Appliquez des objets de stratégie de groupe aux serveurs SMB

ONTAP 9

NetApp
April 24, 2024

Sommaire

Appliquez des objets de stratégie de groupe aux serveurs SMB

Présentation de l'application d'objets de stratégie de groupe aux serveurs SMB

Votre serveur SMB prend en charge les objets de stratégie de groupe (GPO, Group Policy Objects), un ensemble de règles appelées attributs de stratégie de groupe_ qui s'appliquent aux ordinateurs dans un environnement Active Directory. Vous pouvez utiliser des GPO pour gérer centralement les paramètres de toutes les machines virtuelles de stockage (SVM) sur le cluster appartenant au même domaine Active Directory.

Lorsque les stratégies de groupe sont activées sur votre serveur SMB, ONTAP envoie des requêtes LDAP au serveur Active Directory pour demander des informations de stratégie de groupe. Si des définitions de GPO sont applicables à votre serveur SMB, le serveur Active Directory renvoie les informations de GPO suivantes :

- Nom de l'objet GPO
- Version GPO actuelle
- Emplacement de la définition de GPO
- Listes d'UUID (identificateurs uniques universels) pour les jeux de stratégies GPO

Informations associées

Sécurisation de l'accès aux fichiers à l'aide du contrôle d'accès dynamique (DAC)

"Audit et suivi de sécurité SMB et NFS"

Stratégies de groupe prises en charge

Bien que tous les objets de stratégie de groupe (GPO) ne soient pas applicables à vos SVM (Storage Virtual machines) compatibles CIFS, les SVM peuvent reconnaître et traiter l'ensemble des GPO pertinents.

Les GPO suivants sont actuellement pris en charge sur SVM :

- Paramètres de configuration des règles d'audit avancées :

  Accès aux objets : staging de stratégie d'accès central

  Spécifie le type d'événements à auditer pour l'activation de la stratégie d'accès central (CAP), y compris les paramètres suivants :

  - Ne pas auditer
  - Vérifier uniquement les événements de réussite
  - Audit des événements d'échec uniquement
  - Vérifiez à la fois les événements de réussite et d'échec

> Si l'une des trois options d'audit est définie (audit uniquement des événements de réussite, audit uniquement des événements d'échec, audit des événements de réussite et d'échec), ONTAP vérifie à la fois les événements de réussite et d'échec.

Réglez à l'aide du `Audit Central Access Policy Staging` réglage dans le `Advanced Audit Policy Configuration/Audit Policies/Object Access` GPO.

> Pour utiliser les paramètres de stratégie d'audit avancée, l'audit doit être configuré sur le SVM compatible CIFS auquel vous souhaitez appliquer ce paramètre. Si l'audit n'est pas configuré sur le SVM, les paramètres de GPO ne sont pas appliqués et seront supprimés.

- Paramètres du registre :
  - Intervalle d'actualisation des règles de groupe pour les SVM compatibles CIFS

    Réglez à l'aide du `Registry` GPO.
  - Actualisation aléatoire de la stratégie de groupe

    Réglez à l'aide du `Registry` GPO.
  - Publication de hachage pour BranchCache

    La publication Hash pour BranchCache correspond au mode de fonctionnement de BranchCache. Les trois modes de fonctionnement pris en charge sont les suivants :
    - Par action
    - Tous les partages
    - Désactivé Réglez à l'aide du `Registry` GPO.
  - Prise en charge du hachage pour BranchCache

    Les trois paramètres de version de hachage suivants sont pris en charge :
    - BranchCache version 1
    - BranchCache version 2
    - BranchCache versions 1 et 2 Réglez à l'aide du `Registry` GPO.

> Pour utiliser les paramètres de BranchCache, BranchCache doit être configuré sur le SVM compatible CIFS auquel vous souhaitez appliquer ce paramètre. Si BranchCache n'est pas configuré sur le SVM, les paramètres de GPO ne sont pas appliqués et seront supprimés.

- Les paramètres de sécurité
  - Règle d'audit et journal des événements
    - Audit des événements de connexion

      Spécifie le type d'événements de connexion à auditer, notamment les paramètres suivants :
      - Ne pas auditer

- Vérifier uniquement les événements de réussite
- Audit sur les événements de panne
- Vérifiez à la fois les événements de réussite et d'échec Réglez à l'aide du `Audit logon events` réglage dans le `Local Policies/Audit Policy` GPO.

