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
December 20, 2024

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 . . . 1
SMBサーバへのグループポリシーオブジェクトの適用の概要 . . . 1
サポートされるGPO . . . 1
SMBサーバでGPOを使用するための要件 . . . 6
CIFSサーバ上でのGPOサポートの有効化と無効化 . . . 7
SMBサアハテノGPOノコウシンホウホウ . . . 8
CIFSサーバでのGPO設定の手動更新 . . . 9
GPO設定に関する情報を表示する . . . 9
制限されたグループのGPOに関する詳細情報を表示する . . . 14
集約型アクセスポリシーに関する情報を表示する . . . 16
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 . . . 18

SMBサーバへのグループポリシーオブジェクトの適用

SMBサーバへのグループポリシーオブジェクトの適用の概要

SMBサーバは、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は、Active Directory環境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す。GPOを使用して、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。

SMBサーバでGPOが有効になっている場合、ONTAPはActive DirectoryサーバにLDAPクエリを送信してGPO情報を要求します。SMBサーバに適用可能なGPO定義がある場合、Active Directoryサーバは次の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UUID（Universally Unique Identifier）のリスト

関連情報

ダイナミックアクセス制御（DAC）を使用したファイルアクセスの保護

"SMBおよびNFSの監査とセキュリティトレース"

サポートされるGPO

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。

- 監査ポリシーの詳細設定：

  オブジェクトへのアクセス：集約型アクセスポリシーのステージング

  次の設定を含む、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のタイプを指定します。

  - 監査しないでください
  - 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。

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

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 対応の SVM のグループポリシーの更新間隔

    GPOを使用して設定し`Registry`ます。
  - グループポリシーの更新間隔のランダムオフセット

    GPOを使用して設定し`Registry`ます。
  - BranchCache のハッシュの発行

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

    - 共有ごと
    - all-shares
    - Disabled GPOを使用して設定します `Registry`。
  - BranchCache のハッシュバージョンサポート

    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 1.7
    - BranchCache バージョン 1.7
    - BranchCacheバージョン1および2 GPOを使用して設定されます `Registry`。

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
    - ログオンイベントを監査します

      次の設定を含む監査対象のログオンイベントのタイプを指定します。

- 監査しないでください
- 成功イベントのみ監査
- 障害イベントの監査
- GPOの設定を `Local Policies/Audit Policy`使用して、設定された成功イベントと失敗イベントの両方を監査します `Audit logon events`。

> 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。

- オブジェクトへのアクセスを監査する

  次の設定を含む、監査対象のオブジェクトアクセスのタイプを指定します。

  - 監査しないでください
  - 成功イベントのみ監査
  - 障害イベントの監査
  - GPOの設定を `Local Policies/Audit Policy`使用して、設定された成功イベントと失敗イベントの両方を監査します `Audit object access`。

> 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。

- ログの保持方法

  次の設定を含む監査ログの保持方法を指定します。

  - ログファイルのサイズが最大ログサイズを超えたら、イベントログを上書きします
  - GPOの設定を `Event Log`使用して設定されたイベントログを上書きしないでください（ログを手動でクリア） `Retention method for security log`。
- 最大ログサイズ

  監査ログの最大サイズを指定します。

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

> 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を介してファイルセキュリティが適用されるファイルまたはディレクトリのリストを指定します。

GPOを使用して設定し`File System`ます。

SVM内にファイルシステムセキュリティGPOを設定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同期の最大許容値を分単位で指定します。

    GPOの設定 `Account Policies/Kerberos Policy`を使用して設定します `Maximum tolerance for computer clock synchronization`。
  - チケットの有効期間

    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。

    GPOの設定 `Account Policies/Kerberos Policy`を使用して設定します `Maximum lifetime for user ticket`。
  - チケットの更新の有効期間

    ユーザチケット更新の最大有効期間を日数で指定します。

  GPOの設定 `Account Policies/Kerberos Policy`を使用して設定します `Maximum lifetime for user ticket renewal`。
- ユーザ権限の割り当て（権限）
  - 所有権の取得

