Apply Group Policy Objects to SMB servers

ONTAP 9

NetApp
March 21, 2022

This PDF was generated from https://docs.netapp.com/us-en/ontap/smb-admin/applying-group-policy-objects-concept.html on March 21, 2022. Always check docs.netapp.com for the latest.

Table of Contents

Apply Group Policy Objects to SMB servers . . . 1
- Apply Group Policy Objects to SMB servers overview . . . 1
- Supported GPOs . . . 1
- Requirements for using GPOs with your SMB server . . . 6
- Enable or disable GPO support on a CIFS server . . . 6
- How GPOs are updated on the SMB server . . . 7
- Manually updating GPO settings on the CIFS server . . . 9
- Display information about GPO configurations . . . 9
- Display detailed information about restricted group GPOs . . . 14
- Display information about central access policies . . . 16
- Display information about central access policy rules . . . 18

Apply Group Policy Objects to SMB servers

Apply Group Policy Objects to SMB servers overview

Your SMB server supports Group Policy Objects (GPOs), a set of rules known as *group policy attributes* that apply to computers in an Active Directory environment. You can use GPOs to centrally manage settings for all storage virtual machines (SVMs) on the cluster belonging to the same Active Directory domain.

When GPOs are enabled on your SMB server, ONTAP sends LDAP queries to the Active Directory server requesting GPO information. If there are GPO definitions that are applicable to your SMB server, the Active Directory server returns the following GPO information:

- GPO name
- Current GPO version
- Location of the GPO definition
- Lists of UUIDs (universally unique identifiers) for GPO policy sets

Related information

Securing file access by using Dynamic Access Control (DAC)

SMB and NFS auditing and security tracing

Supported GPOs

Although not all Group Policy Objects (GPOs) are applicable to your CIFS-enabled storage virtual machines (SVMs), SVMs can recognize and process the relevant set of GPOs.

The following GPOs are currently supported on SVMs:

- Advanced audit policy configuration settings:

  Object access: Central Access Policy staging

  Specifies the type of events to be audited for central access policy (CAP) staging, including the following settings:

  - Do not audit
  - Audit only success events
  - Audit only failure events
  - Audit both success and failure events

  > If any of the three audit options are set (audit only success events, audit only failure events, audit both success and failure events), ONTAP audits both success and failure events.

  Set by using the `Audit Central Access Policy Staging` setting in the `Advanced Audit Policy Configuration/Audit Policies/Object Access` GPO.

To use advanced audit policy configuration GPO settings, auditing must be configured on the CIFS-enabled SVM to which you want to apply these setting. If auditing is not configured on the SVM, the GPO settings will not be applied and will be dropped.

- Registry settings:
  - Group Policy refresh interval for CIFS-enabled SVM

    Set by using the `Registry` GPO.
  - Group Policy refresh random offset

    Set by using the `Registry` GPO.
  - Hash publication for BranchCache

    The Hash Publication for BranchCache GPO corresponds to the BranchCache operating mode. The following three supported operating modes are supported:

    - Per-share
    - All-shares
    - Disabled Set by using the `Registry` GPO.
  - Hash version support for BranchCache

    The following three hash version settings are supported:

    - BranchCache version 1
    - BranchCache version 2
    - BranchCache versions 1 and 2 Set by using the `Registry` GPO.

To use BranchCache GPO settings, BranchCache must be configured on the CIFS-enabled SVM to which you want to apply these setting. If BranchCache is not configured on the SVM, the GPO settings will not be applied and will be dropped.

- Security settings
  - Audit policy and event log
    - Audit logon events

      Specifies the type of logon events to be audited, including the following settings:

      - Do not audit
      - Audit only success events
      - Audit on failure events
      - Audit both success and failure events Set by using the `Audit logon events` setting in the `Local Policies/Audit Policy` GPO.

If any of the three audit options are set (audit only success events, audit only failure events, audit both success and failure events), ONTAP audits both success and failure events.

- Audit object access

  Specifies the type of object access to be audited, including the following settings:

  - Do not audit
  - Audit only success events
  - Audit on failure events
  - Audit both success and failure events Set by using the `Audit object access` setting in the `Local Policies/Audit Policy` GPO.

  If any of the three audit options are set (audit only success events, audit only failure events, audit both success and failure events), ONTAP audits both success and failure events.

- Log retention method

  Specifies the audit log retention method, including the following settings:

  - Overwrite the event log when size of the log file exceeds the maximum log size
  - Do not overwrite the event log (clear log manually) Set by using the `Retention method for security log` setting in the `Event Log` GPO.

- Maximum log size

  Specifies the maximum size of the audit log.

  Set by using the `Maximum security log size` setting in the `Event Log` GPO.

