Accès sécurisé aux fichiers à l'aide du contrôle d'accès dynamique (DAC)

ONTAP 9

NetApp
September 12, 2024

Sommaire

Accès sécurisé aux fichiers à l'aide du contrôle d'accès dynamique (DAC)

Sécuriser l'accès aux fichiers à l'aide de la présentation du contrôle d'accès dynamique (DAC)

Vous pouvez sécuriser l'accès à l'aide du contrôle d'accès dynamique et en créant des stratégies d'accès centrales dans Active Directory et en les appliquant aux fichiers et dossiers sur les SVM via des objets de stratégie de groupe appliqués (GPO, Applied Group Policy Objects). Vous pouvez configurer l'audit de manière à utiliser les événements d'activation de stratégie d'accès central pour voir les effets des modifications apportées aux stratégies d'accès central avant de les appliquer.

Ajouts aux informations d'identification CIFS

Avant le contrôle d'accès dynamique, un identifiant CIFS incluait une identité de sécurité (de l'utilisateur) et une appartenance au groupe Windows. Avec le contrôle d'accès dynamique, trois autres types d'informations sont ajoutés à l'identité du périphérique, aux réclamations du périphérique et aux réclamations de l'utilisateur :

- Identité du périphérique

  Analogique des informations d'identité de l'utilisateur, à l'exception de l'identité et de l'appartenance au groupe de l'appareil à partir de lequel l'utilisateur se connecte.

- Réclamations de l'appareil

  Assertions sur un principal de sécurité de périphérique. Par exemple, un sinistre de périphérique peut être qu'il est membre d'une UO spécifique.

- Réclamations de l'utilisateur

  Assertions sur un principal de sécurité utilisateur. Par exemple, une réclamation d'utilisateur peut être que son compte AD est membre d'une unité d'organisation spécifique.

Politiques d'accès centralisé

Les stratégies d'accès centrales aux fichiers permettent aux organisations de déployer et de gérer de manière centralisée des stratégies d'autorisation qui incluent des expressions conditionnelles à l'aide de groupes d'utilisateurs, de revendications d'utilisateurs, de revendications de périphériques et de propriétés de ressources.

Par exemple, pour accéder aux données à fort impact sur l'entreprise, un utilisateur doit être un employé à plein temps et n'a accès qu'aux données à partir d'un périphérique géré. Les stratégies d'accès central sont définies dans Active Directory et distribuées aux serveurs de fichiers via le mécanisme GPO.

Mise en place centralisée des stratégies d'accès avec audit avancé

Les politiques d'accès central peuvent être « mises en service », auquel cas elles sont évaluées de manière « par quoi » lors des contrôles d'accès aux fichiers. Les résultats de ce qui se serait passé si la stratégie était en

vigueur et la différence par rapport à ce qui est actuellement configuré sont consignés en tant qu'événement d'audit. De cette façon, les administrateurs peuvent utiliser les journaux d'événements d'audit pour étudier l'impact d'une modification de stratégie d'accès avant de mettre la stratégie en jeu. Après avoir évalué l'impact d'une modification de règle d'accès, la règle peut être déployée via des GPO sur les SVM souhaités.

Informations associées

Stratégies de groupe prises en charge

Application d'objets de stratégie de groupe aux serveurs CIFS

Activation ou désactivation de la prise en charge de GPO sur un serveur CIFS

Affichage des informations sur les configurations GPO

Affichage d'informations sur les règles d'accès central

Affichage d'informations sur les règles de stratégie d'accès central

Configuration des règles d'accès centrales pour sécuriser les données sur les serveurs CIFS

Affichage d'informations sur la sécurité du contrôle d'accès dynamique

"Audit et suivi de sécurité SMB et NFS"

Prise en charge de la fonctionnalité de contrôle dynamique d'accès

Si vous souhaitez utiliser le contrôle d'accès dynamique (DAC) sur votre serveur CIFS, vous devez comprendre comment ONTAP prend en charge la fonctionnalité de contrôle d'accès dynamique dans les environnements Active Directory.

Pris en charge pour le contrôle d'accès dynamique

ONTAP prend en charge la fonctionnalité suivante lorsque le contrôle d'accès dynamique est activé sur le serveur CIFS :

Fonctionnalité	Commentaires
Réclamations dans le système de fichiers	Les revendications sont des paires de nom et de valeur simples qui indiquent une certaine vérité sur un utilisateur. Les informations d'identification utilisateur contiennent des informations sur les sinistres, et les descripteurs de sécurité sur les fichiers peuvent effectuer des vérifications d'accès qui incluent des vérifications de sinistres. Les administrateurs peuvent ainsi mieux contrôler qui peut accéder aux fichiers.