    セキュリティ保護可能なオブジェクトの所有権を取得する権限を持つユーザおよびグループのリストを指定します。

    GPOの設定 `Local Policies/User Rights Assignment`を使用して設定します `Take ownership of files or other objects`。
  - 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、個 々 のリソース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。

    GPOの設定 `Local Policies/User Rights Assignment`を使用して設定します `Manage auditing and security log`。
  - 通知権限の変更（トラバースチェックのバイパス）

    ユーザとグループにトラバースするディレクトリに対する権限がない場合でも、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。

  ユーザがファイルおよびディレクトリの変更通知を受信するには、同じ権限が必要です。GPOの設定 `Local Policies/User Rights Assignment`を使用して設定します `Bypass traverse checking`。

◦ レジストリ値

▪ 署名要求設定

SMB署名要求が有効になっているか無効になっているかを示します。

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

◦ restrict anonymous （匿名の制限

匿名ユーザに対する制限を指定します。次の3つのGPO設定が含まれます。

▪ Security Account Manager （ SAM ）アカウントを列挙しない：

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許可される追加の権限を決定します。このオプションが有効になっている場合は、ONTAPでと表示され `no-enumeration`ます。

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

▪ SAM アカウントと共有は列挙しません

このセキュリティ設定では、SAMアカウントと共有の匿名列挙を許可するかどうかを指定します。このオプションが有効になっている場合は、ONTAPでと表示され `no-enumeration`ます。

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

▪ 共有と名前付きパイプへの匿名アクセスを制限します

共有とパイプへの匿名アクセスを制限します。このオプションが有効になっている場合は、ONTAPでと表示され `no-access`ます。

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

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場合、出力フィールドには、3つのrestrict anonymous GPO設定による制限に関する情報が表示 `Resultant restriction for anonymous user`されます。考えられる制限は次のとおりです。

◦ `no-access`

匿名ユーザは、指定された共有と名前付きパイプへのアクセスを拒否され、SAMアカウントと共有を列挙できません。この制限は、GPOが有効になっている場合に発生し `Network access: Restrict anonymous access to Named Pipes and Shares`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アカウントと共有を列挙することはできません。この制限は、次の両方の条件が満たされている場合に発生します。

▪ `Network access: Restrict anonymous access to Named Pipes and Shares`GPOが無効になってい

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が有効になっている。

◦ `no-restriction`

匿名ユーザにはフルアクセスが付与され、列挙を使用できます。この制限は、次の両方の条件が満たされている場合に発生します。

- `Network access: Restrict anonymous access to Named Pipes and Shares`GPOが無効になっています。
- GPOと `Network access: Do not allow anonymous enumeration of SAM accounts and shares`GPOの両方 `Network access: Do not allow anonymous enumeration of SAM accounts`が無効になっている。
  - 制限されたグループ

    制限されたグループを設定して、組み込みグループまたはユーザ定義グループのメンバーシップを一元管理できます。グループポリシーを使用して制限されたグループを適用すると、CIFSサーバローカルグループのメンバーシップは、適用されたグループポリシーで定義されているメンバーシップリストの設定に一致するように自動的に設定されます。

GPOを使用して設定し `Restricted Groups`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指定します。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限が決定されます。

関連情報

CIFSサーバでのGPOサポートの有効化と無効化

ダイナミックアクセス制御（DAC）を使用したファイルアクセスの保護

"SMBおよびNFSの監査とセキュリティトレース"

CIFSサーバのKerberosセキュリティ設定の変更

BranchCacheを使用したブランチオフィスでのSMB共有のコンテンツのキャッシュ

SMB署名を使用したネットワークセキュリティの強化

トラバースチェックのバイパスの設定

匿名ユーザに対するアクセス制限の設定

SMBサーバでGPOを使用するための要件

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、システムがいくつかの要件を満たしている必要があります。

