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
April 24, 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

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の説明を参照してください

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 Universally Unique Identifier （ UUID ）一覧

関連情報

DAC （ダイナミックアクセス制御）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。

- 高度な監査ポリシー設定：

  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。

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

> 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

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

    を使用して設定します `Registry` GPO：
  - 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
    - 無効 を使用して設定します `Registry` GPO：
  - 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 を使用して設定します `Registry` GPO：

> 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
    - ログオンイベントを監査します

      次の設定を含む監査対象となるログオンイベントの種類を指定します。

- 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
- 成功イベントと失敗イベントの両方を監査します を使用して設定します `Audit logon events` を設定します `Local Policies/Audit Policy` GPO：

> 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となるオブジェクトアクセスの種類を指定します。

  - 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
  - 成功イベントと失敗イベントの両方を監査します を使用して設定します `Audit object access` を設定します `Local Policies/Audit Policy` GPO：

> 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
  - イベントログを上書きしない（手動でログを消去） を使用して設定します `Retention method for security log` を設定します `Event Log` GPO：

- 最大ログサイズ

  監査ログの最大サイズを指定します。

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

> 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 を通して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。

を使用して設定します `File System` GPO：

> 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同期の最大許容誤差を分単位で指定します。

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

  - 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。

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

  - チケットの更新の有効期間

    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。

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

- ユーザ権限の割り当て（権限）
  - 所有権を取得します

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

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

  - 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。

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

  - 通知権限の変更（トラバースチェックのバイパス）

    ユーザとグループがトラバースするディレクトリに対する権限を持っていなくても、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通知を受け取るユーザにも同じ権限が必要です。を使用して設定します `Bypass traverse checking` を設定します `Local Policies/User Rights Assignment` GPO：

- 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。

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

- restrict anonymous （匿名の制限

  匿名ユーザの制限内容に次の 3 つの GPO 設定を指定します。

  - 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付与される追加の権限を決定します。このオプションはと表示されます `no-enumeration` ONTAP （有効になっている場合）。

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

  - 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、匿名による SAM アカウントと共有の列挙を許可するかどうかを決定します。このオプションはと表示されます `no-enumeration` ONTAP （有効になっている場合）。

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

  - 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。このオプションはと表示されます `no-access` ONTAP （有効になっている場合）。

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

    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は、 `Resultant restriction for anonymous user` Output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されます。表示される可能性がある制限結果は、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。この制限結果は、の場合に表示されます `Network access: Restrict anonymous access to Named Pipes and Shares` GPOが有効になっている。

- `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適用されます。

        - 。 `Network access: Restrict anonymous access to Named Pipes and Shares` GPOが無効になっています。
        - またはをクリックします `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、列挙できます。この制限は、次の両方の条件に該当する場合に適用されます。

        - 。 `Network access: Restrict anonymous access to Named Pipes and Shares` GPOが無効になっています。
        - 両方とも `Network access: Do not allow anonymous enumeration of SAM accounts` および `Network access: Do not allow anonymous enumeration of SAM accounts and shares` GPO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、組み込みまたはユーザ定義のグループのメンバーシップを一元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シップは、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。

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

- 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 サーバ上で GPO サポートを有効または無効にします

DAC （ダイナミックアクセス制御）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

匿名ユーザのアクセス制限を設定します

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、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ます。 "ONTAP One"。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 ドメインに参加している必要があります。
- SMB サーバ管理ステータスがオンになっている必要があります。
- 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 GPO のサポートを有効または無効にします

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 サーバ上で 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。

このタスクについて

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
GPOs を有効にします。	`vserver cifs group-policy modify -vserver vserver_name -status enabled`
GPOs 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 サーバ上の GPO 設定を手動で更新します

GPO 設定に関する情報を表示します

SMBサアハテノGPOノコウシンホウホウ

CIFS サーバでの GPO の更新方法の概要

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、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。

- デフォルトでは、すべての GPO を 90 分に 1 回確認し、必要に応じて更新。

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

  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、ウィンドウをシミュレートします `gpupdate.exe`/force`コマンド。

関連情報

CIFS サーバ上の GPO 設定を手動で更新します

CIFS サーバ上の GPO 設定を手動で更新します

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。

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します

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。

このタスクについて

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か、または 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ができます。

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。

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 で定義されています	`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、 vs1 という CIFS 対応の 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 サーバ上で GPO サポートを有効または無効にします

制限されたグループの GPO に関する詳細情報を表示します

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。

このタスクについて

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
- グループポリシーのバージョン
- リンク

  グループポリシーを設定するレベルを指定します。出力される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` 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一連のポリシー
- 制限されたグループ名です
- 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、ここに記載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もできます。

ステップ

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。

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 で定義されています	`vserver cifs group-policy restricted-group show-defined -vserver vserver_name`
CIFS サーバに適用されます	`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 設定に関する情報を表示します

集約型アクセスポリシーに関する情報を表示します

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。

このタスクについて

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
- 修正日時
- 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。

ステップ

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。

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 で定義されています	`vserver cifs group-policy central-access-policy show-defined -vserver` *`vserver_name`*
CIFS サーバに適用されます	`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

DAC （ダイナミックアクセス制御）を使用したファイルアクセスの保護

GPO 設定に関する情報を表示します

集約型アクセスポリシールールに関する情報を表示します

集約型アクセスポリシールールに関する情報を表示します

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。

このタスクについて

定義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 名です
- 集約型アクセスルールの名前
- 説明
- 作成時間
- 修正日時
- 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 で定義されています	`vserver cifs group-policy central-access-rule show-defined -vserver vserver_name`
CIFS サーバに適用されます	`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

DAC （ダイナミックアクセス制御）を使用したファイルアクセスの保護

GPO 設定に関する情報を表示します

集約型アクセスポリシーに関する情報を表示します