Sécurisez l'accès aux fichiers grâce aux autorisations liées aux fichiers

ONTAP 9

NetApp
April 24, 2024

Sommaire

Sécurisez l'accès aux fichiers grâce aux autorisations liées aux fichiers

Configurez les autorisations de fichier NTFS avancées à l'aide de l'onglet sécurité de Windows

Vous pouvez configurer les autorisations de fichier NTFS standard sur les fichiers et les dossiers en utilisant l'onglet **sécurité Windows** de la fenêtre Propriétés Windows.

Avant de commencer

L'administrateur effectuant cette tâche doit disposer d'autorisations NTFS suffisantes pour modifier les autorisations sur les objets sélectionnés.

Description de la tâche

La configuration des autorisations de fichiers NTFS se fait sur un hôte Windows en ajoutant des entrées aux listes de contrôle d'accès discrétionnaire NTFS (DACL) associées à un descripteur de sécurité NTFS. Le descripteur de sécurité est ensuite appliqué aux fichiers et répertoires NTFS. Ces tâches sont traitées automatiquement par l'interface graphique de Windows.

Étapes

1. Dans le menu **Tools** de l'Explorateur Windows, sélectionnez **Map network drive**.
2. Renseignez la boîte de dialogue **Map Network Drive** :

   a. Sélectionnez une lettre **lecteur**.

   b. Dans la zone **Folder**, saisissez le nom du serveur CIFS contenant le partage contenant les données auxquelles vous souhaitez appliquer les autorisations et le nom du partage.

      Si le nom de votre serveur CIFS est ""CIFS_SERVER"" et que votre partage est nommé "`hare1"", vous devez taper `\\CIFS_SERVER\share1`.

      > Vous pouvez spécifier l'adresse IP de l'interface de données du serveur CIFS au lieu du nom du serveur CIFS.

   c. Cliquez sur **Terminer**.

   Le lecteur sélectionné est monté et prêt avec la fenêtre de l'Explorateur Windows affichant les fichiers et dossiers contenus dans le partage.

3. Sélectionnez le fichier ou le répertoire pour lequel vous souhaitez définir les autorisations de fichier NTFS.
4. Cliquez avec le bouton droit de la souris sur le fichier ou le répertoire, puis sélectionnez **Propriétés**.
5. Sélectionnez l'onglet **sécurité**.

   L'onglet **sécurité** affiche la liste des utilisateurs et des groupes pour lesquels les autorisations NTFS sont définies. La zone **autorisations pour** affiche une liste des autorisations Autoriser et refuser en vigueur pour chaque utilisateur ou groupe sélectionné.

6. Cliquez sur **Avancé**.

   La fenêtre Propriétés de Windows affiche des informations sur les autorisations de fichier existantes

attribuées aux utilisateurs et aux groupes.

7. Cliquez sur **Modifier les autorisations**.

   La fenêtre autorisations s'ouvre.

8. Effectuez les opérations souhaitées :

Les fonctions que vous recherchez…	Procédez comme suit…
Configurez des autorisations NTFS avancées pour un nouvel utilisateur ou un nouveau groupe	a. Cliquez sur **Ajouter**. b. Dans la zone **Entrez le nom de l'objet à sélectionner**, saisissez le nom de l'utilisateur ou du groupe que vous souhaitez ajouter. c. Cliquez sur **OK**.
Modifiez les autorisations NTFS avancées d'un utilisateur ou d'un groupe	a. Dans la zone **permissions Entries:**, sélectionnez l'utilisateur ou le groupe dont vous souhaitez modifier les autorisations avancées. b. Cliquez sur **Modifier**.
Supprimez les autorisations NTFS avancées pour un utilisateur ou un groupe	a. Dans la zone **permissions Entries:**, sélectionnez l'utilisateur ou le groupe à supprimer. b. Cliquez sur **Supprimer**. c. Passez à l'étape 13.

   Si vous ajoutez des autorisations NTFS avancées sur un nouvel utilisateur ou un nouveau groupe ou si vous modifiez les autorisations avancées NTFS sur un utilisateur ou un groupe existant, la zone entrée d'autorisation de <objet> s'ouvre.

9. Dans la zone **appliquer à**, sélectionnez la façon dont vous souhaitez appliquer cette entrée d'autorisation de fichier NTFS.

   Si vous configurez des autorisations de fichier NTFS sur un seul fichier, la case **appliquer à** n'est pas active. Le paramètre **appliquer à** est défini par défaut sur **cet objet uniquement**.

10. Dans la zone **permissions**, sélectionnez les cases **Autoriser** ou **refuser** pour les autorisations avancées que vous souhaitez définir sur cet objet.

    - Pour autoriser l'accès spécifié, cochez la case **Autoriser**.
    - Pour ne pas autoriser l'accès spécifié, cochez la case **Deny**. Vous pouvez définir des autorisations sur les droits avancés suivants :
    - **Contrôle total**

      Si vous choisissez ce droit avancé, tous les autres droits avancés sont automatiquement choisis (autoriser ou refuser des droits).

    - **Dossier traverse / fichier d'exécution**
    - **Liste de dossiers / lecture de données**

- **Lire les attributs**
- **Lire les attributs étendus**
- **Créer des fichiers / écrire des données**
- **Créer des dossiers / ajouter des données**
- **Ecrire des attributs**
- **Ecrire des attributs étendus**
- **Supprimer des sous-dossiers et des fichiers**
- **Supprimer**
- **Autorisations de lecture**
- **Modifier les autorisations**
- * Prendre possession*

> Si l'une des zones d'autorisation avancée n'est pas sélectionnable, c'est parce que les autorisations sont héritées de l'objet parent.

