Utilisez les options pour personnaliser les serveurs SMB

ONTAP 9

NetApp
March 24, 2023

Table des matières

Utilisez les options pour personnaliser les serveurs SMB

Options de serveur SMB disponibles

Il est utile de connaître les options disponibles lorsque vous envisagez de personnaliser le serveur SMB. Bien que certaines options soient destinées à une utilisation générale sur le serveur SMB, plusieurs sont utilisées pour activer et configurer des fonctionnalités SMB spécifiques. Les options de serveur SMB sont contrôlées avec le `vserver cifs options modify` option.

La liste suivante indique les options du serveur SMB disponibles au niveau de privilège admin :

- **Configuration de la valeur du délai d'expiration de session SMB**

  La configuration de cette option vous permet de spécifier le nombre de secondes d'inactivité avant la déconnexion d'une session SMB. Une session inactive est une session dans laquelle un utilisateur ne dispose pas de fichiers ou de répertoires ouverts sur le client. La valeur par défaut est 900 secondes.

- **Configuration de l'utilisateur UNIX par défaut**

  La configuration de cette option vous permet de spécifier l'utilisateur UNIX par défaut utilisé par le serveur SMB. ONTAP crée automatiquement un utilisateur par défaut nommé « pcuser » (avec un UID de 65534), crée un groupe nommé « pcuser » (avec un GID de 65534) et ajoute l'utilisateur par défaut au groupe « pcuser ». Lorsque vous créez un serveur SMB, ONTAP configure automatiquement « pcuser » en tant qu'utilisateur UNIX par défaut.

- **Configuration de l'utilisateur UNIX invité**

  La configuration de cette option vous permet de spécifier le nom d'un utilisateur UNIX auquel les utilisateurs qui se connectent à partir de domaines non fiables sont mappés, ce qui permet à un utilisateur d'un domaine non fiable de se connecter au serveur SMB. Par défaut, cette option n'est pas configurée (il n'y a pas de valeur par défaut) ; par conséquent, la valeur par défaut ne permet pas aux utilisateurs de domaines non approuvés de se connecter au serveur SMB.

- **Activation ou désactivation de l'exécution d'une subvention en lecture pour les bits de mode**

  L'activation ou la désactivation de cette option vous permet de spécifier si les clients SMB doivent autoriser l'exécution de fichiers exécutables avec les bits de mode UNIX auxquels ils ont accès en lecture, même lorsque le bit exécutable UNIX n'est pas défini. Cette option est désactivée par défaut.

- **Activation ou désactivation de la possibilité de supprimer des fichiers en lecture seule des clients NFS**

  L'activation ou la désactivation de cette option détermine s'il faut autoriser les clients NFS à supprimer des fichiers ou des dossiers avec l'ensemble d'attributs en lecture seule. La sémantique de suppression NTFS n'autorise pas la suppression d'un fichier ou d'un dossier lorsque l'attribut en lecture seule est défini. La sémantique de suppression UNIX ignore le bit en lecture seule, en utilisant les autorisations du répertoire parent à la place pour déterminer si un fichier ou un dossier peut être supprimé. Le paramètre par défaut est `disabled`, Ce qui entraîne la suppression de la sémantique en NTFS.

- **Configuration des adresses du serveur du service de noms Internet Windows**

  La configuration de cette option vous permet de spécifier une liste d'adresses de serveur WINS (Windows Internet Name Service) en tant que liste délimitée par des virgules. Vous devez indiquer des adresses IPv4. Les adresses IPv6 ne sont pas prises en charge. Il n'y a pas de valeur par défaut.

La liste suivante indique les options du serveur SMB disponibles au niveau de privilège avancé :

- **Octroi d'autorisations de groupe UNIX aux utilisateurs CIFS**

  La configuration de cette option détermine si l'utilisateur CIFS entrant qui n'est pas le propriétaire du fichier peut obtenir l'autorisation de groupe. Si l'utilisateur CIFS n'est pas le propriétaire du fichier de style de sécurité UNIX et que ce paramètre est défini sur `true`, puis l'autorisation de groupe est accordée pour le fichier. Si l'utilisateur CIFS n'est pas le propriétaire du fichier de style de sécurité UNIX et que ce paramètre est défini sur `false`, Les règles UNIX normales sont alors applicables pour accorder l'autorisation de fichier. Ce paramètre s'applique aux fichiers de style de sécurité UNIX dont l'autorisation est définie sur `mode bits` Et ne s'applique pas aux fichiers utilisant le mode de sécurité NTFS ou NFSv4. Le paramètre par défaut est `false`.

