



## **vserver cifs commands**

ONTAP 9.15.1 commands

NetApp  
May 17, 2024

# Table of Contents

vserver cifs commands	1
vserver cifs add-netbios-aliases	1
vserver cifs check	2
vserver cifs create	4
vserver cifs delete	6
vserver cifs modify	7
vserver cifs nbtstat	11
vserver cifs prepare-to-downgrade	14
vserver cifs remove-netbios-aliases	15
vserver cifs repair-modify	17
vserver cifs security-encryption-required-dc-connections-prepare-to-downgrade	17
vserver cifs show	18
vserver cifs start	20
vserver cifs stop	21
vserver cifs branchcache create	21
vserver cifs branchcache delete	23
vserver cifs branchcache hash-create	24
vserver cifs branchcache hash-flush	25
vserver cifs branchcache modify	25
vserver cifs branchcache show	27
vserver cifs cache name-to-sid delete-all	28
vserver cifs cache name-to-sid delete	29
vserver cifs cache name-to-sid show	30
vserver cifs cache settings modify	31
vserver cifs cache settings show	32
vserver cifs cache sid-to-name delete-all	33
vserver cifs cache sid-to-name delete	34
vserver cifs cache sid-to-name show	35
vserver cifs character-mapping create	36
vserver cifs character-mapping delete	37
vserver cifs character-mapping modify	38
vserver cifs character-mapping show	39
vserver cifs connection show	40
vserver cifs domain discovered-servers reset-servers	42
vserver cifs domain discovered-servers show	42
vserver cifs domain discovered-servers discovery-mode modify	44
vserver cifs domain discovered-servers discovery-mode show	45
vserver cifs domain name-mapping-search add	46
vserver cifs domain name-mapping-search modify	46
vserver cifs domain name-mapping-search remove	47
vserver cifs domain name-mapping-search show	47
vserver cifs domain password change	48
vserver cifs domain password reset	49

vserver cifs domain password schedule modify	49
vserver cifs domain password schedule show	50
vserver cifs domain preferred-dc add	52
vserver cifs domain preferred-dc check	53
vserver cifs domain preferred-dc remove	54
vserver cifs domain preferred-dc show	55
vserver cifs domain trusts rediscover	56
vserver cifs domain trusts show	56
vserver cifs group-policy modify	57
vserver cifs group-policy show-applied	58
vserver cifs group-policy show-defined	60
vserver cifs group-policy show	63
vserver cifs group-policy update	64
vserver cifs group-policy central-access-policy show-applied	64
vserver cifs group-policy central-access-policy show-defined	66
vserver cifs group-policy central-access-rule show-applied	68
vserver cifs group-policy central-access-rule show-defined	70
vserver cifs group-policy restricted-group show-applied	72
vserver cifs group-policy restricted-group show-defined	74
vserver cifs home-directory modify	76
vserver cifs home-directory show-user	77
vserver cifs home-directory show	79
vserver cifs home-directory search-path add	80
vserver cifs home-directory search-path remove	80
vserver cifs home-directory search-path reorder	81
vserver cifs home-directory search-path show	82
vserver cifs options modify	82
vserver cifs options show	90
vserver cifs security modify	97
vserver cifs security show	101
vserver cifs session close	105
vserver cifs session show	108
vserver cifs session file close	113
vserver cifs session file show	114
vserver cifs share create	117
vserver cifs share delete	122
vserver cifs share modify	122
vserver cifs share show	125
vserver cifs share access-control create	129
vserver cifs share access-control delete	130
vserver cifs share access-control modify	131
vserver cifs share access-control show	132
vserver cifs share properties add	134
vserver cifs share properties remove	135
vserver cifs share properties show	137

vserver cifs superuser create . . . . .	139
vserver cifs superuser delete . . . . .	139
vserver cifs superuser show . . . . .	140
vserver cifs symlink create . . . . .	141
vserver cifs symlink delete . . . . .	142
vserver cifs symlink modify . . . . .	143
vserver cifs symlink show . . . . .	144
vserver cifs users-and-groups remove-stale-records . . . . .	146
vserver cifs users-and-groups update-names . . . . .	147
vserver cifs users-and-groups local-group add-members . . . . .	148
vserver cifs users-and-groups local-group create . . . . .	149
vserver cifs users-and-groups local-group delete . . . . .	150
vserver cifs users-and-groups local-group modify . . . . .	150
vserver cifs users-and-groups local-group remove-members . . . . .	151
vserver cifs users-and-groups local-group rename . . . . .	152
vserver cifs users-and-groups local-group show-members . . . . .	152
vserver cifs users-and-groups local-group show . . . . .	153
vserver cifs users-and-groups local-user create . . . . .	155
vserver cifs users-and-groups local-user delete . . . . .	156
vserver cifs users-and-groups local-user modify . . . . .	157
vserver cifs users-and-groups local-user rename . . . . .	158
vserver cifs users-and-groups local-user set-password . . . . .	159
vserver cifs users-and-groups local-user show-membership . . . . .	160
vserver cifs users-and-groups local-user show . . . . .	161
vserver cifs users-and-groups privilege add-privilege . . . . .	162
vserver cifs users-and-groups privilege remove-privilege . . . . .	163
vserver cifs users-and-groups privilege reset-privilege . . . . .	164
vserver cifs users-and-groups privilege show . . . . .	165

# vserver cifs commands

## vserver cifs add-netbios-aliases

Add NetBIOS aliases for the CIFS server name

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

```
The `vserver cifs add-netbios-aliases` command creates or adds a list of NetBIOS aliases for the CIFS server name.
```

### Parameters

**-vserver <vserver name> - Vserver**

This parameter specifies the name of the Vserver for which NetBIOS alias are to be created or added.

**-netbios-aliases <NetBIOS>,... - List of NetBIOS Aliases**

This parameter specifies one or more NetBIOS aliases to be added to an existing list of NetBIOS aliases. A new list of NetBIOS aliases is created if the list is currently empty.

### Examples

The following example creates a new list of NetBIOS aliases for Vserver vs\_a.

```
cluster1::> cifs show -display-netbios-aliases

Vserver: vs_a
Server Name: CIFS_SERVER
NetBIOS Aliases: -

cluster1::> cifs add-netbios-aliases -netbios-aliases
alias_1,alias_2,alias_3

cluster1::> cifs show -display-netbios-aliases

Vserver: vs_a
Server Name: CIFS_SERVER
NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

The following example adds several NetBIOS aliases for the CIFS server CIFS\_SERVER on Vserver vs\_a.

```

cluster1::> cifs add-netbios-aliases -netbios-aliases
alias_4,alias_5,alias_6

cluster1::> cifs show -display-netbios-aliases

Vserver: vs_a

    Server Name: CIFS_SERVER
    NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3, ALIAS_4,
                    ALIAS_5, ALIAS_6

cluster1::> vserver cifs add-netbios-aliases -vserver v1 -netbios-aliases
alias_7

cluster1::> cifs show -display-netbios-aliases

Vserver: vs_a

    Server Name: CIFS_SERVER
    NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3, ALIAS_4,
                    ALIAS_5, ALIAS_6, ALIAS_7

```

## vserver cifs check

### Display Validation Status of CIFS Configuration from Each Node

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

Use the `vserver cifs check` command to check the status of configured CIFS server on a particular vserver.

### Parameters

**{ [-fields <fieldname>,...]**

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

**| [-instance ] }**

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver name>] -Vserver**

Use this parameter to specify the Vserver whose CIFS server needs to be validated.

**[-node {<nodename>|local}] - Node**

Use this parameter to specify the node name from which CIFS server connectivity needs to be validated.

**[-netbios-name <TextNoCase>] - CIFS NetBIOS Name**

Use this parameter to display netbios-name of the configured CIFS server.

**[-cifs-status <TextNoCase>] - CIFS Server Status**

Use this parameter to display status of configured CIFS server.

**[-site <TextNoCase>] - CIFS Server Site**

This parameter specifies the site discovered from Data ONTAP for the Active Directory domain associated with the CIFS server. If the discovery fails, this parameter will be updated with the default-site of associated cifs server.

**[-server <TextNoCase>] - Domain Controller Name**

Use this parameter to display Domain name of the configured CIFS server.

**[-server-ip <text>] - Domain Controller IP Addr**

Use this parameter to display IP-address of the configured CIFS server.

**[-status {down|up}] - Connectivity Status**

Use this parameter to display information only about CIFS servers with a status that matches the value you specify.

**[-status-details <text>] - Connectivity Status Details**

Use this parameter to display information only about CIFS servers with status details that match the value you specify.

## Examples

The following example checks the connectivity of CIFS server on vs0 from each node.

```

cluster1::> vs0 cifs check -vs0 vs0
Vs0
      Cifs NetBIOS Name : NEWSERVER
      Cifs Status      : up
      Site              : Bangalore

Node Name DC Server Name      DC Server IP  Status  Status Details
-----
node1     CIFSSERVER.COM        10.11.12.13  up      Response time (msec): 55
node2     CIFSSERVER.COM        10.11.12.13  up      Response time (msec): 70
node3     CIFSSERVER.COM        10.11.12.13  down    Secd: No Server
available.

```

# vserver cifs create

Create a CIFS server

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs create` command creates a CIFS server on a Vserver. When you create the CIFS server, you can add it to an existing CIFS domain, or you can join it to a workgroup. When you add it to an existing CIFS domain, the storage system prompts you to provide the credentials of a user account that has sufficient privileges to add computers to the `-ou` container within the `-domain` domain. The user account must have a password that cannot be empty. If the new CIFS server is joining a domain, this command might take several minutes to complete.



Each Vserver can have only one CIFS server.

## Parameters

### **-vserver <vserver name> - Vserver**

This parameter specifies the name of the Vserver on which to create the CIFS server. The Vserver must already exist.

### **-cifs-server <NetBIOS> - CIFS Server NetBIOS Name**

This parameter specifies the name of the CIFS server (up to 15 characters).

### **{ -domain <TextNoCase> - Fully Qualified Domain Name**

This parameter specifies the name of the Active Directory domain to associate with the CIFS server.

### **[-ou <text>] - Organizational Unit**

This parameter specifies the organizational unit within the Active Directory domain to associate with the CIFS server. By default, this parameter is set to `CN=Computers`. When specifying this parameter, specify only the organizational unit portion of the distinguished name. Data ONTAP appends the value provided for the required `-domain` parameter onto the value provided for `-ou` parameter to produce the Active Directory distinguished name, which is used to associate with the CIFS server.



Nested OUs must be provided in a specific order with all containers separated by a comma. Reading from left to right you travel up the directory tree until you reach the root OU.

### **[-default-site <text>] - Default Site Used by LIFs Without Site Membership**

This parameter specifies the site within the Active Directory domain to associate with the CIFS server if Data ONTAP cannot determine an appropriate site. This parameter will also be used for discovering KDCs in the trusted domain if Data ONTAP cannot determine an appropriate site in the trusted domain.

### **| -workgroup <NetBIOS> - Workgroup Name }**

This parameter specifies the name of the workgroup (up to 15 characters).

### **[-keytab-uri {scheme://(hostname|IPv4 Address|[' 'IPv6 Address']')}] - Kerberos Keytab File URI (privilege: advanced)**

This parameter specifies loading a keytab file from the specified URI. This is applicable if the CIFS server is



being created in realm mode or domain mode.

### **[-status-admin {down|up}] - CIFS Server Administrative Status**

Use this parameter to specify whether the initial administrative status of the cifs server is up or down. The default setting is up.

### **[-comment <text>] - CIFS Server Description**

This optional parameter specifies a text comment for the server. CIFS clients can see this CIFS server description when browsing servers on the network. The comment can be up to 256 characters long. If there is a space in the descriptive remark or the path, you must enclose the entire string in quotation marks.

### **[-netbios-aliases <NetBIOS>,...] - List of NetBIOS Aliases**

This parameter specifies a list of NetBIOS aliases, which are alternate names to the CIFS server name.

## **Examples**

The following example creates a CIFS server CIFSSERVER1 for Vserver vs1 and domain EXAMPLE.com.

```
cluster1::> vsserver cifs create -vserver vs1 -cifs-server CIFSSERVER1
-domain EXAMPLE.com
```

In order to create an Active Directory machine account for the CIFS server, you

must supply the name and password of a Windows account with sufficient privileges to add computers to the "CN=Computers" container within the "EXAMPLE.com" domain.

Enter the user name: Administrator

Enter the password:

```
cluster1::> vsserver cifs create -vserver vs1 -cifs-server CIFSSERVER2
-domain EXAMPLE.com -keytab-uri
```

```
http://nbsweb.eng.btc.netapp.in/~user/Sample1.keytab
```

Info: SMB1 protocol version is disabled on this CIFS server. If required, use

the (privilege: advanced) command "vsserver cifs options modify -vserver vs1

```
-smb1-enabled true" to enable it.
```

The following example creates a CIFS server CIFSSERVER1 for Vserver vs1 and workgroup Sales:

```
cluster1::> vsserver cifs create -vserver vs1 -cifs-server CIFSSERVER1
-workgroup Sales
```

The following example creates a CIFS server CIFSSERVER1 for Vserver vs1 and domain EXAMPLE.com with

a user Administrator1 from a different domain, in this case an administrator from a trusted domain TRUST.LAB.COM:

```
cluster1::~> vsserver cifs create -vsserver vs1 -cifs-server CIFSSERVER1
-domain EXAMPLE.com
```

In order to create an Active Directory machine account for the CIFS server, you must supply the name and password of a Windows account with sufficient privileges to add computers to the "CN=Computers" container within the "EXAMPLE.com" domain.

Enter the user name: Administrator1@TRUST.LAB.COM

Enter the password:

The following example creates a CIFS server CIFSSERVER1 for Vserver vs1 with domain EXAMPLE.com using nested OUs:

```
cluster1::~> vsserver cifs create -vsserver vs1 -cifs-server CIFSSERVER1
-domain EXAMPLE.com -ou OU=developers,OU=engineering,OU=corp
```

In order to create an Active Directory machine account for the CIFS server, you must supply the name and password of a Windows account with sufficient privileges to add computers to the "OU=developers,OU=engineering,OU=corp" container within the "EXAMPLE.com" domain.

Enter the user name: Administrator

Enter the password:

## vserver cifs delete

Delete a CIFS server.

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs delete` command deletes a CIFS server.

### Parameters

**-vsserver <vserver name> -Vserver**

This parameter specifies the Vserver for the CIFS server you want to delete.

**[`-skip-ad-account-delete {true|false}`] - If this option is enabled, the local CIFS configuration will be removed without deleting the AD account. The default setting for this field is false.**

This parameter skips the deletion of the AD account and proceeds directly to the deletion of the local CIFS configuration.

## Examples

The following example deletes the CIFS server from a Vserver named vs1:

```
cluster1::> vserver cifs delete -vserver vs1
```

## vserver cifs modify

Modify a CIFS server

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs modify` command modifies the site within the Active Directory domain to associate with the CIFS server if Data ONTAP cannot determine an appropriate site. You also can modify the name and ou of the CIFS server, join to a new domain or a workgroup, or rejoin to current domain. When a CIFS server is joining a domain, this command might take several minutes to complete.

### Parameters

**`-vserver <vserver name>` - Vserver**

This parameter specifies the Vserver for the CIFS server whose associated site you want to modify.

**[`-cifs-server <NetBIOS>`] - CIFS Server NetBIOS Name**

This parameter specifies the name of the CIFS server (up to 15 characters). Before setting this parameter, the CIFS server must be stopped using the `vserver cifs modify-status-admin`down` command. When the command completes successfully, the administrative status of the CIFS server is automatically set to `up``.

**{ [`-domain <TextNoCase>`] - Fully Qualified Domain Name**

This parameter specifies the fully qualified name of the Active Directory domain to associate with the CIFS server. Before setting this parameter, the CIFS server must be stopped using the `vserver cifs modify-status-admin`down` command. When the command completes successfully, the administrative status of the CIFS server is automatically set to `up``.

**[`-ou <text>`] - Organizational Unit**

This parameter specifies the organization unit within the Active Directory domain to associate with the CIFS server. By default, this parameter is set to `CN=Computers`. Before setting this parameter, the CIFS server must be stopped using the `vserver cifs modify-status-admin`down` command. When the command completes successfully, the administrative status of the CIFS server is automatically set to `up``. Modifications to this parameter are not supported for workgroup CIFS servers.

### **[-default-site <text>] - Default Site Used by LIFs Without Site Membership**

This parameter specifies the site within the Active Directory domain to associate with the CIFS server if Data ONTAP cannot determine an appropriate site. Modifications to this parameter are not supported for workgroup CIFS servers.

### **[-workgroup <NetBIOS>] - Workgroup Name }**

This parameter specifies the name of the workgroup (up to 15 characters).

### **[-keytab-uri {scheme://(hostname|IPv4 Address|[' 'IPv6 Address']')}] - Kerberos Keytab File URI (privilege: advanced)**

This parameter specifies loading a keytab file from the specified URI. This is applicable if the CIFS server is being created in realm mode or domain mode.

### **[-status-admin {down|up}] - CIFS Server Administrative Status**

Use this parameter to modify the administrative status of the cifs server. Modify the administrator status to down to stop cifs access.

### **[-comment <text>] - CIFS Server Description**

Use this parameter to modify the comment of the server.

## **Examples**

The following example changes the default site and administrative status of the CIFS server associated with Vserver "vs1":

```
cluster1::> vsserver cifs modify -vsserver vs1 -default-site default -status
-admin up
```

The following example modifies the Active Directory domain and ou for the CIFS server associated with Vserver "vs1". The administrative status of the CIFS server must be set to "down" to proceed with Active Directory domain modification. If the command completes successfully, the administrative status is automatically set to "up".

```
cluster1::> vsriver cifs modify -vsriver vs1 -domain example.com -ou
ou=example_ou -cifs-server example -status-admin down
```

In order to create an Active Directory machine account for the CIFS server, you must supply the name and password of a Windows account with sufficient privileges to add computers to the "ou=example\_ou" container within the "example.com" domain.

```
Enter the user name: administrator
```

```
Enter the password:
```

```
cluster1::>
```

The following example modifies the CIFS server associated with Vserver "vs1" from a domain to a workgroup. The administrative status of the CIFS server must be set to "down" for this command. If the command completes successfully, the administrative status is automatically set to "up".

```
cluster1::> vsriver cifs modify -vsriver vs1 -workgroup Sales -status
-admin down
```

```
Warning: To enter workgroup mode, all domain-based features must be
disabled
        and their configuration removed automatically by the system,
        including continuously-available shares, shadow copies, and AES.
        However, domain-configured share ACLs such as
        "EXAMPLE.COM\userName" will not work properly, but cannot be
        removed by Data ONTAP. Remove these share ACLs as soon as
possible
        using external tools after the command completes. If AES is
enabled,
        you may be asked to supply the name and password of a Windows
account
        with sufficient privileges to disable it in the "EXAMPLE.COM"
domain.
Do you want to continue? {y|n}: y
```

```
cluster1::>
```

The following example modifies the CIFS server associated with Vserver "vs1" from a workgroup to a domain. The administrative status of the CIFS server must be set to "down" for this command. If the command completes successfully, the administrative status is automatically set to "up".

```
cluster1::> vservice cifs modify -vservice vs1 -domain example.com -status
-admin down
```

In order to create an Active Directory machine account for the CIFS server, you must supply the name and password of a Windows account with sufficient privileges to add computers to the "ou=example\_ou" container within the "example.com" domain.

Enter the user name: administrator

Enter the password:

```
cluster1::>
```

The following example modifies the CIFS server associated with Vservice "vs1" from a workgroup to a domain using keytab-uri. The administrative status of the CIFS server must be set to "down" for this command. If the command completes successfully, the administrative status is automatically set to "up".

```
cluster1::> vservice cifs modify -vservice vs1 -domain example.com -keytab
-uri http://nbsweb.eng.btc.netapp.in/~shravanp/Sample1.keytab -status
-admin down
```

```
cluster1::>
```

The following example modifies the CIFS server name associated with Vservice "vs1" from above example. The administrative status of the CIFS server must be set to "down" to proceed with Active Directory domain modification. If the command completes successfully, the administrative status is automatically set to "up" and there will be a job running to update related configurations.

```
cluster1::> vserver cifs modify -vserver vs1 -cifs-server new_example
-status-admin down
```

In order to create an Active Directory machine account for the CIFS server, you must supply the name and password of a Windows account with sufficient privileges to add computers to the "ou=example\_ou" container within the "example.com" domain.

```
Enter the user name: administrator
```

```
Enter the password:
```

```
Successfully queued CIFS Server Modify job [id: xx] for CIFS server
"NEW_EXAMPLE". To view the status of the job, use the "job show -id
<jobid>"
command.
```

```
cluster1::>
```

## vserver cifs nbtstat

Display NetBIOS information over TCP connection

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs nbtstat` command displays information about NetBIOS over TCP (NBT) connections for the cluster. It displays the IP address associated with the interfaces, the IP addresses of the WINS servers in use, and information about the registered NetBIOS names for the cluster. You can use this command to troubleshoot NetBIOS name resolution problems.



NetBIOS name service (NBNS) over IPv6 is not supported.

### Parameters

```
{ [-fields <fieldname>,...]
```

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

```
| [-instance ] }
```

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-node {<nodename>|local}] - Node**

If you specify this optional parameter, the command displays the NetBIOS name service information only for the specified node.

**[-vserver <vserver name>] - Vserver**

If you specify this optional parameter, the command displays the NetBIOS name service information only for the specified Vserver.

**[-nbt-name <text>] - NBT Name**

If you specify this optional parameter, the command displays the NetBIOS name service information only for the specified NetBIOS name.

**[-netbios-suffix <Hex String>] - NetBIOS Suffix**

If you specify this optional parameter, the command displays the NetBIOS name service information only for the specified NetBIOS suffix.

**[-interface <IP Address>,...] - Interfaces**

If you specify this optional parameter, the command displays the NetBIOS name service information only for the specified IP address.

**[-wins-servers <IP Address>,...] - Servers**

If you specify this optional parameter, the command displays the NetBIOS name service information only for the specified WINS servers.

**[-server-state <text>,...] - Server State (active, inactive)**

If you specify this optional parameter, the command displays the NetBIOS name service information only for the specified WINS server state. The following are possible values for this parameter:

- active
- inactive

**[-nbt-scope <text>] - NBT Scope**

If you specify this optional parameter, the command displays the NetBIOS name service information only for the specified NetBIOS name scope.

**[-nbt-mode <text>] - NBT Mode**

If you specify this optional parameter, the command displays the NetBIOS name service information only for the specified NetBIOS name service mode. The following are possible values for this parameter:

- 'p' - Point to Point
- 'h' - Hybrid
- 'm' - Mixed
- 'b' - Broadcast

**[-state <text>] - State**

If you specify this optional parameter, the command displays the NetBIOS name service information only for the specified NetBIOS name registration state. The following are possible values for this parameter:

- must\_register



- must\_unregister
- wins
- broadcast
- name\_released
- wins\_conflict
- broadcast\_conflict

**[-time-left <integer>] - Time Left**

If you specify this optional parameter, the command displays the NetBIOS name service information only for the specified registration time left in minutes with the WINS server.

**[-type <text>] - Type**

If you specify this optional parameter, the command displays the NetBIOS name service information only for the specified name registration type. The following are possible values for this parameter:

- registered
- active
- permanent
- group

## Examples

The following example displays the NetBIOS name service information.

