将组策略对象应用于 SMB 服务器

ONTAP 9

NetApp
April 24, 2024

目录

将组策略对象应用于 SMB 服务器

将组策略对象应用于 SMB 服务器概述

SMB服务器支持组策略对象(GPO)、这是一组称为_group policy attributes的规则、适用于Active Directory环境中的计算机。您可以使用 GPO 集中管理属于同一 Active Directory 域的集群上所有 Storage Virtual Machine （ SVM ）的设置。

如果SMB服务器上启用了GPO、则ONTAP会将LDAP查询发送到请求GPO信息的Active Directory服务器。如果存在适用于SMB服务器的GPO定义、则Active Directory服务器将返回以下GPO信息：

- GPO名称
- 当前 GPO 版本
- GPO 定义的位置
- GPO 策略集的 UUID 列表（通用唯一标识符）

相关信息

使用动态访问控制（ DAC ）保护文件访问

"SMB 和 NFS 审核和安全跟踪"

支持的 GPO

虽然并非所有组策略对象（ GPO ）都适用于启用了 CIFS 的 Storage Virtual Machine （ SVM ），但 SVM 可以识别和处理相关的 GPO 集。

SVM 当前支持以下 GPO ：

- 高级审核策略配置设置：

  对象访问：中央访问策略暂存

  指定要为中央访问策略（ CAP ）暂存审核的事件类型，包括以下设置：

  - 请勿审核
  - 仅审核成功事件
  - 仅审核失败事件
  - 审核成功和失败事件

  > 如果设置了三个审核选项中的任何一个（仅审核成功事件，仅审核失败事件，审核成功和失败事件），则 ONTAP 将同时审核成功和失败事件。

  使用设置 `Audit Central Access Policy Staging` 中的设置 `Advanced Audit Policy Configuration/Audit Policies/Object Access` GPO。

> 要使用高级审核策略配置 GPO 设置，必须在已启用 CIFS 且要应用这些设置的 SVM 上配置审核。如果未在 SVM 上配置审核，则 GPO 设置将不会应用，并将被丢弃。

- 注册表设置：
  - 已启用 CIFS 的 SVM 的组策略刷新间隔

    使用设置 `Registry` GPO。
  - 组策略刷新随机偏移

    使用设置 `Registry` GPO。
  - BranchCache 的哈希发布

    BranchCache 的哈希发布 GPO 对应于 BranchCache 操作模式。支持以下三种操作模式：
    - 每个共享
    - 所有共享
    - 已禁用 使用设置 `Registry` GPO。
  - BranchCache 的哈希版本支持

    支持以下三种哈希版本设置：
    - BranchCache 1.7 版
    - BranchCache 1.7 版
    - anchCache版本1和2 使用设置 `Registry` GPO。

> 要使用 BranchCache GPO 设置，必须在已启用 CIFS 且要应用这些设置的 SVM 上配置 BranchCache 。如果未在 SVM 上配置 BranchCache ，则 GPO 设置将不会应用，并将被丢弃。

- 安全设置
  - 审核策略和事件日志
    - 审核登录事件

      指定要审核的登录事件的类型，包括以下设置：
      - 请勿审核
      - 仅审核成功事件
      - 审核失败事件
      - 审核成功和失败事件 使用设置 `Audit logon events` 中的设置 `Local Policies/Audit Policy` GPO。

> 如果设置了三个审核选项中的任何一个（仅审核成功事件，仅审核失败事件，审核成功和失败事件），则 ONTAP 将同时审核成功和失败事件。

- 审核对象访问

  指定要审核的对象访问类型，包括以下设置：

  - 请勿审核
  - 仅审核成功事件
  - 审核失败事件
  - 审核成功和失败事件 使用设置 `Audit object access` 中的设置 `Local Policies/Audit Policy` GPO。

  > 如果设置了三个审核选项中的任何一个（仅审核成功事件，仅审核失败事件，审核成功和失败事件），则 ONTAP 将同时审核成功和失败事件。

- 日志保留方法

  指定审核日志保留方法，包括以下设置：

  - 如果日志文件大小超过最大日志大小，则覆盖事件日志
  - 不要覆盖事件日志(手动清除日志) 使用设置 `Retention method for security log` 中的设置 `Event Log` GPO。

- 最大日志大小

  指定审核日志的最大大小。

  使用设置 `Maximum security log size` 中的设置 `Event Log` GPO。

> 要使用审核策略和事件日志 GPO 设置，必须在已启用 CIFS 且要应用这些设置的 SVM 上配置审核。如果未在 SVM 上配置审核，则 GPO 设置将不会应用，并将被丢弃。