  To use audit policy and event log GPO settings, auditing must be configured on the CIFS-enabled SVM to which you want to apply these setting. If auditing is not configured on the SVM, the GPO settings will not be applied and will be dropped.

◦ File system security

Specifies a list of files or directories on which file security is applied through a GPO.

Set by using the `File System` GPO.

The volume path to which the file system security GPO is configured must exist within the SVM.

◦ Kerberos policy

- Maximum clock skew

  Specifies maximum tolerance in minutes for computer clock synchronization.

  Set by using the `Maximum tolerance for computer clock synchronization` setting in

the `Account Policies/Kerberos Policy` GPO.

- Maximum ticket age

  Specifies maximum lifetime in hours for user ticket.

  Set by using the `Maximum lifetime for user ticket` setting in the `Account Policies/Kerberos Policy` GPO.

- Maximum ticket renew age

  Specifies maximum lifetime in days for user ticket renewal.

  Set by using the `Maximum lifetime for user ticket renewal` setting in the `Account Policies/Kerberos Policy` GPO.

◦ User rights assignment (privilege rights)

- Take ownership

  Specifies the list of users and groups that have the right to take ownership of any securable object.

  Set by using the `Take ownership of files or other objects` setting in the `Local Policies/User Rights Assignment` GPO.

- Security privilege

  Specifies the list of users and groups that can specify auditing options for object access of individual resources, such as files, folders, and Active Directory objects.

  Set by using the `Manage auditing and security log` setting in the `Local Policies/User Rights Assignment` GPO.

- Change notify privilege (bypass traverse checking)

  Specifies the list of users and groups that can traverse directory trees even though the users and groups might not have permissions on the traversed directory.

  The same privilege is required for users to receive notifications of changes to files and directories. Set by using the `Bypass traverse checking` setting in the `Local Policies/User Rights Assignment` GPO.

◦ Registry values

- Signing required setting

  Specifies whether required SMB signing is enabled or disabled.

  Set by using the `Microsoft network server: Digitally sign communications (always)` setting in the `Security Options` GPO.

◦ Restrict anonymous

Specifies what the restrictions for anonymous users are and includes the following three GPO settings:

- No enumeration of Security Account Manager (SAM) accounts:

This security setting determines what additional permissions are granted for anonymous connections to the computer. This option is displayed as `no-enumeration` in ONTAP if it is enabled.

Set by using the `Network access: Do not allow anonymous enumeration of SAM accounts` setting in the `Local Policies/Security Options` GPO.

- No enumeration of SAM accounts and shares

  This security setting determines whether anonymous enumeration of SAM accounts and shares is allowed. This option is displayed as `no-enumeration` in ONTAP if it is enabled.

  Set by using the `Network access: Do not allow anonymous enumeration of SAM accounts and shares` setting in the `Local Policies/Security Options` GPO.

- Restrict anonymous access to shares and named pipes

  This security setting restricts anonymous access to shares and pipes. This option is displayed as `no-access` in ONTAP if it is enabled.

  Set by using the `Network access: Restrict anonymous access to Named Pipes and Shares` setting in the `Local Policies/Security Options` GPO.

When displaying information about defined and applied group policies, the `Resultant restriction for anonymous user` output field provides information about the resultant restriction of the three restrict anonymous GPO settings. The possible resultant restrictions are as follows:

- `no-access`

  The anonymous user is denied access to the specified shares and named pipes, and cannot use enumeration of SAM accounts and shares. This resultant restriction is seen if the `Network access: Restrict anonymous access to Named Pipes and Shares` GPO is enabled.

- `no-enumeration`

  The anonymous user has access to the specified shares and named pipes, but cannot use enumeration of SAM accounts and shares. This resultant restriction is seen if both of the following conditions are met:

  - The `Network access: Restrict anonymous access to Named Pipes and Shares` GPO is disabled.
  - Either the `Network access: Do not allow anonymous enumeration of SAM accounts` or the `Network access: Do not allow anonymous enumeration of SAM accounts and shares` GPOs is enabled.

- `no-restriction`

  The anonymous user has full access and can use enumeration. This resultant restriction is seen if both of the following conditions are met:

  - The `Network access: Restrict anonymous access to Named Pipes and Shares` GPO is disabled.
  - Both the `Network access: Do not allow anonymous enumeration of SAM accounts`

and `Network access: Do not allow anonymous enumeration of SAM accounts and shares` GPOs are disabled.

  - Restricted Groups

    You can configure restricted groups to centrally manage membership of either built-in or user-defined groups. When you apply a restricted group through a group policy, the membership of a CIFS server local group is automatically set to match the membership-list settings defined in the applied group policy.

    Set by using the `Restricted Groups` GPO.

