SMBサーバへのグループ ポリシー オブジェクトの適用

ONTAP 9

NetApp
February 12, 2026

目次

SMBサーバへのグループ ポリシー オブジェクトの適用

ONTAP SMB サーバへのグループ ポリシー オブジェクトの適用について学習します

SMBサーバーは、Active Directory環境内のコンピュータに適用される_グループポリシー属性_と呼ばれる一連のルールであるグループポリシーオブジェクト（GPO）をサポートしています。GPOを使用すると、同じActive Directoryドメインに属するクラスタ上のすべてのStorage Virtual Machine（SVM）の設定を一元管理できます。

ONTAPは、SMBサーバでGPOが有効になっている場合、Active DirectoryサーバにLDAPクエリを送信してGPO情報を要求します。Active Directoryサーバは、SMBサーバに適用できるGPO定義がある場合、次のGPO情報を返します。

- GPO名
- 現在のGPOバージョン
- GPO定義の場所
- GPOポリシー セットのUniversally Unique Identifier（UUID）一覧

関連情報

- サーバーのファイル アクセス セキュリティについて学ぶ
- "SMBおよびNFS監査とセキュリティトレース"

サポートされているONTAP SMB GPOについて学ぶ

すべてのグループ ポリシー オブジェクト（GPO）をCIFS対応のStorage Virtual Machine（SVM）に適用できるわけではありませんが、SVMでは関連するGPOを認識して処理することができます。

SVMで現在サポートされているGPOは次のとおりです。

- 高度な監査ポリシー構成の設定：

  オブジェクト アクセス：集中アクセス ポリシーのステージング

  集約型アクセス ポリシー（CAP）のステージングで監査対象となるイベント タイプを次の中から指定します。

  - 監査しない
  - 成功イベントのみを監査する
  - 失敗イベントのみを監査する
  - 成功イベントと失敗イベントの両方を監査する

3つの監査オプション（成功イベントのみ監査、失敗イベントのみ監査、成功イベントと失敗イベントの両方を監査）のいずれかが設定されている場合、ONTAPは成功イベントと失敗イベントの両方を監査します。

`Advanced Audit Policy Configuration/Audit Policies/Object Access` GPO の `Audit Central Access Policy Staging`設定を使用して設定します。

高度な監査ポリシー構成GPO設定を使用するには、その設定を適用するCIFS対応のSVM上で監査を構成する必要があります。SVMで監査が構成されていない場合、GPO設定は適用されず、破棄されます。

- レジストリ設定：
  - CIFS対応SVMのグループポリシー更新間隔

    `Registry` GPO を使用して設定します。

  - グループ ポリシー更新のランダム オフセット

    `Registry` GPO を使用して設定します。

  - BranchCacheのハッシュ公開

    BranchCacheのハッシュの発行GPOは、BranchCacheの動作モードに対応します。次の3つの動作モードがサポートされています。

    - 1株当たり
    - 全株式
    - `Registry` GPO を使用して無効に設定します。

  - BranchCacheのハッシュバージョンのサポート

    次の3つのハッシュ バージョン設定がサポートされています。

    - BranchCache バージョン1
    - BranchCache バージョン2
    - BranchCacheバージョン1および2 `Registry`GPOを使用して設定します。

    BranchCache GPO設定を使用するには、その設定を適用するCIFS対応のSVM上でBranchCacheを構成する必要があります。SVMでBranchCacheが構成されていない場合、GPO設定は適用されず、破棄されます。

- セキュリティ設定
  - 監査ポリシーとイベント ログ

- ログオン イベントの監査

  監査対象となるログオン イベントのタイプを次の中から指定します。

  - 監査しない
  - 成功イベントのみを監査する
  - 障害イベントの監査
  - 成功イベントと失敗イベントの両方を監査します。 `Local Policies/Audit Policy` GPO の `Audit logon events`設定を使用して設定します。

    3つの監査オプション（成功イベントのみ監査、失敗イベントのみ監査、成功イベントと失敗イベントの両方を監査）のいずれかが設定されている場合、ONTAPは成功イベントと失敗イベントの両方を監査します。

- オブジェクト アクセスの監査

  監査対象となるオブジェクト アクセスのタイプを次の中から指定します。

  - 監査しない
  - 成功イベントのみを監査する
  - 障害イベントの監査
  - 成功イベントと失敗イベントの両方を監査します。 `Local Policies/Audit Policy` GPO の `Audit object access`設定を使用して設定します。

