Aplicar objetos de directiva de grupo a servidores SMB

ONTAP 9

NetApp
February 20, 2026

Tabla de contenidos

Aplicar objetos de directiva de grupo a servidores SMB

Obtenga información sobre la aplicación de objetos de directiva de grupo a servidores SMB de ONTAP

El servidor SMB admite objetos de directiva de grupo (GPO), un conjunto de reglas conocidas como atributos de directiva de grupo_ que se aplican a equipos de un entorno de Active Directory. Puede utilizar los GPO para gestionar de forma centralizada la configuración de todas las máquinas virtuales de almacenamiento (SVM) del clúster que pertenece al mismo dominio de Active Directory.

Cuando se habilitan los GPO en el servidor SMB, ONTAP envía consultas LDAP al servidor de Active Directory que solicita información de GPO. Si hay definiciones de GPO aplicables al servidor SMB, el servidor Active Directory devuelve la siguiente información de GPO:

- Nombre de GPO
- Versión de GPO actual
- Ubicación de la definición de GPO
- Listas de UUID (identificadores universales únicos) para conjuntos de directivas de GPO

Información relacionada

- Obtenga más información sobre la seguridad del acceso a archivos para servidores
- "Seguimiento de seguridad y auditoría de SMB y NFS"

Obtenga más información sobre los GPO para SMB de ONTAP compatibles

Aunque no todos los objetos de políticas de grupo (GPO) se aplican a las máquinas virtuales de almacenamiento (SVM) habilitadas para CIFS, las SVM pueden reconocer y procesar el conjunto de objetos de normativa de grupo correspondiente.

Actualmente, los siguientes GPO son compatibles con las SVM:

- Ajustes de configuración de directivas de auditoría avanzadas:

  Acceso a objetos: Escalonamiento de la directiva de acceso central

  Especifica el tipo de eventos que se auditarán para la configuración provisional de la directiva de acceso central (CAP), incluida la siguiente configuración:

  - No auditar
  - Auditar solo los eventos de éxito
  - Auditar solo los eventos de fallo
  - Auditar eventos de éxito y fallo

Si se establece cualquiera de las tres opciones de auditoría (sólo eventos de éxito de auditoría, auditar sólo eventos de fallo, auditar eventos de éxito y de fallo), ONTAP audita tanto eventos de éxito como de fallo.

Se establece mediante la `Audit Central Access Policy Staging` configuración de `Advanced Audit Policy Configuration/Audit Policies/Object Access` GPO.

Para utilizar las opciones de GPO de configuración de directivas de auditoría avanzadas, la auditoría debe configurarse en la SVM habilitada para CIFS a la que desee aplicar estas opciones. Si la auditoría no está configurada en la SVM, la configuración de GPO no se aplicará y se descarta.

- Configuración del registro:
  - Intervalo de actualización de la directiva de grupo para la SVM habilitada para CIFS

    Se establece mediante el `Registry` GPO.
  - Actualización aleatoria de directivas de grupo

    Se establece mediante el `Registry` GPO.
  - Publicación de hash para BranchCache

    El GPO Hash Publication para BranchCache corresponde al modo operativo de BranchCache. Se admiten los tres modos de funcionamiento compatibles siguientes:

    - Por recurso compartido
    - Todos los recursos compartidos
    - Se desactiva mediante `Registry` GPO.
  - Compatibilidad de la versión de hash para BranchCache

    Se admiten las tres configuraciones de la siguiente versión de hash:

    - BranchCache versión 1
    - BranchCache versión 2
    - Las versiones 1 y 2 de BranchCache se establecen mediante `Registry` GPO.

Para usar la configuración de GPO de BranchCache, BranchCache debe configurarse en la SVM habilitada para CIFS a la que desea aplicar esta configuración. Si no se configura BranchCache en la SVM, no se aplicará la configuración de GPO y se descarta.