```

cluster1::> nbtstat
      (vserver cifs nbtstat)

      Vserver: vs1
      Node:    cluster1-01
      Interfaces:
                10.10.10.32
                10.10.10.33
      Servers:
                17.17.1.2 (active )
      NBT Scope:
                [ ]
      NBT Mode:
                [h]
      NBT Name          NetBIOS Suffix   State          Time Left
Type -----
-----
      CLUSTER_1        00             wins           57
      CLUSTER_1        20             wins           57
Vserver: vs1
      Node:    cluster1-02
      Interfaces:
                10.10.10.35
      Servers:
                17.17.1.2 (active )
      CLUSTER_1        00             wins           58
      CLUSTER_1        20             wins           58
      4 entries were displayed.

```

## vserver cifs prepare-to-downgrade

Restore the CIFS Configurations to Earlier Release of Data ONTAP Version

**Availability:** This command is available to *cluster* administrators at the *advanced* privilege level.

### Description

The `vserver cifs prepare-to-downgrade` command restores the CIFS configurations for Data ONTAP based on the input parameter `disable-feature-set`.

### Parameters

**-disable-feature-set <downgrade version> - Data ONTAP Version (privilege: advanced)**

This parameter specifies the Data ONTAP release for which the CIFS configurations are restored. The value can be one of the following:

- 8.3.1 - Restores the CIFS configurations for Data ONTAP release 8.3.1. These features include:
  - FPolicy "close with read" filters from FPolicy events.
  - CIFS server options `-guest-unix-user` and `-is-admin-users-mapped-to-root-enabled`.
  - CIFS security option `is-smb-encryption-required`.
  - Storage-Level Access Guard (SLAG) for qtrees.
  - CIFS share property `encrypt-data`.
- 8.3.2 - Restores the CIFS configurations for Data ONTAP release 8.3.2. These features include:
  - CIFS server option `-grant-unix-group-perms-to-others`.
- 9.0.0 - Restores the CIFS configurations for Data ONTAP release 9.0.0. These features include:
  - Disable CIFS multichannel feature and close all multichannel connections.
  - Delete all the name-mapping entries that have a hostname or an address field configured.
  - Terminate all SMB 3.1 client connections.
  - Terminate all client connections that have large MTU negotiated.
  - Remove the symlink property `no-strict-security`.
  - Remove all symlink pathmap entries with locality `freelink`.

## Examples

```
cluster1::*> vserver cifs prepare-to-downgrade -disable-feature-set 8.3.1
```

```
cluster1::*> vserver cifs prepare-to-downgrade -disable-feature-set 8.3.2
```

```
cluster1::*> vserver cifs prepare-to-downgrade -disable-feature-set 9.0.0
```

## vserver cifs remove-netbios-aliases

### Remove NetBIOS aliases

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The ``vserver cifs remove-netbios-aliases`` command deletes NetBIOS aliases for the CIFS server.

## Parameters

### **-vserver <vserver name> - Vserver**

This parameter specifies the name of the Vserver from which the list of NetBIOS aliases are deleted.

### **-netbios-aliases <NetBIOS>,... - List of NetBIOS Aliases**

This parameter specifies one or more NetBIOS aliases to be deleted. To delete all the NetBIOS aliases of a Vserver use '-'.

## Examples

The following example deletes NetBIOS aliases for the CIFS server CIFS\_SERVER on Vserver vs\_a.

```
cluster1::> cifs show -display-netbios-aliases

Vserver: vs_a
Server Name: CIFS_SERVER
  NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3, ALIAS_4,
                  ALIAS_5, ALIAS_6, ALIAS_7

cluster1::> cifs remove-netbios-aliases -netbios-aliases
alias_1,alias_3,alias_5

cluster1::> cifs show -display-netbios-aliases

Vserver: vs_a
Server Name: CIFS_SERVER
  NetBIOS Aliases: ALIAS_2, ALIAS_4, ALIAS_6, ALIAS_7

cluster1::> cifs remove-netbios-aliases -netbios-aliases alias_7

cluster1::> cifs show -display-netbios-aliases

Vserver: vs_a
Server Name: CIFS_SERVER
  NetBIOS Aliases: ALIAS_2, ALIAS_4, ALIAS_6

cluster1::> cifs remove-netbios-aliases -netbios-aliases -

cluster1::> cifs show -display-netbios-aliases

Vserver: vs_a
Server Name: CIFS_SERVER
  NetBIOS Aliases: -
```

# vserver cifs repair-modify

Repair a partially-failed Vserver CIFS server modify operation

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

## Description

Use this `vserver cifs repair-modify -vserver <vserver name>` command when the background job created during a Vserver CIFS server modify operation fails.

## Parameters

**-vserver <vserver name> - Vserver (privilege: advanced)**

This parameter specifies a Vserver containing a configured CIFS server that has been modified.

## Examples

The following example starts the CIFS server modify job on Vserver vs1 successfully:

```
cluster1::*> vserver cifs repair-modify -vserver vs1

Successfully queued CIFS Server Modify job [id: 10] for CIFS server
"CIFSNAME1".
To view the status of the job, use the "job show -id <jobid>" command.

cluster1::*>
```

The following example fails the command with specific error:

```
cluster1::*> vserver cifs repair-modify -vserver vs2

Error: Job Out of memory. Failed to queue CIFS Server Modify Job for CIFS
server "CIFSNAME2". Retry the operation by running (privilege: advanced)
"vserver cifs repair-modify -vserver vs2".
Error: command failed: unable to save data

cluster1::*>
```

# vserver cifs security-encryption-required-dc-connections-prepare-to-downgrade

Disabled encryption-required-for-dc-connections option and capability for downgrade.

**Availability:** This command is available to *cluster* administrators at the *advanced* privilege level.

## Description

The `vserver cifs security-encryption-required-dc-connections-prepare-to-downgrade` prepares the cluster for downgrade by disabling `SMB3.encrypted.dc.connection` capability

## Examples

```
cluster1::*> vserver cifs security-encryption-required-dc-connections-prepare-to-downgrade
```

## vserver cifs show

Display CIFS servers

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs show` command displays information about CIFS servers. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all CIFS servers:

- Vserver name
- CIFS server NetBIOS name
- Domain or workgroup name
- Authentication style

You can specify the `-fields` parameter to specify which fields of information to display about CIFS servers. In addition to the fields above, you can display the following fields:

- Default site
- Fully-qualified domain name

You can specify additional parameters to display only information that matches those parameters. For instance, to display information only about CIFS servers that are in the CIFS domain named RUBY, run the command with the `-domain-workgroup RUBY` parameter.

You can specify the `-instance`` parameter to display all information for all CIFS servers in list form.

### Parameters

**{ [-fields <fieldname>, ... ]**

If you specify the `-fields <fieldname>, ...` parameter, the command only displays the fields that you specify.

**[ [-display-netbios-aliases ]**

If you specify this parameter, the command displays information about configured NetBIOS aliases.

**[ `-instance` ] }**

If you specify the `-instance` parameter, the command displays detailed information about all entries.

**[ `-vserver` <`vserver name`> ] - Vserver**

If you specify this parameter, the command displays information only about the CIFS servers for the specified Vserver.

**[ `-cifs-server` <`NetBIOS`> ] - CIFS Server NetBIOS Name**

If you specify this parameter, the command displays information only for CIFS servers that match the specified CIFS server NetBIOS name.

**[ `-domain-workgroup` <`CIFS domain`> ] - NetBIOS Domain/Workgroup Name**

If you specify this parameter, the command displays information only for CIFS servers that are in the specified NetBIOS domain or workgroup.

**[ `-domain` <`TextNoCase`> ] - Fully Qualified Domain Name**

If you specify this parameter, the command displays information only for CIFS servers that are in the specified domain.

**[ `-ou` <`text`> ] - Organizational Unit**

If you specify this parameter, the command displays information only for CIFS servers that are in the specified organizational unit.

**[ `-default-site` <`text`> ] - Default Site Used by LIFs Without Site Membership**

If you specify this parameter, the command displays information only for CIFS servers that have the specified default site.

**[ `-workgroup` <`NetBIOS`> ] - Workgroup Name**

If you specify this parameter, the command displays information only for CIFS servers that are in the specified workgroup.

**[ `-auth-style` { `domain` | `workgroup` | `realm` } ] - Authentication Style**

If you specify this parameter, the command displays information only for CIFS servers that match the specified authentication style.

**[ `-status-admin` { `down` | `up` } ] - CIFS Server Administrative Status**

If you specify this parameter, the command displays information only for CIFS servers that match the specified administrative status.

**[ `-comment` <`text`> ] - CIFS Server Description**

If you specify this parameter, the command displays information only for CIFS servers that match the specified comment field.

**[ `-netbios-aliases` <`NetBIOS`>, ... ] - List of NetBIOS Aliases**

If you specify this parameter, the command displays information only for CIFS servers that have specified NetBIOS alias.

## Examples

The following example displays a subset of the information about all CIFS servers:

```

cluster1::> vserver cifs show
Server      Domain/Workgroup
Vserver    Name      Name      Authentication Style
-----
vs1        CIFSSERVER1 EXAMPLE    domain

```

The following example displays all information about all CIFS-enabled Vservers in list form:

```

cluster1::> vserver cifs show -instance
Vserver: vs1
          CIFS Server NetBIOS Name: CIFSSERVER1
          NetBIOS Domain/Workgroup Name: EXAMPLE
          Fully Qualified Domain Name: EXAMPLE.COM
          Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
          Workgroup Name: -
          Authentication Style: domain
CIFS Server Administrative Status: up
CIFS Server Description:
List of NetBIOS Aliases: ALIAS_2, ALIAS_4,
ALIAS_6

```

The following example displays the NetBIOS aliases for the CIFS server CIFSSERVER1

```

cluster1::> cifs show -display-netbios-aliases
Vserver: vs1
Server Name: CIFSSERVER1
NetBIOS Aliases: ALIAS_2, ALIAS_4, ALIAS_6

```

## vserver cifs start

Start a CIFS server

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This command starts the CIFS server on the specified Vserver. The CIFS server must already exist. To create a CIFS server, run [vserver cifs create](#) .

### Parameters



### **-vserver <vserver name> - Vserver**

This parameter specifies a Vserver containing a configured CIFS server that has been stopped.

## Examples

The following example starts the CIFS server on Vserver vs1:

```
cluster1::> cifs start -vserver vs1
```

## Related Links

- [vserver cifs create](#)

## vserver cifs stop

Stop a CIFS server

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

This command stops the CIFS server on the specified Vserver.



Established sessions will be terminated and their open files closed. Workstations with cached data will not be able to save those changes, which could result in data loss.

## Parameters

### **-vserver <vserver name> - Vserver**

This parameter specifies a Vserver containing a configured CIFS server that is running.

## Examples

The following example stops the CIFS server on Vserver vs1:

```
cluster1::> cifs stop -vserver vs1
```

## vserver cifs branchcache create

Create the CIFS BranchCache service

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs branchcache create` command creates the configuration for computing and

retrieving BranchCache hash data. Only a single instance of the BranchCache service can be created on a Vserver.

## Parameters

### **-vserver <vserver name> - Vserver**

This parameter specifies the CIFS-enabled Vserver on which you want to set up the BranchCache service.

### **[-versions {v1-enable|v2-enable|enable-all}] - Supported BranchCache Versions**

This optional parameter specifies a list of versions of the BranchCache protocol that the storage system supports. The default is `enable-all`. This list can include one or more of the following:

- `v1-enable` - This option enables BranchCache Version 1.
- `v2-enable` - This option enables BranchCache Version 2.
- `enable-all` - This option enables all supported versions of BranchCache.

### **-hash-store-path <text> - Path to Hash Store**

This parameter specifies an existing directory into which the hash data is stored. Read-only paths, such as snapshot directories, are not allowed.

### **[-hash-store-max-size {<integer>[KB|MB|GB|TB|PB]}] - Maximum Size of the Hash Store**

This optional parameter specifies the maximum size to use for the hash data. If the size of the hash data exceeds this value, older hashes are deleted to make room for newer hashes. The default is 1 GB.

### **[-server-key <text>] - Encryption Key Used to Secure the Hashes**

This optional parameter specifies a server key that the BranchCache service uses to prevent clients from impersonating the BranchCache server.

### **[-operating-mode <BranchCache Mode>] - CIFS BranchCache Operating Modes**

This optional parameter specifies the mode in which the BranchCache service operates. The default is `per-share`. Possible values include:

- `disable` - This option disables the BranchCache service for the Vserver.
- `all-shares` - This option enables the BranchCache service for all the shares on this Vserver.
- `per-share` - This option enables the BranchCache service on a per-share basis. You can enable the BranchCache service on an existing share by adding the `branchcache` flag in the `-share -properties` parameter of the `vserver cifs share modify` command.

## Examples

The following example creates the BranchCache service on the Vserver named `vs1`. The path to the hash store is `/vs1_hash_store`.

```
cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path /vs1_hash_store
```

The following example creates the BranchCache service on the Vserver vs1. The path to the hash store is /vs\_hash\_store. The service is enabled on all the shares of the Vserver, supports BranchCache version 2, supports a maximum of 1 GB of BranchCache hashes, and secures the hashes using the key "vs1 secret".

```
cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path /vs1_hash_store -operating-mode all-shares -versions v2-enable -hash-store -max-size 1GB -server-key "vs1 secret"
```

## Related Links

- [vserver cifs share modify](#)

## vserver cifs branchcache delete

Stop and remove the CIFS BranchCache service

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs branchcache delete` command stops and removes the Vserver BranchCache configuration.

### Parameters

**-vserver <vserver name> - Vserver**

This parameter specifies the CIFS-enabled Vserver whose BranchCache configuration you want to remove.

**-flush-hashes {true|false} - Delete Existing Hashes**

This parameter specifies whether to keep or delete all existing hashes after deleting the BranchCache service.

### Examples

The following example stops and removes the BranchCache service on the Vserver vs1. It also deletes all existing hashes.

```
cluster1::> vserver cifs branchcache delete -flush-hashes true -vserver vs1
```

# vserver cifs branchcache hash-create

Force CIFS BranchCache hash generation for the specified path or file

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs branchcache hash-create` command causes the BranchCache service to compute hashes for a single file, for a directory, or for all the files in a directory structure if you specify the `-recurse` option.

## Parameters

**-vserver <vserver name> - Vserver**

This parameter specifies the CIFS-enabled Vserver on which the hash is computed.

**-path <text> - Path of File or Directory to Hash**

This parameter specifies the path of the directory or file for which hashes are to be computed. If a file is specified, the hashes are computed on the whole file. If a directory is specified, hashes are computed on all files within the directory.

**-recurse {true|false} - Process All Files in the Directory Recursively**

If this option is set to true and the `-path` parameter specifies a directory, hashes are computed recursively for all directories in the path.

## Examples

The following example creates hashes for the file "report.doc":

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path
/repository/report.doc -recurse false
```

The following example creates hashes for all the files in the directory "repository":

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path
/repository -recurse false
```

The following example recursively creates hashes for all the files and directories inside the directory "documents":

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path
/documents -recurse true
```

# vserver cifs branchcache hash-flush

Flush all generated BranchCache hashes

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs branchcache hash-flush` command deletes all hash data from the configured hash store.

## Parameters

**-vserver <vserver name> - Vserver**

This parameter specifies the CIFS-enabled Vserver whose hash data is to be deleted.

## Examples

The following example flushes all the hashes for Vserver vs1:

```
cluster1::> vserver cifs branchcache hash-flush -vserver vs1
```

# vserver cifs branchcache modify

Modify the CIFS BranchCache service settings

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs branchcache modify` command modifies the configuration for computing and retrieving BranchCache hash data.

## Parameters

**-vserver <vserver name> - Vserver**

This parameter specifies the CIFS-enabled Vserver whose BranchCache service is to be modified.

**[-versions {v1-enable|v2-enable|enable-all}] - Supported BranchCache Versions**

This optional parameter specifies a list of versions of the BranchCache protocol that the storage system supports. The default is `enable-all`. This list can include one or more of the following:

- `v1-enable` - This option enables BranchCache Version 1.
- `v2-enable` - This option enables BranchCache Version 2.
- `enable-all` - This option enables all supported versions of BranchCache.

### **[`-operating-mode <BranchCache Mode>`] - CIFS BranchCache Operating Modes**

This optional parameter specifies the mode in which the BranchCache service operates. The default is `per-share`. Possible values include:

- `disable` - This option disables the BranchCache service for the Vserver.
- `all-shares` - This option enables the BranchCache service for all the shares on this Vserver.
- `per-share` - This option enables the BranchCache service on a per-share basis. You can enable the BranchCache service on an existing share by adding the `branchcache` flag in the `-share -properties` parameter of the `vserver cifs share modify` command.

### **[`-hash-store-max-size {<integer>[KB|MB|GB|TB|PB]}`] - Maximum Size of the Hash Store**

This optional parameter specifies the maximum size to use for the hash data. If the size of the hash data exceeds this value, older hashes are deleted to make room for newer hashes. The default is 1 GB.

### **[`-flush-hashes {true|false}`] - Delete Existing Hashes**

This parameter specifies whether to keep or delete all the existing hashes. This must be set to `true` when modifying the server key.

### **[`-hash-store-path <text>`] - Path to Hash Store**

This parameter specifies an existing directory into which the hash data is stored. Read-only paths, such as snapshot directories, are not allowed.

### **[`-server-key <text>`] - Encryption Key Used to Secure the Hashes**

This optional parameter specifies a server key that the BranchCache service uses to prevent clients from impersonating the BranchCache server. If you specify this parameter, all existing hashes for the Vserver are deleted.

## **Examples**

The following example modifies the BranchCache service on the Vserver named `vs1`. The path to the hash store is `/vs1_hash_store_2`, the server key used to secure the hashes is set to "new vs1 secret", all existing hashes are removed, the service supports all BranchCache versions, and is enabled on a per-share basis.

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -hash-store-path
/vs1_hash_store_2 -server-key "new vs1 secret" -flush-hashes true
-versions enable-all -operating-mode per-share
```

The following example modifies the BranchCache service on the Vserver `vs1`. The service is enabled on all the shares of the Vserver, supports BranchCache version 1, and supports a maximum of 1 TB of BranchCache hashes.

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
all-shares -versions v1-enable -hash-store-max-size 1TB
```

## Related Links

- [vserver cifs share modify](#)

# vserver cifs branchcache show

Display the CIFS BranchCache service status and settings

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs branchcache show` command displays information about the BranchCache configuration for the Vserver. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information:

- Operating Mode
- Allowed Versions
- Maximum Size
- Path

You can specify additional parameters to display only information that matches those parameters.

## Parameters

**{ [-fields <fieldname>,...]**

If you specify the `-fields <fieldname>`, ... parameter, the command displays only the fields that you specify.

**| [-instance ] }**

If you specify the `-instance` parameter, the command displays detailed information about all entries.

**[-vserver <vserver name>] - Vserver**

If you specify this parameter, the command displays information for the specified Vserver.

**[-versions {v1-enable|v2-enable|enable-all}] - Supported BranchCache Versions**

If you specify this parameter, the command displays information for the Vservers that support the specified BranchCache versions.

**[-hash-store-path <text>] - Path to Hash Store**

If you specify this parameter, the command displays information for Vservers that store their hashes at the specified location.

**[-hash-store-max-size {<integer>[KB|MB|GB|TB|PB]}] - Maximum Size of the Hash Store**

If you specify this parameter, the command displays information for Vservers that have a maximum hash store size that is set to the specified value.

**[-server-key <text>] - Encryption Key Used to Secure the Hashes**

If you specify this parameter, the command displays information for Vservers that have the specified server key.

## **[`-operating-mode <BranchCache Mode>`] - CIFS BranchCache Operating Modes**

If you specify this parameter, the command displays information for Vservers whose BranchCache configuration operates in the specified mode.

### **Examples**

The following example displays a subset of the information about the BranchCache service in the cluster.

```
cluster1::> vserver cifs branchcache show
      Operating  Allowed      Max
Vserver  Mode        Versions    Size   Path
-----  -
vs1      per_share  enable_all  1GB  /hash_dir/
```

The following example displays all information about all the Vservers with BranchCache configurations.

```
cluster1::> vserver cifs show -instance
Vserver: vs1
      Supported Versions of BranchCache: enable_all
      Path to Hash Store: /hash_dir/
      Maximum Size of the Hash Store: 1GB
      Encryption Key Used to Secure the Hashes: asdad
      CIFS BranchCache Operating Modes: per_share
```

The following example displays information about BranchCache configurations that store the hash data at the location `/branchcache_hash_store`.

```
cluster1::> vserver cifs branchcache show -hash-store-path
/branchcache_hash_store
      Operating  Allowed      Max
Vserver  Mode        Versions    Size   Path
-----  -
vs1      per_share  enable_all  1GB  /branchcache_hash_store
```

## **vserver cifs cache name-to-sid delete-all**

Delete all the entries for the vserver

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.



## Description

The `vserver cifs cache name-to-sid delete-all` command removes all of the Windows user cache entries cached by the Windows name for the specified Vserver.

## Parameters

**-vserver <vserver name> - Vserver (privilege: advanced)**

Use this parameter to specify the Vserver for which the name-to-sid cache entries need to be deleted.

## Examples

The following example shows how to delete all of the cached name-to-sid entries for Vserver vs0:

```
cluster1::> vserver cifs cache name-to-sid delete-all -vserver vs0
```

## vserver cifs cache name-to-sid delete

Delete an entry

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

## Description

The `vserver cifs cache name-to-sid delete` command removes the Windows user cache entries cached by the Windows name. If cache propagation is enabled, the corresponding sid-to-name cache entry will also be removed.

## Parameters

**-vserver <vserver name> - Vserver (privilege: advanced)**

Use this parameter to specify the Vserver for which the name-to-sid cache entry needs to be deleted.

**-win-name <text> - Windows Name (privilege: advanced)**

Use this parameter to specify the Windows name for which the cached entry needs to be deleted.

## Examples

The following example shows how to delete the name-to-sid cache entry for Vserver vs0 with Windows name user1:

```
cluster1::> vserver cifs cache name-to-sid delete -vserver vs0 -win-name user1
```

# vserver cifs cache name-to-sid show

Display name-to-sid cache entries

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

## Description

The `vserver cifs cache name-to-sid show` command displays the Windows user information cached by Windows name.