◦ 文件系统安全性

指定通过 GPO 应用文件安全性的文件或目录列表。

使用设置 `File System` GPO。

> 配置文件系统安全 GPO 的卷路径必须位于 SVM 中。

◦ Kerberos 策略

- 最大时钟偏差

  指定计算机时钟同步的最大容错（以分钟为单位）。

  使用设置 `Maximum tolerance for computer clock synchronization` 中的设置 `Account Policies/Kerberos Policy` GPO。

- 最长票证期限

  指定用户服务单的最长生命周期（以小时为单位）。

  使用设置 `Maximum lifetime for user ticket` 中的设置 `Account Policies/Kerberos Policy` GPO。

- 最长票证续订期限

  指定用户票证续订的最长生命周期（以天为单位）。

使用设置 `Maximum lifetime for user ticket renewal` 中的设置 `Account Policies/Kerberos Policy` GPO。

- 用户权限分配（权限）

  - 取得所有权

    指定有权取得任何安全对象所有权的用户和组的列表。

    使用设置 `Take ownership of files or other objects` 中的设置 `Local Policies/User Rights Assignment` GPO。

  - 安全权限

    指定可以为文件，文件夹和 Active Directory 对象等单个资源的对象访问指定审核选项的用户和组列表。

    使用设置 `Manage auditing and security log` 中的设置 `Local Policies/User Rights Assignment` GPO。

  - 更改通知权限（绕过遍历检查）

    指定可以遍历目录树的用户和组列表，即使用户和组可能对遍历的目录没有权限也是如此。

用户接收文件和目录更改通知需要相同的权限。使用设置 `Bypass traverse checking` 中的设置 `Local Policies/User Rights Assignment` GPO。

- 注册表值

  - 需要签名设置

    指定是启用还是禁用所需的 SMB 签名。

使用设置 `Microsoft network server: Digitally sign communications (always)` 中的设置 `Security Options` GPO。

- 限制匿名

指定匿名用户的限制并包括以下三个 GPO 设置：

  - 不枚举安全帐户管理器（ SAM ）帐户：

此安全设置可确定为匿名连接到计算机授予哪些其他权限。此选项显示为 `no-enumeration` 在ONTAP中(如果已启用)。

使用设置 `Network access: Do not allow anonymous enumeration of SAM accounts` 中的设置 `Local Policies/Security Options` GPO。

- 不枚举 SAM 帐户和共享

  此安全设置确定是否允许匿名枚举 SAM 帐户和共享。此选项显示为 `no-enumeration` 在ONTAP中(如果已启用)。

  使用设置 `Network access: Do not allow anonymous enumeration of SAM accounts and shares` 中的设置 `Local Policies/Security Options` GPO。

- 限制对共享和命名管道的匿名访问

  此安全设置限制对共享和管道的匿名访问。此选项显示为 `no-access` 在ONTAP中(如果已启用)。

  使用设置 `Network access: Restrict anonymous access to Named Pipes and Shares` 中的设置 `Local Policies/Security Options` GPO。

  显示有关已定义和已应用组策略的信息时、 `Resultant restriction for anonymous user` 输出字段提供有关三个限制匿名GPO设置所产生限制的信息。可能产生的限制如下：

- `no-access`

  匿名用户被拒绝访问指定的共享和命名管道，并且不能使用 SAM 帐户和共享枚举。如果存在、则会显示此结果限制 `Network access: Restrict anonymous access to Named Pipes and Shares` 已启用GPO。

- `no-enumeration`

  匿名用户有权访问指定的共享和命名管道，但不能使用 SAM 帐户和共享枚举。如果同时满足以下两个条件，则会显示由此产生的限制：

  - 。 `Network access: Restrict anonymous access to Named Pipes and Shares` 已禁用GPO。
  - 或 `Network access: Do not allow anonymous enumeration of SAM accounts` 或 `Network access: Do not allow anonymous enumeration of SAM accounts and shares` GPO已启用。

- `no-restriction`

  匿名用户具有完全访问权限，可以使用枚举。如果同时满足以下两个条件，则会显示由此产生的限制：

  - 。 `Network access: Restrict anonymous access to Named Pipes and Shares` 已禁用GPO。
  - 这两个 `Network access: Do not allow anonymous enumeration of SAM accounts` 和 `Network access: Do not allow anonymous enumeration of SAM accounts and shares` 已禁用GPO。

    - 受限组

您可以配置受限组以集中管理内置或用户定义的组的成员资格。通过组策略应用受限组时，CIFS 服务器本地组的成员资格会自动设置为与应用的组策略中定义的成员资格列表设置匹配。

使用设置 `Restricted Groups` GPO。

- 中央访问策略设置

  指定中央访问策略的列表。中央访问策略和关联的中央访问策略规则可确定 SVM 上多个文件的访问权限。

相关信息

在 CIFS 服务器上启用或禁用 GPO 支持

使用动态访问控制（DAC）保护文件访问

"SMB 和 NFS 审核和安全跟踪"