- Configuración de seguridad
  - Política de auditoría y registro de eventos
    - Auditar eventos de inicio de sesión

      Especifica el tipo de eventos de inicio de sesión que se van a auditar, incluida la siguiente configuración:

- No auditar
- Auditar solo los eventos de éxito
- Auditoría de eventos de fallo
- Audite los eventos de éxito y fallo definidos mediante la `Audit logon events` configuración del `Local Policies/Audit Policy` GPO.

> Si se establece cualquiera de las tres opciones de auditoría (sólo eventos de éxito de auditoría, auditar sólo eventos de fallo, auditar eventos de éxito y de fallo), ONTAP audita tanto eventos de éxito como de fallo.

- Auditar el acceso a objetos

  Especifica el tipo de acceso al objeto que se va a auditar, incluida la siguiente configuración:

  - No auditar
  - Auditar solo los eventos de éxito
  - Auditoría de eventos de fallo
  - Audite los eventos de éxito y fallo definidos mediante la `Audit object access` configuración del `Local Policies/Audit Policy` GPO.

> Si se establece cualquiera de las tres opciones de auditoría (sólo eventos de éxito de auditoría, auditar sólo eventos de fallo, auditar eventos de éxito y de fallo), ONTAP audita tanto eventos de éxito como de fallo.

- Método de retención de registros

  Especifica el método de retención del registro de auditoría, incluida la siguiente configuración:

  - Sobrescribir el registro de eventos cuando el tamaño del archivo de registro supere el tamaño máximo del registro
  - No sobrescriba el registro de eventos (borrar registro manualmente) establecido mediante la `Retention method for security log` configuración del `Event Log` GPO.

- Tamaño máximo del registro

  Especifica el tamaño máximo del registro de auditoría.

  Se establece mediante la `Maximum security log size` configuración de `Event Log` GPO.

> Para utilizar la configuración de directiva de auditoría y GPO de registro de eventos, la auditoría debe configurarse en la SVM habilitada para CIFS a la que desea aplicar esta configuración. Si la auditoría no está configurada en la SVM, la configuración de GPO no se aplicará y se descarta.

◦ Seguridad del sistema de archivos

Especifica una lista de archivos o directorios en los que se aplica la seguridad de archivos a través de un GPO.

Se establece mediante el `File System` GPO.

Debe existir la ruta de acceso del volumen donde se configura el GPO de seguridad del sistema de archivos en la SVM.

- Política de Kerberos
  - Desviación máxima del reloj

    Especifica la tolerancia máxima en minutos para la sincronización del reloj del equipo.

    Se establece mediante la `Maximum tolerance for computer clock synchronization` configuración de `Account Policies/Kerberos Policy` GPO.

  - Antigüedad máxima del billete

    Especifica la duración máxima en horas para el ticket de usuario.

    Se establece mediante la `Maximum lifetime for user ticket` configuración de `Account Policies/Kerberos Policy` GPO.

  - Antigüedad máxima de renovación del boleto

    Especifica la duración máxima en días para la renovación de la tarjeta de usuario.

  Se establece mediante la `Maximum lifetime for user ticket renewal` configuración de `Account Policies/Kerberos Policy` GPO.

- Asignación de derechos de usuario (derechos de privilegio)
  - Asuma la propiedad

    Especifica la lista de usuarios y grupos que tienen derecho a asumir la propiedad de cualquier objeto asegurable.

    Se establece mediante la `Take ownership of files or other objects` configuración de `Local Policies/User Rights Assignment` GPO.

  - Privilegio de seguridad

    Especifica la lista de usuarios y grupos que pueden especificar opciones de auditoría para el acceso a objetos de recursos individuales, como archivos, carpetas y objetos de Active Directory.

    Se establece mediante la `Manage auditing and security log` configuración de `Local Policies/User Rights Assignment` GPO.

  - Cambiar privilegio de notificación (comprobación de recorrido de derivación)

    Especifica la lista de usuarios y grupos que pueden recorrer los árboles de directorios aunque los usuarios y los grupos puedan no tener permisos en el directorio de recorrido.

  El mismo privilegio es necesario para que los usuarios reciban notificaciones de cambios en archivos y directorios. Se establece mediante la `Bypass traverse checking` configuración de `Local Policies/User Rights Assignment` GPO.