## Parameters

{ [-fields <fieldname>,...]

If you specify the `-fields <fieldname>`, ... parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance ] }

Use this parameter to display detailed information about the Windows user entries cached by the Windows name.

[-vserver <vserver name>] - Vserver (privilege: advanced)

Use this parameter to specify the Vserver for which the Windows user entries that are cached by the Windows name need to be displayed.

[-win-name <text>] - Windows Name (privilege: advanced)

Use this parameter to specify the Windows name for which the cached entries need to be displayed.

[-sid <text>] - SID (privilege: advanced)

Use this parameter to display information only about the cached Windows user entries that have the specified security identifier (SID).

[-sid-type <integer>] - SID type (privilege: advanced)

Use this parameter to display information only about the cached Windows user entries that have the specified security identifier (SID) type.

[-flags <integer>] - Flags (privilege: advanced)

Use this parameter to display information only about the Windows user entries cached by the Windows name that have the specified flags.

[-domain-name <text>] - Domain Name (privilege: advanced)

Use this parameter to display information only about the Windows user entries cached by the Windows name that have the specified domain name.

[-create-time <MM/DD/YYYY HH:MM:SS>] - Create Time (privilege: advanced)

Use this parameter to display information only about the Windows user entries that were cached at the specified time.

**[`-source {none|files|dns|nis|ldap|netgrp_byname|dc}`] - Source of the Entry (privilege: advanced)**

Use this parameter to display information only about the user entries cached by the Windows name that have the specified lookup source.

## Examples

The following example shows how to display all of the Windows users which are cached by the Windows name:

```
cluster1::> vserver cifs cache name-to-sid show
```

The following example shows how to display all of the Windows user entries cached by the Windows name for Vserver vs0:

```
cluster1::> vserver cifs cache name-to-sid show -vserver vs0
```

## vserver cifs cache settings modify

### Modify CIFS Cache Configuration

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

### Description

The `vserver cifs cache settings modify` command modifies the Windows users cache configuration of the specified Vserver.

### Parameters

**`-vserver <vserver name>` - Vserver (privilege: advanced)**

Use this parameter to specify the Vserver for which the Windows users cache settings need to be modified.

**[`-is-enabled {true|false}`] - Is Cache Enabled? (privilege: advanced)**

Use this parameter to specify if the cache needs to be enabled for the Windows users database. The value *true* means the cache is enabled and the value *false* means the cache is disabled. The default value for this parameter is *false*.

**[`-is-negative-cache-enabled {true|false}`] - Is Negative Cache Enabled? (privilege: advanced)**

Use this parameter to specify if the cache needs to be enabled for the negative entries. Negative entries means the entries which are not present in the Windows users database and the look-up fails. The default value for this parameter is *true*. Negative cache is disabled by default if the parameter *is-enabled* is set to *false*.

**[`-ttl <[<integer>d] [<integer>h] [<integer>m] [<integer>s]>`] - Time to Live (privilege: advanced)**

Use this parameter to specify the time (in hours, minutes, and seconds) for which the positive entries need

to be cached. The positive entries means the entries which are present in the Windows users database and the look-up succeeds. The default value is 24 hours.

**[-negative-ttl <[<integer>d] [<integer>h] [<integer>m] [<integer>s]>] - Negative Time to Live (privilege: advanced)**

Use this parameter to specify the time (in hours, minutes, and seconds) for which the negative entries need to be cached. The default value is 5 minutes.

**[-is-propagation-enabled {true|false}] - Is Propagation Enabled? (privilege: advanced)**

Use this parameter to specify whether the cached user entries need to be propagated to the sid-to-name cache. The default value is *true*. Specify *false* to disable propagation.

## Examples

The following example shows how to modify the Windows users cache configuration settings for Vserver vs0:

```
cluster1::> vsserver cifs cache settings modify -vserver vs0 -ttl 600
-negative-ttl 300
```

The following example shows how to disable the Windows users cache for Vserver vs0:

```
cluster1::> vsserver cifs cache settings modify -vserver vs0 -is-enabled
false
```

## vserver cifs cache settings show

### Display CIFS Cache Configuration

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

### Description

The `vsserver cifs cache settings show` command displays information about the Windows users cache configuration of the specified Vserver.

### Parameters

{ [-fields <fieldname>,...]

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

| [-instance ] }

Use this parameter to display detailed information about the Windows users cache configuration settings.

**[-vserver <vserver name>] - Vserver (privilege: advanced)**

Use this parameter to display information about the Windows users cache configuration settings for the Vserver you specify.

### **[*-is-enabled* {*true*|*false*}] - Is Cache Enabled? (privilege: advanced)**

Use this parameter to display information only about the Windows users cache configuration settings that have the specified cache enabled setting. Value *true* displays only the entries that have cache enabled and value *false* displays only the entries that have cache disabled.

### **[*-is-negative-cache-enabled* {*true*|*false*}] - Is Negative Cache Enabled? (privilege: advanced)**

Use this parameter to display information only about the Windows users cache configuration settings that have the specified negative cache enabled setting. Value *true* displays only the entries that have negative cache enabled and value *false* displays only the entries that have negative cache disabled.

### **[*-ttl* <[<*integer*>*d*] [<*integer*>*h*] [<*integer*>*m*] [<*integer*>*s*]>] - Time to Live (privilege: advanced)**

Use this parameter to display information only about the Windows users cache configuration settings that have the specified Time to Live.

### **[*-negative-ttl* <[<*integer*>*d*] [<*integer*>*h*] [<*integer*>*m*] [<*integer*>*s*]>] - Negative Time to Live (privilege: advanced)**

Use this parameter to display information only about the Windows users cache configuration settings that have the specified negative Time to Live.

### **[*-is-propagation-enabled* {*true*|*false*}] - Is Propagation Enabled? (privilege: advanced)**

Use this parameter to display information only about the Windows users cache configuration settings that have the specified propagation enabled setting. Value *true* displays only the entries that have the propagation of cached entries to sid-to-name cache enabled and value *false* displays only the entries that have the propagation of cached entries to sid-to-name cache disabled.

## **Examples**

The following example shows how to display the Windows users cache configuration settings for all the Vservers:

```
cluster1::> vserver cifs cache settings show
```

The following example shows how to display the Windows users cache configuration settings for Vserver vs0:

```
cluster1::> vserver cifs cache settings show -vserver vs0
```

The following example shows how to display the Windows users cache configuration settings that have cache disabled:

```
cluster1::> vserver cifs cache settings show -is-enabled false
```

## **vserver cifs cache sid-to-name delete-all**

Delete all the entries for the vserver

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

## Description

The `vserver cifs cache sid-to-name delete-all` command removes all of the Windows user cache entries cached by the security identifier (SID) for the specified Vserver.

## Parameters

**-vserver <vserver name> - Vserver (privilege: advanced)**

Use this parameter to specify the Vserver for which the sid-to-name cache entries need to be deleted.

## Examples

The following example shows how to delete all the cached sid-to-name entries for Vserver vs0:

```
cluster1::> vserver cifs cache sid-to-name delete-all -vserver vs0
```

## vserver cifs cache sid-to-name delete

Delete an entry

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

## Description

The `vserver cifs cache sid-to-name delete` command removes the Windows user cache entries cached by security identifier (SID). If cache propagation is enabled, the corresponding name-to-sid cache entry will also be removed.

## Parameters

**-vserver <vserver name> - Vserver (privilege: advanced)**

Use this parameter to specify the Vserver for which the sid-to-name cache entry needs to be deleted.

**-sid <text> - SID (privilege: advanced)**

Use this parameter to specify the security identifier (SID) for which the cached entry needs to be deleted.

## Examples

The following example shows how to delete the sid-to-name cache entry for Vserver vs0 with SID S-1-5-21-1380078113-1824080971-954447143-1152:

```
cluster1::> vserver cifs cache sid-to-name delete -vserver vs0 -sid S-1-5-21-1380078113-1824080971-954447143-1152
```

# vserver cifs cache sid-to-name show

Display sid-to-name cache entries

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

## Description

The `vserver cifs cache sid-to-name show` command displays the Windows user information cached by security identifier (SID).

## Parameters

**{ [-fields <fieldname>,...]**

If you specify the `-fields <fieldname>`, ... parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

**| [-instance ] }**

Use this parameter to display detailed information about the Windows user entries cached by the security identifier (SID).

**[-vserver <vserver name>] - Vserver (privilege: advanced)**

Use this parameter to specify the Vserver for which the Windows user entries that are cached by the security identifier (SID) need to be displayed.

**[-sid <text>] - SID (privilege: advanced)**

Use this parameter to display information only about the cached Windows user entries that have the specified security identifier (SID).

**[-win-name <text>] - Windows Name (privilege: advanced)**

Use this parameter to specify the Windows name for which the cached entries need to be displayed.

**[-sid-type <integer>] - SID type (privilege: advanced)**

Use this parameter to display information only about the cached Windows user entries that have the specified security identifier (SID) type.

**[-sid-mode <integer>] - SID mode (privilege: advanced)**

Use this parameter to display information only about the cached Windows user entries that have the specified security identifier (SID) mode.

**[-flags <integer>] - Flags (privilege: advanced)**

Use this parameter to display information only about the Windows user entries cached by the security identifier (SID) that have the specified flags.

**[-domain-name <text>] - Domain Name (privilege: advanced)**

Use this parameter to display information only about the Windows user entries cached by the security identifier (SID) that have the specified domain name.

### **[`-create-time` <MM/DD/YYYY HH:MM:SS>] - Create Time (privilege: advanced)**

Use this parameter to display information only about the Windows user entries that were cached at the specified time.

### **[`-source` {`none`|`files`|`dns`|`nis`|`ldap`|`netgrp_byname`|`dc`}] - Source of the Entry (privilege: advanced)**

Use this parameter to display information only about the Windows user entries cached by the security identifier (SID) that have the specified lookup source.

## **Examples**

The following example shows how to display all of the Windows users which are cached by the security identifier (SID):

```
cluster1::> vserver cifs cache sid-to-name show
```

The following example shows how to display all of the Windows user entries cached by the security identifier (SID) for Vserver vs0:

```
cluster1::> vserver cifs cache sid-to-name show -vserver vs0
```

## **vserver cifs character-mapping create**

Create character mapping on a volume

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### **Description**

The `vserver cifs character-mapping create` command creates the CIFS character mapping for the specified volume on a particular Vserver.



Choose target characters in the "Private Use Area" of Unicode in the following range: U+E000... U+F8FF.



The target Unicode characters must not appear in existing file names; otherwise, unwanted character mappings would occur, resulting in clients being unable to access mapped files. For example, if ":" is mapped to "-" but "-" appears in files normally, a Windows client using the mapped share to access a file named "a-b" would have its request mapped to the NFS name "a:b", which is not the desired file.

The `vserver cifs character-mapping create` command is not supported for FlexGroups.

### **Parameters**



### **-vserver <vserver name> - Vserver**

This parameter specifies the Vserver on which a volume is located for which you are creating the character mapping. If only one data Vserver exists, you do not need to specify this parameter.

### **-volume <volume name> - Volume Name**

This parameter specifies the name of the volume for which you are creating the character mapping.

### **-mapping <text>,... - Character Mapping**

This parameter specifies the mapping of the invalid CIFS filename characters to valid CIFS filename characters. The mapping consists of a list of source-target character pairs separated by ":". The characters are Unicode characters entered using hexadecimal digits. For example: 3C:E03C.



The permissible Unicode character set for source mapping is: 0x01-0x19, 0x5C, 0x3A, 0x2A, 0x3F, 0x22, 0x3C, 0x3E, 0x7C, 0xB1.

## **Examples**

The following example creates a character mapping for a volume vol1 on Vserver vs1.

```
cluster1::> vserver cifs character-mapping create -volume vol1 -mapping
3c:e17c, 3e:f17d, 2a:f745
cluster1::> vserver cifs character-mapping show
```

Vserver	Volume Name	Character Mapping
vs1	vol1	3c:e17c, 3e:f17d, 2a:f745

## **vserver cifs character-mapping delete**

Delete character mapping on a volume

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### **Description**

The `vserver cifs character-mapping delete` command deletes the CIFS character mapping for the specified volume on a particular Vserver.

The `vserver cifs character-mapping delete` command is not supported for FlexGroups.

### **Parameters**

#### **-vserver <vserver name> - Vserver**

This parameter specifies the Vserver on which a Volume is located for which you are deleting the character mapping. If only one data Vserver exists, you do not need to specify this parameter.

### **-volume <volume name> - Volume Name**

This parameter specifies the name of the volume for which you are deleting the character mapping.

## Examples

The following example deletes all character mappings for a volume vol1 on Vserver vs1.

```
cluster1::> vserver cifs character-mapping delete -volume vol1
```

## vserver cifs character-mapping modify

Modify character mapping on a volume

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs character-mapping modify` command modifies the CIFS character mapping for the specified volume on a particular Vserver.

You can modify a particular volume's character mapping by specifying the following two parameters in the modify command:

- Vserver associated with the volume
- Name of the Volume



Choose target characters in the "Private Use Area" of Unicode in the following range: U+E000... U+F8FF.



The target Unicode characters must not appear in existing file names; otherwise, unwanted character mappings would occur, resulting in clients being unable to access mapped files. For example, if ":" is mapped to "-" but "-" appears in files normally, a Windows client using the mapped share to access a file named "a-b" would have its request mapped to the NFS name "a:b", which is not the desired file.

The `vserver cifs character-mapping modify` command is not supported for FlexGroups.

### Parameters

#### **-vserver <vserver name> - Vserver**

This parameter specifies the Vserver on which a Volume is located for which you are modifying the character mapping. If only one data Vserver exists, you do not need to specify this parameter.

#### **-volume <volume name> - Volume Name**

This parameter specifies the name of the volume for which you are modifying the character mapping.

## **[`-mapping <text>,...`] - Character Mapping**

This parameter specifies the mapping of the invalid CIFS filename characters to valid CIFS filename characters. The mapping consists of a list of source-target character pairs separated by ":". The characters are Unicode characters entered using hexadecimal digits. For example: 3C:E03C.



The permissible Unicode character set for source mapping is: 0x01-0x19, 0x5C, 0x3A, 0x2A, 0x3F, 0x22, 0x3C, 0x3E, 0x7C, 0xB1.

## **Examples**

The following example modifies a character mapping for a volume vol1 on Vserver vs1.

```
cluster1::> vserver cifs character-mapping modify -volume vol1 -mapping
3c:e17d, 3e:f17e, 2a:f746
cluster1::> vserver cifs character-mapping show
```

Vserver	Volume Name	Character Mapping
vs1	vol1	3c:e17d, 3e:f17e, 2a:f746

## **vserver cifs character-mapping show**

Display character mapping on volumes

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### **Description**

The `vserver cifs character-mapping show` command displays information about character mapping configured for volumes. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about character mapping configured for volumes:

- Vserver name
- Volume name
- Character mapping

### **Parameters**

**{ [`-fields <fieldname>,...`] }**

If you specify this parameter, the command displays only the fields that you specify.

**| [`-instance ]` }**

If you specify the `-instance` parameter, the command displays detailed information about all entries.

**[`-vserver <vserver name>`] - Vserver**

If you specify this parameter, the command displays information about character mapping configured for all

the volumes that belong to the specified Vserver.

#### **[`-volume <volume name>`] - Volume Name**

If you specify this parameter, the command displays information about the character mapping configured for all the volumes that match the specified volume name.

#### **[`-mapping <text>,...`] - Character Mapping**

If you specify this parameter, the command displays information about the character mapping configured for all volumes that match the specified mapping.

## Examples

The following example displays information about all character mappings configured for volumes

```
cluster1::> vserver cifs character-mapping show
```

Vserver	Volume Name	Character Mapping
vs1	vol1	3c:e17d, 3e:f17e

## vserver cifs connection show

Displays established CIFS connections

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs connection show` command displays information about established CIFS connections.

### Parameters

**{ [`-fields <fieldname>,...`] }**

Use this parameter to display only the specified fields

**[`-instance ]` }**

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[`-node {<nodename>|local}`] - Node**

Use this parameter to display information about CIFS connections on the specified node.

**[`-vserver <vserver name>`] - Vserver**

Use this parameter to display information about CIFS connections on the specified CIFS-enabled SVM.

**[`-connection-id <integer>`] - Connection ID**

Use this parameter to display information about CIFS connections that match the specified connection ID.

**[-session-id <integer>,...] - Session ID**

Use this parameter to display information about CIFS connections that match the specified session ID.

**[-workstation-ip <IP Address>] - Workstation IP Address**

Use this parameter to display information about CIFS connections that are established through the specified data LIF IP address.

**[-workstation-port <integer>] - Workstation Port Number**

Use this parameter to display information about CIFS connections that are opened from the specified Port number.

**[-lif-ip <IP Address>] - Incoming Data LIF IP Address**

Use this parameter to display information about CIFS connections that are opened from the specified IP address.

**[-network-context-id <integer>] - Network Context ID (privilege: advanced)**

Use this parameter to display information about CIFS connections that match the specified network context ID.

## Examples

The following example displays information about all CIFS connections:

```
cluster1::> vserver cifs connection show
Node:      node1
Vserver:   vs1
Connection Session
ID         IDs
-----
127834     1,2
Workstation
IP Port    LIF IP
-----
172.17.193.172 15536    10.53.50.42
```

The following example displays information about a CIFS connection at advanced privilege level:

```
cluster1::*> vserver cifs connection show
Node:      node1
Vserver:   vs1
Connection Session
Network
ID         IDs
-----
127834     1,2
Workstation
IP Port    LIF IP
-----
172.17.193.172 15536    10.53.50.42 2
Context ID
```

The following example displays information about a CIFS connection with session-id 1:

```
cluster1::~*> vserver cifs connection show -session-id 1 -instance

Vserver: vs1
Node: node1
        Connection ID: 127834
          Session ID: 1
            Workstation IP Address: 172.17.193.172
            Workstation Port Number: 15536
            Incoming Data LIF IP Address: 10.53.50.42
            Network Context ID: 2
```

## vserver cifs domain discovered-servers reset-servers

Reset and rediscover servers for a Vserver

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs domain discovered-servers reset-servers` command discards information the storage system has stored about domain controllers, LDAP, and NIS servers. After that, it begins the discovery process to reacquire current information about external servers.

### Parameters

**-vserver <vserver name> -Vserver**

This parameter specifies the name of the Vserver.

### Examples

The following is an example use of this command. It produces no output.

```
cluster1::> vserver cifs domain discovered-servers reset-servers

cluster1::>
```

## vserver cifs domain discovered-servers show

Display discovered server information

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs domain discovered-servers show` command displays information about the discovered servers for the CIFS domains of one or more Vservers. Server displays are grouped by node and

Vserver, and each group is preceded by the node and Vserver identification. Within each grouping, the server display is limited to those associated with the domain specified by the domain parameter, if it is present.

## Parameters

**{ [-fields <fieldname>,...]**

If you specify the `-fields <fieldname>`, ... parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

**| [-instance ] }**

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-node {<nodename>|local}] - Node**

If you use this parameter, the command only displays servers for the specified node.

**[-vserver <vserver name>] - Vserver**

If you use this parameter, the command only displays servers for the specified Vserver.

**[-domain <TextNoCase>] - Fully Qualified Domain Name**

If you use this parameter, the command only displays servers in the specified domain.

**[-type {Unknown|KERBEROS|MS-LDAP|MS-DC|LDAP}] - Server Type**

If you use this parameter, the command only displays servers of the specified type.

**[-name <text>] - Server Name**

If you use this parameter, the command only displays servers the with the specified name. This can result in multiple lines because the same server may provide multiple services.

**[-address <InetAddress>] - Server Address**

If you use this parameter, the command only displays servers with the specified IP address. This can result in multiple lines because the same server may provide multiple services.

**[-preference {unknown|preferred|favored|adequate}] - Preference**

If you use this parameter, the command only displays servers of the specified preference level.

**[-status {OK|unavailable|slow|expired|undetermined|unreachable}] - Status**

If you use this parameter, the command only displays servers of the specified status.

**[-dc-functional-level**

**{win2000|unknown|win2003|win2008|win2008r2|win2012|win2012r2|win2016|winthreshold  
}] - DC Functional Level**

If you use this parameter, the command only displays servers with the specified functional level.

**[-is-dc-read-only {true|false}] - Is DC Read Only**

If this parameter is set to true, the command only displays servers with read only domain controller. If set to false, the command only displays servers with writable domain controller.

## Examples

The following example display shows the information provided by this command.

```
cluster1::> vserver cifs domain discovered-servers show
```

```
Node: node1
```

```
Vserver: vs1
```

Domain Name	Type	Preference	DC-Name	DC-Address	Status
-----	-----	-----	-----	-----	-----
-----					
" "	NIS	preferred	192.168.10.222	192.168.10.222	OK
example.com	MS-LDAP	adequate	DC-1	192.168.192.24	OK
example.com	MS-LDAP	adequate	DC-2	192.168.192.25	OK
example.com	MS-DC	adequate	DC-1	192.168.192.24	OK
example.com	MS-DC	adequate	DC-2	192.168.192.25	OK

5 entries were displayed.

## vserver cifs domain discovered-servers discovery-mode modify

### Modify Server Discovery Mode

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

### Description

The `vserver cifs domain discovered-servers discovery-mode modify` command modifies the configuration for the server discovery mode of one or more Data Vservers. This option controls the way domain controllers(DCs) are discovered.

### Parameters

**-vserver <vserver name> - Vserver (privilege: advanced)**

Use this parameter to specify the Vserver for which you want to modify the server discovery mode.

**[-mode {all|site|none}] - Server Discovery Mode (privilege: advanced)**

Use this parameter to specify the server discovery mode for the Vserver. Following are the possible values for this parameter:

- all - Discover all the DCs in the domain, including the DCs local to the site. If trusted domains are present, then discover all the KDCs in the trusted domain as well, to be used for kerberos communication (default).
- site - Discover the DCs local to the site. If trusted domains are present, then discover KDCs local to the trusted domain site as well, to be used for kerberos communication.
- none - Discover nothing. Depend only on preferred-dc configured.



## Examples

The following example disables server discovery for a Vserver.

```
cluster1::*> vserver cifs domain discovered-servers discovery-mode modify
-vserver vs1 -mode none
```

## vserver cifs domain discovered-servers discovery-mode show

### Display Server Discovery Mode

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

### Description

The `vserver cifs domain discovered-servers discovery-mode show` command displays information about the discovery mode for domain controllers(DCs) of one or more Vservers.

