Comment les styles de sécurité affectent l'accès aux données

ONTAP 9

NetApp
September 12, 2024

Sommaire

Comment les styles de sécurité affectent l'accès aux données

Styles de sécurité et leurs effets

Il existe quatre styles de sécurité différents : UNIX, NTFS, mixte et unifié. Chaque style de sécurité a un effet différent sur la façon dont les autorisations sont traitées pour les données. Vous devez comprendre les différents effets pour vous assurer que vous sélectionnez le style de sécurité approprié à vos fins.

Il est important de comprendre que les styles de sécurité ne déterminent pas quels types de clients peuvent ou ne peuvent pas accéder aux données. Les styles de sécurité déterminent uniquement le type d'autorisations que ONTAP utilise pour contrôler l'accès aux données et le type de client pouvant modifier ces autorisations.

Par exemple, si un volume utilise le style de sécurité UNIX, les clients SMB peuvent toujours accéder aux données (à condition qu'ils s'authentifient et autorisent correctement) en raison de la nature multiprotocole de ONTAP. Toutefois, ONTAP utilise des autorisations UNIX que seuls les clients UNIX peuvent modifier à l'aide d'outils natifs.

Style de sécurité	Clients pouvant modifier des autorisations	Autorisations que les clients peuvent utiliser	Un style de sécurité efficace	Clients pouvant accéder aux fichiers
UNIX	NFS	Bits de mode NFSv3	UNIX	NFS et SMB
		Listes de contrôle d'accès NFSv4.x		
NTFS	PME	ALC NTFS	NTFS	
Mixte	NFS ou SMB	Bits de mode NFSv3	UNIX	
		ACL.NFSv4		
		ALC NTFS	NTFS	
Unifiée (Pour Infinite volumes uniquement, dans ONTAP 9.4 et les versions antérieures.)	NFS ou SMB	Bits de mode NFSv3	UNIX	
		ACL NFSv4.1		
		ALC NTFS	NTFS	

Les volumes FlexVol prennent en charge les styles de sécurité UNIX, NTFS et mixte. Lorsque le style de sécurité est mixte ou unifié, les autorisations effectives dépendent du type de client qui a modifié les autorisations pour la dernière fois, car les utilisateurs définissent le style de sécurité sur une base individuelle. Si le dernier client ayant modifié des autorisations était un client NFSv3, les autorisations sont des bits en mode UNIX NFSv3. Si le dernier client était un client NFSv4, les autorisations sont définies comme listes de contrôle d'accès NFSv4. Si le dernier client était un client SMB, les autorisations sont des listes de contrôle d'accès Windows NTFS.

La méthode de sécurité unifiée est uniquement disponible avec des volumes infinis, qui ne sont plus pris en charge dans ONTAP 9.5 et versions ultérieures. Pour plus d'informations, voir Présentation de la gestion des volumes FlexGroup.

À partir de ONTAP 9.2, le `show-effective-permissions` paramètre au `vserver security file-directory` La commande vous permet d'afficher les autorisations effectives accordées à un utilisateur Windows ou UNIX sur le chemin d'accès au fichier ou au dossier spécifié. De plus, le paramètre facultatif `-share-name` vous permet d'afficher l'autorisation de partage effective.

> ONTAP définit au départ certaines autorisations de fichier par défaut. Par défaut, le style de sécurité effectif sur toutes les données des volumes de style de sécurité UNIX, mixte et unifié est UNIX et le type d'autorisation effectif est bits de mode UNIX (0755 sauf indication contraire) jusqu'à ce qu'un client soit configuré comme autorisé par le style de sécurité par défaut. Par défaut, le style de sécurité effectif sur toutes les données des volumes de style de sécurité NTFS est NTFS et dispose d'une liste de contrôle d'accès permettant un contrôle total à tous.

Où et quand définir les styles de sécurité

Les styles de sécurité peuvent être définis sur les volumes FlexVol (volumes root ou de données) et les qtrees. Les styles de sécurité peuvent être définis manuellement au moment de la création, hérités automatiquement ou modifiés ultérieurement.

Choisissez le style de sécurité à utiliser sur les SVM

Pour vous aider à choisir le style de sécurité à utiliser sur un volume, vous devez tenir compte de deux facteurs. Le facteur principal est le type d'administrateur qui gère le système de fichiers. Le facteur secondaire désigne le type d'utilisateur ou de service qui accède aux données du volume.

Lorsque vous configurez le style de sécurité sur un volume, vous devez tenir compte des besoins de votre environnement pour vous assurer que vous sélectionnez le meilleur style de sécurité et éviter les problèmes liés à la gestion des autorisations. Vous pouvez décider des considérations suivantes :

Style de sécurité	Choisissez si…
UNIX	• Le système de fichiers est géré par un administrateur UNIX. • La plupart des utilisateurs sont des clients NFS. • Une application accédant aux données utilise un utilisateur UNIX comme compte de service.
NTFS	• Le système de fichiers est géré par un administrateur Windows. • La majorité des utilisateurs sont des clients SMB. • Une application accédant aux données utilise un utilisateur Windows comme compte de service.
Mixte	Le système de fichiers est géré à la fois par les administrateurs et utilisateurs d'UNIX et de Windows, et il se compose de clients NFS et SMB.

Fonctionnement de l’héritage du style de sécurité

Si vous ne spécifiez pas le style de sécurité lors de la création d’un nouveau volume FlexVol ou d’un qtree, il hérite de son style de sécurité de différentes manières.

Les styles de sécurité sont hérités de la manière suivante :

- Un volume FlexVol hérite du style de sécurité du volume root de son SVM contenant.
- Un qtree hérite du style de sécurité de son volume FlexVol.
- Un fichier ou un répertoire hérite du style de sécurité de son volume FlexVol ou qtree.

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.