- Central access policy settings

  Specifies a list of central access policies. Central access policies and the associated central access policy rules determine access permissions for multiple files on the SVM.

Related information

Enabling or disabling GPO support on a CIFS server

Securing file access by using Dynamic Access Control (DAC)

SMB and NFS auditing and security tracing

Modifying the CIFS server Kerberos security settings

Using BranchCache to cache SMB share content at a branch office

Using SMB signing to enhance network security

Configuring bypass traverse checking

Configuring access restrictions for anonymous users

Requirements for using GPOs with your SMB server

To use Group Policy Objects (GPOs) with your SMB server, your system must meet several requirements.

- SMB must be licensed on the cluster.
- A SMB server must be configured and joined to a Windows Active Directory domain.
- The SMB server admin status must be on.
- GPOs must be configured and applied to the Windows Active Directory Organizational Unit (OU) containing the SMB server computer object.
- GPO support must be enabled on the SMB server.

Enable or disable GPO support on a CIFS server

You can enable or disable Group Policy Object (GPO) support on a CIFS server. If you enable GPO support on a CIFS server, the applicable GPOs that are defined on the group policy—the policy that is applied to the organizational unit (OU) that contains the

CIFS server computer object—are applied to the CIFS server.

About this task

GPOs cannot be enabled on CIFS servers in workgroup mode.

Steps

1. Perform one of the following actions:

If you want to…	Enter the command…
Enable GPOs	`vserver cifs group-policy modify -vserver vserver_name -status enabled`
Disable GPOs	`vserver cifs group-policy modify -vserver vserver_name -status disabled`

2. Verify that GPO support is in the desired state: `vserver cifs group-policy show -vserver +vserver_name_`

   Group Policy Status for CIFS servers in workgroup mode is displayed as “disabled”.

Example

The following example enables GPO support on storage virtual machine (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
```

Related information

Supported GPOs

Requirements for using GPOs with your CIFS server

How GPOs are updated on the CIFS server

Manually updating GPO settings on the CIFS server

Displaying information about GPO configurations

How GPOs are updated on the SMB server

How GPOs are updated on the CIFS server overview

By default, ONTAP retrieves and applies Group Policy Object (GPO) changes every 90

minutes. Security settings are refreshed every 16 hours. If you want to update GPOs to apply new GPO policy settings before ONTAP automatically updates them, you can trigger a manual update on a CIFS server with an ONTAP command.

- By default, all GPOs are verified and updated as needed every 90 minutes.

  This interval is configurable and can be set using the `Refresh interval` and `Random offset` GPO settings.

  ONTAP queries Active Directory for changes to GPOs. If the GPO version numbers recorded in Active Directory are higher than those on the CIFS server, ONTAP retrieves and applies the new GPOs. If the version numbers are the same, GPOs on the CIFS server are not updated.

- Security Settings GPOs are refreshed every 16 hours.

  ONTAP retrieves and applies Security Settings GPOs every 16 hours, whether or not these GPOs have changed.

  > The 16-hour default value cannot be changed in the current ONTAP version. It is a Windows client default setting.

- All GPOs can be updated manually with an ONTAP command.

  This command simulates the Windows `gpupdate.exe`/force` command.

Related information

Manually updating GPO settings on the CIFS server

What to do if GPO updates are failing

Under some circumstances, Group Policy Object (GPO) updates from Windows 2012 domain controllers might fail, which leads to nothing being visible under the `Central Access Policy Settings` section of the output for the `vserver cifs group-policy show-defined` command. You should know how to correct this issue if it occurs.

Underlying cause	Remedy
When ONTAP attempts to connect to the Windows 2012 domain controller to perform the GPO update, the connection might fail with the error `error 0xc00000bd (NT STATUS_DUPLICATE_NAME).` This error occurs when the server name used to make the connection is different from the NetBIOS name of the CIFS server. There are various reasons this might occur, including the use of aliases. Additionally, ONTAP pads the NetBIOS name used when connecting to the domain controller to make the name length equal to 15 characters. This can make it appear that the CIFS server name and the NetBIOS name are different.	1. Disable NetBIOS name checking on the Windows server by adding the following registry key with the value set to `1`: `"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\DisableStrictNameChecking"` To learn more about this registry key, contact Microsoft Support. Microsoft Support 2. Reboot the domain controller.

Manually updating GPO settings on the CIFS server

If you want to update Group Policy Object (GPO) settings on your CIFS server immediately, you can manually update the settings. You can update only changed settings or you can force an update for all settings, including the settings that were applied previously but have not changed.

Step

1. Perform the appropriate action:

If you want to update…	Enter the command…
Changed GPO settings	`vserver cifs group-policy update -vserver` *`vserver_name`*
All GPO settings	`vserver cifs group-policy update -vserver` *`vserver_name`* `-force-reapply -all-settings true`

Related information

How GPOs are updated on the CIFS server

Display information about GPO configurations

You can display information about Group Policy Object (GPO) configurations that are defined in Active Directory and about GPO configurations applied to the CIFS server.

About this task

You can display information about all GPO configurations defined in the Active Directory of the domain to which the CIFS server belongs, or you can display information only about GPO configurations applied to a CIFs server.

Steps

1. Display information about GPO configurations by performing one of the following actions:

If you want to display information about all Group Policy configurations…	Enter the command…
Defined in Active Directory	`vserver cifs group-policy show-defined -vserver vserver_name`
Applied to a CIFS-enabled storage virtual machine (SVM)	`vserver cifs group-policy show-applied -vserver vserver_name`

Example

The following example displays the GPO configurations defined in the Active Directory to which the CIFS-enabled SVM named vs1 belongs:

