



Gérer les listes de contrôle d'accès NFSv4

ONTAP 9

NetApp
April 24, 2024

Sommaire

- Gérer les listes de contrôle d'accès NFSv4 1
 - Avantages des listes de contrôle d'accès NFSv4 1
 - Fonctionnement des listes de contrôle d'accès NFSv4 1
 - Activer ou désactiver la modification des listes de contrôle d'accès NFSv4 2
 - Comment ONTAP utilise les listes de contrôle d'accès NFSv4 pour déterminer si elles peuvent supprimer un fichier 2
 - Activer ou désactiver les ACL NFSv4. 3
 - Modifier la limite ACE maximale pour les listes de contrôle d'accès NFSv4 3

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)	<code>vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled</code>
Désactivez la conservation et déposez les ACL NFSv4 lors du changement de bits de mode	<code>vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled</code>

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 : <code>vserver nfs modify -vserver vserver_name -v4.0-acl enabled</code>
Désactivez les listes de contrôle d'accès NFSv4.0	Saisissez la commande suivante : <code>vserver nfs modify -vserver vserver_name -v4.0-acl disabled</code>
Activer les ACL NFSv4.1	Saisissez la commande suivante : <code>vserver nfs modify -vserver vserver_name -v4.1-acl enabled</code>
Désactiver les listes de contrôle d'accès NFSv4.1	Saisissez la commande suivante : <code>vserver nfs modify -vserver vserver_name -v4.1-acl disabled</code>

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
```

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.