修改 CIFS 服务器 Kerberos 安全设置

使用 BranchCache 在分支机构缓存 SMB 共享内容

使用 SMB 签名增强网络安全性

配置绕过遍历检查

配置匿名用户的访问限制

对 SMB 服务器使用 GPO 的要求

要对 SMB 服务器使用组策略对象（GPO），您的系统必须满足多项要求。

- SMB 必须在集群上获得许可。SMB许可证包含在中 "ONTAP One"。如果您没有ONTAP One、并且未安装许可证、请联系您的销售代表。
- 必须配置 SMB 服务器并将其加入 Windows Active Directory 域。
- SMB 服务器管理员状态必须为 on 。
- 必须配置 GPO 并将其应用于包含 SMB 服务器计算机对象的 Windows Active Directory 组织单位（OU）。
- 必须在 SMB 服务器上启用 GPO 支持。

在 CIFS 服务器上启用或禁用 GPO 支持

您可以在 CIFS 服务器上启用或禁用组策略对象（GPO）支持。如果在 CIFS 服务器上启用 GPO 支持，则在组策略（即应用于包含 CIFS 服务器计算机对象的组织单位（OU）的策略）上定义的适用 GPO 将应用于 CIFS 服务器。

关于此任务

无法在工作组模式下在 CIFS 服务器上启用 GPO 。

步骤

1. 执行以下操作之一：

如果您要 ...	输入命令 ...
启用 GPOs：	`vserver cifs group-policy modify -vserver vserver_name -status enabled`
禁用 GPOs	`vserver cifs group-policy modify -vserver vserver_name -status disabled`

2. 验证GPO支持是否处于所需状态： `vserver cifs group-policy show -vserver +vserver_name_`

   在工作组模式` 下， CIFS 服务器的组策略状态显示为 " 已 `d" 。

示例

以下示例将在 Storage Virtual Machine （ SVM ） vs1 上启用 GPO 支持：

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

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

            Vserver: vs1
Group Policy Status: enabled
```

相关信息

支持的 GPO

在CIFS服务器中使用GPO的要求

如何在 CIFS 服务器上更新 GPO

手动更新 CIFS 服务器上的 GPO 设置

显示有关 GPO 配置的信息

如何在SMB服务器上更新GPO

如何在 CIFS 服务器概述中更新 GPO

默认情况下， ONTAP 每 90 分钟检索并应用组策略对象（ GPO ）更改一次。安全设置每 16 小时刷新一次。如果要在 ONTAP 自动更新 GPO 之前更新 GPO 以应用新的 GPO 策略设置，则可以使用 ONTAP 命令在 CIFS 服务器上触发手动更新。

- 默认情况下，所有 GPO 都会根据需要每 90 分钟进行一次验证和更新。

  此间隔可配置、并可使用进行设置 `Refresh interval` 和 `Random offset` GPO设置。

  ONTAP 会查询 Active Directory 以了解对 GPO 的更改。如果 Active Directory 中记录的 GPO 版本号高于 CIFS 服务器上的版本号，则 ONTAP 将检索并应用新的 GPO 。如果版本号相同，则不会更新 CIFS 服务器上的 GPO 。

- 安全设置 GPO 每 16 小时刷新一次。

  ONTAP 每 16 小时检索并应用一次安全设置 GPO ，无论这些 GPO 是否已更改。

  > 在当前 ONTAP 版本中，不能更改 16 小时的默认值。这是 Windows 客户端的默认设置。

- 可以使用 ONTAP 命令手动更新所有 GPO 。

  此命令模拟Windows `gpupdate.exe`/force`命令。

相关信息

手动更新 CIFS 服务器上的 GPO 设置

手动更新 CIFS 服务器上的 GPO 设置

如果要立即更新 CIFS 服务器上的组策略对象（GPO）设置，可以手动更新这些设置。您只能更新已更改的设置，也可以强制更新所有设置，包括先前应用但尚未更改的设置。

步骤

1. 执行相应的操作：

要更新的内容	输入命令 ...
已更改 GPO 设置	`vserver cifs group-policy update -vserver` *`vserver_name`*
所有 GPO 设置	`vserver cifs group-policy update -vserver` *`vserver_name`* `-force-reapply -all-settings true`

相关信息

如何在 CIFS 服务器上更新 GPO

显示有关 GPO 配置的信息

您可以显示有关 Active Directory 中定义的组策略对象（GPO）配置以及应用于 CIFS 服务器的 GPO 配置的信息。

关于此任务

您可以显示 CIFS 服务器所属域的 Active Directory 中定义的所有 GPO 配置的信息，也可以仅显示应用于 CIFS 服务器的 GPO 配置的信息。

步骤

1. 通过执行以下操作之一显示有关 GPO 配置的信息：

要显示有关所有组策略配置的信息 ...	输入命令 ...
在 Active Directory 中定义	`vserver cifs group-policy show-defined -vserver vserver_name`
应用于启用了 CIFS 的 Storage Virtual Machine （SVM）	`vserver cifs group-policy show-applied -vserver vserver_name`

示例

以下示例显示了在启用了 CIFS 且名为 vs1 的 SVM 所属的 Active Directory 中定义的 GPO 配置：