    3つの監査オプション（成功イベントのみ監査、失敗イベントのみ監査、成功イベントと失敗イベントの両方を監査）のいずれかが設定されている場合、ONTAPは成功イベントと失敗イベントの両方を監査します。

- ログ保持方法

  監査ログの保持方法を次の中から指定します。

  - ログ ファイルのサイズが最大ログ サイズを超えた場合にイベント ログを上書きする
  - イベント ログを上書きしない（ログを手動でクリアする） `Event Log` GPO 内の `Retention method for security log`設定を使用して設定します。

- 最大ログ サイズ

  監査ログの最大サイズを指定します。

  `Event Log` GPO の `Maximum security log size`設定を使用して設定します。

  監査ポリシーとイベント ログGPO設定を使用するには、その設定を適用するCIFS対応のSVM上で監査を構成する必要があります。SVMで監査が構成されていない場合、GPO設定は適用されず、破棄されます。

- ファイルシステムのセキュリティ

  GPOでファイル セキュリティを適用するファイルまたはディレクトリのリストを指定します。

  `File System` GPO を使用して設定します。

  SVM内にファイルシステム セキュリティGPOを構成するボリューム パスが存在している必要があります。

- Kerberosポリシー
  - 最大クロック スキュー

    コンピュータ クロックの同期の許容最大誤差を分単位で指定します。

    `Account Policies/Kerberos Policy` GPO の `Maximum tolerance for computer clock synchronization`設定を使用して設定します。

  - チケットの最大有効期間

    ユーザ チケットの最大有効期間を時間単位で指定します。

    `Account Policies/Kerberos Policy` GPO の `Maximum lifetime for user ticket`設定を使用して設定します。

  - チケットの最大更新期間

    ユーザ チケットの更新の最大有効期間を日単位で指定します。

    `Account Policies/Kerberos Policy` GPO の `Maximum lifetime for user ticket renewal`設定を使用して設定します。

- ユーザー権限の割り当て（特権）
  - 所有権の取得

    セキュリティ保護が可能なオブジェクトの所有権を取得できるユーザとグループのリストを指定します。

    `Local Policies/User Rights Assignment` GPO の `Take ownership of files or other objects`設定を使用して設定します。

  - セキュリティ権限

ファイル、フォルダ、Active Directoryオブジェクトなどの個々のリソースへのオブジェクト アクセスの監査オプションを指定できるユーザとグループのリストを指定します。

`Local Policies/User Rights Assignment` GPO の `Manage auditing and security log`設定を使用して設定します。

- 通知権限の変更（トラバース チェックのバイパス）

  トラバースするディレクトリに対する権限がなくても、ディレクトリ ツリーをトラバースできるユーザとグループのリストを指定します。

ファイルやディレクトリの変更に関する通知をユーザーが受け取る場合にも、同じ権限が必要です。`Local Policies/User Rights Assignment` GPOの `Bypass traverse checking`設定を使用して設定します。

- レジストリ値
  - 署名必須設定

    SMB署名要求を有効にするか無効にするかを指定します。

    `Security Options` GPO の `Microsoft network server: Digitally sign communications (always)`設定を使用して設定します。

- 匿名アクセスを制限する

  匿名ユーザに対する制限を、次の3つのGPO設定で指定します。

  - セキュリティ アカウント マネージャー (SAM) アカウントの列挙がありません：

    このセキュリティ設定は、コンピュータへの匿名接続に対して付与される追加の権限を決定します。このオプションは、有効になっている場合、ONTAPでは `no-enumeration`と表示されます。

    `Local Policies/Security Options` GPO の `Network access: Do not allow anonymous enumeration of SAM accounts`設定を使用して設定します。

  - SAM アカウントと共有の列挙なし

    このセキュリティ設定は、SAMアカウントと共有の匿名列挙を許可するかどうかを決定します。このオプションは、有効になっている場合、ONTAPでは `no-enumeration`として表示されます。

    `Local Policies/Security Options` GPO の `Network access: Do not allow anonymous enumeration of SAM accounts and shares`設定を使用して設定します。

  - 共有と名前付きパイプへの匿名アクセスを制限する

このセキュリティ設定は、共有およびパイプへの匿名アクセスを制限します。このオプションは、有効になっている場合、ONTAPでは `no-access`と表示されます。

`Local Policies/Security Options` GPO の `Network access: Restrict anonymous access to Named Pipes and Shares`設定を使用して設定します。

