nfs4_acl

Listes de contrôle d'accès NFSv4

Le format de sortie pour une ACL NFSv4 est :

```
A::OWNER@:rwatTnNcCy
A::alice@nfsdomain.org:rxtncy
A::bob@nfsdomain.org:rwadtTnNcCy
A:g:GROUP@:rtncy
D:g:GROUP@:waxTC
A::EVERYONE@:rtncy
D::EVERYONE@:waxTC
```

Format d'ACL

une ACL NFSv4 est écrite comme une acl_spec, consistant d'une ou plusieurs ace_specs. Une simple ACE NFSv4 est une ace_spec de 4 champs sous la forme : **type :flags :principal :permissions**

Types d'ACE

- **A** Allow - autorise un principal à effectuer les actions
- **D** Deny - Empêche le principal d'effectuer des actions
- **U** Audit - Log toute tentative d'accès par un principal nécessitant les permissions.
- **L** Alarm - génère une alarme système à une tentative d'accès

Flags d'ACE

Il y a 3 types de flags : groupe, héritage et administration. Noter que les ACE sont hérités de l'ACL du répertoire parent à leur création.

Flags de groupe

- **g** groupe -indique que le principal représente un groupe

Flags d'héritage

- **d** Les sous-répertoires créés héritent de l'ACE
- **f** Les fichier créé héritent de l'ACE, sans les flags d'héritage.
- **n** Les sous-répertoires créé héritent de l'ACE, sans les flags d'héritage

i L'ACE n'est pas considérée dans les vérifications de permissions, mais sont héritables ; cependant, ce flag est supprimé des ACE héritées

Flags d'administration

S Déclenche une alarm/audit quand le principal est autorisé à effectuer une action couverte par les permissions

F Déclenche une alarm/audit quand le principal n'est pas autorisé à effectuer une action couverte par les permissions

Principaux d'ACE

Un principal est soit un utilisateur nommé, soit un groupe, ou un des 3 principaux spéciaux : OWNER@, GROUP@, et EVERYONE@, qui représentent les distinctions POSIX.

Permissions d'ACE

r fichier : lire les données / répertoire : lister le contenu

w fichier : écrire des données / répertoire : Créer des fichiers

a fichier : Ajouter des données / répertoire : Créer des sous-répertoires

x fichier : Exécuter / répertoires : Changer de répertoire

d Supprime le fichier/répertoire.

D répertoire : supprimer les fichiers et sous-répertoires.

t Lire les attributs du fichier/répertoire

T Changer les attributs du fichier/répertoire

n Lire les attributs nommés du fichier/répertoire

N Changer les attributs nommés du fichier/répertoire

c Lire les ACL

C Changer les ACL

o Changer le propriétaire du fichier/répertoire

y Autorise les clients à utiliser les E/S synchrones avec le serveur.

Flags d'héritage

Les flags d'héritage peuvent être divisés en 2 catégories : primaire (héritage fichier/répertoire) et secondaires (pas de propagation d'héritage et héritage uniquement), qui sont seulement significatifs dans la mesure où ils affectent les 2 flags primaires.

Les flags no-propagate-inherit et inherit-only peuvent être difficiles à retenir : le premier détermine si l'ACE hérité d'un nouveau répertoire enfant est lui-même héritable ; le second détermine si une ACE héritable affecte le répertoire parent (en plus d'être héritable). Ils peuvent être utilisés en tandem.

Quand un sous-répertoire hérite d'une ACE de l'ACL du répertoire parent, cela peut être fait de 2 manières différentes dépendant de l'implémentation du serveur :

- Dans le premier cas, la même ACE est définis dans l'ACL du sous-répertoire

- Dans le second cas, 2 ACE différentes sont définis dans l'ACL du sous-répertoire : un avec tous les flags d'héritage enlevés, et un avec le flag inherit-only. Cette approche simplifie la modification des droits d'accès aux sous-répertoire lui-même sans modifier les ACE héritables.

Accès refusés

les ACE deny devraient être évités autant que possible, cela augmente la confusion et la complexité. L'ordre des ACE est importante, et en dépit de l'ambiguïté de la rfc3530, les permissions non explicitement autorisées sont refusées.