- Valores del Registro

- Firma Configuración requerida

  Especifica si la firma SMB necesaria está habilitada o deshabilitada.

Se establece mediante la `Microsoft network server: Digitally sign communications (always)` configuración de `Security Options` GPO.

- Restringir anónimo

Especifica cuáles son las restricciones para los usuarios anónimos e incluye las tres configuraciones de GPO siguientes:

- No hay enumeración de cuentas del Administrador de cuentas de seguridad (SAM):

  Esta configuración de seguridad determina qué permisos adicionales se conceden para las conexiones anónimas al equipo. Esta opción se muestra como `no-enumeration` en ONTAP si está habilitada.

  Se establece mediante la `Network access: Do not allow anonymous enumeration of SAM accounts` configuración de `Local Policies/Security Options` GPO.

- No hay enumeración de cuentas y recursos compartidos de SAM

  Esta configuración de seguridad determina si se permite la enumeración anónima de cuentas SAM y recursos compartidos. Esta opción se muestra como `no-enumeration` en ONTAP si está habilitada.

  Se establece mediante la `Network access: Do not allow anonymous enumeration of SAM accounts and shares` configuración de `Local Policies/Security Options` GPO.

- Restringir el acceso anónimo a recursos compartidos y canalizaciones con nombre

  Esta configuración de seguridad restringe el acceso anónimo a recursos compartidos y tuberías. Esta opción se muestra como `no-access` en ONTAP si está habilitada.

  Se establece mediante la `Network access: Restrict anonymous access to Named Pipes and Shares` configuración de `Local Policies/Security Options` GPO.

  Cuando se muestra información sobre las políticas de grupo definidas y aplicadas, el `Resultant restriction for anonymous user` campo de salida proporciona información sobre la restricción resultante de los tres valores de GPO anónimos de restricción. Las posibles restricciones resultantes son las siguientes:

° `no-access`

Al usuario anónimo se le deniega el acceso a los recursos compartidos especificados y a las canalizaciones con nombre, y no se puede utilizar la enumeración de cuentas y recursos compartidos SAM. Esta restricción resultante se ve si el `Network access: Restrict anonymous access to Named Pipes and Shares` GPO está habilitado.

° `no-enumeration`

El usuario anónimo tiene acceso a los recursos compartidos y canalizaciones con nombre especificados, pero no puede utilizar la enumeración de cuentas y recursos compartidos SAM. Esta

restricción resultante se observa si se cumplen las dos condiciones siguientes:

- El `Network access: Restrict anonymous access to Named Pipes and Shares` GPO está desactivado.
- `Network access: Do not allow anonymous enumeration of SAM accounts`O los `Network access: Do not allow anonymous enumeration of SAM accounts and shares` objetos de normativa de grupo están activados.

° `no-restriction`

El usuario anónimo tiene acceso completo y puede utilizar la enumeración. Esta restricción resultante se observa si se cumplen las dos condiciones siguientes:

- El `Network access: Restrict anonymous access to Named Pipes and Shares` GPO está desactivado.
- Los `Network access: Do not allow anonymous enumeration of SAM accounts` `Network access: Do not allow anonymous enumeration of SAM accounts and shares` GPO y están desactivados.
  - Grupos restringidos

    Puede configurar grupos restringidos para administrar de forma centralizada la pertenencia a grupos integrados o definidos por el usuario. Cuando aplica un grupo restringido a través de una directiva de grupo, la pertenencia a un grupo local de servidor CIFS se establece automáticamente para que coincida con la configuración de la lista de miembros definida en la directiva de grupo aplicada.

Se establece mediante el `Restricted Groups` GPO.

- Configuración de la directiva de acceso central

  Especifica una lista de directivas de acceso central. Las políticas de acceso central y las reglas de política de acceso central asociadas determinan los permisos de acceso para varios archivos en la SVM.

