Configuration des règles d'audit des fichiers et des dossiers

ONTAP 9

NetApp
April 24, 2024

Sommaire

Configuration des règles d’audit des fichiers et des dossiers

Configuration des règles d’audit des fichiers et des dossiers

L’implémentation de l’audit sur les événements d’accès aux fichiers et aux dossiers est un processus en deux étapes. Vous devez d’abord créer et activer une configuration d’audit sur les serveurs virtuels de stockage (SVM). Ensuite, vous devez configurer des stratégies d’audit sur les fichiers et dossiers que vous souhaitez surveiller. Vous pouvez configurer des stratégies d’audit pour surveiller les tentatives d’accès réussies et échouées.

Vous pouvez configurer les règles d’audit SMB et NFS. Les règles d’audit SMB et NFS diffèrent entre les exigences de configuration et les fonctionnalités d’audit.

Si les stratégies d’audit appropriées sont configurées, ONTAP surveille les événements d’accès SMB et NFS comme spécifié dans les règles d’audit uniquement si les serveurs SMB ou NFS sont exécutés.

Configurez les règles d’audit sur les répertoires et les fichiers de style de sécurité NTFS

Avant de pouvoir auditer les opérations de fichiers et de répertoires, vous devez configurer des stratégies d’audit sur les fichiers et répertoires pour lesquels vous souhaitez collecter les informations d’audit. Cela permet en plus de configurer et d’activer la configuration d’audit. Vous pouvez configurer les stratégies d’audit NTFS en utilisant l’onglet sécurité Windows ou l’interface de ligne de commande ONTAP.

Configuration des stratégies d’audit NTFS à l’aide de l’onglet sécurité de Windows

Vous pouvez configurer les stratégies d’audit NTFS sur les fichiers et les répertoires en utilisant l’onglet **sécurité Windows** de la fenêtre Propriétés Windows. Il s’agit de la même méthode utilisée lors de la configuration de stratégies d’audit sur des données résidant sur un client Windows, qui vous permet d’utiliser la même interface graphique que celle que vous êtes habitué à utiliser.

Ce dont vous avez besoin

L’audit doit être configuré sur la machine virtuelle de stockage (SVM) qui contient les données auxquelles vous appliquez des listes de contrôle d’accès système (SACL).

Description de la tâche

La configuration des stratégies d’audit NTFS se fait en ajoutant des entrées aux SACL NTFS 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. Le descripteur de sécurité peut contenir des listes de contrôle d’accès discrétionnaire (DACL) pour l’application d’autorisations d’accès aux fichiers et aux dossiers, des listes SACL pour l’audit des fichiers et des dossiers, ou des listes SACL et des listes DALC.

Pour définir les stratégies d'audit NTFS à l'aide de l'onglet sécurité Windows, procédez comme suit sur un hôte Windows :

Étapes

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

   a. Sélectionnez une lettre **lecteur**.

   b. Dans la zone **Folder**, saisissez le nom du serveur SMB qui contient le partage, en tenant les données à auditer et le nom du partage.

      Vous pouvez indiquer l'adresse IP de l'interface de données du serveur SMB au lieu du nom du serveur SMB.

      Si votre nom de serveur SMB est "SMB_SERVER" et que votre partage est nommé "share1", vous devez entrer `\\SMB_SERVER\share1`.

   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 activer l'accès d'audit.
4. Cliquez avec le bouton droit de la souris sur le fichier ou le répertoire, puis sélectionnez **Propriétés**.
5. Sélectionnez l'onglet **sécurité**.
6. Cliquez sur **Avancé**.
7. Sélectionnez l'onglet **Audit**.
8. Effectuez les opérations souhaitées :

Si vous voulez	Procédez comme suit
Configuration de l'audit pour un nouvel utilisateur ou un nouveau groupe	a. Cliquez sur **Ajouter**. b. Dans la zone entrer le nom de l'objet à sélectionner, saisissez le nom de l'utilisateur ou du groupe que vous souhaitez ajouter. c. Cliquez sur **OK**.
Supprimer l'audit d'un utilisateur ou d'un groupe	a. Dans la zone entrer le nom de l'objet à sélectionner, sélectionnez l'utilisateur ou le groupe que vous souhaitez supprimer. b. Cliquez sur **Supprimer**. c. Cliquez sur **OK**. d. Ignorer le reste de cette procédure.

Modifier l'audit d'un utilisateur ou d'un groupe	a. Dans la zone entrer le nom de l'objet à sélectionner, sélectionnez l'utilisateur ou le groupe que vous souhaitez modifier. b. Cliquez sur **Modifier**. c. Cliquez sur **OK**.

Si vous configurez l'audit sur un utilisateur ou un groupe ou si vous modifiez l'audit sur un utilisateur ou un groupe existant, la zone entrée d'audit pour <objet> s'ouvre.