Fonctionnalité	Commentaires
Expressions conditionnelles pour les vérifications d'accès aux fichiers	Lors de la modification des paramètres de sécurité d'un fichier, les utilisateurs peuvent ajouter des expressions conditionnelles arbitrairement complexes au descripteur de sécurité du fichier. L'expression conditionnelle peut inclure des vérifications pour les sinistres.
Contrôle centralisé de l'accès aux fichiers via des règles d'accès centrales	Les stratégies d'accès central sont des types de listes de contrôle d'accès stockées dans Active Directory et peuvent être balisées vers un fichier. L'accès au fichier n'est accordé que si les contrôles d'accès du Security Descriptor sur disque et de la stratégie d'accès centrale balisée permettent l'accès.cela permet aux administrateurs de contrôler l'accès aux fichiers à partir d'un emplacement central (AD) sans avoir à modifier le Security Descriptor sur disque.
Mise en place de stratégies d'accès centrales	Ajoute la capacité d'essayer des changements de sécurité sans affecter l'accès réel aux fichiers, en "mettant en place" un changement aux politiques d'accès central, et en voyant l'effet de la modification dans un rapport d'audit.
Affichage d'informations sur la sécurité des règles d'accès centrales à l'aide de l'interface de ligne de commande de ONTAP	Étend le `vserver security file-directory show` commande pour afficher les informations sur les règles d'accès central appliquées.
Suivi de la sécurité qui inclut les stratégies d'accès centralisé	Étend le `vserver security trace` famille de commandes permettant d'afficher les résultats qui incluent des informations sur les stratégies d'accès central appliquées.

Non pris en charge pour le contrôle d'accès dynamique

ONTAP ne prend pas en charge la fonctionnalité suivante lorsque le contrôle d'accès dynamique est activé sur le serveur CIFS :

Fonctionnalité	Commentaires
Classification automatique des objets du système de fichiers NTFS	Il s'agit d'une extension de l'infrastructure de classification de fichiers Windows qui n'est pas prise en charge dans ONTAP.
Audit avancé autre que la mise en place de stratégies d'accès centrales	Seul le staging de stratégie d'accès central est pris en charge pour l'audit avancé.

Considérations relatives à l'utilisation du contrôle d'accès dynamique et des règles d'accès central avec des serveurs CIFS

Vous devez garder à l'esprit certaines considérations lorsque vous utilisez le contrôle d'accès dynamique (DAC) et les règles d'accès central pour sécuriser les fichiers et dossiers sur les serveurs CIFS.

L'accès NFS peut être refusé à la racine si la règle de stratégie s'applique à l'utilisateur de domaine\administrateur

Dans certaines circonstances, l'accès NFS à la racine peut être refusé lorsque la sécurité de la stratégie d'accès centrale est appliquée aux données auxquelles l'utilisateur root tente d'accéder. Le problème se produit lorsque la stratégie d'accès central contient une règle appliquée au domaine\administrateur et que le compte racine est mappé au compte domaine\administrateur.

Au lieu d'appliquer une règle à l'utilisateur domaine/administrateur, vous devez appliquer la règle à un groupe avec des privilèges d'administration, tels que le groupe domaine/administrateurs. De cette façon, vous pouvez mapper root sur le compte domaine\administrateur sans que ce problème n'ait d'impact sur la racine.

Le groupe BUILTIN\Administrators du serveur CIFS a accès aux ressources lorsque la stratégie d'accès central appliquée n'est pas trouvée dans Active Directory

Il est possible que les ressources contenues dans le serveur CIFS aient des règles d'accès centrales qui leur sont appliquées, mais lorsque le serveur CIFS utilise le SID de la stratégie d'accès centrale pour tenter de récupérer des informations à partir d'Active Directory, le SID ne correspond à aucun SID de stratégie d'accès centrale existant dans Active Directory. Dans ces circonstances, le serveur CIFS applique la stratégie de restauration par défaut locale pour cette ressource.

La stratégie de récupération par défaut locale permet au groupe BUILTIN\Administrators du serveur CIFS d'accéder à cette ressource.