### Parameters

**{ [-fields <fieldname>,...]**

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

**| [-instance ] }**

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver name>] - Vserver (privilege: advanced)**

If you use this parameter, the command only displays discovery mode for the specified Vserver.

**[-mode {all|site|none}] - Server Discovery Mode (privilege: advanced)**

If you use this parameter, the command only displays Vservers with the specified mode.

### Examples

The following example shows the server discovery mode for all Vservers.

```
cluster1::*> vserver cifs domain discovered-servers discovery-mode show
Vserver          Mode
-----
vs1              all
vs2              site
vs3              none
3 entries were displayed.
```

# vserver cifs domain name-mapping-search add

Add to the list of trusted domains for name-mapping

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs domain name-mapping-search add` command adds one or more trusted domains to the list of trusted domains to be used in preference to all others by the specified Vserver for looking up Windows user names when performing Windows user to UNIX user name-mapping. If a list already exists for the specified vserver, the new list is merged with the existing list. This command is not supported for workgroup CIFS servers.

## Parameters

**-vserver <vserver name> - Vserver**

This parameter specifies the name of the Vserver for which you want to add trusted domains.

**-trusted-domains <domain name>,... - Trusted Domains**

This parameter specifies a comma-delimited list of fully-qualified domain names of the trusted domains for the home domain.

## Examples

The following example adds two trusted domains (`cifs1.example.com` and `cifs2.example.com`) to the preferred list used by Vserver `vs1`:

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

# vserver cifs domain name-mapping-search modify

Modify the list of trusted domains for name-mapping search

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs domain name-mapping-search modify` command modifies the current list of trusted domains to be used in preference to all others by the specified Vserver to lookup Windows user names when performing Windows user to UNIX user name-mapping. The new list overwrites the existing list. This command is not supported for workgroup CIFS servers.

## Parameters

**-vserver <vserver name> - Vserver**

This parameter specifies the name of the Vserver for which you want to modify the trusted domain list.

### **-trusted-domains <domain name>,... - Trusted Domains**

This parameter specifies a comma-delimited list of fully qualified domain names of the trusted domains of the home domain.

## **Examples**

The following example modifies the trusted domain list used by Vserver vs1:

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1
-trusted-domains cifs3.example.com
```

## **vserver cifs domain name-mapping-search remove**

Remove from the list of trusted domains for name-mapping search

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## **Description**

The `vserver cifs domain name-mapping-search remove` command removes one or more trusted domains from the list used by the specified Vserver to lookup Windows user names when performing Windows user to UNIX user name-mapping. If a list of trusted domains is not provided, the entire trusted domain list for the specified Vserver is removed. This command is not supported for workgroup CIFS servers.

## **Parameters**

### **-vserver <vserver name> - Vserver**

This parameter specifies the name of the Vserver from which you want to remove trusted domains.

### **[-trusted-domains <domain name>,...] - Trusted Domains**

This parameter specifies a comma-delimited list of trusted domains of the home domain.

## **Examples**

The following example removes two trusted domains from the list used by Vserver vs1:

```
cluster1::> vserver cifs domain name-mapping-search remove -trusted
-domains cifs1.example.com, cifs2.example.com
```

## **vserver cifs domain name-mapping-search show**

Display the list of trusted domains for name-mapping searches

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs domain name-mapping-search show` command displays information about trusted domains of the home domain by Vserver.

## Parameters

**{ [-fields <fieldname>,...]**

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

**| [-instance ] }**

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver name>] - Vserver**

This parameter specifies the name of the Vserver for which you want to display information about the trusted domains.

**[-trusted-domains <domain name>,...] - Trusted domains**

This parameter specifies a comma-delimited list of fully qualified domain names of trusted domains for which you want to display information.

## Examples

The following example displays information about all preferred trusted domains:

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver           Trusted Domains
-----
vserver_1         CIFS1.EXAMPLE.COM
```

## vserver cifs domain password change

Generate a new password for the CIFS server's machine account and change it in the Windows Active Directory domain.

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs domain password change` changes the domain account password for a CIFS server. This command is not supported for workgroup CIFS servers.

## Parameters

**-vserver <vserver name> - Vserver**

This parameter specifies the name of the Vserver for whose CIFS server you want to change the domain account password.

## Examples

The following example changes the password for the CIFS server on a Vserver named vs1.

```
cluster1::> vserver cifs domain password change -vserver vs1

cluster1::>
```

## vserver cifs domain password reset

Reset the CIFS server's machine account password in the Windows Active Directory domain.

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs domain password reset` command resets the domain account password for a CIFS server. This may be required if the password stored along with the machine account in the Windows Active Directory domain is changed or reset without the Vserver's knowledge. The operation requires the credentials for a user with permission to reset the password in the organizational unit (OU) that the machine account is a member of. This command is not supported for workgroup CIFS servers.

### Parameters

**-vserver <vserver name> -Vserver**

This parameter specifies the name of the Vserver for whose CIFS server you want to reset the domain account password.

## Examples

The following example resets the password for the CIFS server on a Vserver named vs1.

```
cluster1::> vserver cifs domain password reset -vserver vs1

Enter your user ID: Administrator
Enter your password:

cluster1::>
```

## vserver cifs domain password schedule modify

Modify the domain account password change schedule

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs domain password schedule modify` command enables you to modify a domain account password change schedule for a CIFS server. This command is not supported for workgroup CIFS servers.

## Parameters

### **-vserver <vserver name> - Vserver**

This specifies the name of the Vserver containing the CIFS server for which you want to change the domain account password.

### **[-is-schedule-enabled {true|false}] - Is Password Change Schedule Enabled**

This specifies whether the domain account password change schedule is enabled.

### **[-schedule-weekly-interval <integer>] - Interval in Weeks for Password Change Schedule**

This specifies the number of weeks after which the scheduled domain account password change must occur.

### **[-schedule-randomized-minute <integer>] - Minutes Within Which Schedule Start Can be Randomized**

This specifies the minutes within which the scheduled domain account password change must begin.

### **[-schedule-day-of-week <cron\_dayofweek>] - Day of Week for Password Change Schedule**

This sets the day of week when the scheduled domain account password change occurs.

### **[-schedule-time-of-day <HH:MM:SS>] - Start Time for Password Change Schedule**

This sets the time in HH:MM:SS at which the scheduled domain account password change starts.

## Examples

The following example enables the domain account password change schedule and configures it to run at any time between 23:00:00 to 00:59:00 (one hour before midnight to one hour after midnight) on every 4th Sunday.

```
cluster1::> vserver cifs domain password schedule modify -is-schedule
-enabled true -schedule-randomized-minute 120 -schedule-weekly-interval 4
-schedule-time-of-day 23:00:00 -schedule-day-of-week sunday
```

## vserver cifs domain password schedule show

Display the domain account password change schedule

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs domain password schedule show` command displays the domain account password change schedule configuration. It displays the following fields:

- Vserver: Vserver for which the schedule is configured
- Schedule Enabled: Whether the schedule is enabled or disabled for this Vserver
- Schedule Interval: Weeks after which the password change schedule occurs again for this Vserver
- Schedule Randomized Within: Minutes within which the schedule must begin for this Vserver
- Schedule: Password change schedule currently set on this Vserver
- Last Successful Password Change/Reset Time: Time at which the last password change or reset happened successfully on this Vserver
- Warning: Warning message, applicable only when the change password job is deleted with the feature still enabled on this Vserver

## Parameters

**{ [-fields <fieldname>,...]**

If you specify the `-fields <fieldname>`, ... parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

**| [-instance ] }**

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver name>] - Vserver**

If you specify this parameter, the command displays information for the specified Vserver.

**[-is-schedule-enabled {true|false}] - Is Password Change Schedule Enabled**

If you specify this parameter, the command displays information for all the Vservers on which the `is-schedule-enabled` value applies.

**[-schedule-weekly-interval <integer>] - Interval in Weeks for Password Change Schedule**

If you specify this parameter, the command displays information for all the Vservers on which the `schedule-weekly-interval` value applies.

**[-schedule-randomized-minute <integer>] - Minutes Within Which Schedule Start Can be Randomized**

If you specify this parameter, the command displays information for all the Vservers on which the `schedule-randomized-minute` value applies.

**[-schedule-last-changed <text>] - Last Successful Password Change/Reset Time**

If you specify this parameter, the command displays information for all the Vservers on which the `schedule-last-changed` value applies.

**[-schedule-description <text>] - Schedule Description**

If you specify this parameter, the command displays information for all the Vservers on which the `schedule-description` value applies.

**[-schedule-warn-msg <text>] - Warning Message in Case Job Is Deleted**

If you specify this parameter, the command displays information for all the Vservers on which the `schedule-warn-msg` value applies.

## Examples

The following example shows the domain account password change schedule configuration when the password change feature is enabled for Vserver vs1.

```
cluster1::> vserver cifs domain password schedule show
Vserver: vs1
Schedule Enabled: true
      Schedule Interval: 4   week
Schedule Randomized Within: 120 min
      Schedule: Fri@23:00
      Last Changed At: Thu Apr  4 02:35:23 2013
```

The following example shows the domain account password change schedule configuration when the password change job has been accidentally deleted.

```
cluster1::> vserver cifs domain password schedule show
Vserver: vs1
Schedule Enabled: true
      Schedule Interval: 4   week
Schedule Randomized Within: 120 min
      Schedule: Fri@23:00
      Last Changed At: Thu Apr  4 02:35:23 2013
      Warning: Password change job was deleted. Re-enable
the password change schedule.
```

## vserver cifs domain preferred-dc add

Add to a list of preferred domain controllers

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs domain preferred-dc add` command adds one or more domain controllers to be used in preference to all others by the specified Vserver for interactions with the specified domain. If a list already exists for the specified domain, the new list is merged with the existing list. This command is not supported for workgroup CIFS servers.



Each Vserver discovers domain controllers and attempts to sort them internally based on real-world performance. Therefore it should not be necessary to create a preferred list of domain controllers under most circumstances.

### Parameters



### **-vserver <vserver name> - Vserver**

This parameter specifies the name of the Vserver for which you want to add preferred domain controllers.

### **-domain <TextNoCase> - Fully Qualified Domain Name**

This parameter specifies the fully-qualified name of the domain that the domain controllers belong to.

### **-preferred-dc <InetAddress>, ... - Preferred Domain Controllers**

This parameter specifies a comma-delimited list of IP addresses for domain controllers that belong to the domain specified in the `-domain` parameter.

### **[`-skip-config-validation {true|false}`] - Skip Configuration Validation**

Use this parameter to skip the Preferred-DC configuration validation.

The hosts specified with the `-DC-servers` parameter are validated to verify that each of the DC servers are reachable, and is providing NETLOGON services.

The validation fails if there is no valid Preferred-DC server.

## Examples

The following example adds two domain controllers (192.168.0.100 and 192.168.0.101) to the preferred list used by Vserver `vs1` when connecting to the `example.com` domain:

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain
example.com -preferred-dc 192.168.0.100,192.168.0.101
```

## vserver cifs domain preferred-dc check

Display validation status of the Preferred-DC configuration

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

Use the `vserver cifs domain preferred-dc check` command to check the status of configured preferred DC on a particular vserver.

### Parameters

**{ [`-fields <fieldname>`, ... ] }**

If you specify the `-fields <fieldname>`, ... parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

**| [`-instance` ] }**

If you specify the `-instance` parameter, the command displays detailed information about all fields.

### **-vserver <vserver> - Vserver**

Use this parameter to specify the Vserver whose preferred DC needs to be validated.

### **[-server-ip <text>,...] - DC Address**

Use this parameter to display IP-address of the configured CIFS Preferred-DC servers.

### **[-domain <TextNoCase>,...] - Domain Name**

Use this parameter to display Domain name of the configured CIFS Preferred-DCs.

### **[-status {down|up}] - DC Status**

Use this parameter to display information only about CIFS Preferred-DC servers with a status that matches the value you specify.

### **[-status-details <text>,...] - Status Details**

Use this parameter to display information only about CIFS Preferred-DC servers with status details that match the value you specify.

## **Examples**

The following example checks the connectivity of preferred DC on vserver vs0.

```
cluster1::> vserver cifs domain preferred-dc check -vserver vs0

Vserver : vs0

Domain Name          DC Address          Status          Status Details
-----
example.com          1.1.1.1             up              Response time
(msec): 426
example.com          1.1.1.2             up              Response time
(msec): 425
example1.com         2.2.2.2             up              Response time
(msec): 423
example2.com         3.3.3.3             up              Response time
(msec): 422
```

## **vserver cifs domain preferred-dc remove**

Remove from a list of preferred domain controllers

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### **Description**

The `vserver cifs domain preferred-dc remove` command removes one or more domain controllers from the list used by the specified Vserver for interactions with the specified domain. If a list of preferred domain controllers is not provided, the entire list for the specified domain is removed. This command is not supported for workgroup CIFS servers.

## Parameters

### **-vserver <vserver name> - Vserver**

This parameter specifies the name of the Vserver from which you want to remove preferred domain controllers.

### **-domain <TextNoCase> - Fully Qualified Domain Name**

This parameter specifies the fully-qualified name of the domain that the domain controllers belong to.

### **[-preferred-dc <InetAddress>, ...] - Preferred Domain Controllers**

This parameter specifies a comma-delimited list of IP addresses for domain controllers that belong to the domain specified in the `-domain` parameter.

## Examples

The following example removes one domain controller (192.168.0.101) from the preferred list used by Vserver `vs1` when connecting to the `example.com` domain:

```
cluster1::> vserver cifs domain preferred-dc remove -vserver vs1 -domain
example.com -preferred-dc 192.168.0.101
```

## vserver cifs domain preferred-dc show

Display a list of preferred domain controllers

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs domain preferred-dc show` command displays lists of preferred domain controllers by Vserver and domain.

## Parameters

### **{ [-fields <fieldname>, ...]**

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

### **| [-instance ] }**

If you specify the `-instance` parameter, the command displays detailed information about all fields.

### **[-vserver <vserver name>] - Vserver**

This parameter specifies the name of the Vserver for which you want to display preferred domain controllers.

### **[-domain <TextNoCase>] - Fully Qualified Domain Name**

This parameter specifies the fully-qualified name of the domain of the domain controllers to display.

## **[`-preferred-dc <InetAddress>,...`] - Preferred Domain Controllers**

This parameter specifies a comma-delimited list of IP addresses for domain controllers to display.

### **Examples**

The following example displays all preferred domain controllers for all Vservers:

```
cluster1::> vservers cifs domain preferred-dc show
Vserver          Domain Name          Preferred Domain Controllers
-----
vs1              example.com          192.168.0.100, 192.168.0.101
```

## **vservers cifs domain trusts rediscover**

Reset and rediscover trusted domains for a Vserver

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### **Description**

The `vservers cifs domain trusts rediscover` command discards information the Vserver has stored about trusted domains. After that, it begins the discovery process to reacquire current information about trusted domains. This command is not supported for workgroup CIFS servers.

### **Parameters**

**`-vservers <vservers name>` - Vserver**

This parameter specifies the name of the Vserver.

### **Examples**

The following example rediscovered trusted domains. It produces no output.

```
cluster1::> vservers cifs domain trusts rediscover
```

## **vservers cifs domain trusts show**

Display discovered trusted domain information

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### **Description**

The `vservers cifs domain trusts show` command displays information about the trusted domains for the CIFS home domain of one or more Vservers. The displayed trusted domain information is grouped by node

and Vserver, and each group is preceded by the node and Vserver identification. This command is not supported for workgroup CIFS servers.

## Parameters

**{ [-fields <fieldname>,...]**

If you specify the `-fields <fieldname>`, ... parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

**| [-instance ] }**

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-node {<nodename>|local}] - Node**

If you use this parameter, the command displays information only about trusted domains of the home domains for the specified node.

**[-vserver <vserver name>] - Vserver**

If you use this parameter, the command displays information only about trusted domains of the home domain for the specified Vserver.

**[-home-domain <domain name>] - Home Domain Name**

If you use this parameter, the command displays information only about trusted domains of the home domain with the specified name.

**[-trusted-domain <domain name>,...] - Trusted Domain Name**

If you use this parameter, the command displays information only about trusted domains with the specified name.

## Examples

The following example displays information about all the bidirectional trusted domains for `node-01` and `vserver_1`.

```
cluster1::> vserver cifs domain trusts show -node node-01 -vserver
vserver_1
Node: node-01
Vserver: vserver_1

Home Domain                Trusted Domain
-----
EXAMPLE.COM                CIFS1.EXAMPLE.COM,
                           CIFS2.EXAMPLE.COM
```

## vserver cifs group-policy modify

Change group policy configuration

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs group-policy modify` command modifies the group policy configuration of a CIFS server. This command is not supported for workgroup CIFS servers.

## Parameters

### **-vserver <vserver name> - Vserver**

This parameter specifies the Vserver whose group policy configuration you want to modify.

### **[-status {enabled|disabled}] - Group Policy Status**

This parameter specifies whether the CIFS-enabled Vserver's group policy is enabled or disabled.

## Examples

The following example enables the group policy for CIFS-enabled Vserver `vs1`.

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

## vserver cifs group-policy show-applied

Show currently applied group policy setting

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Parameters

### **{ [-fields <fieldname>, ...]**

If you specify the `-fields <fieldname>`, ... parameter, the command only displays the fields that you specify.

### **| [-instance ] }**

If you specify the `-instance` parameter, the command displays detailed information about all entries.

### **[-vserver <vserver name>] - Vserver**

If you specify this parameter, the command displays only group policy information that has been applied to the Vserver you specify.

### **[-gpo-index <integer>] - GPO Index**

If you specify this parameter, the command displays only group policy information at `gpo-index`.

## Examples

The following example displays all group policy information about all group policies that have been applied to a Vserver:

```
cluster1::> vserver cifs group-policy show-applied
```

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:  
    /voll/home  
    /voll/dirl  
  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:
    /voll/home
    /voll/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
2 entries were displayed.
```

## vserver cifs group-policy show-defined

Show applicable group policy settings defined in Active Directory

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.



## Parameters

**{ [-fields <fieldname>,...]**

If you specify the -fields <fieldname>, ... parameter, the command only displays the fields that you specify.

**| [-instance ] }**

If you specify the -instance parameter, the command displays detailed information about all entries.

**[-vserver <vserver name>] - Vserver**

If you specify this parameter, the command displays only group policy information that has been defined in Active Directory for the Vserver that you specify.

**[-gpo-index <integer>] - GPO Index**

If you specify this parameter, the command displays only group policy information at gpo-index.

## Examples

The following example displays all group policy information for all group policies that have been defined in Active Directory:

```
cluster1::> vserver cifs group-policy show-defined

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:
    /voll/home
    /voll/dirl
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
```

## vserver cifs group-policy show

Show group policy configuration

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs group-policy show` command displays information about group policy configuration for CIFS-enabled Vserver. It displays all or a subset of the group policy configuration matching the criteria that you specify.

### Parameters

**{ [-fields <fieldname>,...]**

If you specify the `-fields <fieldname>`, ... parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

**| [-instance ] }**

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver name>] - Vserver**

If you specify this parameter, the command displays group policy configuration only for the Vserver that you specify.

**[-status {enabled|disabled}] - Group Policy Status**

If you specify this parameter, the command displays group policy configuration only for the Vservers that match the status you specify.

### Examples

The following example displays group policy configuration for all Vservers:

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

Vserver	GPO Status
vs1	disabled

## vserver cifs group-policy update

Apply group policy settings defined in Active Directory

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs group-policy update` command applies the group-policy settings defined in Active Directory for the given Vserver. This command is not supported for workgroup CIFS servers.

### Parameters

**-vserver <vserver name> - Vserver Name**

This parameter specifies the CIFS-enabled Vserver to which the group-policy settings be applied.

**[-force-reapply-all-settings {true|false}] - Force Re-apply All Settings**

This parameter specifies whether to ignore all processing optimizations and re-apply all settings. The default is false.

### Examples

The following example applies the group-policy settings defined in Active Directory for Vserver vs1.

```
cluster1::> vserver cifs group-policy update -vserver vs1 -force-reapply  
-all-settings true
```

## vserver cifs group-policy central-access-policy show-applied

Show currently applied central access policies

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs group-policy central-access-policy show-applied` command displays information about the central access policies assigned to Vservers. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all CIFS servers:

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

## Parameters

**{ [-fields <fieldname>,...]**

If you specify the -fields <fieldname>, ... parameter, the command only displays the fields that you specify.

**| [-instance ] }**

If you specify the -instance parameter, the command displays detailed information about all entries.

**[-vserver <vserver name>] - Vserver**

If you specify this parameter, the command displays information only for central access policies for the specified Vserver.

**[-name <TextNoCase>] - Name**

If you specify this parameter, the command displays information only for central access policies that match the specified name.

**[-sid <windows sid>] - Identifier**

If you specify this parameter, the command displays information only for central access policies that match the specified SID.

**[-description <text>] - Description**

If you specify this parameter, the command displays information only for central access policies that match the specified description.

**[-ctime <Date>] - Creation Time**

If you specify this parameter, the command displays information only for central access policies that match the specified creation time.

**[-mtime <Date>] - Modification Time**

If you specify this parameter, the command displays information only for central access policies that match the specified modification time.

**[-rules <TextNoCase>,...] - Central Access Rules**

If you specify this parameter, the command displays information only for central access policies that match the specified member rules.

## Examples

The following example displays information for all central access policies:

```

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

2 entries were displayed.

```

## vserver cifs group-policy central-access-policy show-defined

Show applicable central access policies defined in the Active Directory

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs group-policy central-access-policy show-defined` command displays information about the central access policies that are defined in the Active Directory. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all CIFS servers:

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

## Parameters

**{ [-fields <fieldname>,...]**

If you specify the -fields <fieldname>, ... parameter, the command only displays the fields that you specify.

**| [-instance ] }**

If you specify the -instance parameter, the command displays detailed information about all entries.

**[-vserver <vserver name>] - Vserver**

If you specify this parameter, the command displays information only for central access policies for the specified Vserver.

**[-name <TextNoCase>] - Name**

If you specify this parameter, the command displays information only for central access policies that match the specified name.

**[-sid <windows sid>] - Identifier**

If you specify this parameter, the command displays information only for central access policies that match the specified SID.

**[-description <text>] - Description**

If you specify this parameter, the command displays information only for central access policies that match the specified description.

**[-ctime <Date>] - Creation Time**

If you specify this parameter, the command displays information only for central access policies that match the specified creation time.

**[-mtime <Date>] - Modification Time**

If you specify this parameter, the command displays information only for central access policies that match the specified modification time.

**[-rules <TextNoCase>,...] - Central Access Rules**

If you specify this parameter, the command displays information only for central access policies that match the specified member rules.