Información relacionada

- Habilitar o deshabilitar la compatibilidad con GPO en los servidores
- Obtenga más información sobre la seguridad del acceso a archivos para servidores
- "Seguimiento de seguridad y auditoría de SMB y NFS"
- Modificar la configuración de seguridad del servidor
- Obtenga información sobre cómo usar BranchCache para almacenar en caché contenido compartido en una sucursal
- Aprenda a utilizar la firma ONTAP para mejorar la seguridad de la red
- Obtenga información sobre cómo configurar la comprobación de recorrido de derivación
- Configurar restricciones de acceso para usuarios anónimos

Requisitos del servidor SMB de ONTAP para GPO

Para utilizar objetos de directiva de grupo (GPO) con el servidor SMB, el sistema debe cumplir varios requisitos.

- Las licencias de SMB deben estar en el clúster. La licencia SMB se incluye con "ONTAP One". Si no tiene ONTAP One y la licencia no está instalada, póngase en contacto con su representante de ventas.
- Debe haber un servidor SMB configurado y Unido a un dominio de Windows Active Directory.
- El estado del administrador del servidor SMB debe ser on.
- Los GPO deben configurarse y aplicarse a la unidad organizativa (OU) de Active Directory de Windows que contiene el objeto de equipo servidor SMB.
- La compatibilidad con GPO debe estar habilitada en el servidor SMB.

Habilitar o deshabilitar la compatibilidad de GPO en los servidores SMB de ONTAP

Puede habilitar o deshabilitar la compatibilidad con objetos de directiva de grupo (GPO) en un servidor CIFS. Si habilita la compatibilidad de GPO en un servidor CIFS, los GPO aplicables definidos en la directiva de grupo (la directiva que se aplica a la unidad organizativa (OU) que contiene el objeto de equipo del servidor CIFS) se aplican al servidor CIFS.

Acerca de esta tarea

Los GPO no pueden habilitarse en servidores CIFS en modo de grupo de trabajo.

Pasos

1. Ejecute una de las siguientes acciones:

Si desea…	Introduzca el comando…
Habilite los GPO	`vserver cifs group-policy modify -vserver` *`vserver_name`* `-status enabled`
Deshabilitar GPO	`vserver cifs group-policy modify -vserver` *`vserver_name`* `-status disabled`

2. Compruebe que el soporte de GPO está en el estado deseado: `vserver cifs group-policy show -vserver +vserver_name_`

   El estado de la directiva de grupo de los servidores CIFS en el modo de grupo se muestra como "desactivado".