9. Dans la case **appliquer à**, sélectionnez la façon dont vous souhaitez appliquer cette entrée d'audit.

   Vous pouvez sélectionner l'une des options suivantes :

   - **Ce dossier, sous-dossiers et fichiers**
   - **Ce dossier et sous-dossiers**
   - **Ce dossier uniquement**
   - **Ce dossier et fichiers**
   - **Sous-dossiers et fichiers uniquement**
   - **Sous-dossiers uniquement**
   - **Fichiers uniquement** Si vous configurez l'audit sur un seul fichier, la case **appliquer à** n'est pas active. Le paramètre de case **appliquer à** est défini par défaut sur **cet objet uniquement**.

   > Étant donné que l'audit utilise les ressources de l'SVM, sélectionnez uniquement le niveau minimal qui fournit les événements d'audit qui répondent à vos exigences de sécurité.

10. Dans la case **Access**, sélectionnez ce que vous voulez auditer et si vous voulez auditer les événements réussis, les événements d'échec, ou les deux.
    - Pour auditer les événements réussis, cochez la case succès.
    - Pour auditer les événements d'échec, cochez la case échec.

      Sélectionnez uniquement les actions à surveiller pour répondre à vos exigences de sécurité. Pour plus d'informations sur ces événements auditables, consultez votre documentation Windows. Vous pouvez auditer les événements suivants :

    - **Contrôle total**
    - **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*

11. Si vous ne souhaitez pas que le paramètre d'audit se propage aux fichiers et dossiers suivants du conteneur d'origine, sélectionnez la case **appliquer ces entrées d'audit aux objets et/ou aux conteneurs dans ce conteneur uniquement**.
12. Cliquez sur **appliquer**.
13. Une fois que vous avez terminé d'ajouter, de supprimer ou de modifier des entrées d'audit, cliquez sur **OK**.

    La zone entrée d'audit pour <objet> se ferme.

14. Dans la zone **Audit**, sélectionnez les paramètres d'héritage de ce dossier.

    Sélectionnez uniquement le niveau minimal qui fournit les événements d'audit qui répondent à vos exigences de sécurité. Vous pouvez choisir l'une des options suivantes :

    - Sélectionnez l'option inclure les entrées d'audit héritées de la boîte parent de cet objet.
    - Sélectionnez remplacer toutes les entrées d'audit héritées sur tous les descendants avec des entrées d'audit héritées de cet objet.
    - Sélectionnez les deux cases.
    - Sélectionnez aucune case. Si vous définissez des SACLs sur un seul fichier, la boîte remplacer toutes les entrées d'audit héritées sur tous les descendants avec des entrées d'audit héritables de cet objet n'est pas présente dans la zone Audit.

15. Cliquez sur **OK**.

    La zone Audit se ferme.

Configuration des règles d'audit NTFS à l'aide de l'interface de ligne de commande ONTAP

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

Vous pouvez configurer les règles d'audit NTFS en utilisant le `vserver security file-directory` famille de commande.

Vous pouvez uniquement configurer les SACLs NTFS à l'aide de l'interface de ligne de commande. La configuration des SACLs NFSv4 n'est pas prise en charge avec cette famille de commandes ONTAP. Consultez les pages man pour plus d'informations sur l'utilisation de ces commandes pour configurer et ajouter des CLS NTFS aux fichiers et dossiers.

Configurer l'audit pour les fichiers et répertoires de style de sécurité UNIX

Vous configurez l'audit des répertoires et des fichiers de style de sécurité UNIX en ajoutant des ACE d'audit aux listes de contrôle d'accès NFSv4.x. Cela vous permet de

surveiller certains événements d’accès aux fichiers et aux répertoires NFS à des fins de sécurité.

Description de la tâche

Pour NFSv4.x, les ACE discrétionnaires et système sont tous deux stockés dans la même liste de contrôle d’accès. Ils ne sont pas stockés dans des listes de contrôle d’accès (DACL) et des listes de contrôle d’accès (SALC) distinctes. Par conséquent, vous devez faire preuve de prudence lorsque vous ajoutez des ACE d’audit à une liste de contrôle d’accès existante pour éviter d’écraser et de perdre une liste de contrôle d’accès existante. L’ordre dans lequel vous ajoutez les ACE d’audit à une liste de contrôle d’accès existante n’a aucune importance.

Étapes

1. Récupérez la liste de contrôle d’accès existante pour le fichier ou le répertoire à l’aide de la `nfs4_getfacl` ou une commande équivalente.

   Pour plus d’informations sur la manipulation des listes de contrôle d’accès, consultez les pages de manuels de votre client NFS.

2. Ajoutez les ACE d’audit souhaités.
3. Appliquez la liste de contrôle d’accès mise à jour au fichier ou au répertoire à l’aide de la `nfs4_setfacl` ou une commande équivalente.