## Examples

The following example displays information for all central access policies:

```
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
```

```
2 entries were displayed.
```

## vserver cifs group-policy central-access-rule show-applied

Show currently applied central access rules

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs group-policy central-access-rule show-applied` command displays information about the central access rules assigned to Vservers. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all CIFS servers:

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



## Parameters

**{ [-fields <fieldname>,...]**

If you specify the -fields <fieldname>, ... parameter, the command only displays the fields that you specify.

**| [-instance ] }**

If you specify the -instance parameter, the command displays detailed information about all entries.

**[-vserver <vserver name>] - Vserver**

If you specify this parameter, the command displays information only for central access rules for the specified Vserver.

**[-name <TextNoCase>] - Name**

If you specify this parameter, the command displays information only for central access rules that match the specified name.

**[-description <text>] - Description**

If you specify this parameter, the command displays information only for central access rules that match the specified description.

**[-ctime <Date>] - Creation Time**

If you specify this parameter, the command displays information only for central access rules that match the specified creation time.

**[-mtime <Date>] - Modification Time**

If you specify this parameter, the command displays information only for central access rules that match the specified modification time.

**[-effective <text>] - Effective Security Policy**

If you specify this parameter, the command displays information only for central access rules that match the specified effective security policy.

**[-proposed <text>] - Proposed Security Policy**

If you specify this parameter, the command displays information only for central access rules that match the specified proposed security policy.

**[-resource <text>] - Resource Condition**

If you specify this parameter, the command displays information only for central access rules that match the specified resource condition.

## Examples

The following example displays information for all central access rules:

```

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)

2 entries were displayed.

```

## vserver cifs group-policy central-access-rule show-defined

Show applicable central access rules defined in the Active Directory

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs group-policy central-access-rule show-defined` command displays information about the central access rules that are defined in the Active Directory. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all CIFS servers:

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

## Parameters

**{ [-fields <fieldname>,...]**

If you specify the -fields <fieldname>, ... parameter, the command only displays the fields that you specify.

**| [-instance ] }**

If you specify the -instance parameter, the command displays detailed information about all entries.

**[-vserver <vserver name>] - Vserver**

If you specify this parameter, the command displays information only for central access rules for the specified Vserver.

**[-name <TextNoCase>] - Name**

If you specify this parameter, the command displays information only for central access rules that match the specified name.

**[-description <text>] - Description**

If you specify this parameter, the command displays information only for central access rules that match the specified description.

**[-ctime <Date>] - Creation Time**

If you specify this parameter, the command displays information only for central access rules that match the specified creation time.

**[-mtime <Date>] - Modification Time**

If you specify this parameter, the command displays information only for central access rules that match the specified modification time.

**[-effective <text>] - Effective Security Policy**

If you specify this parameter, the command displays information only for central access rules that match the specified effective security policy.

**[-proposed <text>] - Proposed Security Policy**

If you specify this parameter, the command displays information only for central access rules that match the specified proposed security policy.

**[-resource <text>] - Resource Condition**

If you specify this parameter, the command displays information only for central access rules that match the specified resource condition.

## Examples

The following example displays information for all central access rules:

```

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)

2 entries were displayed.

```

## vserver cifs group-policy restricted-group show-applied

Show the applied restricted-group settings.

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs group-policy restricted-group show-applied` command displays settings of all the restricted groups applied to a Vserver.

If you do not specify any parameters, the command displays the following information about all the restricted groups applied to all the Vservers in the cluster.

- Group Policy Name: Specifies the name of the group policy.
- Version: Specifies the version of the group policy.
- Link: Specifies the level in which the group policy is configured. Possible values are:
  - Local: Group policy is configured in Data ONTAP.
  - Site: Group policy is configured at the site level in the Domain Controller.
  - Domain: Group policy is configured at the domain level in the Domain Controller.
  - OrganizationalUnit: Group policy is configured at the OU level in the Domain controller.
- RSOP: Resultant set of policies derived from all the group policies defined at various levels.
- Group Name: Specifies the name of a restricted group.
- Members: Specifies users and groups who belong to and who do not belong to the restricted group.

- **MemberOf**: Specifies list of groups to which the restricted group is added. A group can be a member of groups other than the groups listed here.

## Parameters

**{ [-fields <fieldname>,...]**

If you specify the `-fields <fieldname>`, ... parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

**| [-instance ] }**

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver name>] - Vserver**

If this parameter is specified, the command displays the restricted-group information that has been applied to the specified Vserver.

**[-index <integer>] - Index**

If this parameter is specified, the command displays the specified index for the group policy in the restricted group. The restricted-group information for the group policy at the specified index.

**[-group-name <text>] - Group Name**

If this parameter is specified, the command displays the restricted-group information for the specified group name.

**[-group-policy-name <text>] - Group Policy Name**

If this parameter is specified, the command displays the restricted-group information for the specified group policy name.

**[-uuid <UUID>] - UUID**

If this parameter is specified, the command displays the restricted-group information for the specified UUID of the group policy.

**[-version <integer>] - Version**

If this parameter is specified, the command displays the restricted-group information for the specified version of the group policy.

**[-link <gpo-link>] - Link Type**

If this parameter is specified, the command displays the restricted-group information for the specified link for the group policy.

**[-members <gpoUserGroup>,...] - Members, List of Users/groups**

If this parameter is specified, the command displays the restricted-group information for the specified members of users and groups.

**[-member-of <gpoUserGroup>,...] - MemberOf, List of Groups**

If this parameter is specified, the command displays the restricted-group information for the specified member of the group.

## Examples

The following example displays information about all restricted groups that have been applied to a Vserver.

```
cluster1::> vserver cifs group-policy restricted-group show-applied

Vserver: vs_1
-----

    Group Policy Name: gp01
          Version: 16
          Link: OrganizationalUnit
    Group Name: grp1
          Members: usr1
          MemberOf: GPO\g9
Group Policy Name: Resultant Set of Policy
          Version: 0
          Link: RSOP
    Group Name: grp1
          Members: usr1
          MemberOf: GPO\g9
```

## vserver cifs group-policy restricted-group show-defined

Show the defined restricted-group settings.

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs group-policy restricted-group show-defined` command displays settings of all the restricted groups defined in Domain Controller for a Vserver.

If you do not specify any parameters, the command displays the following information about all the restricted groups defined in Domain Controller for all the Vservers in the cluster.

- Group Policy Name: Specifies the name of the group policy.
- Version: Specifies the version of the group policy.
- Link: Specifies the level in which the group policy is configured. Possible values are:
  - Local: Group policy is configured in Data ONTAP.
  - Site: Group policy is configured at the site level in the Domain Controller.
  - Domain: Group policy is configured at the domain level in the Domain Controller.
  - OrganizationalUnit: Group policy is configured at the OU level in the Domain Controller.
  - RSOP: Resultant set of policies derived from all the group policies defined at various levels.
- Group Name: Specifies the name of a restricted group.

- **Members:** Specifies users and groups who belong to and who do not belong to the restricted group.
- **MemberOf:** Specifies list of groups to which the restricted group is added. A group can be a member of groups other than the groups listed here.

## Parameters

**{ [-fields <fieldname>,...]**

If you specify the `-fields <fieldname>`, ... parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

**| [-instance ] }**

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver name>] - Vserver**

If this parameter is specified, the command displays the restricted-group information that is defined in Domain Controller for the specified Vserver.

**[-index <integer>] - Index**

If this parameter is specified, the command displays the specified index for the group policy in the restricted group. The restricted-group information for the group policy at the specified index.

**[-group-name <text>] - Group Name**

If this parameter is specified, the command displays the restricted-group information for the specified group name.

**[-group-policy-name <text>] - Group Policy Name**

If this parameter is specified, the command displays the restricted-group information for the specified group policy name.

**[-uuid <UUID>] - UUID**

If this parameter is specified, the command displays the restricted-group information for the specified UUID of the group policy.

**[-version <integer>] - Version**

If this parameter is specified, the command displays the restricted-group information for the specified version of the group policy.

**[-link <gpo-link>] - Link Type**

If this parameter is specified, the command displays the restricted-group information for the specified link for the group policy.

**[-members <gpoUserGroup>,...] - Members, List of Users/groups**

If this parameter is specified, the command displays the restricted-group information for the specified members of users and groups.

**[-member-of <gpoUserGroup>,...] - MemberOf, List of Groups**

If this parameter is specified, the command displays the restricted-group information for the specified member of the group.

## Examples

The following example displays information about all restricted groups that are defined in Domain Controller for a Vserver.

```
cluster1::> vsserver cifs group-policy restricted-group show-defined

Vserver: vs_1
-----

      Group Policy Name: gp01
            Version: 16
            Link: OrganizationalUnit
      Group Name: grp1
            Members: usr1
            MemberOf: GPO\g9
Group Policy Name: Resultant Set of Policy
            Version: 0
            Link: RSOP
      Group Name: grp1
            Members: usr1
            MemberOf: GPO\g9
```

## vsserver cifs home-directory modify

Modify attributes of CIFS home directories

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vsserver cifs home-directory modify` command modifies the CIFS home directory configuration for a CIFS server. To use the home directory option `s` (`-is-home-dirs-access-for-admin-enabled` or/and `-is-home-dirs-access-for-public-enabled`), a home directory share must be configured with a dynamic share pattern preceded by a tilde (~). Valid dynamic share patterns are `~%w` and `%d%w`. The pattern `%u` is not supported with the `se` option `s`.

### Parameters

#### **-vsserver <vserver> -Vserver**

This parameter specifies the name of the CIFS server for which you want to modify the CIFS home directory configuration.

#### **[-is-home-dirs-access-for-admin-enabled {true|false}] - Is Home Directory Access for Admin Enabled**

This optional parameter specifies whether a user with Windows administrative privileges can connect to another user's home directory. The default value for this parameter is `true`.



## `[-is-home-dirs-access-for-public-enabled {true|false}]` - Is Home Directory Access for Public Enabled (privilege: advanced)

This optional parameter specifies whether any user can connect to another user's home directory. The default value for this parameter is *false*.

### Examples

The following example modifies the CIFS home directory configuration for the Vserver "vs1". It enables users with Windows administrative privileges to connect to another user's home directory, and enables any user to connect to another user's home directory.

```
cluster1::> vserver cifs home-directory modify -vserver vs1 -is-home-dirs
-access-for-admin-enabled true
-is-home-dirs-access-for-public-enabled true
```

The following example shows the usage of the share creation pattern `%d/%w`.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name ~%d~%w
-path %d/%w -share-properties homedirectory
```

The following example shows the usage of the share creation pattern `~%w`.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name ~%w -path
%d/%w -share-properties homedirectory
```

## vserver cifs home-directory show-user

Display the Home Directory Path for a User

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs home-directory show-user` command prints the path of a user's CIFS home directory. Use this command if multiple CIFS home directory paths exist and you want to see which path holds the user's CIFS home directory.

### Parameters

`{ [-fields <fieldname>,...]`

If you specify this parameter, the command displays only the fields that you specify.

`| [-instance ] }`

If you specify the `-instance` parameter, the command displays detailed information about all entries.

### **-vserver <vserver> - Vserver**

Use this required parameter to specify the Vserver that contains the home directory of the user specified with the required `-username` parameter.

### **-username <text> - User Name**

Use this required parameter to locate the home directory of the specified user. You must enter this parameter in the following format: `user`, `domain/user` or `cifs_server_name/user`.

### **[-path <text>] - Path**

If you specify this parameter, the command displays information about the user's home directory with the specified path.

### **[-share-name <text>] - Share Name**

If you specify this parameter, the command displays information about the user's home directory with the specified home-directory share.

## **Examples**

The following command displays information about the home directory of user `gpo\rpuser1` belonging to Vserver `vs1`.

```
cluster1::> vserver cifs home-directory show-user -vserver vs1 -username
gpo\rpuser1
Vserver   : vs1
  Username : GPO/rpuser1
ShareName                               Home Dir Path
-----
root                                       /home/rpuser1
rpuser1                                   /home/rpuser1
~GPO~rpuser1                             /home/GPO/rpuser1
```

The following command displays information about the home directory of user `gpo\rpuser1` belonging to Vserver `vs1` at share path `/home/rpuser1`.

```
cluster1::> vserver cifs home-directory show-user -vserver vs1 -username
gpo\rpuser1 -path /home/rpuser1
Vserver   : vs1
  Username : GPO/rpuser1
ShareName                               Home Directory Path
-----
root                                       /home/rpuser1
rpuser1                                   /home/rpuser1
2 entries were displayed.
```

The following command displays information about the home directory of user `gpo\rpuser1` belonging to `Vserver vs1` at share `_GPO~rpuser1`.

```
cluster1::> vserver cifs home-directory show-user -vserver vs1 -username
gpo\rpuser1 -share-name ~GPO~rpuser1
Vserver   : vs1
  Username : GPO/rpuser1
ShareName                               Home Directory Path
-----
~GPO~rpuser1                            /home/GPO/rpuser1
```

## vserver cifs home-directory show

Display home directory configurations

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs home-directory show` command displays the CIFS home directory configuration for one or more Vservers.

### Parameters

**{ [-fields <fieldname>,...]**

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

**| [-instance ] }**

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver>] - Vserver**

If you specify this parameter, the command displays CIFS home directory configuration for the specified Vserver.

**[-is-home-dirs-access-for-admin-enabled {true|false}] - Is Home Directory Access for Admin Enabled**

If you specify this parameter, the command displays home directory configuration for CIFS servers that have the specified setting.

**[-is-home-dirs-access-for-public-enabled {true|false}] - Is Home Directory Access for Public Enabled (privilege: advanced)**

If you specify this parameter, the command displays home directory configuration for CIFS servers that have the specified setting.

## Examples

The following example lists the CIFS home directory configuration for a Vserver on the cluster.

```
cluster1::> vserver cifs home-directory show -vserver vs1
Vserver: vs1
Is Home Directory Access for Admin Enabled: true
```

At the advanced privilege level or above, the output displays the information below:

```
cluster1::*> vserver cifs options show
Vserver: vs1
  Is Home Directory Access for Admin Enabled: true
  Is Home Directory Access for Public Enabled: false
```

## vserver cifs home-directory search-path add

Add a home directory search path

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs home-directory search-path add` command adds a search path to a CIFS home directory configuration.

### Parameters

**-vserver <vserver name> - Vserver**

This parameter specifies the CIFS-enabled Vserver containing the CIFS home directory configuration to which you want to add the search path.

**-path <text> - Path**

This parameter specifies the search path you want to add.

### Examples

The following example adds the path `/home1` to the CIFS home directory configuration on Vserver `vs1`.

```
cluster1::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1
```

## vserver cifs home-directory search-path remove

Remove a home directory search path

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs home-directory search-path remove` command removes a search path from a CIFS home directory configuration.

## Parameters

**-vserver <vserver name> - Vserver**

This parameter specifies the CIFS-enabled Vserver containing the CIFS home directory configuration from which you want to remove the search path.

**-path <text> - Path**

This parameter specifies the search path you want to remove.

## Examples

The following example removes the path `/home1` from the CIFS home directory configuration on Vserver `vs1`.

```
cluster1::> vserver cifs home-directory search-path remove -vserver vs1
-path /home1
```

# vserver cifs home-directory search-path reorder

Change the search path order used to find a match

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs home-directory search-path reorder` command moves a search path to a new position in the search path order in the CIFS home directory configuration for the CIFS-enabled Vserver.

## Parameters

**-vserver <vserver name> - Vserver**

This parameter specifies the CIFS enabled Vserver for which you want to reorder searches.

**-path <text> - Path**

This parameter specifies the search path you want to move.

**-to-position <integer> - Target Position**

This parameter specifies the new position of the search path in the search path order.

## Examples

The following example moves the search path `/home1` to position 1 in the search path order for the CIFS home

directory configuration on Vserver vs1.

```
cluster1::> vsserver cifs home-directory search-path reorder -vsserver vs1
-path /home1 -to-position 1
```

## vserver cifs home-directory search-path show

Display home directory search paths

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vsserver cifs home-directory search-path show` command displays information about the search paths that are in the home directory configuration for the CIFS-enabled Vservers.

### Parameters

{ [-fields <fieldname>,...]

If you specify this parameter, the command only displays the fields that you specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all entries.

[-vsserver <vsserver name>] - Vserver

If you specify this parameter, the command displays home directory configuration for the CIFS-enabled Vserver that you specify.

[-path <text>] - Path

If you specify this parameter, the command displays information only for the search path that you specify.

### Examples

The following example displays information about search paths for all CIFS home directories on all CIFS-enabled Vservers:

```
cluster1::> vsserver cifs home-directory search-path show
Vserver      Position Path
-----
vs1          1       /home1
vs2          2       /home2
```

## vserver cifs options modify

Modify CIFS options

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs options modify` command modifies CIFS options for a CIFS server.

## Parameters

### **-vserver <vserver name> - Vserver**

This parameter specifies the name of the CIFS server for which you want to modify CIFS options.

### **[-default-unix-user <text>] - Default UNIX User**

This optional parameter specifies the name of the default UNIX user for the CIFS server.

### **[-read-grants-exec {enabled|disabled}] - Read Grants Exec for Mode Bits**

This optional parameter specifies whether the CIFS server does read grant execution for mode bits.

### **[-wins-servers <InetAddress>, ...] - Windows Internet Name Service (WINS) Addresses**

This optional parameter specifies a list of Windows Internet Name Server (WINS) addresses for the CIFS server. You must specify the WINS servers using an IP address. You can enter multiple WINS addresses as a comma-delimited list.



Use an IPv4 address because WINS over IPv6 is not supported.

### **[-smb1-enabled {true|false}] - (DEPRECATED)-Enable SMB1 Protocol (privilege: advanced)**

This optional parameter specifies whether the CIFS server negotiates the SMB 1.0 version of the CIFS protocol. The default value for this parameter is false.



This parameter is deprecated because the SMB1 protocol is obsolete and considered insecure. It might be removed in a future release.

### **[-smb2-enabled {true|false}] - Enable all SMB2 Protocols (privilege: advanced)**

This optional parameter specifies whether the CIFS server negotiates the SMB 2 version of the CIFS protocol. The default value for this parameter is true.

### **[-smb3-enabled {true|false}] - Enable SMB3 Protocol (privilege: advanced)**

This optional parameter specifies whether the CIFS server negotiates the SMB 3 version of the CIFS protocol. The default value for this parameter is true.

### **[-smb31-enabled {true|false}] - Enable SMB3.1 Protocol (privilege: advanced)**

This optional parameter specifies whether the CIFS server negotiates the SMB 3.1 version of the CIFS protocol. The default value for this parameter is true.

### **[-max-mpx <integer>] - Maximum Simultaneous Operations per TCP Connection (privilege: advanced)**

This optional parameter specifies the maximum number of simultaneous operations the CIFS server reports it can process per TCP connection.

**[-shadowcopy-dir-depth <integer>] - Maximum Depth of Directories to Shadow Copy (privilege: advanced)**

This optional parameter specifies the maximum depth of directories on which to create shadow copies in the CIFS server. The default for this parameter is 5. The value 0 indicates that all sub-directories should be shadow copied. This parameter is not supported for workgroup CIFS servers. Directories and files within a FlexGroup will not be shadow copied because FlexGroups do not support shadow copy.

**[-copy-offload-enabled {true|false}] - Enable Copy Offload Feature (privilege: advanced)**

This optional parameter enables the Copy Offload feature in the CIFS server. If set to false, the Copy Offload feature is disabled. The default for this parameter is true.

**[-is-copy-offload-direct-copy-enabled {true|false}] - Is Direct-copy Copy Offload Mechanism Enabled (privilege: advanced)**

This optional parameter enables the direct-copy mechanism for ODX copy offload in the CIFS server. If set to false, the direct-copy mechanism is disabled. The default for this parameter is true. + The direct-copy mechanism increases the performance of the copy offload operation when Windows clients try to open the source file of a copy in a mode that prevents the file being changed while the copy is in progress. If turned off, regular copy offloading takes place.

**[-default-unix-group <text>] - Default UNIX Group**

This optional parameter specifies the name of the default UNIX group for the CIFS server. If you do not specify a default UNIX group, the CIFS ACL to NFSv4 ACL translation may result in incomplete NFSv4 ACL information. This parameter is not supported by Vservers with FlexVol volumes.

**[-shadowcopy-enabled {true|false}] - Enable Shadow Copy Feature (VSS) (privilege: advanced)**

This optional parameter enables the Shadow Copy (VSS) feature in the CIFS server when set to true. The VSS feature is disabled when set to false. The default for this parameter is true. This parameter is not supported for workgroup CIFS servers. Directories and files within a FlexGroup will not be shadow copied because FlexGroups do not support shadow copy.

**[-is-referral-enabled {true|false}] - Refer Clients to More Optimal LIFs (privilege: advanced)**

This optional parameter specifies whether the CIFS server automatically refers clients to a data LIF local to the node which hosts the root of the requested share. The default value for this parameter is false.

**[-is-local-auth-enabled {true|false}] - Is Local User Authentication Enabled (privilege: advanced)**

This optional parameter specifies whether local user authentication is enabled for the CIFS server.

**[-is-local-users-and-groups-enabled {true|false}] - Is Local Users and Groups Enabled (privilege: advanced)**

This optional parameter specifies whether the local users and groups feature is enabled for the CIFS server.

**[-is-use-junctions-as-reparse-points-enabled {true|false}] - Is Reparse Point Support Enabled (privilege: advanced)**

This optional parameter specifies whether the CIFS server exposes junction points to Windows clients as reparse points. The default value for this parameter is true. This parameter is only active if the client has negotiated use of the SMB 2 or SMB 3 protocol.

**[-is-exportpolicy-enabled {true|false}] - Is Export Policies for CIFS Enabled (privilege: advanced)**

This optional parameter specifies whether the CIFS server uses export policies to control client access. The default value for this parameter is false.



**`[-is-unix-nt-acl-enabled {true|false}] - Is NT ACLs on UNIX Security-style Volumes Enabled (privilege: advanced)`**

This optional parameter specifies whether the CIFS server has the NT ACLs enabled on UNIX security-style volumes. The default value for this parameter is true.

**`[-is-trusted-domain-enum-search-enabled {true|false}] - Is Enumeration of Trusted Domain and Search Capability Enabled (privilege: advanced)`**

This optional parameter specifies whether the CIFS server supports enumeration of bidirectional trusted domains. It also supports the search in all the bidirectional trusted domains when performing Windows user lookups for UNIX user to Windows user name mapping. The default value is true. This parameter is not supported for workgroup CIFS servers.

**`[-client-session-timeout <integer>] - Idle Timeout Before CIFS Session Disconnect (secs)`**

This optional parameter specifies the amount of idle time (in seconds) before a CIFS session is disconnected. The default value for this parameter is 900 seconds.

**`[-is-dac-enabled {true|false}] - Is Dynamic Access Control (DAC) Enabled (privilege: advanced)`**

This optional parameter enables the Dynamic Access Control (DAC) feature in the CIFS server when set to true. The DAC feature is disabled when set to false. The default for this parameter is false. This parameter is not supported for workgroup CIFS servers.