- クラスタでSMBのライセンスが有効になっている必要があります。SMBライセンスはに含まれて いる"ONTAP One"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。

CIFSサーバ上でのGPOサポートの有効化と無効化

CIFSサーバでGroup Policy Object（GPO；グループポリシーオブジェクト）のサポートを有効または無効にすることができます。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（OU）に適用されるポリシー）で定義されている該当するGPOがCIFSサーバに適用されます。

タスクの内容

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	入力するコマンド
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になってい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

次の例では、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

サポートされるGPO

CIFSサーバでGPOを使用するための要件

CIFSサーバでのGPOの更新方法

CIFSサーバでのGPO設定の手動更新

GPO設定に関する情報の表示

SMBサアハテノGPOノコウシンホウホウ

CIFSサアハテノGPOノコウシンノカイヨウ

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分ごとに取得して適用します。セキュリティ設定は16時間ごとに更新されます。ONTAPで自動的に更新される前にGPOを更新して新しいGPOポリシー設定を適用する場合は、ONTAPコマンドを使用してCIFSサーバで手動更新をトリガーできます。

- デフォルトでは、すべてのGPOが90分ごとに検証され、必要に応じて更新されます。

  この間隔は設定可能で、および `Random offset`GPO設定を使用して設定できます `Refresh interval`。

  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は16時間ごとに更新されます。

  ONTAPは、変更の有無にかかわらず、16時間ごとに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、すべてのGPOを手動で更新できます。

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

関連情報

CIFSサーバでのGPO設定の手動更新

CIFSサーバでのGPO設定の手動更新

CIFSサーバのGroup Policy Object（GPO；グループポリシーオブジェクト）設定をすぐに更新する場合は、設定を手動で更新できます。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。

ステップ

1. 適切な操作を実行します。

更新する項目	入力するコマンド
GPO設定が変更されました	`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

CIFSサーバでのGPOの更新方法

GPO設定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。

タスクの内容

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することも、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て、GPO設定に関する情報を表示します。

情報を表示するグループポリシー設定	入力するコマンド
Active Directoryデテイギ	`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、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

CIFSサーバでのGPOサポートの有効化と無効化

制限されたグループのGPOに関する詳細情報を表示する

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。

タスクの内容

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指定します。指定可能な出力値は次のとおりです。

  - `Local`グループポリシーがONTAPで設定されている状況
  - `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`グループポリシーがドメインコントローラのドメインレベルで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Organizational Unit（OU；組織単位）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一連のポリシー
- 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リスト

  グループは、ここにリストされているグループ以外のグループのメンバーになることができます。

ステップ

1. 次のいずれかの操作を実行して、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。

情報を表示する制限されたグループのすべての**GPO**	入力するコマンド
Active Directoryデテイギ	`vserver cifs group-policy restricted-group show-defined -vserver vserver_name`
CIFSサアハニテキヨウ	`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
```

次の例では、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

集約型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、Group Policy Object（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に関する情報も表示できます。

タスクの内容

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
- 説明
- 作成時間
- 更新日時
- メンバールール

ワークグループモードのCIFSサーバはGPOをサポートしていないため表示されません。

ステップ

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

情報を表示するすべての集約型アクセスポリシー	入力するコマンド
Active Directoryデテイギ	`vserver cifs group-policy central-access-policy show-defined -vserver` *`vserver_name`*
CIFSサアハニテキヨウ	`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

ダイナミックアクセス制御（DAC）を使用したファイルアクセスの保護

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

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

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。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。

タスクの内容

定義済みおよび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
- 説明
- 作成時間
- 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た、情報を表示するすべての集約型アクセスポリシールール	入力するコマンド
Active Directoryデテイギ	`vserver cifs group-policy central-access-rule show-defined -vserver vserver_name`
CIFSサアハニテキヨウ	`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ている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、クラスタ上の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ている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

ダイナミックアクセス制御（DAC）を使用したファイルアクセスの保護

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

著作権に関する情報

商標に関する情報