Ejemplo

En el siguiente ejemplo, se habilita la compatibilidad de GPO en máquinas virtuales de almacenamiento (SVM) 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
```

Información relacionada

Obtenga más información sobre los GPO compatibles

Requisitos del servidor para GPO

Obtenga información sobre cómo actualizar GPO en servidores SMB

Actualizar manualmente la configuración de GPO en servidores SMB

Mostrar información acerca de las configuraciones de GPO

Cómo se actualizan los GPO en el servidor SMB

Obtenga información sobre la actualización de GPO en servidores SMB de ONTAP

De forma predeterminada, ONTAP recupera y aplica los cambios de objeto de directiva de grupo (GPO) cada 90 minutos. La configuración de seguridad se actualiza cada 16 horas. Si desea actualizar GPO para aplicar nuevas configuraciones de directivas de GPO antes de que ONTAP las actualice automáticamente, puede activar una actualización manual en un servidor CIFS con un comando ONTAP.

- De forma predeterminada, todos los GPO se verifican y actualizan según sea necesario cada 90 minutos.

  Este intervalo se puede configurar y se puede ajustar mediante `Refresh interval` `Random offset` los ajustes de y GPO.

  ONTAP consulta a Active Directory los cambios realizados en los GPO. Si los números de versión de GPO registrados en Active Directory son superiores a los del servidor CIFS, ONTAP recupera y aplica los nuevos GPO. Si los números de versión son los mismos, los GPO en el servidor CIFS no se actualizan.

- Configuración de seguridad los GPO se actualizan cada 16 horas.

  ONTAP recupera y aplica los GPO de configuración de seguridad cada 16 horas, independientemente de que estos GPO hayan cambiado o no.

  > El valor predeterminado de 16 horas no se puede cambiar en la versión actual de ONTAP. Es una configuración predeterminada del cliente Windows.

- Todos los GPO se pueden actualizar manualmente con un comando ONTAP.

  Este comando simula el `gpupdate.exe` comando Windows/force`.

Información relacionada

Actualizar manualmente la configuración de GPO en servidores SMB

Actualice manualmente la configuración de GPO en los servidores SMB de ONTAP

Si desea actualizar inmediatamente la configuración del objeto de directiva de grupo (GPO) en el servidor CIFS, puede actualizar manualmente la configuración. Sólo puede actualizar los ajustes modificados o puede forzar una actualización para todos los ajustes, incluidos los que se aplicaron anteriormente pero no se han modificado.

Paso

1. Ejecute la acción adecuada:

Si desea actualizar…	Introduzca el comando…
Ha cambiado la configuración de GPO	`vserver cifs group-policy update -vserver vserver_name`
Todas las configuraciones de GPO	`vserver cifs group-policy update -vserver vserver_name -force-reapply -all-settings true`

Información relacionada

Obtenga información sobre cómo actualizar GPO en servidores SMB

Mostrar información sobre las configuraciones de GPO SMB de ONTAP

Puede mostrar información acerca de las configuraciones de objeto de directiva de grupo (GPO) definidas en Active Directory y acerca de las configuraciones de GPO aplicadas al servidor CIFS.

Acerca de esta tarea

Puede mostrar información acerca de todas las configuraciones de GPO definidas en Active Directory del dominio al que pertenece el servidor CIFS o solo puede mostrar información acerca de las configuraciones de GPO aplicadas a un servidor CIFS.

Pasos

1. Mostrar información acerca de las configuraciones de GPO realizando una de las siguientes acciones:

Si desea mostrar información acerca de todas las configuraciones de directiva de grupo…	Introduzca el comando…
Definido en Active Directory	`vserver cifs group-policy show-defined -vserver vserver_name`

Si desea mostrar información acerca de todas las configuraciones de directiva de grupo…	Introduzca el comando…
Aplicado a una máquina virtual de almacenamiento (SVM) habilitada para CIFS	`vserver cifs group-policy show-applied -vserver vserver_name`

Ejemplo

En el siguiente ejemplo, se muestran las configuraciones de GPO definidas en Active Directory al que pertenece la SVM habilitada para CIFS con el nombre vs1:

```
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
```

En el siguiente ejemplo, se muestran las configuraciones de GPO aplicadas a la SVM vs1 habilitada para 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
```

Información relacionada

Habilitar o deshabilitar la compatibilidad con GPO en los servidores

Mostrar información sobre los GPO de grupo restringido SMB de ONTAP

Puede mostrar información detallada sobre los grupos restringidos que se definen como objetos de directiva de grupo (GPO) en Active Directory y que se aplican al servidor CIFS.

Acerca de esta tarea

De forma predeterminada, se muestra la siguiente información:

- Nombre de la política de grupo
- Versión de la directiva de grupo
- Enlace

  Especifica el nivel en el que se configura la directiva de grupo. Los valores de salida posibles incluyen los siguientes:

  - `Local` Cuando la política de grupo está configurada en ONTAP
  - `Site` cuando la política de grupo se configura en el nivel de sitio en el controlador de dominio
  - `Domain` cuando la política de grupo se configura en el nivel de dominio en el controlador de dominio
  - `OrganizationalUnit` Cuando la directiva de grupo se configura en el nivel de unidad organizativa (OU) en el controlador de dominio
  - `RSOP` para el conjunto resultante de políticas derivadas de todas las políticas de grupo definidas en varios niveles
- Nombre de grupo restringido
- Los usuarios y grupos que pertenecen al grupo restringido y que no pertenecen al mismo
- Lista de grupos a los que se agrega el grupo restringido

  Un grupo puede ser miembro de grupos distintos de los que se enumeran aquí.