**`[-restrict-anonymous {no-restriction|no-enumeration|no-access}] - Restrictions for Anonymous User (privilege: advanced)`**

This optional parameter controls the access restrictions of non-authenticated sessions and applies the restrictions for the anonymous user based on the permitted values. The default value for this parameter is no-restriction. Permitted values for this option are:

- no-restriction - This option specifies no access restriction for anonymous users (default).
- no-enumeration - This option specifies that only enumeration is restricted.
- no-access - This option specifies that access is restricted for anonymous users.

**`[-is-read-only-delete-enabled {enabled|disabled}] - Is Deletion of Read-Only Files Enabled`**

This optional parameter controls deletion of read-only files and directories. NTFS delete semantics forbid deletion of a file or directory when the read-only attribute is set. UNIX delete semantics ignore it, focusing instead on parent directory permissions, which some applications require. This option is used to select the desired behavior. By default this option is disabled, yielding NTFS behavior.

**`[-file-system-sector-size {512|4096 (in bytes)}] - Size of File System Sector Reported to SMB Clients (bytes) (privilege: advanced)`**

This optional parameter specifies the size of file system sector reported to SMB clients (in bytes). The default value for this parameter is 4096. Valid values are 512 and 4096.

**`[-is-fake-open-enabled {true|false}] - Is Fake Open Support Enabled (privilege: advanced)`**

This optional parameter specifies whether the CIFS server supports fake open requests. This parameter allows you to optimize the open and close requests coming from SMB 2 clients. The default value for this parameter is true.

**`[-is-unix-extensions-enabled {true|false}] - Is UNIX Extensions Enabled (privilege: advanced)`**

When set to true, this optional parameter enables the UNIX Extensions feature in the CIFS server. If set to

false, the UNIX Extensions feature is disabled. The default for this parameter is false. UNIX Extensions allows POSIX/UNIX style security to be displayed through the CIFS protocol.

**`[-is-search-short-names-enabled {true|false}] - Is Search Short Names Support Enabled (privilege: advanced)`**

This optional parameter specifies whether the CIFS server supports searching short names. A search query with this option enabled will try to match 8.3 file names along with long file names. The default value for this parameter is false.

**`[-is-advanced-sparse-file-support-enabled {true|false}] - Is Advanced Sparse File Support Enabled (privilege: advanced)`**

This optional parameter specifies whether the CIFS server supports the advanced sparse file capabilities. This allows CIFS clients to query the allocated ranges of a file and to write zeroes or free data blocks for ranges of a file.

**`[-is-fsctl-file-level-trim-enabled {true|false}] - Is Fsctl File Level Trim Enabled (privilege: advanced)`**

This optional parameter specifies whether trim requests (FSCTL\_FILE\_LEVEL\_TRIM) are supported on the CIFS server.

**`[-guest-unix-user <text>] - Map the Guest User to Valid UNIX User (privilege: advanced)`**

This optional parameter specifies that an unauthenticated user coming from any untrusted domain can be mapped to a specified UNIX user for the CIFS server. If the CIFS server cannot authenticate the user against a domain controller for the home domain or a trusted domain or the local database, and this option is enabled, the CIFS server considers the user as a guest user and maps the user to the specified UNIX user. The UNIX user must be a valid user.

**`[-smb1-max-buffer-size <integer>] - Maximum Buffer Size Used for SMB1 Message (privilege: advanced)`**

This optional parameter specifies the maximum buffer size used for an SMB 1.0 message that the CIFS server can receive. If the LARGE\_READ or LARGE\_WRITE capability is negotiated during session setup, then 'Read' or 'Write' SMB 1.0 operations are allowed to exceed the configured 'smb1-max-buffer-size' value. This parameter does not have any effect on SMB 2 or SMB 3 buffer size. The default value for this parameter is 65535. The supported range for this parameter is 4356 through 65535.

**`[-max-same-user-sessions-per-connection <integer>] - Maximum Same User Sessions per TCP Connection (privilege: advanced)`**

This optional parameter specifies the maximum number of CIFS sessions that can be set up by the same user per TCP connection. The default value of this parameter is 2500. The maximum value of this parameter is 4294967295.

**`[-max-same-tree-connect-per-session <integer>] - Maximum Same Tree Connect per Session (privilege: advanced)`**

This optional parameter specifies the maximum number of CIFS tree connects to the same share per CIFS session. The default value of this parameter is 5000. The maximum value of this parameter is 4294967295.

**`[-max-opens-same-file-per-tree <integer>] - Maximum Opens on Same File per Tree (privilege: advanced)`**

This optional parameter specifies the maximum number of existing opens on the same file per CIFS tree. The default value of this parameter is 1000. The maximum value of this parameter is 4294967295.

**[`-max-watches-set-per-tree <integer>`] - Maximum Watches Set per Tree (privilege: advanced)**

This optional parameter specifies the maximum number of watches, also known as change notifies, that can be set per CIFS tree. Tree here refers to a share connect from a single client. The default value of this parameter is 500. The maximum value of this parameter is 4294967295.

**[`-is-admin-users-mapped-to-root-enabled {true|false}`] - Map Administrators to UNIX User 'root' (privilege: advanced)**

If this optional parameter is set to true, Windows users who are members of the "BUILTIN\Administrators" group are mapped to UNIX user 'root' unless a user who is a member of this group is explicitly mapped to a UNIX user. If a Windows user is a member of the "BUILTIN\Administrators" group and an explicit user mapping exists for that user, the explicit name mapping takes precedence. If this parameter is set to false, users that are members of the "BUILTIN\Administrators" group are not mapped to UNIX 'root'. The default value for this parameter is true.

**[`-is-advertise-dfs-enabled {true|false}`] - (DEPRECATED)-Enable DFS Referral Advertisement (privilege: advanced)**

This optional parameter specifies whether to advertise DFS referral of the CIFS protocol. The default value for this parameter is false. This option is not applicable to SMB 1.0.



This parameter is deprecated and may be removed in a future release of Data ONTAP. The functionality provided by this parameter is now controlled by the `-symlink-properties` parameter instead.

**[`-is-path-component-cache-enabled {true|false}`] - Is Path Component Cache Enabled (privilege: advanced)**

This optional parameter specifies whether the path component cache is enabled. The default value for this parameter is true.

**[`-win-name-for-null-user <TextNoCase>`] - Map Null User to Windows User or Group (privilege: advanced)**

This optional parameter specifies a valid Windows user or group name that will be added to the CIFS credentials for a NULL user Session.

**[`-is-hide-dotfiles-enabled {true|false}`] - Is Hide Dot Files Enabled (privilege: advanced)**

This optional parameter specifies whether the CIFS server supports hiding dot files. Directory enumeration with this option enabled hides files and directories that begin with a dot ("."). The default value for this parameter is false.

**[`-is-client-version-reporting-enabled {true|false}`] - Is Client Version Reporting Enabled (privilege: advanced)**

If this parameter is set to true, CIFS client version tracking information is collected by AutoSupport. The default value of this parameter is true.

**[`-is-client-dup-detection-enabled {true|false}`] - Is Client Duplicate Session Detection Enabled (privilege: advanced)**

This optional parameter specifies whether the CIFS server supports duplicate session detection. Duplicate sessions that come from the same client with VcNumber of zero with this option enabled will be closed, and is only applicable for SMB 1.0 clients. The default value for this parameter is true.

**[`-grant-unix-group-perms-to-others {true|false}`] - Grant UNIX Group Permissions to Others (privilege: advanced)**

This optional parameter specifies whether the incoming CIFS user who is not the owner of the file, can be granted the group permission. If the CIFS incoming user is not the owner of UNIX security-style file and this option is set to true, then at all times the file's "group" permissions are granted. If the CIFS incoming user is not the owner of UNIX security-style file and this option is set to false, then the normal UNIX rules are applicable to grant the permissions. The default value of this parameter is false.

**`[-is-multichannel-enabled {true|false}] - Is Multichannel Enabled (privilege: advanced)`**

This optional parameter specifies whether the CIFS server supports Multichannel or not. The default value for this parameter is false.

**`[-max-connections-per-session <integer>] - Maximum Connections Allowed Per Multichannel Session (privilege: advanced)`**

This optional parameter specifies the maximum number of connections allowed per Multichannel session. The default value for this parameter is 32.

**`[-max-lifs-per-session <integer>] - Maximum LIFs Advertised Per Multichannel Session (privilege: advanced)`**

This optional parameter specifies the maximum number of network interfaces advertised per Multichannel session. The default value for this parameter is 256.

**`[-is-large-mtu-enabled {true|false}] - Is Large MTU Enabled (privilege: advanced)`**

This optional parameter specifies whether the CIFS server supports the SMB 2.1 "large MTU" feature. The default value for this parameter is true.

**`[-is-netbios-over-tcp-enabled {true|false}] - Is NetBIOS over TCP (port 139) Enabled (privilege: advanced)`**

This optional parameter specifies whether the CIFS server supports the NetBIOS over TCP (port 139) feature. The default value for this parameter is true.

**`[-is-nbns-enabled {true|false}] - Is NBNS over UDP (port 137) Enabled (privilege: advanced)`**

This optional parameter specifies whether the CIFS server supports the NBNS protocol. The default value for this parameter is *false*.

**`[-widelink-as-reparse-point-versions <CIFS Dialects>,...] - Protocol Versions for Which Widelink Will Be Reported as Reparse Point (privilege: advanced)`**

This optional parameter specifies the CIFS protocol versions for which the widelink is reported as reparse point. The default value for this parameter is *SMB1*.



Any values entered for this parameter is replaced with the existing values.

**`[-max-credits <integer>] - Maximum Credits to Grant (privilege: advanced)`**

This optional parameter specifies the maximum number of outstanding requests on a CIFS connection. The default value for this parameter is 128.

**`[-is-inherit-modebits-with-nfsv4acl-enabled {true|false}] - Enable Modebits on CIFS File Inheriting NFSv4 ACLs (privilege: advanced)`**

This optional parameter specifies whether to set mode bits on the files created by the cifs user that inherit NFSv4 acls. This parameter is not supported for SMB1 clients.

## **[`-is-share-enum-permission-check-enabled {true|false}`] - Check Share Permission for NetShareEnumAll Request (privilege: advanced)**

If this parameter is set to `true`, the NetShareEnum call will only respond with the shares the user has access to. The default value is `false` which means it will respond with all shares.

## **Examples**

The following example modifies CIFS options for the Vserver "vs1". It changes the default UNIX user, disables read grants exec, disables SMB2.x, changes maximum multiplex count to 1124, changes the file system sector size reported to SMB clients to 512, disables the direct-copy offload mechanism for ODX copy offload, enables the UNIX Extensions feature, disables fake open requests changes WINS servers to 192.168.11.112 and changes the client session timeout to 6000.

```
cluster1::> vsserver cifs options modify -vs1
  -default-unix-user pcuser -read-grants-exec disabled
  -smb2-enabled false -max-mpx 1124 -file-system-sector-size
  512 -is-copy-offload-direct-copy-enabled false
  -is-unix-extensions-enabled true -is-fake-open-enabled false
  -wins-servers 192.168.11.112 -client-session-timeout 6000
```

The following example modifies CIFS options for the Vserver "vs1". It enables the advanced sparse file support .

```
cluster1::> vsserver cifs options modify -vs1
  -is-advanced-sparse-file-support-enabled true
```

The following example modifies CIFS options for the Vserver "vs1". It modifies limits for maximum opens on the same file, max sessions by the same user, max tree connects per session, and max watches set.

```
cluster1::> vsserver cifs options modify -vs1
  -max-same-user-sessions-per-connection 100
  -max-same-tree-connect-per-session 100 -max-opens-same-file-per-tree 150
  -max-watches-set-per-tree 200
```

The following example modifies CIFS options for the Vserver "vs1". It modifies the option to disable the path component cache. .

```
cluster1::> vsserver cifs options modify -vs1
  -is-path-component-cache-enabled false
```

The following example modifies CIFS options for the Vserver "vs1". It modifies the option to disable CIFS client version tracking.

```
cluster1::> vsserver cifs options modify -vsserver vs1
-is-client-version-reporting-enabled false
```

The following example modifies CIFS option for the Vserver "vs1". It modifies the option to enable granting of UNIX group permissions to others.

```
cluster1::> vsserver cifs options modify -vsserver vs1
-grant-unix-group-perms-to-others true
```

## vserver cifs options show

Display CIFS options

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vsserver cifs options show` command displays the CIFS configuration options for one or more Vservers.

### Parameters

**{ [-fields <fieldname>,...]**

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

**| [-instance ] }**

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vsserver <vsserver name>] - Vserver**

If you specify this parameter, the command only displays CIFS options for the specified Vserver.

**[-default-unix-user <text>] - Default UNIX User**

If you specify this parameter, the command displays options for CIFS server with the specified UNIX user.

**[-read-grants-exec {enabled|disabled}] - Read Grants Exec for Mode Bits**

If this parameter is set to `enabled`, the command displays options for CIFS servers that grant execution access when granting read access using mode bits. If set to `disabled`, the command displays options for CIFS servers that do not grant execution access when granting read access using mode bits.

**[-wins-servers <InetAddress>,... ] - Windows Internet Name Service (WINS) Addresses**

If you specify this parameter, the command displays CIFS options only for CIFS servers that use the specified Windows Internet Name Server (WINS) addresses.

**[-smb1-enabled {true|false}] - (DEPRECATED)-Enable SMB1 Protocol (privilege: advanced)**

If this parameter is set to `true`, the command displays options for CIFS servers where SMB 1.0 version of

the CIFS protocol is negotiated. If set to false, the command displays options for CIFS servers where SMB 1.0 version of the CIFS protocol is not negotiated.



This parameter is deprecated because the SMB1 protocol is obsolete and considered insecure. It might be removed in a future release.

**[`-smb2-enabled {true|false}`] - Enable all SMB2 Protocols (privilege: advanced)**

If this parameter is set to true, the command displays options for CIFS servers where SMB 2 version of the CIFS protocol is negotiated. If set to false, the command displays options for CIFS servers where SMB 2 version of the CIFS protocol is not negotiated.

**[`-smb3-enabled {true|false}`] - Enable SMB3 Protocol (privilege: advanced)**

If this parameter is set to true, the command displays options for CIFS servers where SMB 3 version of the CIFS protocol is negotiated. If set to false, the command displays options for CIFS servers where SMB 3 version of the CIFS protocol is not negotiated.

**[`-smb31-enabled {true|false}`] - Enable SMB3.1 Protocol (privilege: advanced)**

If this parameter is set to true, the command displays options for CIFS servers where SMB 3.1 version of the CIFS protocol is negotiated. If set to false, the command displays options for CIFS servers where SMB 3.1 version of the CIFS protocol is not negotiated.

**[`-max-mpx <integer>`] - Maximum Simultaneous Operations per TCP Connection (privilege: advanced)**

If you specify this parameter, the command displays options for CIFS server with the specified maximum number of simultaneous operations the CIFS server can process per TCP connection.

**[`-shadowcopy-dir-depth <integer>`] - Maximum Depth of Directories to Shadow Copy (privilege: advanced)**

If you specify this parameter, the command displays options only for CIFS servers that are configured with the specified depth of directories on which to create shadow copies.

**[`-copy-offload-enabled {true|false}`] - Enable Copy Offload Feature (privilege: advanced)**

If set to true, this command displays options only for CIFS servers where the Copy Offload feature is enabled. If set to false, options are displayed for CIFS servers where the Copy Offload feature is disabled.

**[`-is-copy-offload-direct-copy-enabled {true|false}`] - Is Direct-copy Copy Offload Mechanism Enabled (privilege: advanced)**

If set to true, this command displays options only for CIFS servers where the direct-copy mechanism for ODX Copy Offload is enabled. If set to false, options are displayed for CIFS servers where the direct-copy offload mechanism is disabled. + The direct-copy mechanism increases the performance of the copy offload operation when Windows clients try to open the source file of a copy in a mode that prevents the file being changed while the copy is in progress. If turned off, regular copy offloading takes place.

**[`-default-unix-group <text>`] - Default UNIX Group**

If you specify this parameter, the command displays options for CIFS server with the specified default UNIX group.

**[`-shadowcopy-enabled {true|false}`] - Enable Shadow Copy Feature (VSS) (privilege: advanced)**

If set to true, this command displays options only for CIFS servers where the Shadow Copy (VSS) feature is enabled. If set to false, options are displayed for CIFS servers where the Shadow Copy (VSS) feature is disabled.

**`[-is-referral-enabled {true|false}] - Refer Clients to More Optimal LIFs (privilege: advanced)`**

If set to true, the command displays options for the CIFS server where the CIFS server automatically refers clients to a data LIF local to the node which hosts the root of the requested share. If set to false, the command displays options for the CIFS server where the mechanism, to automatically refer the clients to data LIF local to the node which hosts the root of the requested share, is disabled.

**`[-is-local-auth-enabled {true|false}] - Is Local User Authentication Enabled (privilege: advanced)`**

If this parameter is set to true, the command displays CIFS options only for CIFS servers where local user authentication is enabled. If set to false, the command displays options for CIFS servers where local user authentication is disabled.

**`[-is-local-users-and-groups-enabled {true|false}] - Is Local Users and Groups Enabled (privilege: advanced)`**

If this parameter is set to true, the command displays CIFS options only for CIFS servers where the local users and groups feature is enabled. If set to false, the command displays options for CIFS servers where the local users and groups feature is disabled.

**`[-is-use-junctions-as-reparse-points-enabled {true|false}] - Is Reparse Point Support Enabled (privilege: advanced)`**

If you specify this parameter, the command only displays CIFS options for Vservers which have the specified reparse point setting.

**`[-is-exportpolicy-enabled {true|false}] - Is Export Policies for CIFS Enabled (privilege: advanced)`**

If you specify this parameter, the command only displays CIFS options for Vservers which have the specified export policy setting.

**`[-is-unix-nt-acl-enabled {true|false}] - Is NT ACLs on UNIX Security-style Volumes Enabled (privilege: advanced)`**

If this parameter is set to true, the command only displays CIFS options for Vservers that have the NT ACLs on UNIX security-style volumes enabled. If set to false, the command displays CIFS options for Vservers that have the NT ACLS on UNIX security-style volumes disabled.

**`[-is-trusted-domain-enum-search-enabled {true|false}] - Is Enumeration of Trusted Domain and Search Capability Enabled (privilege: advanced)`**

If this parameter is set to true, the command displays CIFS options only for CIFS servers that support enumeration of bidirectional trusted domains and that support searching in all bidirectional trusted domains when performing Windows user lookups for UNIX user to Windows user name mapping. If set to false, the command displays options for CIFS servers that do not support enumeration of bidirectional trusted domains.

**`[-client-session-timeout <integer>] - Idle Timeout Before CIFS Session Disconnect (secs)`**

If you specify this parameter, the command displays options only for CIFS servers that are configured with the specified client session timeout value (in seconds).

**`[-is-dac-enabled {true|false}] - Is Dynamic Access Control (DAC) Enabled (privilege: advanced)`**

If set to true, this command displays options only for CIFS servers where the Dynamic Access Control (DAC) feature is enabled. If set to false, options are displayed for CIFS servers where the Dynamic Access Control (DAC) feature is disabled.



**[~~-restrict-anonymous~~ {no-restriction|no-enumeration|no-access}] - Restrictions for Anonymous User (privilege: advanced)**

If you specify this parameter, the command displays CIFS options only for CIFS servers that have the specified permitted value for the anonymous user. Permitted values for this option are:

- no-restriction - There is no access restriction for anonymous users.
- no-enumeration - Only enumeration is restricted.
- no-access - Access is restricted for anonymous users.

**[~~-is-read-only-delete-enabled~~ {enabled|disabled}] - Is Deletion of Read-Only Files Enabled**

If you specify this parameter, the command displays options only for CIFS servers that have the specified is-read-only-delete-enabled setting.

**[~~-file-system-sector-size~~ {512|4096 (in bytes)}] - Size of File System Sector Reported to SMB Clients (bytes) (privilege: advanced)**

If you specify this parameter, the command displays options only for CIFS servers that are configured with the specified file system sector size (in bytes).

**[~~-is-fake-open-enabled~~ {true|false}] - Is Fake Open Support Enabled (privilege: advanced)**

If you set this parameter to true, the command displays options for CIFS servers where fake open is enabled. If set to false, the command displays options for CIFS servers where fake open is disabled.

**[~~-is-unix-extensions-enabled~~ {true|false}] - Is UNIX Extensions Enabled (privilege: advanced)**

If set to true, this command displays options only for CIFS servers where the UNIX Extensions feature is enabled. If set to false, options are displayed for CIFS servers where the UNIX Extensions feature is disabled. UNIX Extensions allows POSIX/UNIX style security to be displayed through the CIFS protocol.

**[~~-is-search-short-names-enabled~~ {true|false}] - Is Search Short Names Support Enabled (privilege: advanced)**

If you set this parameter to true, the command displays options for CIFS servers where search short names is enabled. If set to false, the command displays options for CIFS servers where search short names is disabled.

**[~~-is-advanced-sparse-file-support-enabled~~ {true|false}] - Is Advanced Sparse File Support Enabled (privilege: advanced)**

If set to true, the command displays options for CIFS servers where the advanced sparse file capabilities for CIFS are enabled. If set to false, options are displayed for CIFS servers where the advanced sparse file capabilities for CIFS are disabled.

**[~~-is-fsctl-file-level-trim-enabled~~ {true|false}] - Is Fsctl File Level Trim Enabled (privilege: advanced)**

If set to true, the command displays options for all the CIFS servers where trim requests (FSCTL\_FILE\_LEVEL\_TRIM) are supported. If set to false, options are displayed for all the CIFS servers where trim requests (FSCTL\_FILE\_LEVEL\_TRIM) are not supported.

**[~~-guest-unix-user~~ <text>] - Map the Guest User to Valid UNIX User (privilege: advanced)**

If you specify this parameter, the command displays options for CIFS server with the specified guest UNIX user.

**[-smb1-max-buffer-size <integer>] - Maximum Buffer Size Used for SMB1 Message (privilege: advanced)**

If you specify this parameter, the command displays options only for CIFS servers that are configured with the specified maximum buffer size value.

**[-max-same-user-sessions-per-connection <integer>] - Maximum Same User Sessions per TCP Connection (privilege: advanced)**

If you specify this parameter, the command displays options only for CIFS server that are configured with the specified maximum same user session per connection.

**[-max-same-tree-connect-per-session <integer>] - Maximum Same Tree Connect per Session (privilege: advanced)**

If you specify this parameter, the command displays options only for CIFS server that are configured with the specified maximum same tree connects per session.