11. Si vous souhaitez que les sous-dossiers et les fichiers de cet objet héritent de ces autorisations, cochez la case **appliquer ces autorisations aux objets et/ou aux conteneurs dans ce conteneur uniquement**.
12. Cliquez sur **OK**.
13. Une fois que vous avez terminé d'ajouter, de supprimer ou de modifier des autorisations NTFS, spécifiez le paramètre d'héritage de cet objet :

    - Sélectionnez la case **inclure les autorisations héritables dans la boîte parent** de cet objet.

      Il s'agit de la valeur par défaut.

    - Sélectionnez la case **remplacer toutes les autorisations d'objet enfant par des autorisations héritables de cet objet**.

      Ce paramètre n'est pas présent dans la zone autorisations si vous définissez des autorisations de fichier NTFS sur un seul fichier.

      > Soyez prudent lorsque vous sélectionnez ce paramètre. Ce paramètre supprime toutes les autorisations existantes sur tous les objets enfants et les remplace par les paramètres d'autorisation de cet objet. Vous pourriez supprimer par inadvertance les autorisations que vous ne souhaitez pas supprimer. Il est particulièrement important lorsque vous définissez des autorisations dans un volume mixte de style de sécurité ou qtree. Si les objets enfant ont un style de sécurité UNIX effectif, la propagation des autorisations NTFS à ces objets enfant entraîne le ONTAP changement de style de sécurité UNIX au style de sécurité NTFS, et toutes les autorisations UNIX sur ces objets enfants sont remplacées par des autorisations NTFS.

    - Sélectionnez les deux cases.
    - Sélectionnez aucune case.
14. Cliquez sur **OK** pour fermer la case **permissions**.
15. Cliquez sur **OK** pour fermer la case **Paramètres de sécurité avancés pour <objet>**.

Pour plus d'informations sur la définition des autorisations NTFS avancées, consultez votre documentation

Windows.

Informations associées

Configurez et appliquez la sécurité des fichiers sur les fichiers et dossiers NTFS à l'aide de l'interface de ligne de commande

Affichage d'informations sur la sécurité des fichiers sur les volumes de style de sécurité NTFS

Affichage d'informations sur la sécurité des fichiers sur des volumes de style de sécurité mixtes

Affichage d'informations sur la sécurité des fichiers sur des volumes de style de sécurité UNIX

Configurez les autorisations d'accès aux fichiers NTFS à l'aide de l'interface de ligne de commande ONTAP

Vous pouvez configurer les autorisations d'accès aux fichiers NTFS sur les fichiers et les répertoires à l'aide de l'interface de ligne de commande ONTAP. Cela vous permet de configurer les autorisations d'accès aux fichiers NTFS sans avoir à vous connecter aux données à l'aide d'un partage SMB sur un client Windows.

Vous pouvez configurer les autorisations d'accès aux fichiers NTFS en ajoutant des entrées aux listes de contrôle d'accès discrétionnaire NTFS (DACL) associées à un descripteur de sécurité NTFS. Le descripteur de sécurité est ensuite appliqué aux fichiers et répertoires NTFS.

Vous ne pouvez configurer les autorisations de fichier NTFS qu'à l'aide de la ligne de commande. Vous ne pouvez pas configurer les listes de contrôle d'accès NFSv4 en utilisant l'interface de ligne de commandes.

Étapes

1. Créez un descripteur de sécurité NTFS.

   ```
   vserver security file-directory ntfs create -vserver svm_name -ntfs-sd
   ntfs_security_descriptor_name -owner owner_name -group primary_group_name
   -control-flags-raw raw_control_flags
   ```

2. Ajoutez des listes de contrôle d'accès discrétionnaire au descripteur de sécurité NTFS.

   ```
   vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd
   ntfs_security_descriptor_name -access-type {deny|allow} -account account_name
   -rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to
   {this-folder|sub-folders|files}
   ```

3. Créez une stratégie de sécurité de fichiers/répertoires.

   ```
   vserver security file-directory policy create -vserver svm_name -policy-name
   policy_name
   ```

Comment les autorisations d'accès aux fichiers UNIX permettent de contrôler l'accès aux fichiers sur SMB

Un volume FlexVol peut avoir l'un des trois types de style de sécurité suivants : NTFS, UNIX ou mixte. Vous pouvez accéder aux données via SMB quel que soit le style de sécurité. Cependant, des autorisations appropriées sur les fichiers UNIX sont nécessaires pour accéder aux données à l'aide de la sécurité effective d'UNIX.

Lorsque vous accédez aux données via SMB, plusieurs contrôles d'accès sont utilisés pour déterminer si un utilisateur est autorisé à effectuer une action demandée :

- Droits d'exportation

  La configuration des autorisations d'exportation pour l'accès SMB est facultative.

- Partager les autorisations
- Autorisations liées aux fichiers

  Les types d'autorisations de fichier suivants peuvent être appliqués aux données sur lesquelles l'utilisateur souhaite effectuer une action :

  - NTFS
  - ACL UNIX NFSv4
  - Bits mode UNIX

Pour les données avec des ACL NFSv4 ou des bits de mode UNIX définis, les autorisations de style UNIX sont utilisées afin de déterminer les droits d'accès aux fichiers aux données. L'administrateur du SVM doit définir l'autorisation appropriée pour garantir que les utilisateurs disposent des droits nécessaires pour effectuer l'action souhaitée.

> Les données d'un volume de type sécurité mixte peuvent avoir un style de sécurité NTFS ou UNIX. Si les données ont un style de sécurité UNIX effectif, les autorisations NFSv4 ou les bits du mode UNIX sont utilisés pour déterminer les droits d'accès aux fichiers aux données.