```
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
```

The following example displays the GPO configurations applied to the CIFS-enabled SVM vs1:

```
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
```

Related information

Enabling or disabling GPO support on a CIFS server

Display detailed information about restricted group GPOs

You can display detailed information about restricted groups that are defined as Group Policy Objects (GPOs) in Active Directory and that are applied to the CIFS server.

About this task

By default, the following information is displayed:

- Group policy name
- Group policy version
- Link

  Specifies the level in which the group policy is configured. Possible output values include the following:

  - `Local` when the group policy is configured in ONTAP
  - `Site` when the group policy is configured at the site level in the domain controller
  - `Domain` when the group policy is configured at the domain level in the domain controller
  - `OrganizationalUnit` when the group policy is configured at the Organizational Unit (OU) level in the domain controller
  - `RSOP` for the resultant set of policies derived from all the group policies defined at various levels
- Restricted group name
- The users and groups who belong to and who do not belong to the restricted group
- The list of groups to which the restricted group is added

  A group can be a member of groups other than the groups listed here.

Step

1. Display information about all restricted group GPOs by performing one of the following actions:

If you want to display information about all restricted group GPOs…	Enter the command…
Defined in Active Directory	`vserver cifs group-policy restricted-group show-defined -vserver vserver_name`
Applied to a CIFS server	`vserver cifs group-policy restricted-group show-applied -vserver vserver_name`

Example

The following example displays information about restricted group GPOs defined in the Active Directory domain to which the CIFS-enabled SVM named vs1 belongs:

```
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
```

The following example displays information about restricted groups GPOs applied to the CIFS-enabled SVM vs1:

```
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
```

Related information

Displaying information about GPO configurations

Display information about central access policies

You can display detailed information about the central access policies that are defined in Active Directory. You can also display information about the central access policies that are applied to the CIFS server through group policy objects (GPOs).

About this task

By default, the following information is displayed:

- SVM name
- Name of the central access policy
- SID
- Description
- Creation time
- Modification time
- Member rules

CIFS servers in workgroup mode are not displayed because they do not support GPOs.

Step

1. Display information about central access policies by performing one of the following actions:

If you want to display information about all central access policies…	Enter the command…
Defined in Active Directory	`vserver cifs group-policy central-access-policy show-defined -vserver` *vserver_name*
Applied to a CIFS server	`vserver cifs group-policy central-access-policy show-applied -vserver` *vserver_name*

Example

The following example displays information for all the central access policies that are defined in 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
```

The following example displays information for all the central access policies that are applied to the storage virtual machines (SVMs) on the cluster:

```
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
```

Related information

Securing file access by using Dynamic Access Control (DAC)

Displaying information about GPO configurations

Displaying information about central access policy rules

Display information about central access policy rules

You can display detailed information about central access policy rules that are associated with central access policies defined in Active Directory. You can also display information about central access policies rules that are applied to the CIFS server through central access policy GPOs (group policy objects).

About this task

You can display detailed information about defined and applied central access policy rules. By default, the following information is displayed:

- Vserver name
- Name of the central access rule
- Description
- Creation time
- Modification time
- Current permissions
- Proposed permissions

- Target resources

Table 1. Step

If you want to display information about all central access policy rules associated with central access policies…	Enter the command…
Defined in Active Directory	`vserver cifs group-policy central-access-rule show-defined -vserver vserver_name`
Applied to a CIFS server	`vserver cifs group-policy central-access-rule show-applied -vserver vserver_name`

Example

The following example displays information for all central access policy rules associated with central access policies defined in 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)
```

The following example displays information for all central access policy rules associated with central access policies applied to storage virtual machines (SVMs) on the cluster:

```
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)
```

Related information

Securing file access by using Dynamic Access Control (DAC)

Displaying information about GPO configurations

Displaying information about central access policies

Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system- without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.