



Gérer la manière dont la sécurité des fichiers est présentée aux clients SMB pour les données de type sécurité UNIX

ONTAP 9

NetApp
April 24, 2024

Sommaire

- Gérer la manière dont la sécurité des fichiers est présentée aux clients SMB pour les données de type sécurité UNIX 1
 - Gérer la manière dont la sécurité des fichiers est présentée aux clients SMB pour une présentation des données de type sécurité UNIX 1
 - Activez ou désactivez la présentation des listes de contrôle d'accès NTFS pour les données de type de sécurité UNIX 2
 - Comment ONTAP préserve les autorisations UNIX 2
 - Gérez les autorisations UNIX à l'aide de l'onglet sécurité Windows 2

Gérer la manière dont la sécurité des fichiers est présentée aux clients SMB pour les données de type sécurité UNIX

Gérer la manière dont la sécurité des fichiers est présentée aux clients SMB pour une présentation des données de type sécurité UNIX

Vous pouvez choisir comment présenter la sécurité des fichiers aux clients SMB pour les données de style de sécurité UNIX en activant ou désactivant la présentation d'ACL NTFS aux clients SMB. Chaque paramètre présente des avantages, que vous devez comprendre pour choisir le paramètre le mieux adapté aux besoins de votre entreprise.

Par défaut, ONTAP présente des autorisations UNIX sur des volumes de type sécurité UNIX aux clients SMB comme des listes de contrôle d'accès NTFS. Dans certains cas, cette option est souhaitable, notamment :

- Vous souhaitez afficher et modifier les autorisations UNIX à l'aide de l'onglet **sécurité** de la zone Propriétés de Windows.

Vous ne pouvez pas modifier les autorisations d'un client Windows si l'opération n'est pas autorisée par le système UNIX. Par exemple, vous ne pouvez pas modifier la propriété d'un fichier que vous ne possédez pas, car le système UNIX ne permet pas cette opération. Cette restriction empêche les clients SMB de contourner les autorisations UNIX définies sur les fichiers et dossiers.

- Les utilisateurs modifient et enregistrent des fichiers sur le volume de style de sécurité UNIX en utilisant certaines applications Windows, par exemple Microsoft Office, où ONTAP doit préserver les autorisations UNIX pendant les opérations de sauvegarde.
- Votre environnement compte certaines applications Windows qui doivent lire les listes de contrôle d'accès NTFS sur les fichiers qu'elles utilisent.

Dans certaines circonstances, vous pouvez désactiver la présentation des autorisations UNIX en tant que listes de contrôle d'accès NTFS. Si cette fonctionnalité est désactivée, ONTAP présente les volumes de style de sécurité UNIX en tant que volumes FAT aux clients SMB. Il existe des raisons spécifiques de vouloir présenter des volumes de style sécurité UNIX en tant que volumes FAT aux clients SMB :

- Vous ne modifiez que les autorisations UNIX en utilisant des montages sur des clients UNIX.

L'onglet sécurité n'est pas disponible lorsqu'un volume de style de sécurité UNIX est mappé sur un client SMB. Le lecteur mappé semble être formaté avec le système de fichiers FAT, qui ne dispose pas d'autorisations de fichier.

- Vous utilisez des applications sur SMB qui définissent les listes de contrôle d'accès NTFS sur les fichiers et dossiers auxquels vous accédez, ce qui peut échouer si les données résident sur des volumes de style de sécurité UNIX.

Si ONTAP signale le volume comme FAT, l'application n'essaie pas de modifier une ACL.

Informations associées

[Configuration des styles de sécurité sur les volumes FlexVol](#)

Activez ou désactivez la présentation des listes de contrôle d'accès NTFS pour les données de type de sécurité UNIX

Vous pouvez activer ou désactiver la présentation des listes de contrôle d'accès NTFS aux clients SMB pour les données de style de sécurité UNIX (volumes de style sécurité UNIX et volumes de type sécurité mixte avec sécurité effective UNIX).