Paso

1. Muestre información acerca de todos los GPO de grupo restringidos realizando una de las siguientes acciones:

Si desea mostrar información sobre todos los GPO de grupo restringidos…	Introduzca el comando…
Definido en Active Directory	`vserver cifs group-policy restricted-group show-defined -vserver vserver_name`
Aplicado a un servidor CIFS	`vserver cifs group-policy restricted-group show-applied -vserver vserver_name`

Ejemplo

En el siguiente ejemplo, se muestra información sobre los objetos de normativa de grupo restringidos definidos en el dominio de Active Directory al que pertenece la SVM habilitada para CIFS, llamada 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
```

En el siguiente ejemplo, se muestra información sobre los objetos de normativa de grupo restringidos aplicados a la SVM vs1 habilitada para 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
```

Información relacionada

Mostrar información acerca de las configuraciones de GPO

Muestra información sobre las políticas de acceso central de SMB de ONTAP

Puede mostrar información detallada acerca de las directivas de acceso central definidas en Active Directory. También puede mostrar información sobre las políticas de acceso central que se aplican al servidor CIFS a través de objetos de política de grupo (GPO).

Acerca de esta tarea

De forma predeterminada, se muestra la siguiente información:

- Nombre de SVM
- Nombre de la política de acceso central
- SID
- Descripción
- Hora de creación
- Tiempo de modificación
- Normas de los miembros

Los servidores CIFS en el modo de grupo de trabajo no se muestran porque no admiten los GPO.

Paso

1. Muestre información acerca de las directivas de acceso central realizando una de las siguientes acciones:

Si desea mostrar información sobre todas las directivas de acceso central…	Introduzca el comando…
Definido en Active Directory	`vserver cifs group-policy central-access-policy show-defined -vserver` *`vserver_name`*
Aplicado a un servidor CIFS	`vserver cifs group-policy central-access-policy show-applied -vserver` *`vserver_name`*

Ejemplo

El siguiente ejemplo muestra información de todas las directivas de acceso central definidas en 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
```

El siguiente ejemplo muestra información de todas las políticas de acceso central que se aplican a las máquinas virtuales de almacenamiento (SVM) del clúster:

```
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
```

Información relacionada

- Obtenga más información sobre la seguridad del acceso a archivos para servidores
- Mostrar información acerca de las configuraciones de GPO
- Muestra información acerca de las reglas de la política de acceso central

Mostrar información sobre las reglas de política de acceso central de SMB de ONTAP

Puede mostrar información detallada acerca de las reglas de directiva de acceso central asociadas a las directivas de acceso central definidas en Active Directory. También puede mostrar información sobre las reglas de políticas de acceso central que se aplican al servidor CIFS a través de los GPO de la política de acceso central (objetos de política de grupo).

Acerca de esta tarea

Puede mostrar información detallada acerca de las reglas de directiva de acceso central definidas y aplicadas. De forma predeterminada, se muestra la siguiente información:

- Nombre del Vserver
- Nombre de la regla de acceso central
- Descripción
- Hora de creación
- Tiempo de modificación

- Permisos actuales
- Permisos propuestos
- Recursos objetivo

Si desea mostrar información acerca de todas las reglas de directiva de acceso central asociadas con las directivas de acceso central…	Introduzca el comando…
Definido en Active Directory	`vserver cifs group-policy central-access-rule show-defined -vserver vserver_name`
Aplicado a un servidor CIFS	`vserver cifs group-policy central-access-rule show-applied -vserver vserver_name`

Ejemplo

En el siguiente ejemplo se muestra información de todas las reglas de directiva de acceso central asociadas a las directivas de acceso central definidas en 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)
```

El siguiente ejemplo muestra información de todas las reglas de políticas de acceso central asociadas con las políticas de acceso centrales aplicadas a las máquinas virtuales de almacenamiento (SVM) en el clúster:

```
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)
```

Información relacionada

- Obtenga más información sobre la seguridad del acceso a archivos para servidores
- Mostrar información acerca de las configuraciones de GPO
- Muestra información sobre las políticas de acceso central