> Si l'une des trois options d'audit est définie (audit uniquement des événements de réussite, audit uniquement des événements d'échec, audit des événements de réussite et d'échec), ONTAP vérifie à la fois les événements de réussite et d'échec.

- Auditer l'accès aux objets

  Spécifie le type d'accès aux objets à auditer, y compris les paramètres suivants :

  - Ne pas auditer
  - Vérifier uniquement les événements de réussite
  - Audit sur les événements de panne
  - Vérifiez à la fois les événements de réussite et d'échec Réglez à l'aide du `Audit object access` réglage dans le `Local Policies/Audit Policy` GPO.

> Si l'une des trois options d'audit est définie (audit uniquement des événements de réussite, audit uniquement des événements d'échec, audit des événements de réussite et d'échec), ONTAP vérifie à la fois les événements de réussite et d'échec.

- Méthode de conservation des journaux

  Spécifie la méthode de conservation du journal d'audit, y compris les paramètres suivants :

  - Remplacez le journal des événements lorsque la taille du fichier journal dépasse la taille maximale du journal
  - Ne pas écraser le journal des événements (effacer le journal manuellement) Réglez à l'aide du `Retention method for security log` réglage dans le `Event Log` GPO.

- Taille maximale du journal

  Spécifie la taille maximale du journal d'audit.

  Réglez à l'aide du `Maximum security log size` réglage dans le `Event Log` GPO.

> Pour utiliser les paramètres de stratégie d'audit et de stratégie GPO du journal des événements, l'audit doit être configuré sur le SVM compatible CIFS auquel vous souhaitez appliquer ce paramètre. Si l'audit n'est pas configuré sur le SVM, les paramètres de GPO ne sont pas appliqués et seront supprimés.

◦ Sécurité du système de fichiers

Spécifie une liste de fichiers ou de répertoires sur lesquels la sécurité des fichiers est appliquée via un GPO.

Réglez à l'aide du `File System` GPO.

> Le chemin d'accès au volume auquel la stratégie de sécurité du système de fichiers est configurée doit exister au sein de la SVM.

- Règle Kerberos
  - Inclinaison maximale de l'horloge

    Spécifie la tolérance maximale en minutes pour la synchronisation de l'horloge de l'ordinateur.

    Réglez à l'aide du `Maximum tolerance for computer clock synchronization` réglage dans le `Account Policies/Kerberos Policy` GPO.

  - Âge maximum du billet

    Spécifie la durée de vie maximale en heures pour le ticket utilisateur.

    Réglez à l'aide du `Maximum lifetime for user ticket` réglage dans le `Account Policies/Kerberos Policy` GPO.

  - Âge maximum de renouvellement du billet

    Spécifie la durée de vie maximale en jours pour le renouvellement du ticket utilisateur.

  Réglez à l'aide du `Maximum lifetime for user ticket renewal` réglage dans le `Account Policies/Kerberos Policy` GPO.

- Attribution de droits utilisateur (droits de privilège)
  - Devenir propriétaire

    Indique la liste des utilisateurs et des groupes qui ont le droit de prendre possession de tout objet sécurisé.

    Réglez à l'aide du `Take ownership of files or other objects` réglage dans le `Local Policies/User Rights Assignment` GPO.

  - Privilège de sécurité

    Indique la liste des utilisateurs et des groupes qui peuvent spécifier des options d'audit pour l'accès aux objets de ressources individuelles, telles que des fichiers, des dossiers et des objets Active Directory.

    Réglez à l'aide du `Manage auditing and security log` réglage dans le `Local Policies/User Rights Assignment` GPO.

  - Changer le privilège de notification (vérification de la traverse de dérivation)

    Indique la liste des utilisateurs et des groupes qui peuvent traverser les arborescences de répertoires, même si les utilisateurs et les groupes ne disposent pas des autorisations sur le répertoire de traversée.

  Le même privilège est requis pour que les utilisateurs reçoivent des notifications sur les modifications apportées aux fichiers et aux répertoires. Réglez à l'aide du `Bypass traverse checking` réglage dans le `Local Policies/User Rights Assignment` GPO.

- Valeurs de registre
  - Paramètre de signature requis

    Indique si la signature SMB requise est activée ou désactivée.

  Réglez à l'aide du `Microsoft network server: Digitally sign communications (always)` réglage dans le `Security Options` GPO.

