attr

Attributs étendus

Les attributs étendus sont des paires nom :valeur associés de manière permanente avec les fichiers et les répertoires, similaire aux chaînes d'environnement associés avec un processus. Un attribut peut être définis ou non-définis. S'il est définis, sa valeur peut être vide ou non-vide

Les attributs étendus sont des extensions aux attributs normaux qui sont associés avec tous les inodes dans le système de fichier. Ils sont souvent utilisé pour fournir des fonctionnalités additionnels au système de fichier, par exemple, des fonctionnalités de sécurité additionnels tels que les ACL.

Les utilisateurs avec un accès en recherche sur un fichier ou répertoire peut récupérer une liste de noms d'attributs définis pour ce fichier ou répertoire.

Les attributs étendus sont accedés comme des objets atomique. Lire récupère toute la valeur d'un attribut et le stocke dans un tampon. Écrire remplace une valeur précédente avec une nouvelle valeur.

L'espace consommé par les attributs étendus sont comptés dans le quota disque.

Actuellement, le support pour les attributs étendus est implémenté dans les systèmes de fichier ext2, ext3, ext4, XFS, JFS et reiserfs.

Espaces de nom d'attribut étendus

Les noms d'attribut sont des chaînes terminés par un 0. Le nom d'attribut est toujours spécifié sous la forme pleinement qualifié namespace.attribute. par exemple user.mime_type, trusted.md5sum, system.posix_acl_access, ou security.selinux.

Le mécanisme d'espace de nom est utilisé pour définir les différentes classes d'attribut étendus. Ces différentes classe existent pour de nombreuses raisons, par exemple les permissions et capabilities requises pour manipuler les attributs étendus d'un espace de nom peut différer d'un autre.

Actuellement les classes d'attribut étendus security, system, trusted, et user sont définis comme décris ci-dessous. D'autres classes pourront être ajoutés dans le future.

Attributs de sécurité étendus

L'espace de nom d'attribut de sécurité est utilisé par les module de sécurité du kernel, tels que SELinux. Les permissions d'accès en lecture et écriture aux attributs de sécurité dépend de la stratégie implémenté pour chaque attribut de sécurité par le module de sécurité. Quand aucun module de sécurité n'est chargé, tous les processus ont un accès en lecture aux attributs de sécurité étendu, et l'accès en écriture est limitée aux processus qui ont la capability CAP_SYS_ADMIN.

Attributs système étendu

Les attributs système étendus sont utilisés par le kernel pour stocker des objets système tels que des listes de contrôle d'accès et des capabilities. Les permissions d'accès en lecture et écriture au attributs système dépendent de la stratégie implémenté pour chaque attribut système implémenté par le système de fichier dans le kernel.

Attributs étendus de confiance

Les attributs étendus de confiance sont visibles et accessible seulement aux processus qui ont la capability CAP_SYS_ADMIN. Les attributs dans cette classe sont utilisés pour implémenter des mécanismes dans l'espace utilisateur qui conserve des informations dans des attributs étendus que des processus ordinaire ne devraient pas avoir accès.

Attributs utilisateur étendus

Les attributs utilisateur étendus peuvent être assignés aux fichier et répertoires pour stocker des informations additionnelles tels que le type mime, jeu de caractère ou encodage d'un fichier. Les permissions d'accès pour les attributs utilisateur sont définis par les bits de permission de fichier.

Les bits de permission de fichier des fichiers régulier sont interprétés différemment des bits de permission de fichier des fichier spéciaux et des liens symboliques. Pour les fichier régulier et les répertoires les bits de permission de fichier définissent l'accès au contenu des fichiers, alors que pour les fichiers spéciaux de périphériques ils définissent l'accès au périphérique décris par le fichier spécial. Les permissions de fichier des liens symboliques ne sont pas utilisé pour la vérification d'accès. Ces différences permettent aux utilisateurs de consommer des ressources système d'une manière non contrôlable par les quotas disques pour les fichier spéciaux et les répertoires.

Pour cette raison, les attributs utilisateur étendus sont seulement permis pour les fichier régulier et les répertoire, let l'accès aux attributs utilisateurs étendus est restreint au propriétaire et aux utilisateurs avec les capabilities appropriés pour les répertoire avec le sticky bit mis.

Différences de système de fichiers

Le kernel et le système de fichiers peuvent placer des limites sur le nombre et la taille maximum d'attributs étendus qui peuvent être associés avec un fichier. Certains système de fichier comme ext2/3 et reiserfs exigent que le système de fichier soit monté avec l'option de montage user_xattr pour que les attributs étendus soient utilisés.

Dans les implémentations ext2/3/4 courante, chaque attribut étendu doit être contenu dans un seul block du système de fichier.

Dans les implémentations reiserfs et XFS, il n'y a pas de limite pratique sur le nombre ou la taille d'attributs étendus associé avec un fichier, et les algorithmes utilisé pour stocker les informations d'attribut sur le disque sont scalaires.

Dans l'implémentation du système de fichier JFS, les noms peuvent avoir jusqu'à 255 octets et des valeurs jusqu'à 64Ko.

Notes

Vu que les systèmes de fichier sur lequel les attributs étendus sont stockés peuvent également être utilisés dans les architecture avec un ordre d'octets différent et une taille de mot différent, le stockage des valeurs d'attribut doivent faire d'objet d'une attention particulière.