- **Activation ou désactivation de SMB 1.0**

  SMB 1.0 est désactivé par défaut sur un SVM pour lequel un serveur SMB est créé dans ONTAP 9.3.

  > À partir de ONTAP 9.3, SMB 1.0 est désactivé par défaut pour les nouveaux serveurs SMB créés dans ONTAP 9.3. Vous devez migrer vers une version SMB plus récente dès que possible pour préparer des améliorations en matière de sécurité et de conformité. Contactez votre représentant NetApp pour plus d'informations.

- **Activation ou désactivation de SMB 2.x**

  SMB 2.0 est la version minimale de SMB qui prend en charge le basculement de LIF. Si vous désactivez SMB 2.x, ONTAP désactive également automatiquement SMB 3.X.

  SMB 2.0 est pris en charge uniquement sur les SVM. L'option est activée par défaut sur les SVM

- **Activation ou désactivation de SMB 3.0**

  SMB 3.0 est la version minimale de SMB qui prend en charge les partages disponibles en continu. Windows Server 2012 et Windows 8 sont les versions minimales de Windows qui prennent en charge SMB 3.0.

  SMB 3.0 est pris en charge uniquement sur les SVM. L'option est activée par défaut sur les SVM

- **Activation ou désactivation de SMB 3.1**

  Windows 10 est la seule version de Windows qui prend en charge SMB 3.1.

  SMB 3.1 est pris en charge uniquement sur les SVM. L'option est activée par défaut sur les SVM

- **Activation ou désactivation de l'allègement de charge des copies ODX**

  L'allègement de la charge des copies ODX est utilisé automatiquement par les clients Windows qui la prennent en charge. Cette option est activée par défaut.

- **Activation ou désactivation du mécanisme de copie directe pour le déchargement de copies ODX**

  Le mécanisme de copie directe augmente les performances de l'opération de déchargement de copie lorsque les clients Windows essaient d'ouvrir le fichier source d'une copie dans un mode qui empêche la modification du fichier pendant la copie. Par défaut, le mécanisme de copie directe est activé.

- **Activation ou désactivation des renvois de nœuds automatiques**

  Avec les référencements automatiques des nœuds, le serveur SMB fait automatiquement référence aux clients à une LIF de données locale au nœud qui héberge les données accédées via le partage demandé.

- **Activation ou désactivation des stratégies d'exportation pour SMB**

  Cette option est désactivée par défaut.

- **Activation ou désactivation de l'utilisation de points de jonction en tant que points de réanalyse**

  Si cette option est activée, le serveur SMB expose les points de jonction aux clients SMB comme points de réanalyse. Cette option n'est valide que pour les connexions SMB 2.x ou SMB 3.0. Cette option est activée par défaut.

  Cette option n'est prise en charge que sur les SVM. L'option est activée par défaut sur les SVM

- **Configuration du nombre maximal d'opérations simultanées par connexion TCP**

  La valeur par défaut est 255.

- **Activation ou désactivation de la fonctionnalité des groupes et des utilisateurs Windows locaux**

  Cette option est activée par défaut.

- **Activation ou désactivation de l'authentification des utilisateurs Windows locaux**

  Cette option est activée par défaut.

- **Activation ou désactivation de la fonctionnalité de copie en double VSS**

  ONTAP utilise la fonctionnalité Shadow Copy pour effectuer des sauvegardes distantes des données stockées à l'aide de la solution Hyper-V sur SMB.

  Cette option n'est prise en charge que sur les SVM et uniquement dans les configurations Hyper-V sur SMB. L'option est activée par défaut sur les SVM

- **Configuration de la profondeur du répertoire de copie en double**

  La configuration de cette option vous permet de définir la profondeur maximale des répertoires sur lesquels créer des clichés instantanés lors de l'utilisation de la fonctionnalité copie en double.

  Cette option n'est prise en charge que sur les SVM et uniquement dans les configurations Hyper-V sur SMB. L'option est activée par défaut sur les SVM

- **Activation ou désactivation des fonctionnalités de recherche multidomaine pour le mappage de noms**

  Si cette option est activée, lorsqu'un utilisateur UNIX est mappé à un utilisateur de domaine Windows à l'aide d'un caractère générique (*) dans la partie domaine du nom d'utilisateur Windows (par exemple

*\joe), ONTAP recherche l'utilisateur spécifié dans tous les domaines avec des approbations bidirectionnelles vers le domaine d'origine. Le domaine personnel est le domaine qui contient le compte informatique du serveur SMB.