- Limiter l'anonymat

  Indique les restrictions pour les utilisateurs anonymes et inclut les trois paramètres de stratégie de groupe suivants :

  - Pas d'énumération des comptes de Security Account Manager (SAM) :

    Ce paramètre de sécurité détermine les autorisations supplémentaires accordées pour les connexions anonymes à l'ordinateur. Cette option s'affiche sous la forme `no-enumeration` Dans ONTAP, si elle est activée.

    Réglez à l'aide du `Network access: Do not allow anonymous enumeration of SAM accounts` réglage dans le `Local Policies/Security Options` GPO.

  - Pas d'énumération des comptes et des partages SAM

    Ce paramètre de sécurité détermine si l'énumération anonyme des comptes et partages SAM est autorisée. Cette option s'affiche sous la forme `no-enumeration` Dans ONTAP, si elle est activée.

    Réglez à l'aide du `Network access: Do not allow anonymous enumeration of SAM accounts and shares` réglage dans le `Local Policies/Security Options` GPO.

  - Limiter l'accès anonyme aux partages et aux canaux nommés

    Ce paramètre de sécurité limite l'accès anonyme aux partages et aux tuyaux. Cette option s'affiche sous la forme `no-access` Dans ONTAP, si elle est activée.

    Réglez à l'aide du `Network access: Restrict anonymous access to Named Pipes and Shares` réglage dans le `Local Policies/Security Options` GPO.

    Lors de l'affichage d'informations sur les stratégies de groupe définies et appliquées, le `Resultant restriction for anonymous user` Le champ sortie fournit des informations sur la restriction résultant des trois paramètres de GPO anonymes de restriction. Les restrictions possibles résultantes sont les suivantes :

- `no-access`

  L'utilisateur anonyme refuse l'accès aux partages spécifiés et aux canaux nommés, et ne peut pas utiliser l'énumération des comptes et des partages SAM. Cette restriction résultante est visible si le `Network access: Restrict anonymous access to Named Pipes and Shares` L'objet GPO est activé.

- `no-enumeration`

  L'utilisateur anonyme a accès aux partages spécifiés et aux canaux nommés, mais ne peut pas utiliser

l'énumération des comptes et partages SAM. Cette restriction résultante est observée si les deux conditions suivantes sont remplies :

  - Le `Network access: Restrict anonymous access to Named Pipes and Shares` GPO est désactivé.
  - Soit le `Network access: Do not allow anonymous enumeration of SAM accounts` ou le `Network access: Do not allow anonymous enumeration of SAM accounts and shares` Les stratégies de groupe sont activées.

  - `no-restriction`

    L'utilisateur anonyme dispose d'un accès complet et peut utiliser l'énumération. Cette restriction résultante est observée si les deux conditions suivantes sont remplies :

    - Le `Network access: Restrict anonymous access to Named Pipes and Shares` GPO est désactivé.
    - Les deux `Network access: Do not allow anonymous enumeration of SAM accounts` et `Network access: Do not allow anonymous enumeration of SAM accounts and shares` Les GPO sont désactivés.
      - Groupes restreints

        Vous pouvez configurer des groupes restreints pour gérer de manière centralisée l'appartenance à des groupes intégrés ou définis par l'utilisateur. Lorsque vous appliquez un groupe restreint via une stratégie de groupe, l'appartenance à un groupe local de serveur CIFS est automatiquement définie pour correspondre aux paramètres de liste d'appartenance définis dans la stratégie de groupe appliquée.

  Réglez à l'aide du `Restricted Groups` GPO.

- Paramètres de stratégie d'accès centralisé

  Spécifie une liste de stratégies d'accès centralisé. Les politiques d'accès central et les règles de politique d'accès central associées déterminent les autorisations d'accès pour plusieurs fichiers sur la SVM.

Informations associées

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

Sécurisation de l'accès aux fichiers à l'aide du contrôle d'accès dynamique (DAC)

"Audit et suivi de sécurité SMB et NFS"

Modification des paramètres de sécurité Kerberos du serveur CIFS

Utilisation de BranchCache pour mettre en cache le contenu de partage SMB dans une succursale

Utilisation de la signature SMB pour améliorer la sécurité du réseau

Configuration de la vérification de la traverse de dérivation

Configuration des restrictions d'accès pour les utilisateurs anonymes

Conditions requises pour l'utilisation de stratégies de groupe avec votre serveur SMB

Pour utiliser des stratégies de groupe (GPO, Group Policy Objects) avec votre serveur SMB, votre système doit répondre à plusieurs exigences.

