateur ou de groupe associé avec l'entrée d'ACL pour les entrées de type de tag ACL_USER ou ACL_GROUP, et est vide pour toutes les autres entrées. Un identifiant d'utilisateur peut être un nom d'utilisateur ou un UID. Un identifiant de groupe peut être un nom de groupe ou un ID.

Le troisième champ contient les permissions d'accès discrétionnaires. Les permission de lire, écrire, et recherche/exécution sont représentés par les caractères r,w et y, respectivement. Chacun de ces caractères est remplacé par le caractère '-' pour indiquer qu'une permission est absente. En convertissant de la forme texte en représentation interne, les permissions absente n'ont pas besoin d'être spécifiés.

Les espaces blanc sont autorisé au début et à la fin de chaque entrée d'ACL, et immédiatement avant et après un séparateur de champ.

Forme de texte long

La forme de texte long contient une entrée d'ACL par ligne. En plus, un '#' peut commencer un commentaire qui s'étend jusqu'à la fin de la ligne. Si une entrée d'ACL ACL_USER, ACL_GROUP_OBJ ou ACL_GROUP contient des permissions qui ne sont pas contenus dans ACL_MASK, l'entrée est suivie par un '#', la chaîne 'effective', et les permissions d'accès effectif définis par cette entrée.

Exemple :

```
user::rw-
user:lisa:rw- #effective:r-
group::r-
group:toolies:rw- #effective:r-
mask::r-
other::r-
```

Forme de texte court

La forme de texte court est une séquence d'entrées d'ACL séparés par des virgules, et est utilisant comme entrée. Les commantaires ne sont pas supportés. Les mots clé de type de tag d'entrée peuvent apparaître soit sous le forme complète, soit sous forme d'une seule lettre. Les abréviations sont pour user (u), group (g), mask (m) et other (o). Les permission peuvent contenir au moins un caractère de chaque dans n'importe quel ordre.

Exemple :

```
u::rw-,u:lisa:rw-,g::r-,g:toolies:rw-,m::r-,o::r-
g:toolies:rw,u:lisa:rw,u::wr,g::r,o::r,m::r
```

Dans les systèmes qui supportent les ACL, les utilitaires de fichier ls, cp et mv changent leur comportement de la manière suivante :

- Pour les fichier qui ont une ACL par défaut ou une ACL d'accès qui contient plus que les 3 entrées requise, ls -l affiche un signe + après la chaîne de permissions.
- Si le flag -p est spécifié, l'utilisataire cp préserve également les ACL. Si ce n'est pas possible, une alerte est produite.
- mv préserve toujours les ACL. Si ce n'est pas possible, une alerte est produite.