Vous pouvez également configurer une liste de domaines de confiance préférés en alternative à la recherche de tous les domaines de confiance bidirectionnels. Si cette option est activée et qu'une liste préférée est configurée, la liste préférée est utilisée pour effectuer des recherches de mappage de noms de domaines multiples.

La valeur par défaut est d'activer les recherches de mappage de noms multidomaine.

- **Configuration de la taille du secteur du système de fichiers**

  La configuration de cette option vous permet de configurer la taille du secteur du système de fichiers en octets que ONTAP communique aux clients SMB. Cette option comporte deux valeurs valides : `4096` et `512`. La valeur par défaut est `4096`. Vous devrez peut-être définir cette valeur sur `512` Si l'application Windows ne prend en charge qu'une taille de secteur de 512 octets.

- **Activation ou désactivation du contrôle d'accès dynamique**

  L'activation de cette option vous permet de sécuriser les objets sur le serveur SMB à l'aide du contrôle d'accès dynamique (DAC), y compris l'utilisation de l'audit pour définir des règles d'accès centrales et l'utilisation d'objets de stratégie de groupe pour mettre en œuvre des règles d'accès centrales. L'option est désactivée par défaut.

  Cette option n'est prise en charge que sur les SVM.

- **Définition des restrictions d'accès pour les sessions non authentifiées (restriction anonyme)**

  La définition de cette option détermine les restrictions d'accès pour les sessions non authentifiées. Les restrictions sont appliquées aux utilisateurs anonymes. Par défaut, il n'existe aucune restriction d'accès pour les utilisateurs anonymes.

- **Activation ou désactivation de la présentation des listes de contrôle d'accès NTFS sur des volumes avec sécurité effective UNIX (volumes de type sécurité UNIX ou volumes de type sécurité mixte avec sécurité effective UNIX)**

  L'activation ou la désactivation de cette option détermine comment la sécurité des fichiers sur les fichiers et les dossiers avec la sécurité UNIX est présentée aux clients SMB. Lorsqu'elle est activée, ONTAP présente aux clients SMB les fichiers et les dossiers des volumes dotés de la sécurité UNIX comme ayant la sécurité des fichiers NTFS avec les ACL NTFS. S'il est désactivé, ONTAP présente les volumes dont la sécurité UNIX est de type FAT, sans aucun fichier sécurisé. Par défaut, les volumes sont présentés comme ayant la sécurité de fichiers NTFS avec les ACL NTFS.

- **Activation ou désactivation de la fonctionnalité fausse ouverture SMB**

  L'activation de cette fonctionnalité améliore les performances de SMB 2.x et de SMB 3.0 en optimisant la manière dont ONTAP effectue des requêtes ouvertes et fermés lors des requêtes relatives aux attributs des fichiers et des répertoires. Par défaut, la fonctionnalité de faux ouverture SMB est activée. Cette option est utile uniquement pour les connexions effectuées avec SMB 2.x ou version ultérieure.

- **Activation ou désactivation des extensions UNIX**

  L'activation de cette option active les extensions UNIX sur un serveur SMB. Les extensions UNIX permettent d'afficher la sécurité du style POSIX/UNIX via le protocole SMB. Par défaut, cette option est désactivée.

Si vous avez des clients SMB basés sur UNIX, tels que des clients Mac OSX, dans votre environnement, vous devez activer les extensions UNIX. L'activation des extensions UNIX permet au serveur SMB de transmettre des informations de sécurité POSIX/UNIX sur SMB au client UNIX, qui convertit ensuite les informations de sécurité en sécurité POSIX/UNIX.

- **Activation ou désactivation du support pour les recherches de noms courts**

  L'activation de cette option permet au serveur SMB d'effectuer des recherches sur des noms courts. Une requête de recherche avec cette option activée tente de faire correspondre 8.3 noms de fichier avec des noms de fichier longs. La valeur par défaut de ce paramètre est `false`.

- **Activation ou désactivation de la prise en charge de la publicité automatique des capacités DFS**

  L'activation ou la désactivation de cette option détermine si les serveurs SMB annoncent automatiquement les fonctionnalités DFS aux clients SMB 2.x et SMB 3.0 qui se connectent aux partages. ONTAP utilise des référencements DFS dans la mise en œuvre de liens symboliques pour l'accès SMB. Si cette option est activée, le serveur SMB annonce toujours les fonctionnalités DFS, que l'accès à la liaison symbolique soit activé ou non. S'il est désactivé, le serveur SMB annonce les fonctionnalités DFS uniquement lorsque les clients se connectent aux partages où l'accès à la liaison symbolique est activé.