定義済みおよび適用済みのグループ ポリシーに関する情報を表示する際、 `Resultant restriction for anonymous user`出力フィールドには、匿名を制限する3つのGPO設定の結果的な制限に関する情報が表示されます。結果として生じる可能性のある制限は次のとおりです：

- no-access

  匿名ユーザーは指定された共有および名前付きパイプへのアクセスを拒否され、SAMアカウントと共有の列挙も使用できません。この制限は、 `Network access: Restrict anonymous access to Named Pipes and Shares`GPOが有効になっている場合に表示されます。

- no-enumeration

  匿名ユーザは、指定された共有と名前付きパイプにアクセスできますが、SAMアカウントと共有は列挙できません。この制限は、次の両方の条件に該当する場合に表示されます。

  - `Network access: Restrict anonymous access to Named Pipes and Shares`GPO は無効になっています。
  - `Network access: Do not allow anonymous enumeration of SAM accounts`または `Network access: Do not allow anonymous enumeration of SAM accounts and shares`GPO のいずれかが有効になっています。

- no-restriction

  匿名ユーザにはフル アクセスが付与され、列挙できます。この制限は、次の両方の条件に該当する場合に表示されます。

  - `Network access: Restrict anonymous access to Named Pipes and Shares`GPO は無効になっています。
  - `Network access: Do not allow anonymous enumeration of SAM accounts`と `Network access: Do not allow anonymous enumeration of SAM accounts and shares`の両方のGPOが無効になっています。
    - 制限付きグループ

      制限されたグループを設定して、組込みグループやユーザ定義グループのメンバーを集中管理することができます。グループ ポリシーを通して制限されたグループを適用する場合、CIFS サーバ ローカル グループのメンバーは、適用されるグループ ポリシーで定義されているメンバー リスト設定に一致するように自動的に設定されます。

      `Restricted Groups` GPO を使用して設定します。

- 集約型アクセス ポリシーの設定

集約型アクセス ポリシーのリストを示します。集約型アクセス ポリシーと関連付けられた集約型アクセス ポリシー ルールによって、SVM上の複数のファイルに対するアクセス権が決定されます。

関連情報

- サーバー上の GPO サポートを有効または無効にする
- サーバーのファイル アクセス セキュリティについて学ぶ
- "SMBおよびNFS監査とセキュリティトレース"
- サーバーのセキュリティ設定を変更する
- BranchCacheを使用してブランチオフィスで共有コンテンツをキャッシュする方法について学習します
- ONTAP署名を使用してネットワークセキュリティを強化する方法について学習します
- バイパス トラバース チェックの設定について学ぶ
- 匿名ユーザに対するアクセス制限の設定

ONTAP SMBサーバのGPO要件

SMBサーバでグループ ポリシー オブジェクト（GPO）を使用するには、いくつかの要件を満たしている必要があります。

- クラスタにはSMBのライセンスが必要です。SMBライセンスは"ONTAP One"に含まれています。ONTAP Oneをお持ちでなく、ライセンスがインストールされていない場合は、営業担当者にお問い合わせください。
- SMBサーバが設定され、Windows Active Directoryドメインに追加されている必要があります。
- SMBサーバ管理ステータスがオンである必要があります。
- GPOが設定され、SMBサーバ コンピュータ オブジェクトを含むWindows Active Directoryの組織単位（OU）に適用されている必要があります。
- SMBサーバでGPOのサポートが有効になっている必要があります。

ONTAP SMBサーバでGPOサポートを有効または無効にする

CIFSサーバでグループ ポリシー オブジェクト（GPO）のサポートを有効または無効にできます。CIFSサーバでGPOのサポートを有効にすると、グループ ポリシー（CIFSサーバ コンピュータ オブジェクトを含む組織単位に適用されるポリシー）に定義されている該当するGPOがCIFSサーバに適用されます。

タスク概要

GPOはワークグループ モードのCIFSサーバでは有効にできません。

手順

1. 次のいずれかを実行します。

状況	コマンドを入力してください...
GPOを有効にする	`vserver cifs group-policy modify -vserver vserver_name -status enabled`
GPOを無効にする	`vserver cifs group-policy modify -vserver vserver_name -status disabled`