Activer ou désactiver la présentation du contrôle d'accès dynamique

L'option qui vous permet d'utiliser le contrôle d'accès dynamique (DAC) pour sécuriser les objets sur votre serveur CIFS est désactivée par défaut. Vous devez activer cette option si vous souhaitez utiliser le contrôle d'accès dynamique sur votre serveur CIFS. Si vous décidez par la suite de ne pas utiliser le contrôle d'accès dynamique pour sécuriser les objets stockés sur le serveur CIFS, vous pouvez désactiver cette option.

Description de la tâche

Une fois le contrôle d'accès dynamique activé, le système de fichiers peut contenir des listes de contrôle d'accès avec des entrées liées au contrôle d'accès dynamique. Si le contrôle d'accès dynamique est désactivé, les entrées de contrôle d'accès dynamique actuelles seront ignorées et les nouvelles ne seront pas autorisées.

Cette option n'est disponible qu'au niveau de privilège avancé.

Étape

1. Définissez le niveau de privilège sur avancé : `set -privilege advanced`
2. Effectuez l'une des opérations suivantes :

Si vous voulez que le contrôle d'accès dynamique soit…	Entrez la commande…
Activé	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled true`
Désactivé	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled false`

3. Revenir au niveau de privilège administrateur : `set -privilege admin`

Informations associées

Configuration des règles d'accès centrales pour sécuriser les données sur les serveurs CIFS

Gérer les listes de contrôle d'accès qui contiennent des ACE de contrôle d'accès dynamique lorsque le contrôle d'accès dynamique est désactivé

Si vous disposez de ressources dont les listes de contrôle d'accès sont appliquées avec les ACE de contrôle d'accès dynamique et que vous désactivez le contrôle d'accès dynamique sur la machine virtuelle de stockage (SVM), vous devez supprimer les ACE de contrôle d'accès dynamique avant de pouvoir gérer les ACE de contrôle d'accès non dynamique sur cette ressource.

Description de la tâche

Une fois le contrôle d'accès dynamique désactivé, vous ne pouvez pas supprimer les ACE existants de contrôle d'accès non dynamique ou ajouter de nouveaux ACE de contrôle d'accès non dynamique tant que vous n'avez pas supprimé les ACE de contrôle d'accès dynamique existants.

Vous pouvez utiliser n'importe quel outil que vous utilisez normalement pour gérer les listes de contrôle d'accès pour effectuer ces étapes.

Étapes

1. Déterminez quels ACE de contrôle d'accès dynamique sont appliqués à la ressource.
2. Supprimez les ACE de contrôle d'accès dynamique de la ressource.
3. Ajoutez ou supprimez des ACE de contrôle d'accès non dynamiques comme vous le souhaitez de la ressource.

Configurez les règles d'accès centrales pour sécuriser les données sur les serveurs CIFS

Il existe plusieurs étapes à suivre pour sécuriser l'accès aux données sur le serveur CIFS

à l'aide de stratégies d'accès centrales, notamment l'activation du contrôle d'accès dynamique (DAC) sur le serveur CIFS, la configuration de stratégies d'accès central dans Active Directory, l'application des règles d'accès central aux conteneurs Active Directory avec des GPO, Et activation des stratégies de groupe sur le serveur CIFS.

Avant de commencer

- L'Active Directory doit être configuré pour utiliser les stratégies d'accès central.
- Vous devez disposer d'un accès suffisant sur les contrôleurs de domaine Active Directory pour créer des stratégies d'accès centrales et pour créer et appliquer des GPO aux conteneurs contenant les serveurs CIFS.
- Vous devez disposer d'un accès administratif suffisant sur le SVM (Storage Virtual machine) pour exécuter les commandes nécessaires.

Description de la tâche

Les stratégies d'accès central sont définies et appliquées aux objets de stratégie de groupe (GPO, Group Policy Objects) d'Active Directory. Vous pouvez consulter la bibliothèque Microsoft TechNet pour obtenir des instructions sur la configuration des stratégies d'accès centralisé et des GPO.

"Bibliothèque Microsoft TechNet"

Étapes

1. Activer le contrôle dynamique d'accès sur le SVM si celui-ci n'est pas déjà activé à l'aide de `vserver cifs options modify` commande.