Description de la tâche

Si vous activez cette option, ONTAP présente les fichiers et les dossiers sur les volumes avec un style de sécurité UNIX efficace aux clients SMB comme ayant des listes de contrôle d'accès NTFS. Si vous désactivez cette option, les volumes sont présentés en tant que volumes FAT aux clients SMB. Par défaut, cette valeur doit présenter des listes de contrôle d'accès NTFS aux clients SMB.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Configurez le paramètre d'option ACL NTFS UNIX : `vserver cifs options modify -vserver vserver_name -is-unix-nt-acl-enabled {true|false}`
3. Vérifiez que l'option est réglée sur la valeur souhaitée : `vserver cifs options show -vserver vserver_name`
4. Retour au niveau de privilège admin : `set -privilege admin`

Comment ONTAP préserve les autorisations UNIX

Lorsque les fichiers d'un volume FlexVol qui disposent actuellement d'autorisations UNIX sont modifiés et enregistrés par des applications Windows, ONTAP peut préserver les autorisations UNIX.

Lorsque des applications sur des clients Windows modifient et enregistrent des fichiers, elles lisent les propriétés de sécurité du fichier, créent un nouveau fichier temporaire, appliquent ces propriétés au fichier temporaire, puis donnent au fichier temporaire le nom du fichier d'origine.

Lorsque les clients Windows effectuent une requête pour les propriétés de sécurité, ils reçoivent une ACL construite qui représente exactement les autorisations UNIX. Le seul but de cette liste de contrôle d'accès construite est de préserver les autorisations UNIX du fichier lorsque les fichiers sont mis à jour par les applications Windows pour s'assurer que les fichiers résultants ont les mêmes autorisations UNIX. ONTAP ne définit pas d'ACL NTFS à l'aide de la liste de contrôle d'accès construite.

Gérez les autorisations UNIX à l'aide de l'onglet sécurité Windows

Si vous souhaitez manipuler les autorisations UNIX de fichiers ou de dossiers dans des volumes ou des qtrees de style sécurité mixtes sur des SVM, vous pouvez utiliser l'onglet sécurité sur les clients Windows. Vous pouvez également utiliser des applications qui peuvent interroger et définir des listes de contrôle d'accès Windows.

- Modification des autorisations UNIX

Vous pouvez utiliser l'onglet sécurité Windows pour afficher et modifier les autorisations UNIX pour un volume ou qtree de style de sécurité mixte. Si vous utilisez l'onglet principal sécurité Windows pour modifier les autorisations UNIX, vous devez d'abord supprimer l'ACE que vous souhaitez modifier (ceci définit les bits de mode sur 0) avant d'effectuer vos modifications. Vous pouvez également utiliser l'éditeur avancé pour modifier les autorisations.

Si des autorisations de mode sont utilisées, vous pouvez modifier directement les autorisations de mode pour l'UID, le GID et d'autres (tous les autres utilisateurs disposant d'un compte sur l'ordinateur). Par exemple, si l'UID affiché possède des autorisations r-x, vous pouvez modifier les autorisations UID sur rwx.

- Modification des autorisations UNIX en autorisations NTFS

Vous pouvez utiliser l'onglet sécurité Windows pour remplacer les objets de sécurité UNIX par des objets de sécurité Windows sur un volume ou qtree de style de sécurité mixte, où les fichiers et les dossiers ont une méthode de sécurité efficace UNIX.

Vous devez d'abord supprimer toutes les entrées d'autorisation UNIX répertoriées pour pouvoir les remplacer par les objets utilisateur et groupe Windows souhaités. Vous pouvez ensuite configurer des listes de contrôle d'accès NTFS sur les objets utilisateur et groupe Windows. En supprimant tous les objets de sécurité UNIX et en ajoutant uniquement des utilisateurs et des groupes Windows à un fichier ou à un dossier dans un volume ou qtree de style de sécurité mixte, vous modifiez le style de sécurité effectif sur le fichier ou le dossier d'UNIX à NTFS.

Lors de la modification des autorisations sur un dossier, le comportement par défaut de Windows consiste à propager ces modifications à tous les sous-dossiers et fichiers. Par conséquent, vous devez modifier le choix de propagation sur le paramètre souhaité si vous ne souhaitez pas propager de modification du style de sécurité à tous les dossiers, sous-dossiers et fichiers enfants.

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.