Gérer les listes de contrôle d'accès NFSv4

ONTAP 9

NetApp
April 24, 2024

Sommaire

Gérer les listes de contrôle d'accès NFSv4

Avantages des listes de contrôle d'accès NFSv4

Il existe de nombreux avantages pour activer les listes de contrôle d'accès NFSv4.

Voici quelques-uns des avantages majeurs apportés par les ACL NFSv4 :

- Contrôle plus précis de l'accès des utilisateurs aux fichiers et aux répertoires
- Sécurité NFS renforcée
- Interopérabilité accrue avec CIFS
- Suppression de la limitation NFS de 16 groupes par utilisateur

Fonctionnement des listes de contrôle d'accès NFSv4

Un client utilisant des listes de contrôle d'accès NFSv4 peut définir et afficher des listes de contrôle d'accès sur les fichiers et les répertoires du système. Lorsqu'un nouveau fichier ou sous-répertoire est créé dans un répertoire comportant une liste de contrôle d'accès, le nouveau fichier ou sous-répertoire hérite de toutes les entrées ACL (ACE) de la liste de contrôle d'accès qui ont été marquées avec les indicateurs d'héritage appropriés.

Lorsqu'un fichier ou un répertoire est créé à la suite d'une requête NFSv4, l'ACL du fichier ou répertoire résultant dépend du fait que la demande de création de fichier inclut une ACL ou uniquement les autorisations d'accès aux fichiers UNIX standard, et si le répertoire parent possède une ACL :

- Si la requête inclut une liste de contrôle d'accès, cette liste de contrôle d'accès est utilisée.
- Si la demande comprend uniquement des autorisations d'accès aux fichiers UNIX standard mais que le répertoire parent possède une ACL, les ACE de l'ACL du répertoire parent sont hérités par le nouveau fichier ou répertoire tant que les ACE ont été balisés avec les indicateurs d'héritage appropriés.

  Une ACL parent est héritée même si `-v4.0-acl` est défini sur `off`.

- Si la requête inclut uniquement les autorisations d'accès aux fichiers UNIX standard et que le répertoire parent ne dispose pas d'ACL, le mode fichier client est utilisé pour définir les autorisations d'accès aux fichiers UNIX standard.
- Si la requête inclut uniquement les autorisations d'accès aux fichiers UNIX standard et que le répertoire parent dispose d'une ACL non héritable, le nouvel objet est créé uniquement avec des bits de mode.

Si le `-chown-mode` le paramètre a été défini sur `restricted` à l'aide des commandes dans `vserver nfs` ou `vserver export-policy rule` Familles, la propriété des fichiers ne peut être modifiée que par le superutilisateur, même si les autorisations sur disque définies avec les ACL NFSv4 permettent à un utilisateur non-root de modifier la propriété des fichiers. Pour plus d'informations, consultez les pages de manuel correspondantes.

Activer ou désactiver la modification des listes de contrôle d'accès NFSv4

Lorsque ONTAP reçoit un `chmod` Commande pour un fichier ou un répertoire avec une liste de contrôle d'accès, la liste de contrôle d'accès est par défaut conservée et modifiée pour refléter le changement de bit de mode. Vous pouvez désactiver le `-v4-acl -preserve` Paramètre pour modifier le comportement si vous souhaitez que la liste de contrôle d'accès soit supprimée.

Description de la tâche

Lors de l'utilisation d'un style de sécurité unifié, ce paramètre indique également si les autorisations de fichier NTFS sont conservées ou supprimées lorsqu'un client envoie une commande chmod, chgroup ou chown pour un fichier ou un répertoire.

La valeur par défaut de ce paramètre est activée.

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Saisissez la commande suivante…
Activer la conservation et la modification des listes de contrôle d'accès NFSv4 existantes (par défaut)	`vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled`
Désactivez la conservation et déposez les ACL NFSv4 lors du changement de bits de mode	`vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled`

3. Retour au niveau de privilège admin :

   ```
   set -privilege admin
   ```

Comment ONTAP utilise les listes de contrôle d'accès NFSv4 pour déterminer si elles peuvent supprimer un fichier

Pour déterminer s'il peut supprimer un fichier, ONTAP utilise une combinaison du bit DE SUPPRESSION du fichier et du bit DE SUPPRESSION_ENFANT du répertoire contenant. Pour plus d'informations, consultez le document NFS 4.1 RFC 5661.

Activer ou désactiver les ACL NFSv4

Pour activer ou désactiver les ACL NFSv4, vous pouvez modifier le `-v4.0-acl` et `-v4.1-acl` options. Ces options sont désactivées par défaut.

Description de la tâche

Le `-v4.0-acl` ou `-v4.1-acl` Option contrôle la définition et l'affichage des ACL NFSv4 ; elle ne contrôle pas l'application de ces listes de contrôle d'accès pour la vérification de l'accès.

Étape

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Alors…
Activez les listes de contrôle d'accès NFSv4.0	Saisissez la commande suivante : `vserver nfs modify -vserver vserver_name -v4.0-acl enabled`
Désactivez les listes de contrôle d'accès NFSv4.0	Saisissez la commande suivante : `vserver nfs modify -vserver vserver_name -v4.0-acl disabled`
Activer les ACL NFSv4.1	Saisissez la commande suivante : `vserver nfs modify -vserver vserver_name -v4.1-acl enabled`
Désactiver les listes de contrôle d'accès NFSv4.1	Saisissez la commande suivante : `vserver nfs modify -vserver vserver_name -v4.1-acl disabled`

Modifier la limite ACE maximale pour les listes de contrôle d'accès NFSv4

Vous pouvez modifier le nombre maximal d'ACE autorisés pour chaque ACL NFSv4 en modifiant le paramètre `-v4-acl-max-aces`. Par défaut, la limite est définie sur 400 ACE pour chaque ACL. L'augmentation de cette limite peut permettre de réussir la migration des données avec des listes de contrôle d'accès contenant plus de 400 ACE vers les systèmes de stockage exécutant ONTAP.

Description de la tâche

L'augmentation de cette limite peut avoir un impact sur les performances des clients accédant aux fichiers avec des listes de contrôle d'accès NFSv4.

Étapes

1. Définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

2. Modifier la limite ACE maximale pour les listes de contrôle d'accès NFSv4 :

   ```
   vserver nfs modify -v4-acl-max-aces max_ace_limit
   ```

   Plage valide de

   `max_ace_limit` est `192` à `1024`.

3. Retour au niveau de privilège admin :

   ```
   set -privilege admin
   ```