2. GPO サポートが目的の状態であることを確認します（：） `vserver cifs group-policy show -vserver +vserver_name_`

   ワークグループ モードの CIFS サーバーのグループ ポリシー ステータスは「disabled」と表示されます。

例

次の例は、Storage Virtual Machine（SVM）vs1でGPOサポートを有効にします。

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

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

            Vserver: vs1
Group Policy Status: enabled
```

関連情報

サポートされているGPOについて学ぶ

GPOのサーバ要件

SMBサーバ上のGPOの更新について学ぶ

SMBサーバのGPO設定を手動で更新する

GPO設定に関する情報の表示

SMBサーバでのGPOの更新方法

ONTAP SMBサーバ上のGPOの更新について学ぶ

デフォルトでは、ONTAPはグループ ポリシー オブジェクト（GPO）の変更を90分に1回取得して適用します。セキュリティ設定は16時間に1回更新されます。ONTAPで自動的に更新される前にGPOを更新し、新しいGPOポリシー設定を適用するには、ONTAPコマンドを使用してCIFSサーバで手動更新をトリガーします。

- デフォルトで、すべてのGPOを90分に1回確認し、必要に応じて更新。

この間隔は構成可能であり、 `Refresh interval`および `Random offset` GPO 設定を使用して設定できます。

ONTAPは、GPOの変更がないかどうかをActive Directoryに照会します。Active Directoryに記録されているGPOのバージョン番号がCIFSサーバ上のGPOのバージョン番号より大きい場合、ONTAPは新しいGPOを取得して適用します。バージョン番号が同じ場合、CIFSサーバ上のGPOは更新されません。

- セキュリティ設定のGPOを16時間に1回更新。

  ONTAPは、変更の有無にかかわらず、16時間に1回セキュリティ設定のGPOを取得して適用します。

  デフォルト値の16時間は、現在のONTAPバージョンでは変更できません。これはWindowsクライアントのデフォルト設定です。

- ONTAPコマンドを使用して手動ですべてのGPOを更新。

  このコマンドは、Windows の `gpupdate.exe`/force`コマンドをシミュレートします。

関連情報

SMBサーバのGPO設定を手動で更新する

ONTAP SMBサーバのGPO設定を手動で更新する

CIFSサーバのグループ ポリシー オブジェクト（GPO）設定を直ちに更新するには、設定を手動で更新します。変更された設定のみを更新することも、以前に適用されていて変更されていない設定を含めてすべての設定を強制的に更新することもできます。

手順

1. 適切な処理を実行します。

アップデートしたい場合...	コマンドを入力してください...
変更したGPO設定	`vserver cifs group-policy update -vserver` *`vserver_name`*
すべてのGPO設定	`vserver cifs group-policy update -vserver` *`vserver_name`* `-force-reapply -all-settings true`

関連情報

SMBサーバ上のGPOの更新について学ぶ

ONTAP SMB GPO 構成に関する情報を表示する

Active Directoryで定義されているグループ ポリシー オブジェクト（GPO）設定およびCIFSサーバに適用されているGPO設定に関する情報を表示できます。

タスク概要

CIFSサーバが属しているドメインのActive Directoryで定義されているすべてのGPO設定に関する情報を表示できます。また、CIFSサーバに適用されているGPO設定に関する情報のみを表示することもできます。

手順

1. 次のいずれかの操作を実行し、GPO設定に関する情報を表示します。

すべてのグループポリシー設定に関する情報を表示する場合...	コマンドを入力してください...
Active Directoryで定義されている	`vserver cifs group-policy show-defined -vserver vserver_name`
CIFS対応のStorage Virtual Machine（SVM）に適用されている	`vserver cifs group-policy show-applied -vserver vserver_name`

例

次の例は、FlexVolを備えたCIFS対応のvs1という名前のSVMが属するActive Directoryで定義されているGPO設定を表示します。

```
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
```

次の例は、CIFS対応のSVM vs1に適用されているGPO設定を表示します。