- SMB doit être sous licence sur le cluster. La licence SMB est incluse avec "ONTAP One". Si vous n'avez pas ONTAP One et que la licence n'est pas installée, contactez votre ingénieur commercial.
- Un serveur SMB doit être configuré et joint à un domaine Windows Active Directory.
- L'état admin du serveur SMB doit être on.
- Les GPO doivent être configurés et appliqués à l'unité organisationnelle (ou) Windows Active Directory contenant l'objet ordinateur serveur SMB.
- La prise en charge des GPO doit être activée sur le serveur SMB.

Activer ou désactiver la prise en charge de GPO sur un serveur CIFS

Vous pouvez activer ou désactiver la prise en charge des objets de stratégie de groupe (GPO, Group Policy Object) sur un serveur CIFS. Si vous activez la prise en charge GPO sur un serveur CIFS, les GPO applicables définis sur la stratégie de groupe—la stratégie appliquée à l'unité organisationnelle (ou) qui contient l'objet ordinateur de serveur CIFS—sont appliqués au serveur CIFS.

Description de la tâche

Les GPO ne peuvent pas être activés sur les serveurs CIFS en mode Workgroup.

Étapes

1. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Entrez la commande…
Activer les stratégies de groupe	`vserver cifs group-policy modify -vserver` *`vserver_name`* `-status enabled`
Désactiver les stratégies de groupe	`vserver cifs group-policy modify -vserver` *`vserver_name`* `-status disabled`

2. Vérifiez que la prise en charge des stratégies de groupe est dans l'état souhaité : `vserver cifs group-policy show -vserver +vserver_name_`

   L'état de la stratégie de groupe pour les serveurs CIFS en mode groupe de travail s'affiche en tant que « désactivé ».

Exemple

L'exemple suivant illustre la prise en charge de GPO sur SVM (Storage Virtual machine) vs1 :

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled

cluster1::> vserver cifs group-policy show -vserver vs1

            Vserver: vs1
Group Policy Status: enabled
```

Informations associées

Stratégies de groupe prises en charge

Configuration requise pour l'utilisation des objets de stratégie de groupe avec votre serveur CIFS

Mise à jour des stratégies de groupe sur le serveur CIFS

Mise à jour manuelle des paramètres GPO sur le serveur CIFS

Affichage des informations sur les configurations GPO

Mise à jour des objets GPO sur le serveur SMB

Mise à jour des stratégies de groupe sur la présentation du serveur CIFS

Par défaut, ONTAP récupère et applique les modifications des objets de stratégie de groupe (GPO) toutes les 90 minutes. Les paramètres de sécurité sont actualisés toutes les 16 heures. Si vous voulez mettre à jour les GPO pour appliquer de nouveaux paramètres de stratégie GPO avant que ONTAP ne les mette à jour automatiquement, vous pouvez déclencher une mise à jour manuelle sur un serveur CIFS à l'aide d'une commande ONTAP.

- Par défaut, tous les GPO sont vérifiés et mis à jour au besoin toutes les 90 minutes.

  Cet intervalle est configurable et peut être défini à l'aide du `Refresh interval` et `Random offset` Paramètres GPO.

  ONTAP interroge Active Directory pour les modifications apportées aux stratégies de groupe. Si les numéros de version de GPO enregistrés dans Active Directory sont supérieurs à ceux du serveur CIFS, ONTAP récupère et applique les nouveaux GPO. Si les numéros de version sont identiques, les GPO sur le serveur CIFS ne sont pas mis à jour.

- Les stratégies de sécurité sont actualisées toutes les 16 heures.

  ONTAP récupère et applique les stratégies de groupe de paramètres de sécurité toutes les 16 heures, que ces stratégies de groupe aient été modifiées ou non.

  > La valeur par défaut de 16 heures ne peut pas être modifiée dans la version ONTAP actuelle. Il s'agit d'un paramètre par défaut du client Windows.

- Tous les GPO peuvent être mis à jour manuellement à l'aide d'une commande ONTAP.

Cette commande simule Windows `gpupdate.exe``commande /force'.

Informations associées

Mise à jour manuelle des paramètres GPO sur le serveur CIFS

Mise à jour manuelle des paramètres GPO sur le serveur CIFS

Si vous souhaitez mettre à jour immédiatement les paramètres des objets GPO (Group Policy Object) sur votre serveur CIFS, vous pouvez mettre à jour les paramètres manuellement. Vous pouvez uniquement mettre à jour les paramètres modifiés ou forcer une mise à jour pour tous les paramètres, y compris les paramètres qui ont été appliqués auparavant mais qui n'ont pas été modifiés.

Étape

1. Effectuez l'action appropriée :

Si vous voulez mettre à jour…	Entrez la commande…
Paramètres de GPO modifiés	`vserver cifs group-policy update -vserver` *`vserver_name`*
Tous les paramètres GPO	`vserver cifs group-policy update -vserver` *`vserver_name`* `-force-reapply -all-settings true`

Informations associées

Mise à jour des stratégies de groupe sur le serveur CIFS

Affiche des informations sur les configurations GPO

Vous pouvez afficher des informations sur les configurations GPO (Group Policy Object) définies dans Active Directory et à propos des configurations GPO appliquées au serveur CIFS.

Description de la tâche

Vous pouvez afficher des informations sur toutes les configurations GPO définies dans Active Directory du domaine auquel appartient le serveur CIFS ou afficher des informations uniquement sur les configurations GPO appliquées à un serveur CIFS.

Étapes

1. Pour afficher des informations sur les configurations GPO, effectuez l'une des opérations suivantes :

Si vous souhaitez afficher des informations sur toutes les configurations de stratégie de groupe…	Entrez la commande…
Défini dans Active Directory	`vserver cifs group-policy show-defined -vserver vserver_name`
Appliquée à une machine virtuelle de stockage (SVM) compatible CIFS	`vserver cifs group-policy show-applied -vserver vserver_name`

Exemple

L'exemple suivant présente les configurations GPO définies dans Active Directory à laquelle la SVM compatible CIFS vs1 appartient :

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

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 : version1
  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
    Status: enabled
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication for Mode BranchCache: per-share
    Hash Version Support for BranchCache: version1
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
```