- **Configuration du nombre maximum de crédits SMB**

  Depuis ONTAP 9.4, configurer le `-max-credits` Vous permet de limiter le nombre de crédits à accorder sur une connexion SMB lorsque les clients et le serveur exécutent SMB version 2 ou ultérieure. La valeur par défaut est 128.

- **Activation ou désactivation de la prise en charge de SMB Multichannel**

  Activation du `-is-multichannel-enabled` Option dans les versions ONTAP 9.4 et ultérieures permet au serveur SMB d'établir plusieurs connexions pour une seule session SMB lorsque les cartes réseau appropriées sont déployées sur le cluster et ses clients. Cela améliore le débit et la tolérance aux pannes. La valeur par défaut de ce paramètre est `false`.

  Lorsque SMB Multichannel est activé, vous pouvez également spécifier les paramètres suivants :

  - Nombre maximum de connexions autorisées par session multicanal. La valeur par défaut de ce paramètre est 32.
  - Nombre maximum d'interfaces réseau annoncées par session multicanal. La valeur par défaut de ce paramètre est 256.

Configuration des options du serveur SMB

Vous pouvez configurer les options du serveur SMB à tout moment après avoir créé un serveur SMB sur une machine virtuelle de stockage (SVM).

Étape

1. Effectuez l'action souhaitée :

Si vous souhaitez configurer les options du serveur SMB…	Entrez la commande…
Au niveau de privilège admin	`vserver cifs options modify -vserver` *`vserver_name options`*
Au niveau de privilège avancé	a. `set -privilege advanced` b. `vserver cifs options modify -vserver` *`vserver_name options`* c. `set -privilege admin`

Pour plus d'informations sur la configuration des options du serveur SMB, reportez-vous à la page de manuel du `vserver cifs options modify` commande.

Configurez l'autorisation d'accorder le groupe UNIX aux utilisateurs SMB

Vous pouvez configurer cette option pour accorder des autorisations de groupe à des fichiers ou des répertoires, même si l'utilisateur SMB entrant n'est pas le propriétaire du fichier.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Configurez l'autorisation Grant UNIX Group comme il convient :

Si vous le souhaitez	Saisissez la commande
Activez l'accès aux fichiers ou répertoires pour obtenir les autorisations de groupe même si l'utilisateur n'est pas le propriétaire du fichier	`vserver cifs options modify –grant-unix-group-perms-to-others true`
Désactivez l'accès aux fichiers ou répertoires pour obtenir les autorisations de groupe même si l'utilisateur n'est pas le propriétaire du fichier	`vserver cifs options modify –grant-unix-group-perms-to-others false`

3. Vérifiez que l'option est réglée sur la valeur souhaitée : `vserver cifs options show –fields grant-unix-group-perms-to-others`
4. Retour au niveau de privilège admin : `set -privilege admin`

Configurez les restrictions d'accès pour les utilisateurs anonymes

Par défaut, un utilisateur anonyme et non authentifié (également appelé *null user*) peut accéder à certaines informations sur le réseau. Vous pouvez utiliser une option de

serveur SMB pour configurer les restrictions d'accès pour l'utilisateur anonyme.

Description de la tâche

Le `-restrict-anonymous` L'option de serveur SMB correspond au `RestrictAnonymous` Entrée de registre dans Windows.

Les utilisateurs anonymes peuvent lister ou énumérer certains types d'informations système provenant des hôtes Windows sur le réseau, y compris les noms d'utilisateur et les détails, les stratégies de compte et les noms de partage. Vous pouvez contrôler l'accès de l'utilisateur anonyme en spécifiant l'un des trois paramètres de restriction d'accès suivants :

Valeur	Description
`no-restriction` (valeur par défaut)	Spécifie aucune restriction d'accès pour les utilisateurs anonymes.
`no-enumeration`	Spécifie que seule l'énumération est restreinte pour les utilisateurs anonymes.
`no-access`	Spécifie que l'accès est restreint pour les utilisateurs anonymes.

Étapes

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Configurez le paramètre restreindre l'anonymat : `vserver cifs options modify -vserver` *`vserver_name`* `-restrict-anonymous {no-restriction|no-enumeration|no-access}`
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`

Informations associées

Options de serveur SMB disponibles

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

Configuration des styles de sécurité sur les qtrees

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.