   ```
   vserver cifs options modify -vserver vs1 -is-dac-enabled true
   ```

2. Activez les objets de stratégie de groupe (GPO, Group policy objects) sur le serveur CIFS s'ils ne sont pas déjà activés à l'aide de l' `vserver cifs group-policy modify` commande.

   ```
   vserver cifs group-policy modify -vserver vs1 -status enabled
   ```

3. Créez des règles d'accès centrales et des stratégies d'accès central sur Active Directory.
4. Créez un objet de stratégie de groupe (GPO) pour déployer les stratégies d'accès central sur Active Directory.
5. Appliquez l'objet GPO au conteneur où se trouve le compte d'ordinateur du serveur CIFS.
6. Mettre à jour manuellement les GPO appliqués au serveur CIFS à l'aide de `vserver cifs group-policy update` commande.

   ```
   vserver cifs group-policy update -vserver vs1
   ```

7. Vérifiez que la stratégie d'accès central GPO est appliquée aux ressources du serveur CIFS à l'aide de `vserver cifs group-policy show-applied` commande.

   L'exemple suivant montre que la stratégie de domaine par défaut comporte deux stratégies d'accès central appliquées au serveur CIFS :

   ```
   vserver cifs group-policy show-applied
   ```

   ```
   Vserver: vs1
   ```

```
-----------------------------
    GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2

    GPO Name: Resultant Set of Policy
       Level: RSOP
  Advanced Audit Settings:
```

```
        Object Access:
            Central Access Policy Staging: failure
    Registry Settings:
        Refresh Time Interval: 22
        Refresh Random Offset: 8
        Hash Publication Mode for BranchCache: per-share
        Hash Version Support for BranchCache: all-versions
    Security Settings:
        Event Audit and Event Log:
            Audit Logon Events: none
            Audit Object Access: success
            Log Retention Method: overwrite-as-needed
            Max Log Size: 16384
        File Security:
            /vol1/home
            /vol1/dir1
        Kerberos:
            Max Clock Skew: 5
            Max Ticket Age: 10
            Max Renew Age:  7
        Privilege Rights:
            Take Ownership: usr1, usr2
            Security Privilege: usr1, usr2
            Change Notify: usr1, usr2
        Registry Values:
            Signing Required: false
        Restrict Anonymous:
            No enumeration of SAM accounts: true
            No enumeration of SAM accounts and shares: false
            Restrict anonymous access to shares and named pipes: true
            Combined restriction for anonymous user: no-access
        Restricted Groups:
            gpr1
            gpr2
    Central Access Policy Settings:
        Policies: cap1
                  cap2
  2 entries were displayed.
```

Informations associées

Affichage des informations sur les configurations GPO

Affichage d'informations sur les règles d'accès central

Affichage d'informations sur les règles de stratégie d'accès central

Afficher des informations sur la sécurité du contrôle d'accès dynamique

Vous pouvez afficher des informations sur la sécurité DAC (Dynamic Access Control) sur des volumes NTFS et sur des données avec la sécurité efficace NTFS sur des volumes de type sécurité mixtes. Cela comprend de l'information sur les ACE conditionnels, les ACE de ressources et les ACE de politique d'accès central. Les résultats vous permettent de valider votre configuration de sécurité ou de résoudre les problèmes d'accès aux fichiers.

Description de la tâche

Vous devez fournir le nom de la machine virtuelle de stockage (SVM) et le chemin d'accès aux données dont vous souhaitez afficher les informations de sécurité des fichiers ou des dossiers. Vous pouvez afficher les valeurs de sortie sous forme de récapitulatif ou sous forme de liste détaillée.

Étape

1. Afficher les paramètres de sécurité des fichiers et des répertoires avec le niveau de détail souhaité :

Pour afficher les informations…	Saisissez la commande suivante…
Sous forme récapitulative	`vserver security file-directory show -vserver vserver_name -path path`
Avec détails étendus	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`
Où la sortie est affichée avec les SID de groupe et d'utilisateur	`vserver security file-directory show -vserver vserver_name -path path -lookup-names false`
A propos de la sécurité des fichiers et des répertoires pour les fichiers et les répertoires où le masque binaire hexadécimal est traduit en format texte	`vserver security file-directory show -vserver vserver_name -path path -textual-mask true`