L'exemple suivant présente les configurations GPO appliquées au SVM vs1 compatible CIFS :

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

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
```

Informations associées

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

Affiche des informations détaillées sur les GPO de groupe restreints

Vous pouvez afficher des informations détaillées sur les groupes restreints qui sont définis comme objets de stratégie de groupe (GPO, Group Policy Objects) dans Active Directory et qui sont appliqués au serveur CIFS.

Description de la tâche

Par défaut, les informations suivantes sont affichées :

- Nom de la stratégie de groupe
- Version de la stratégie de groupe
- Lien

  Spécifie le niveau dans lequel la stratégie de groupe est configurée. Les valeurs de sortie possibles sont les suivantes :

  - `Local` Lorsque la stratégie de groupe est configurée dans ONTAP
  - `Site` lorsque la stratégie de groupe est configurée au niveau du site dans le contrôleur de domaine
  - `Domain` lorsque la stratégie de groupe est configurée au niveau du domaine dans le contrôleur de domaine
  - `OrganizationalUnit` Lorsque la stratégie de groupe est configurée au niveau de l'unité organisationnelle (ou) dans le contrôleur de domaine
  - `RSOP` pour l'ensemble résultant de règles dérivées de toutes les stratégies de groupe définies à différents niveaux
- Nom de groupe restreint
- Utilisateurs et groupes qui appartiennent à et qui n'appartiennent pas au groupe restreint
- Liste des groupes auxquels le groupe restreint est ajouté

  Un groupe peut être membre de groupes autres que ceux répertoriés ici.

Étape

1. Afficher des informations sur tous les GPO de groupe restreints en effectuant l'une des actions suivantes :

Si vous souhaitez afficher des informations sur tous les GPO de groupe restreints…	Entrez la commande…
Défini dans Active Directory	`vserver cifs group-policy restricted-group show-defined -vserver vserver_name`
Appliqué à un serveur CIFS	`vserver cifs group-policy restricted-group show-applied -vserver vserver_name`

Exemple

L'exemple suivant affiche les informations relatives aux stratégies de groupe restreintes définies dans le domaine Active Directory auquel appartient la SVM compatible CIFS nommée vs1 :

```
cluster1::> vserver cifs group-policy restricted-group show-defined
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
            Group Name: group1
               Members: user1
              MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
            Group Name: group1
               Members: user1
              MemberOf: EXAMPLE\group9
```

L'exemple suivant affiche les informations relatives aux groupes restreints GPO appliqués au SVM vs1 activé pour CIFS :