```
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
```

関連情報

サーバー上の GPO サポートを有効または無効にする

ONTAP SMB 制限グループ GPO に関する情報を表示する

Active Directoryでグループ ポリシー オブジェクト（GPO）として定義されている制限されたグループ、およびCIFSサーバに適用されている制限されたグループに関する詳細情報を表示できます。

タスク概要

デフォルトでは、次の情報が表示されます。

- グループ ポリシー名
- グループ ポリシー バージョン
- リンク

  グループ ポリシーが設定されているレベルを示します。次の値が出力されます。

  - `Local`グループ ポリシーが ONTAP で設定されている場合
  - `Site`グループ ポリシーがドメイン コントローラのサイト レベルで設定されている場合
  - `Domain`ドメイン コントローラでドメイン レベルでグループ ポリシーが設定されている場合
  - `OrganizationalUnit`グループ ポリシーがドメイン コントローラの組織単位（OU）レベルで設定されている場合
  - `RSOP`さまざまなレベルで定義されたすべてのグループ ポリシーから派生したポリシーの結果セット
- 制限されたグループ名
- 制限されたグループに属するユーザとグループ、および属さないユーザとグループ
- 制限されたグループが追加されているグループの一覧

  グループは、このリストのグループ以外のグループのメンバーになることもできます。

手順

1. 次のいずれかの操作を実行し、制限されたグループのすべてのGPOに関する情報を表示します。

すべての制限されたグループ **GPO** に関する情報を表示する場合：	コマンドを入力してください...
Active Directoryで定義されている	`vserver cifs group-policy restricted-group show-defined -vserver vserver_name`
CIFSサーバに適用されている	`vserver cifs group-policy restricted-group show-applied -vserver vserver_name`

例

次の例は、CIFS対応のvs1という名前のSVMが属するActive Directoryドメインで定義されている、制限されたグループのGPOに関する情報を表示します。

```
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
```

次の例は、CIFS対応のSVM vs1に適用されている、制限されたグループのGPOに関する情報を表示します。

```
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
```

関連情報

GPO設定に関する情報の表示

ONTAP SMB集中アクセスポリシーに関する情報を表示する

Active Directoryで定義されている集約型アクセス ポリシーに関する詳細情報を表示できます。また、グループ ポリシー オブジェクト（GPO）を介してCIFSサーバに適用されている集約型アクセス ポリシーに関する情報も表示できます。

タスク概要

デフォルトでは、次の情報が表示されます。

- SVM名
- 集約型アクセス ポリシーの名前
- SID
- 概要
- 作成日時
- 更新日時
- メンバー ルール

ワークグループ モードのCIFSサーバについては、GPOをサポートしていないため情報は表示されません。

手順

1. 次のいずれかの操作を実行し、集約型アクセス ポリシーに関する情報を表示します。

すべての集中アクセス ポリシーに関する情報を表示する場合...	コマンドを入力してください...
Active Directoryで定義されている	`vserver cifs group-policy central-access-policy show-defined -vserver` *`vserver_name`*
CIFSサーバに適用されている	`vserver cifs group-policy central-access-policy show-applied -vserver` *`vserver_name`*

例

次の例は、Active Directoryで定義されているすべての集約型アクセス ポリシーの情報を表示します。

```
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
```

次の例は、クラスタ上のStorage Virtual Machine（SVM）に適用されているすべての集約型アクセス ポリシーの情報を表示します。

```
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
```

関連情報

- サーバーのファイル アクセス セキュリティについて学ぶ
- GPO設定に関する情報の表示
- 集約型アクセス ポリシー ルールに関する情報の表示

ONTAP SMB集中アクセスポリシールールに関する情報を表示する

Active Directoryで定義されている集約型アクセス ポリシーに関連付けられた集約型アクセス ポリシー ルールに関する詳細情報を表示できます。また、集約型アクセス ポリシーのGPO（グループ ポリシー オブジェクト）を介してCIFSサーバに適用されている集約型アクセス ポリシー ルールに関する情報も表示できます。

タスク概要

定義されているか適用されている集約型アクセス ポリシー ルールに関する詳細情報を表示できます。デフォルトでは、次の情報が表示されます。

- SVM名
- 集約型アクセス ルールの名前
- 概要
- 作成日時
- 更新日時

- 現在の権限
- 推奨される権限
- ターゲット リソース

集約型アクセス ポリシーに関連付けられているすべての集約型アクセス ポリシー ルールに関する情報を表示する場合...	コマンドを入力してください...
Active Directoryで定義されている	`vserver cifs group-policy central-access-rule show-defined -vserver vserver_name`
CIFSサーバに適用されている	`vserver cifs group-policy central-access-rule show-applied -vserver vserver_name`

例

次の例は、Active Directoryで定義されている集約型アクセス ポリシーに関連付けられたすべての集約型アクセス ポリシー ルールの情報を表示します。

```
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)
```

次の例は、クラスタ上でStorage Virtual Machine（SVM）に適用されている集約型アクセス ポリシーに関連付けられたすべての集約型アクセス ポリシー ルールの情報を表示します。

```
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)
```

関連情報

- サーバーのファイル アクセス セキュリティについて学ぶ
- GPO設定に関する情報の表示
- 集約型アクセス ポリシーに関する情報の表示