**[-max-opens-same-file-per-tree <integer>] - Maximum Opens on Same File per Tree (privilege: advanced)**

If you specify this parameter, the command displays options only for CIFS server that are configured with the specified maximum opens on same file per tree.

**[-max-watches-set-per-tree <integer>] - Maximum Watches Set per Tree (privilege: advanced)**

If you specify this parameter, the command displays options only for CIFS server that are configured with the specified maximum watches set per tree. Tree here refers to a share connect from a single client.

**[-is-admin-users-mapped-to-root-enabled {true|false}] - Map Administrators to UNIX User 'root' (privilege: advanced)**

If you set this parameter to true, the command displays options for CIFS servers where members of "BUILTIN\Administrators" group are mapped to UNIX user 'root'. If set to false, the command displays options for CIFS servers where members of the "BUILTIN\Administrators" group are not mapped to UNIX user 'root'.

**[-is-advertise-dfs-enabled {true|false}] - (DEPRECATED)-Enable DFS Referral Advertisement (privilege: advanced)**

If this parameter is set to true, the command displays CIFS options only for CIFS servers where DFS referral advertisement is enabled. If set to false, the command displays options for CIFS servers where DFS referral advertisement is disabled. This option is not applicable to SMB 1.0.



This parameter is deprecated and may be removed in a future release of Data ONTAP. The functionality provided by this parameter is now controlled by the `-symlink-properties` parameter instead.

**[-is-path-component-cache-enabled {true|false}] - Is Path Component Cache Enabled (privilege: advanced)**

If this parameter is set to true, the command displays options for CIFS servers where the path component cache is enabled. If set to false, the command displays options for CIFS servers where the path component cache is disabled.

**[-win-name-for-null-user <TextNoCase>] - Map Null User to Windows User or Group (privilege: advanced)**

If you specify this parameter, the command displays options only for CIFS servers that are configured to add the specified windows user or group into CIFS credentials for null sessions.

**`[-is-hide-dotfiles-enabled {true|false}] - Is Hide Dot Files Enabled (privilege: advanced)`**

When set to true, this optional parameter enables the Hide Dot Files feature in the CIFS server. If set to false, the Hide Dot Files feature is disabled. The default value for this parameter is false.

**`[-is-client-version-reporting-enabled {true|false}] - Is Client Version Reporting Enabled (privilege: advanced)`**

If this parameter is set to true, the command displays options for CIFS servers where CIFS client version tracking is enabled. If set to false, the command displays options for CIFS servers where CIFS client version tracking is disabled.

**`[-is-client-dup-detection-enabled {true|false}] - Is Client Duplicate Session Detection Enabled (privilege: advanced)`**

If this parameter is set to true, the command displays options for CIFS servers where client duplicate session detection is enabled. If set to false, the command displays options for CIFS servers where client duplicate session detection is not enabled.

**`[-grant-unix-group-perms-to-others {true|false}] - Grant UNIX Group Permissions to Others (privilege: advanced)`**

If this parameter is set to true, the command displays CIFS options only for CIFS servers where grant unix group permissions to others feature is enabled. If set to false, the command displays options for CIFS servers where grant unix group permissions to others feature is disabled.

**`[-is-multichannel-enabled {true|false}] - Is Multichannel Enabled (privilege: advanced)`**

If this parameter is set to true, the command displays options for CIFS servers where the multichannel is enabled. If set to false, the command displays options for CIFS servers where the multichannel is disabled.

**`[-max-connections-per-session <integer>] - Maximum Connections Allowed Per Multichannel Session (privilege: advanced)`**

If you specify this parameter, the command displays options only for CIFS server that are configured with the specified maximum connections allowed per multichannel session.

**`[-max-lifs-per-session <integer>] - Maximum LIFs Advertised Per Multichannel Session (privilege: advanced)`**

If you specify this parameter, the command displays options only for CIFS server that are configured with the specified maximum network interfaces advertised per multichannel session.

**`[-is-large-mtu-enabled {true|false}] - Is Large MTU Enabled (privilege: advanced)`**

If you specify this parameter, the command displays options only for CIFS servers that are configured to support the SMB 2.1 "Large MTU" feature.

**`[-is-netbios-over-tcp-enabled {true|false}] - Is NetBIOS over TCP (port 139) Enabled (privilege: advanced)`**

If you specify this parameter, the command displays options only for CIFS servers that are configured to support the NetBIOS over TCP (port 139) feature.

**`[-is-nbns-enabled {true|false}] - Is NBNS over UDP (port 137) Enabled (privilege: advanced)`**

If you specify this parameter, the command displays CIFS options only for CIFS servers that use the specified setting for the NBNS protocol.

**`[-widelink-as-reparse-point-versions <CIFS Dialects>,...] - Protocol Versions for Which Widelink Will Be Reported as Reparse Point (privilege: advanced)`**

If you specify this parameter, the command displays CIFS options only for the CIFS servers that matches the specified CIFS protocol versions for which widelinks are reported as reparse points. If a list is entered, entries are returned that matches all the specified versions.

**[-max-credits <integer>] - Maximum Credits to Grant (privilege: advanced)**

If you specify this parameter, the command displays options only for CIFS servers that are configured with the specified maximum credits.

**[-is-inherit-modebits-with-nfsv4acl-enabled {true|false}] - Enable Modebits on CIFS File Inheriting NFSv4 ACLs (privilege: advanced)**

If you specify this parameter, mode bits are set on the files created by the cifs user that inherit nfsv4 acs.

**[-is-share-enum-permission-check-enabled {true|false}] - Check Share Permission for NetShareEnumAll Request (privilege: advanced)**

If this parameter is set to true, the command only displays CIFS options for Vservers that enabled share permission check for NetShareEnumAll request. If set to false, options are displayed for CIFS servers that disabled share permission check for NetShareEnumAll request.

## Examples

The following example lists CIFS options for a Vserver on the cluster.

```
cluster1::> vsserver cifs options show

Vserver: vs1

Client Session Timeout: 900
Default Unix Group: -
Default Unix User: pcuser
Guest Unix User: guestusers
Read Grants Exec: disabled
WINS Servers: -
```

At the advanced level, the output displays the information below.

```
cluster1::*> vsserver cifs options show

Vserver: vs1
Client Session Timeout: 900

Copy Offload Enabled: true
Default Unix Group: -
Default Unix User: pcuser
Guest Unix User: -
Are Administrators mapped to 'root': true
Is Advanced Sparse File Support Enabled: true
Direct-Copy Copy Offload Enabled: true
Export Policies Enabled: false
Grant Unix Group Permissions to Others: true
```

```

        Is Advertise DFS Enabled: true
    Is Client Duplicate Session Detection Enabled: true
        Is Client Version Reporting Enabled: true
            Is DAC Enabled: false
        Is Fake Open Support Enabled: true
    Is Hide Dot Files Support Enabled: false
        Is Large MTU Enabled: true
        Is Local Auth Enabled: true
    Is Local Users and Groups Enabled: true
        Is Multichannel Enabled: false
    Is NetBIOS over TCP (port 139) Enabled: true
        Is Referral Enabled: false
    Is Search Short Names Support Enabled: false
Is Trusted Domain Enumeration And Search Enabled: true
        Is UNIX Extensions Enabled: false
    Is Use Junction as Reparse Point Enabled: true
        Max Multiplex Count: 255
    Max Connections per Multichannel Session: 32
        Max LIFs per Multichannel Session: 256
    Max Same User Session Per Connection: 2500
        Max Same Tree Connect Per Session: 5000
            Max Opens Same File Per Tree: 1000
            Max Watches Set Per Tree: 500
        NBNS Interfaces : -
    Is Path Component Cache Enabled: true
NT ACLs on UNIX Security Style Volumes Enabled: true
        Read Grants Exec: disabled
        Read Only Delete: disabled
    Reported File System Sector Size: 4096
        Restrict Anonymous: no-restriction
    Shadowcopy Dir Depth: 5
        Shadowcopy Enabled: true
            SMB1 Enabled: true
    Max Buffer Size for SMB1 Message: 65535
        SMB2 Enabled: true
        SMB3 Enabled: true
        SMB3.1 Enabled: true
    Map Null User to Windows User or Group: cifsGroup
        WINS Servers: -
    Report Widelink as Reparse Point Versions: SMB1

```

## vserver cifs security modify

Modify CIFS security settings

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs security modify` command modifies CIFS server security settings.

## Parameters

### **-vserver <vserver name> - Vserver**

This parameter specifies the name of the Vserver whose CIFS security settings you want to modify.

### **[-kerberos-clock-skew <integer>] - Maximum Allowed Kerberos Clock Skew**

This parameter specifies the maximum allowed Kerberos ticket clock skew in minutes. The default setting is 5 minutes.

### **[-kerberos-ticket-age <integer>] - Kerberos Ticket Lifetime**

This parameter specifies the Kerberos ticket lifetime in hours. The default setting is 10 hours.

### **[-kerberos-renew-age <integer>] - Maximum Kerberos Ticket Renewal Days**

This parameter specifies the maximum Kerberos ticket renewal lifetime in days. The default setting is 7 days.

### **[-kerberos-kdc-timeout <integer>] - Timeout for Kerberos KDC Connections (Secs)**

This parameter specifies the timeout for sockets on KDCs after which all KDCs are marked as unreachable. The default setting is 3 seconds.

### **[-is-signing-required {true|false}] - Require Signing for Incoming CIFS Traffic**

This parameter specifies whether signing is required for incoming CIFS traffic. The default setting is *false*.

### **[-is-password-complexity-required {true|false}] - Require Password Complexity for Local User Accounts**

This parameter specifies whether password complexity is required for CIFS local users. If this parameter is set to *true*, password complexity is required. If the value is set to *false*, password complexity is not required. The default setting is *true* for CIFS servers.

### **[-use-start-tls-for-ad-ldap {true|false}] - Use start\_tls for AD LDAP Connections**

This parameter specifies whether to use Start TLS over AD LDAP connections. When enabled, the communication between the Data ONTAP LDAP Client and the LDAP Server will be encrypted using Start TLS. Start TLS is a mechanism to provide secure communication by using the TLS/SSL protocols. The default setting is *false*.



Ensure right certificates are installed for CIFS home domain and trusted domains.

### **[-is-aes-encryption-enabled {true|false}] - (DEPRECATED)-Is AES-128 and AES-256 Encryption for Kerberos Enabled**

This parameter specifies whether to use Kerberos AES-128 and AES-256 encryption types for authentication. When enabled, and depending on negotiation with the KDC service, it is possible for authentication operations to utilize these encryption types. The default setting is *true*.



This parameter is deprecated and might be removed from a future release.

**`[-lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}] - LM Compatibility Level`**

This parameter specifies the LM compatibility level. The default setting is *lm-ntlm-ntlmv2-krb* (LM, NTLM, NTLMv2 and Kerberos).

**`[-is-smb-encryption-required {true|false}] - Require SMB Encryption for Incoming CIFS Traffic`**

This parameter specifies whether SMB encryption is required when accessing shares in the Vserver. When enabled and depending on negotiation during session setup, it is possible that data transfers between the client and the server are made secure by encrypting the SMB traffic. The default setting is *false*.

**`[-session-security-for-ad-ldap {none|sign|seal}] - Client Session Security`**

This parameter specifies the level of security to be used for LDAP communications. The default setting is *none*.

LDAP Client Session Security can be one of the following:

- none - No Signing or Sealing.
- sign - Sign LDAP traffic.
- seal - Seal and Sign LDAP traffic.

**`[-smb1-enabled-for-dc-connections {false|true|system-default}] - (DEPRECATED)-SMB1 Enabled for DC Connections`**

This parameter specifies whether SMB1 is enabled for use with connections to domain controllers. The default setting is *system-default*.

SMB1 Enabled For DC Connections can be one of the following:

- false - SMB1 is not enabled.
- true - SMB1 is enabled.
- system-default - This sets the option to whatever is the default for the release of Data ONTAP that is running. For this release it is: SMB1 is enabled.



This parameter is deprecated because the SMB1 protocol is obsolete and considered insecure. It might be removed in a future release.

**`[-smb2-enabled-for-dc-connections {false|true|system-default}] - SMB2 Enabled for DC Connections`**

This parameter specifies whether SMB2 is enabled for use with connections to domain controllers. The default setting is *system-default*.

SMB2 Enabled For DC Connections can be one of the following:

- false - SMB2 is not enabled.
- true - SMB2 is enabled.
- system-default - This sets the option to whatever is the default for the release of Data ONTAP that is running. For this release it is: SMB2 is enabled.

### **[`-referral-enabled-for-ad-ldap {true|false}`] - LDAP Referral Chasing Enabled For AD LDAP Connections**

This parameter specifies whether LDAP referral is enabled for AD LDAP connections. The default setting is *false*.

### **[`-use-ldaps-for-ad-ldap {true|false}`] - Use LDAPS for Secure Active Directory LDAP Connections**

This parameter specifies whether to use LDAPS over AD LDAP connections. When enabled, the communication between the Data ONTAP LDAP Client and the LDAP Server will be encrypted using LDAPS and port 636 will be used. LDAPS is a mechanism to provide secure communication by using the TLS/SSL protocols and port 636. The default setting is *false*.



Ensure right certificates are installed for CIFS home domain and trusted domains.

### **[`-encryption-required-for-dc-connections {true|false}`] - Encryption is required for DC Connection**

This parameter specifies whether encryption is required for use with connections to domain controllers. The default setting is *false*.

Encryption required For DC Connections can be one of the following:

- *false* - Encryption is not required.
- *true* - Encryption is required.

### **[`-aes-enabled-for-netlogon-channel {true|false}`] - AES session key enabled for NetLogon channel**

This parameter specifies whether AES session key will be negotiated as part of the NetLogon secure channel establishment. The default setting is *true*.

### **[`-try-channel-binding-for-ad-ldap {true|false}`] - Try Channel Binding For AD LDAP Connections**

This parameter specifies whether channel binding will be tried for AD LDAP connections. The default setting is *true*. Channel binding will be tried only if `-use-start-tls-for-ad-ldap` or `-use-ldaps-for-ad-ldap` is enabled along with `-session-security-for-ad-ldap` set to either *sign* or *seal*.

### **[`-advertised-enc-types <CIFS Kerberos Encryption Type>,...`] - Encryption Types Advertised to Kerberos**

Encryption types advertised to Kerberos. The default setting is ``aes-256``,`aes-128`,`rc4`,`des``.

## **Examples**

The following example makes the following changes: the Kerberos clock skew is set to 3 minutes, the Kerberos ticket lifetime to 8 hours and it makes signing required for Vserver "vs1".



```

cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock-skew
3 -kerberos-ticket-age 8 -is-signing-required true
cluster1::> vserver cifs security show
Vserver: vs1
Kerberos Clock Skew:          3 minutes
                                Kerberos Ticket Age:          8
hours
                                Kerberos Renewal Age:          7
days
                                Kerberos KDC Timeout:          3
seconds
                                Is Signing Required:          true
                                Is Password Complexity Required: true
                                Use start_tls For AD LDAP connection: false
                                Is AES Encryption Enabled:      true
                                LM Compatibility Level:         krb
                                Is SMB Encryption Required:     false
                                Client Session Security:        none
                                SMB1 Enabled For DC Connections: system-default
                                SMB2 Enabled For DC Connections: system-default
LDAP Referral Chasing Enabled For AD LDAP Connections: false
                                Use LDAPS for AD LDAP Connections: true
                                Encryption required For DC Connections: false
                                AES enabled for Netlogon channel: false
                                Try Channel Binding For AD LDAP Connections: true
                                Encryption Types Advertised to Kerberos: aes-256, aes-128,
des, rc4

```

## vserver cifs security show

Display CIFS security settings

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs security show` command displays information about CIFS server security settings.

### Parameters

{ [-fields <fieldname>,...]

If you specify the `-fields` parameter, the command only displays the fields that you specify.

| [-instance ] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver name>] - Vserver**

This parameter specifies the name of the Vserver whose CIFS security settings you want to display.

**[-kerberos-clock-skew <integer>] - Maximum Allowed Kerberos Clock Skew**

If this parameter is specified, the command displays information only about the security settings that match the specified Kerberos ticket clock skew.

**[-kerberos-ticket-age <integer>] - Kerberos Ticket Lifetime**

If this parameter is specified, the command displays information only about the security settings that match the specified Kerberos ticket age.

**[-kerberos-renew-age <integer>] - Maximum Kerberos Ticket Renewal Days**

If this parameter is specified, the command displays information only about the security settings that match the specified Kerberos renewal age.

**[-kerberos-kdc-timeout <integer>] - Timeout for Kerberos KDC Connections (Secs)**

If this parameter is specified, the command displays information only about the security settings that match the specified Kerberos KDC timeout.

**[-realm <text>] - Kerberos Realm**

If this parameter is specified, the command displays information only about the security settings that match the specified Kerberos realm.

**[-kdc-ip <text>,...] - KDC IP Address**

If this parameter is specified, the command displays information only about the security settings that match the specified KDC IP address.

**[-kdc-name <text>,...] - KDC Name**

If this parameter is specified, the command displays information only about the security settings that match the specified KDC name.

**[-site <text>,...] - KDC Site**

If this parameter is specified, the command displays information only about the security settings that match the specified Windows site.

**[-is-signing-required {true|false}] - Require Signing for Incoming CIFS Traffic**

This parameter specifies whether signing is required for incoming CIFS traffic. If this parameter is specified, the command displays information only about the security settings that match the specified value for is-signing-required.

**[-is-password-complexity-required {true|false}] - Require Password Complexity for Local User Accounts**

If this parameter is set to *true*, the command displays CIFS security configuration information only for CIFS servers where password complexity for local user accounts is required. If set to *false*, the command displays security configuration information for CIFS servers where password complexity for local user accounts is not required.

**[-use-start-tls-for-ad-ldap {true|false}] - Use start\_tls for AD LDAP Connections**

If this parameter is set to *true*, the command displays CIFS security configuration information only for CIFS servers where Start TLS is used for communication with the AD LDAP Server. If set to *false*, the

command displays CIFS security configuration information only for CIFS servers where Start TLS is not used for communication with the AD LDAP Server.

**`[-is-aes-encryption-enabled {true|false}] - (DEPRECATED)-Is AES-128 and AES-256 Encryption for Kerberos Enabled`**

If this parameter is set to *true*, the command displays CIFS security configuration information only for CIFS servers where AES-128 and AES-256 encryption types for Kerberos are enabled. If set to *false*, the command displays security configuration information for CIFS servers where AES-128 and AES-256 encryption types for Kerberos are disabled.



This parameter is deprecated and may be removed from a future release.

**`[-lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}] - LM Compatibility Level`**

If this parameter is specified, the command displays information only about the security settings that match the specified LM compatibility level.

**`[-is-smb-encryption-required {true|false}] - Require SMB Encryption for Incoming CIFS Traffic`**

If this parameter is set to *true*, the command displays CIFS security configuration information only for CIFS servers where SMB encryption is required. If set to *false*, the command displays security configuration information for CIFS servers where SMB encryption is not required.

**`[-session-security-for-ad-ldap {none|sign|seal}] - Client Session Security`**

If this parameter is set to *seal*, the command displays CIFS security configuration information only for CIFS servers where both signing and sealing are required for LDAP communications. If set to *sign*, the command displays security configuration information for CIFS servers where only signing is required for LDAP communications. If set to *none*, the command displays security configuration information for CIFS servers where no security is required for LDAP communications.

**`[-smb1-enabled-for-dc-connections {false|true|system-default}] - (DEPRECATED)-SMB1 Enabled for DC Connections`**

If this parameter is set to *true*, the command displays CIFS security configuration information only for CIFS servers where SMB1 is enabled for use with connections to domain controllers. If set to *false*, the command displays security configuration information for CIFS servers where SMB1 is not enabled for use with connections to domain controllers. If set to *system-default*, the command displays security configuration information for CIFS servers where the system-default setting (SMB1 enabled) is used for connections to domain controllers.



This parameter is deprecated because the SMB1 protocol is obsolete and considered insecure. It might be removed in a future release.

**`[-smb2-enabled-for-dc-connections {false|true|system-default}] - SMB2 Enabled for DC Connections`**

If this parameter is set to *true*, the command displays CIFS security configuration information only for CIFS servers where SMB2 is enabled for use with connections to domain controllers. If set to *false*, the command displays security configuration information for CIFS servers where SMB2 is not enabled for use with connections to domain controllers. If set to *system-default*, the command displays security configuration information for CIFS servers where the system-default setting (SMB2 enabled) is used for connections to domain controllers.

**`[-referral-enabled-for-ad-ldap {true|false}]` - LDAP Referral Chasing Enabled For AD LDAP Connections**

If this parameter is set to *true*, the command displays CIFS security configuration information only for CIFS servers where LDAP referral is enabled for AD LDAP connections. If set to *false*, the command displays security configuration information for CIFS servers where LDAP referral is not enabled for AD LDAP connections.

**`[-use-ldaps-for-ad-ldap {true|false}]` - Use LDAPS for Secure Active Directory LDAP Connections**

If this parameter is set to *true*, the command displays CIFS security configuration information only for CIFS servers where LDAPS is used for communication with the AD LDAP Server. If set to *false*, the command displays CIFS security configuration information only for CIFS servers where LDAPS is not used for communication with the AD LDAP Server.

**`[-encryption-required-for-dc-connections {true|false}]` - Encryption is required for DC Connection**

If this parameter is set to *true*, the command displays CIFS security configuration information only for CIFS servers where encryption is required for use with connections to domain controllers. If set to *false*, the command displays security configuration information for CIFS servers where encryption is not required for use with connections to domain controllers.

**`[-aes-enabled-for-netlogon-channel {true|false}]` - AES session key enabled for NetLogon channel**

If this parameter is set to *true*, the command displays CIFS security configuration information only for CIFS servers where AES session key is used for Netlogon secure channel. If set to *false*, the command displays CIFS security configuration information only for CIFS servers where AES session key is not used for Netlogon secure channel.

**`[-try-channel-binding-for-ad-ldap {true|false}]` - Try Channel Binding For AD LDAP Connections**

If this parameter is set to *true*, the command displays CIFS security configuration information only for CIFS servers where channel binding is tried for AD LDAP connections. If set to *false*, the command displays CIFS security configuration information only for CIFS servers where channel binding is not tried for AD LDAP connections.

**`[-advertised-enc-types <CIFS Kerberos Encryption Type>,...]` - Encryption Types Advertised to Kerberos**

If this parameter is specified, the command displays information only about the security settings that match the specified advertised encryption types.