```
cluster1::> vserver cifs group-policy restricted-group show-applied
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
            Group Name: group1
               Members: user1
              MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
            Group Name: group1
               Members: user1
              MemberOf: EXAMPLE\group9
```

Informations associées

Affichage des informations sur les configurations GPO

Afficher des informations sur les stratégies d'accès central

Vous pouvez afficher des informations détaillées sur les stratégies d'accès central définies dans Active Directory. Vous pouvez également afficher des informations sur les stratégies d'accès central appliquées au serveur CIFS via des objets de stratégie de groupe (GPO).

Description de la tâche

Par défaut, les informations suivantes sont affichées :

- Nom du SVM
- Nom de la stratégie d'accès central
- SID
- Description
- Heure de création
- Heure de modification
- Règles des membres

> Les serveurs CIFS en mode groupe de travail ne sont pas affichés car ils ne prennent pas en charge les GPO.

Étape

1. Afficher des informations sur les stratégies d'accès central en effectuant l'une des actions suivantes :

Si vous souhaitez afficher des informations sur toutes les stratégies d'accès central…	Entrez la commande…
Défini dans Active Directory	`vserver cifs group-policy central-access-policy show-defined -vserver` *`vserver_name`*
Appliqué à un serveur CIFS	`vserver cifs group-policy central-access-policy show-applied -vserver` *`vserver_name`*

Exemple

L'exemple suivant affiche les informations pour toutes les stratégies d'accès central définies dans Active Directory :

```
cluster1::> vserver cifs group-policy central-access-policy show-defined

Vserver  Name                 SID
-------- --------------------
-----------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

L'exemple suivant affiche les informations de toutes les règles d'accès central appliquées aux SVM (Storage Virtual machine) sur le cluster :

```
cluster1::> vserver cifs group-policy central-access-policy show-applied

Vserver    Name                 SID
-------- --------------------
----------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

Informations associées

Sécurisation de l'accès aux fichiers à l'aide du contrôle d'accès dynamique (DAC)

Affichage des informations sur les configurations GPO

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

Afficher des informations sur les règles de stratégie d'accès central

Vous pouvez afficher des informations détaillées sur les règles de stratégie d'accès central associées aux stratégies d'accès central définies dans Active Directory. Vous pouvez également afficher des informations sur les règles d'accès central appliquées au serveur CIFS via des stratégies d'accès centrales (objets de stratégie de groupe).

Description de la tâche

Vous pouvez afficher des informations détaillées sur les règles de stratégie d'accès central définies et appliquées. Par défaut, les informations suivantes sont affichées :

- Nom d'un vserver
- Nom de la règle d'accès central
- Description
- Heure de création
- Heure de modification

- Autorisations en cours
- Autorisations proposées
- Ressources cibles

Si vous souhaitez afficher des informations sur toutes les règles de stratégie d'accès central associées aux stratégies d'accès central…	Entrez la commande…
Défini dans Active Directory	`vserver cifs group-policy central-access-rule show-defined -vserver vserver_name`
Appliqué à un serveur CIFS	`vserver cifs group-policy central-access-rule show-applied -vserver vserver_name`

Exemple

L'exemple suivant affiche les informations de toutes les règles de stratégie d'accès central associées aux stratégies d'accès central définies dans Active Directory :

```
cluster1::> vserver cifs group-policy central-access-rule show-defined

Vserver    Name
---------- --------------------
vs1        r1
           Description: rule #1
         Creation Time: Tue Oct 22 09:33:48 2013
     Modification Time: Tue Oct 22 09:33:48 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1        r2
           Description: rule #2
         Creation Time: Tue Oct 22 10:27:57 2013
     Modification Time: Tue Oct 22 10:27:57 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

L'exemple suivant affiche les informations de toutes les règles d'accès central associées aux règles d'accès central appliquées aux SVM (Storage Virtual machine) sur le cluster :

```
cluster1::> vserver cifs group-policy central-access-rule show-applied

Vserver    Name
---------- --------------------
vs1        r1
           Description: rule #1
         Creation Time: Tue Oct 22 09:33:48 2013
     Modification Time: Tue Oct 22 09:33:48 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1        r2
           Description: rule #2
         Creation Time: Tue Oct 22 10:27:57 2013
     Modification Time: Tue Oct 22 10:27:57 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

Informations associées

Sécurisation de l'accès aux fichiers à l'aide du contrôle d'accès dynamique (DAC)

Affichage des informations sur les configurations GPO

Affichage d'informations sur les règles d'accès central