```
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
```

以下示例显示了应用于启用了 CIFS 的 SVM vs1 的 GPO 配置：

```
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
```

相关信息

在 CIFS 服务器上启用或禁用 GPO 支持

显示有关受限组 GPO 的详细信息

您可以显示有关在 Active Directory 中定义为组策略对象（GPO）并应用于 CIFS 服务器的受限组的详细信息。

关于此任务

默认情况下，将显示以下信息：

- 组策略名称
- 组策略版本
- 链接。

  指定配置组策略的级别。可能的输出值包括：

  - `Local` 在ONTAP中配置组策略时
  - `Site` 在域控制器中的站点级别配置组策略时
  - `Domain` 在域控制器的域级别配置组策略时
  - `OrganizationalUnit` 在域控制器的组织单位(OU)级别配置组策略时
  - `RSOP` 根据在不同级别定义的所有组策略生成的一组策略
- 受限组名称
- 属于和不属于受限制组的用户和组
- 添加受限制组的组的列表

  组可以是此处列出的组以外的组的成员。

步骤

1. 通过执行以下操作之一显示有关所有受限组 GPO 的信息：

要显示有关所有受限组 **GPO** 的信息 ...	输入命令 ...
在 Active Directory 中定义	`vserver cifs group-policy restricted-group show-defined -vserver vserver_name`
应用于 CIFS 服务器	`vserver cifs group-policy restricted-group show-applied -vserver vserver_name`

示例

以下示例显示了有关在启用了 CIFS 且名为 vs1 的 SVM 所属的 Active Directory 域中定义的受限组 GPO 的信息：

```
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
```

以下示例显示了应用于启用了 CIFS 的 SVM vs1 的受限组 GPO 的信息：

```
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
```

相关信息

显示有关 GPO 配置的信息

显示有关中央访问策略的信息

您可以显示有关 Active Directory 中定义的中央访问策略的详细信息。您还可以显示有关通过组策略对象（GPO）应用于 CIFS 服务器的中央访问策略的信息。

关于此任务

默认情况下，将显示以下信息：

- SVM name
- 中央访问策略的名称
- SID
- Description
- 创建时间
- 修改时间
- 成员规则

> 工作组模式下的 CIFS 服务器不会显示，因为它们不支持 GPO 。

步骤

1. 通过执行以下操作之一显示有关中央访问策略的信息：

要显示有关所有中央访问策略的信息 ...	输入命令 ...
在 Active Directory 中定义	`vserver cifs group-policy central-access-policy show-defined -vserver` *`vserver_name`*
应用于 CIFS 服务器	`vserver cifs group-policy central-access-policy show-applied -vserver` *`vserver_name`*

示例

以下示例显示了 Active Directory 中定义的所有中央访问策略的信息：

```
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
```

以下示例显示了应用于集群上的 Storage Virtual Machine （SVM）的所有中央访问策略的信息：

```
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
```

相关信息

使用动态访问控制（DAC）保护文件访问

显示有关 GPO 配置的信息

显示有关中央访问策略规则的信息

显示有关中央访问策略规则的信息

您可以显示与 Active Directory 中定义的中央访问策略关联的中央访问策略规则的详细信息。您还可以显示有关通过中央访问策略 GPO （组策略对象）应用于 CIFS 服务器的中央访问策略规则的信息。

关于此任务

您可以显示有关已定义和应用的中央访问策略规则的详细信息。默认情况下，将显示以下信息：

- Vserver name
- 中央访问规则的名称
- Description
- 创建时间
- 修改时间
- 当前权限
- 建议的权限

- 目标资源

要显示与中央访问策略关联的所有中央访问策略规则的信息 ...	输入命令 ...
在 Active Directory 中定义	`vserver cifs group-policy central-access-rule show-defined -vserver vserver_name`
应用于 CIFS 服务器	`vserver cifs group-policy central-access-rule show-applied -vserver vserver_name`

示例

以下示例显示了与 Active Directory 中定义的中央访问策略关联的所有中央访问策略规则的信息：

```
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)
```

以下示例显示了与应用于集群上 Storage Virtual Machine （ SVM ）的中央访问策略关联的所有中央访问策略规则的信息：

```
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)
```

相关信息

使用动态访问控制（DAC）保护文件访问

显示有关 GPO 配置的信息

显示有关中央访问策略的信息