Exemples

L'exemple suivant affiche les informations de sécurité du contrôle d'accès dynamique sur le chemin `/vol1` Au SVM vs1 :

```
cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
                           Vserver: vs1
                         File Path: /vol1
                  File Inode Number: 112
                     Security Style: mixed
                    Effective Style: ntfs
                     DOS Attributes: 10
             DOS Attributes in Text: ----D---
             Expanded Dos Attribute: -
                       Unix User Id: 0
                      Unix Group Id: 1
                     Unix Mode Bits: 777
             Unix Mode Bits in Text: rwxrwxrwx
                               ACLs: NTFS Security Descriptor
                                     Control:0xbf14
                                     Owner:CIFS1\Administrator
                                     Group:CIFS1\Domain Admins
                                     SACL - ACEs
                                        ALL-Everyone-0xf01ff-OI|CI|SA|FA
                                        RESOURCE ATTRIBUTE-Everyone-0x0

("Department_MS",TS,0x10020,"Finance")
                                        POLICY ID-All resources - No Write-
0x0-OI|CI
                                     DACL - ACEs
                                        ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI
                                        ALLOW-Everyone-0x1f01ff-OI|CI
                                        ALLOW CALLBACK-DAC\user1-0x1200a9-
OI|CI

((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@D
evice.department==@Resource.Department_MS)
```

Informations associées

Affichage des informations sur les configurations GPO

Affichage d'informations sur les règles d'accès central

Affichage d'informations sur les règles de stratégie d'accès central

Considérations relatives au contrôle d'accès dynamique

Vous devez savoir ce qui se passe lors du retour à une version de ONTAP qui ne prend pas en charge le contrôle d'accès dynamique (DAC) et ce que vous devez faire avant et

après le rétablissement.

Si vous souhaitez restaurer le cluster vers une version de ONTAP qui ne prend pas en charge le contrôle d'accès dynamique et que le contrôle d'accès dynamique est activé sur une ou plusieurs machines virtuelles de stockage (SVM), vous devez effectuer les opérations suivantes avant le rétablissement :

- Vous devez désactiver le contrôle d'accès dynamique sur tous les SVM sur lesquels il est activé sur le cluster.
- Vous devez modifier toutes les configurations d'audit sur le cluster contenant le `cap-staging` type d'événement pour utiliser uniquement le `file-op` type d'événement.

Vous devez comprendre et agir sur certaines considérations importantes concernant la restauration des fichiers et dossiers avec les ACE Dynamic Access Control :

- Si le cluster est rétabli, les ACE de contrôle d'accès dynamique existants ne sont pas supprimés ; cependant, ils seront ignorés lors des vérifications d'accès aux fichiers.
- Comme les ACE de contrôle d'accès dynamique sont ignorés après réversion, l'accès aux fichiers change sur les fichiers avec les ACE de contrôle d'accès dynamique.

  Cela pourrait permettre aux utilisateurs d'accéder aux fichiers qu'ils ne pouvaient pas accéder ou ne pouvaient pas accéder aux fichiers qu'ils pouvaient auparavant.

- Vous devez appliquer des ACE de contrôle d'accès non dynamique aux fichiers concernés pour restaurer leur niveau de sécurité précédent.

  Cette opération peut être effectuée avant le rétablissement ou immédiatement après la fin de la nouvelle version.

> Les ACE de contrôle d'accès dynamique étant ignorés après la réversion, il n'est pas nécessaire de les supprimer lors de l'application d'ACE de contrôle d'accès non dynamique aux fichiers affectés. Toutefois, si vous le souhaitez, vous pouvez les supprimer manuellement.

Où trouver des informations supplémentaires sur la configuration et l'utilisation du contrôle d'accès dynamique et des stratégies d'accès central

Des ressources supplémentaires sont disponibles pour vous aider à configurer et utiliser le contrôle d'accès dynamique et les stratégies d'accès central.

Vous trouverez des informations sur la configuration des stratégies de contrôle d'accès dynamique et d'accès central dans Active Directory dans la bibliothèque Microsoft TechNet.

"Microsoft TechNet : présentation des scénarios de contrôle d'accès dynamique"

"Microsoft TechNet : scénario de stratégie d'accès centralisé"

Les références suivantes peuvent vous aider à configurer le serveur SMB afin qu'il utilise et prend en charge les stratégies de contrôle d'accès dynamique et d'accès central :

- **Utilisation de stratégies de groupe sur le serveur SMB**

Application d’objets de stratégie de groupe aux serveurs SMB

- **Configuration de l’audit NAS sur le serveur SMB**

  "Audit et suivi de sécurité SMB et NFS"