## Examples

The following example displays CIFS server security settings.

```

cluster1::> vserver cifs security show
Vserver: vs1
Kerberos Clock Skew:          3 minutes
                                Kerberos Ticket Age:          8
hours
                                Kerberos Renewal Age:           7
days
                                Kerberos KDC Timeout:          3
seconds
                                Is Signing Required:           true
                                Is Password Complexity Required: true
                                Use start_tls For AD LDAP connection: false
                                Is AES Encryption Enabled:      false
                                LM Compatibility Level:          krb
                                Is SMB Encryption Required:     false
                                Client Session Security:        none
                                SMB1 Enabled For DC Connections: system-default
                                SMB2 Enabled For DC Connections: system-default
LDAP Referral Chasing Enabled For AD LDAP Connections: false
                                Use LDAPS for AD LDAP Connections: true
                                Encryption required For DC Connections: false
AES session key enabled for NetLogon channel: false
                                Try Channel Binding For AD LDAP Connections: true
                                Encryption Types Advertised to Kerberos: des, rc4

```

The following example displays the Kerberos clock skew for all Vservers.

```

cluster1::> vserver cifs security show -fields kerberos-clock-skew
vserver kerberos-clock-skew
-----
vs1      5

```

## vserver cifs session close

Close an open CIFS session

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs session close` command closes the specified CIFS sessions.

## Parameters

### **-node {<nodename>|local} - Node**

If you specify this parameter, the command will close all the opened CIFS sessions on the specified node.

### **-vserver <vserver name> - Vserver**

If you specify this parameter, the command will close all the opened CIFS sessions on the specified CIFS-enabled Vserver.

### **-session-id <integer> - Session ID**

If you specify this parameter, the command will close the open CIFS session that matches the specified session ID.

### **[-connection-id <integer>] - Connection ID**

If you specify this parameter, the command will close all the opened CIFS sessions that match the specified connection ID.

### **[-lif-address <IP Address>] - Incoming Data LIF IP Address**

If you specify this parameter, the command will close all the opened CIFS sessions that are established through the specified data LIF IP address.

### **[-address <IP Address>] - Workstation IP address**

If you specify this parameter, the command will close all the opened CIFS sessions that are opened from the specified IP address.

### **[-auth-mechanism <Authentication Mechanism>] - Authentication Mechanism**

If you specify this parameter, the command will close all the opened CIFS sessions that used the specified authentication mechanism. The authentication mechanism can include one of the following:

- NTLMv1 - NTLMv1 authentication mechanism
- NTLMv2 - NTLMv2 authentication mechanism
- Kerberos - Kerberos authentication mechanism
- Anonymous - Anonymous authentication mechanism

### **[-windows-user <TextNoCase>] - Windows User**

If you specify this parameter, the command will close all the opened CIFS sessions that are established for the specified CIFS user. The acceptable format for CIFS user is [domain]\user.

### **[-unix-user <text>] - UNIX User**

If you specify this parameter, the command will close all the opened CIFS sessions that are established for the specified UNIX user.

### **[-protocol-version <CIFS Dialects>] - Protocol Version**

If you specify this parameter, the command will close all the opened CIFS sessions that are established over the specified version of CIFS protocol. The protocol version can include one of the following:

- SMB1 - SMB 1.0
- SMB2 - SMB 2.0
- SMB2\_1 - SMB 2.1

- SMB3 - SMB 3.0
- SMB3\_1 - SMB 3.1

### **[-continuously-available <CIFS Open File Protection>] - Continuously Available**

If you specify this parameter, the command will close all the opened CIFS sessions with open files that have the specified level of continuously available protection. The open files are "continuously available" if they are opened from an SMB 3 client through a share with the "continuously\_available" property set. These open files are capable of non-disruptively recovering from takeover and giveback as well as general aggregate relocation between partners in a high-availability relationship. This is in addition to the traditional SMB 2 capability allowing clients to recover from LIF migration and other brief network interruptions.



The CA protection levels depict the continuous availability at the connection level so it might not be accurate for a session if the connection has multiple sessions. Streams opened through a continuously available share are permitted, but are not currently made continuously available. Directories may be opened through a continuously available share, but, by design, will not appear continuously available as clients do not open them that way. These protection levels are applicable to the sessions on read/write volumes residing on storage failover aggregates.

The continuously available status can be one of the following:

- No - The session contains one or more open file but none of them are continuously available.
- Yes - The session contains one or more open files and all of them are continuously available.
- Partial - The session contains at least one continuously available open file but other open files that are not.

### **[-is-session-signed {true|false}] - Is Session Signed**

If you specify this parameter, the command will close all the opened CIFS sessions that are established with the specified SMB signing option.

### **[-smb-encryption-status {unencrypted|encrypted|partially-encrypted}] - SMB Encryption Status**

If you specify this parameter, the command will close all the opened CIFS sessions that are established over the specified SMB encryption status.

The SMB encryption status can be one of the following:

- unencrypted - The CIFS session is not encrypted.
- encrypted - The CIFS session is fully encrypted. Vserver level encryption is enabled and encryption happens for the entire session.
- partially-encrypted - The CIFS session is partially encrypted. Share level encryption is enabled and encryption is initiated when the tree-connect occurs.

## **Examples**

The following example closes all open CIFS sessions on all the nodes with protocol-version SMB2:

```
cluster1::> cifs session close -node * -protocol-version SMB2
2 entries were acted on.
```

The following example closes all open CIFS sessions for all Vservers on node node1:

```
cluster1::> cifs session close -node node1 -vserver *
3 entries were acted on.
```

## vserver cifs session show

Display established CIFS sessions

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs session show` command displays information about established CIFS sessions. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all CIFS sessions:

- Node name
- Vserver name
- CIFS connection ID
- CIFS session ID
- Workstation IP address
- CIFS user name
- CIFS open files
- Session idle time

You can specify additional parameters to display only information that matches those parameters. For example, to display information only about CIFS sessions established on connection ID 2012, run the command with the `-connection-id` parameter set to `2012`.

### Parameters

**{ [-fields <fieldname>,...]**

If you specify this parameter, the command only displays the fields that you specify.

**| [-active-volumes ]**

If you specify this parameter, the command displays the list of Volumes that session has been connected.

**| [-show-win-unix-creds ]**

If you specify this parameter along with a valid session-id, the command displays Windows and UNIX credentials along with the detailed information about matching CIFS sessions.



**[ [-instance ] ] }**

If you specify this parameter, the command displays detailed information about matching CIFS sessions.

**[ -node {<nodename>|local} ] - Node**

If you specify this parameter, the command displays information about the CIFS sessions on the specified node.

**[ -vserver <vserver name> ] - Vserver**

If you specify this parameter, the command displays information about CIFS sessions on the specified CIFS-enabled Vserver.

**[ -session-id <integer> ] - Session ID**

If you specify this parameter, the command displays information about the CIFS session that match the specified session ID.

**[ -connection-id <integer> ] - Connection ID**

If you specify this parameter, the command displays information about CIFS sessions that match the specified connection ID.

**[ -lif-address <IP Address> ] - Incoming Data LIF IP Address**

If you specify this parameter, the command displays information about CIFS sessions that are established through the specified data LIF IP address.

**[ -address <IP Address> ] - Workstation IP address**

If you specify this parameter, the command displays information about CIFS sessions that are opened from the specified IP address.

**[ -auth-mechanism <Authentication Mechanism> ] - Authentication Mechanism**

If you specify this parameter, the command displays information about CIFS sessions that used the specified authentication mechanism. The authentication mechanism can include one of the following:

- None - Could not authenticate
- NTLMv1 - NTLMv1 authentication mechanism
- NTLMv2 - NTLMv2 authentication mechanism
- Kerberos - Kerberos authentication mechanism
- Anonymous - Anonymous authentication mechanism

**[ -windows-user <TextNoCase> ] - Windows User**

If you specify this parameter, the command displays information about CIFS sessions that are established for the specified CIFS user. The acceptable format for CIFS user is [domain]\user.

**[ -unix-user <text> ] - UNIX User**

If you specify this parameter, the command displays information about CIFS sessions that are established for the specified UNIX user.

**[ -shares <integer> ] - Open Shares**

If you specify this parameter, the command displays information about CIFS sessions that have the specified number of CIFS shares opened.

### **[-files <integer>] - Open Files**

If you specify this parameter, the command displays information about CIFS sessions that have the specified number of regular CIFS files opened.

### **[-other <integer>] - Open Other**

If you specify this parameter, the command displays information about CIFS sessions that have the specified number of special CIFS files opened such as streams or directories.

### **[-connected-time <[<integer>d] [<integer>h] [<integer>m] [<integer>s]>] - Connected Time**

If you specify this parameter, the command displays information about CIFS sessions that are established for the specified time duration.

### **[-idle-time <[<integer>d] [<integer>h] [<integer>m] [<integer>s]>] - Idle Time**

If you specify this parameter, the command displays information about CIFS sessions on which there is no activity for the specified time duration.

### **[-protocol-version <CIFS Dialects>] - Protocol Version**

If you specify this parameter, the command displays information about CIFS sessions that are established over the specified version of CIFS protocol. The protocol version can include one of the following:

- SMB1 - SMB 1.0
- SMB2 - SMB 2.0
- SMB2\_1 - SMB 2.1
- SMB3 - SMB 3.0
- SMB3\_1 - SMB 3.1

### **[-continuously-available <CIFS Open File Protection>] - Continuously Available**

If you specify this parameter, the command displays information about CIFS sessions with open files that have the specified level of continuously available protection. The open files are "continuously available" if they are opened from an SMB 3 client through a share with the "continuously\_available" property set. These open files are capable of non-disruptively recovering from takeover and giveback as well as general aggregate relocation between partners in a high-availability relationship. This is in addition to the traditional SMB 2 capability allowing clients to recover from LIF migration and other brief network interruptions.



The CA protection levels depict the continuous availability at the connection level so it might not be accurate for a session if the connection has multiple sessions. Streams opened through a continuously available share are permitted, but are not currently made continuously available. Directories may be opened through a continuously available share, but, by design, will not appear continuously available as clients do not open them that way. These protection levels are applicable to the sessions on read/write volumes residing on storage failover aggregates.

The continuously available status can be one of the following:

- No - The session contains one or more open file but none of them are continuously available.
- Yes - The session contains one or more open files and all of them are continuously available.
- Partial - The session contains at least one continuously available open file but other open files that are not.

### **[`-is-session-signed` {`true`|`false`}] - Is Session Signed**

If you specify this parameter, the command displays information about CIFS sessions that are established with the specified SMB signing option.

### **[`-user-type` {`local-user`|`domain-user`|`guest-user`|`anonymous-user`}] - User Authenticated as**

If you specify this parameter, the command displays information about CIFS sessions that are established for the specified user type. The user type can include one of the following:

- `local-user` - Authenticated as a local CIFS user
- `domain-user` - Authenticated as a domain user
- `guest-user` - Authenticated as a guest user
- `anonymous-user` - Authenticated as an anonymous or null user

### **[`-netbios-name` <text>] - NetBIOS Name**

If you specify this parameter, the command displays information about CIFS sessions that are established with the specified NetBIOS Name.

### **[`-smb-encryption-status` {`unencrypted`|`encrypted`|`partially-encrypted`}] - SMB Encryption Status**

If you specify this parameter, the command displays information about CIFS sessions that are established with the specified SMB encryption status.

The SMB encryption status can be one of the following:

- `unencrypted` - The CIFS session is not encrypted.
- `encrypted` - The CIFS session is fully encrypted. Vserver level encryption is enabled and encryption happens for the entire session.
- `partially-encrypted` - The CIFS session is partially encrypted. Share level encryption is enabled and encryption is initiated when the tree-connect occurs.

### **[`-connection-count` <integer>] - Connection Count**

If you specify this parameter, the command displays information about CIFS sessions that have the specified number of CIFS connections.

### **[`-is-large-mtu-enabled` {`true`|`false`}] - Is Large MTU Enabled**

If you specify this parameter, the command displays information about CIFS sessions that are established with the specified Large MTU option.

### **[`-vol-names` <volume name>,...] - Volumes List**

If you specify this parameter, the command displays information about CIFS sessions that are established with the specified volume names.

### **[`-share-names` <Share>,...] - Open Shares Lists**

If you specify this parameter, the command displays information about CIFS sessions that are established including the specified share names.

## Examples

The following example displays information about all CIFS sessions:

```
cluster1::> vserver cifs session show
Node:      node1
Vserver:   vs1
Connection Session                               Open
Idle      Connection                               Files
ID         ID      Workstation      Windows User      Files
Time                               Count
-----
-----
127834     1      172.17.193.172  CIFSQA\          2
22s                               4
                               Administrator
```

The following example displays information about a CIFS session with session-id 1.

```
cluster1::> vserver cifs session show -session-id 1 -instance
Node: node1
      Vserver: vs1
      Session ID: 1
      Connection ID: 127834
Incoming Data LIF IP Address: 10.53.13.224
      Workstation: 172.17.193.172
      Authentication Mechanism: NTLMv2
      Windows User: CIFSQA\Administrator
      UNIX User: root
      Open Shares: 2
      Open Files: 2
      Open Other: 0
      Connected Time: 2d 17h 58m 5s
      Idle Time: 22s
      Protocol Version: SMB3
      Continuously Available: No
      Is Session Signed: true
      User Authenticated as: domain-user
      NetBIOS Name: ALIAS1
      SMB Encryption Status: encrypted
      Connection Count: 4
Windows Unix Credentials: -
      Active Volumes: voll,fg
```

# vserver cifs session file close

Close an open CIFS file

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs session file close` command closes the specified open CIFS file.

## Parameters

**-node {<nodename>|local} - Node**

If you specify this parameter, the command will close all the opened CIFS files on the specified node.

**-vserver <vserver name> - Vserver**

If you specify this parameter, the command will close all the opened CIFS files on the specified CIFS-enabled Vserver.

**-file-id <integer> - File ID**

If you specify this parameter, the command will close the opened CIFS file that matches the specified file ID.

**[-connection-id <integer>] - Connection ID**

If you specify this parameter, the command will close all the opened CIFS files connected on the specified connection ID.

**[-session-id <integer>] - Session ID**

If you specify this parameter, the command will close all the opened CIFS files connected on the specified session ID.

## Examples

The following example closes all the opened CIFS files that are connected to the data LIFs of Vserver vs1 on the node node1 with the connection-id 1:

```
cluster1::> vserver cifs session file close -node node1 -vserver vs1
-connection-id 1
5 entries were acted on.
```

The following example closes all the opened CIFS files on the node node1 with the file-id 1, connection-id 1 and the session-id 1:

```
cluster1::> vserver cifs session file close -node node1 -file-id 1
-connection-id 1 -session-id 1
2 entries were acted on.
```

# vserver cifs session file show

Display opened CIFS files

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs session file show` command displays information about all open CIFS files. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all open CIFS files:

- Node name
- Vserver name
- CIFS connection ID
- CIFS session ID
- CIFS file ID
- CIFS file type
- CIFS file open mode
- CIFS file hosting volume
- CIFS share name
- CIFS file path
- Continuously available protection level

```
You can specify additional parameters to display only information that matches those parameters. For example, to display information only about CIFS files opened on connection ID 2012, run the command with the `-connection-id parameter set to ` 2012.
```

## Parameters

**{ [-fields <fieldname>,...]**

If you specify this parameter, the command only displays the fields that you specify.

**| [-instance ] }**

If you specify this parameter, the command displays detailed information about matching open CIFS files.

**[-node {<nodename>|local}] - Node**

If you specify this parameter, the command displays information about the open CIFS files on the specified node.

**[-vserver <vserver name>] - Vserver**

If you specify this parameter, the command displays information about open CIFS files on the specified CIFS-enabled Vserver.

**[-file-id <integer>] - File ID**

If you specify this parameter, the command displays information about the open CIFS file that match the specified file ID.

**[-connection-id <integer>] - Connection ID**

If you specify this parameter, the command displays information about open CIFS files that are opened on the specified connection ID.

**[-session-id <integer>] - Session ID**

If you specify this parameter, the command displays information about the CIFS file that are opened on the specified session ID.

**[-connection-count <integer>] - Connection Count**

If you specify this parameter, the command displays information about CIFS files opened through a session that have the specified number of CIFS connections.

**[-file-type <CIFS File Type>] - File Type**

If you specify this parameter, the command displays information about opened CIFS files that are of the specified file type. The file type can be any of these: Regular, Symlink, Stream, or Directory.

**[-open-mode <CIFS Open Mode>] - Open Mode**

If you specify this parameter, the command displays information about CIFS files that are opened with the specified mode. The open mode can include one or more of the following:

- R - This property specifies that the file is opened for read.
- W - This property specifies that the file is opened for write.
- D - This property specifies that the file is opened for delete.

The open mode can have multiple values specified as a list with no commas.

**[-hosting-aggregate <aggregate name>] - Aggregate Hosting File**

If you specify this parameter, the command displays information about open CIFS files that reside on the specified aggregate.

**[-hosting-volume <volume name>] - Volume Hosting File**

If you specify this parameter, the command displays information about open CIFS files that reside on the specified volume.

**[-share <Share>] - CIFS Share**

If you specify this parameter, the command displays information about CIFS files that are opened over the specified CIFS share.

**[-path <text>] - Path from CIFS Share**

If you specify this parameter, the command displays information about open CIFS files that match the specified CIFS file path.

**[-share-mode <CIFS Open Mode>] - Share Mode**

If you specify this parameter, the command displays information about open CIFS files that are opened with the specified share mode. The share mode can include one or more of the following:

- R - This property specifies that the file is shared for read.
- W - This property specifies that the file is shared for write.
- D - This property specifies that the file is shared for delete.

The share mode can have multiple values specified as a list with no commas.

#### **[-range-locks <integer>] - Range Locks**

If you specify this parameter, the command displays information about open CIFS files that have the specified number of range locks.

#### **[-continuously-available <CIFS Open File Protection>] - Continuously Available**

If you specify this parameter, the command displays information about open CIFS files with or without continuously available protection. The open files are "continuously available" if they are opened from an SMB 3 client through a share with the "continuously\_available" property set. These open files are capable of non-disruptively recovering from takeover and giveback as well as general aggregate relocation between partners in a high-availability relationship. Streams opened through a continuously available share are permitted, but are not currently made continuously available. Directories may be opened through a continuously available share, but, by design, will not appear continuously available as clients do not open them that way. These protection levels are applicable to the files on read/write volumes residing on storage failover aggregates.

The continuously available status can be one of the following:

- No - The open file is not continuously available.
- Yes - The open file is continuously available.

#### **[-reconnected <text>] - Reconnected**

If you specify this parameter, the command displays information about open CIFS files that have the specified reconnected state. The reconnected state can be one of the following:

- No - The open file is not reconnected.
- Yes - The open file is reconnected.

#### **[-flexgroup-msid <integer>] - FlexGroup MSID**

If you specify this parameter, the command displays information about open CIFS files that reside on the volume within the FlexGroup with the specified MSID..

## **Examples**

The following example displays information about all open CIFS files:



```

cluster1::> vserver cifs session file show

Node:      node1
Vserver:   vs1
Connection: 2192
Session:    1
Connection Count: 4
File      File      Open Hosting      Continuously
ID        Type        Mode Volume        Share              Available
-----
7         Regular   rw  rootvs1          rootca             Yes
Path: \win8b8.txt

```

The following example displays information about a CIFS file with file-id 7.

```

cluster1::> vserver cifs session file show -file-id 7 -instance
Node: node1
      Vserver: vs1
      File ID: 7
      Connection ID: 2192
      Session ID: 1
      Connection count: 4
      File Type: Regular
      Open Mode: rw
Aggregate Hosting File: aggr1
      Volume Hosting File: rootvs1
      CIFS Share: rootca
      Path from CIFS Share: \win8b8.txt
      Share Mode: rd
      Range Locks: 0
Continuously Available: Yes
      Reconnected: No

```

## vserver cifs share create

Create a CIFS share

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs share create` command creates a CIFS share.

## Parameters

### **-vserver <vserver name> - Vserver**

This parameter specifies the CIFS-enabled Vserver on which you want to create a CIFS share.

### **-share-name <Share> - Share**

This parameter specifies the name of the CIFS share that you want to create. A share name can be up to 80 characters long. If this is a home directory share (designated as such by specifying the *homedirectory* on the *-share-properties* parameter), you can include %w (Windows user name), %u (UNIX user name) and %d (Windows domain name) variables in any combination with this parameter to generate shares dynamically, with the resultant share names based on the authenticating user's Windows user name, UNIX user name, and/or Windows domain name. If the share is used by administrators to connect to other users' home directory (the option *is-home-dirs-access-for-admin-enabled* is set to true) or by a user to connect to other users' home directory (the option *is-home-dirs-access-for-public-enabled* is set to true) , the dynamic share pattern must be preceded by a tilde (~).

### **-path <text> - Path**

This parameter specifies the path to the CIFS share. This path must exist in a volume. A directory path name can be up to 256 characters long. If there is a space in the path name, you must enclose the entire string in quotation marks (for example, "/new volume/mount here"). If this is a home directory share as specified by value of home directory on the *-share-properties* parameter, you can make the path name dynamic by specifying the %w (Windows user name), %u (UNIX user name), or %d (domain name) variables or any of their combination as a part of the value of this parameter.

### **[-share-properties <share properties>,...] - Share Properties**

This optional parameter specifies a list of properties for the share. The list can include one or more of the following:

- *homedirectory* - This property specifies that the share and path names are dynamic. Specify this value for a home directory share. In a home directory share, Data ONTAP can dynamically generate the share's name and path by substituting %w, %u, and %d variables with the corresponding Windows user name, UNIX user name, and domain, respectively, specified as the value of the *-share-name* and *-path* parameters. For instance, if a dynamic share is defined with a name of %d%w\_ , a user logged on as barbara from a domain named *FIN* sees the share as *FIN\_barbara* . Using the *homedirectory* value specifies that the share and path names are dynamically expanded. This property cannot be added or removed after share creation.
- *oplocks* - This property specifies that the share uses opportunistic locks, also known as client-side caching. Oplocks are enabled on shares by default; however, some applications do not work well when oplocks are enabled. In particular, database applications such as Microsoft Access are vulnerable to corruption when oplocks are enabled. An advantage of shares is that a single path can be shared multiple times, with each share having different properties. For instance, if a path named /dept/finance contains both a database and other types of files, you can create two shares to it, one with oplocks disabled for safe database access and one with oplocks enabled for client-side caching.
- *browsable* - This property allows Windows clients to browse the share. This is the default initial property for all shares.
- *showsnapshot* - This property specifies that Snapshot copies can be viewed and traversed by clients.
- *changenotify* - This property specifies that the share supports ChangeNotify requests. This is a default initial property for all shares.
- *attributecache* - This property enables the file attribute caching on the CIFS share in order to provide faster access of attributes over SMB 1.0.



For certain workloads, stale file attribute data could be delivered to a client.

- continuously-available - This property permits SMB clients that support it to open files in a persistent manner. Files opened this way are protected from disruptive events, such as failover and giveback. This option is not supported for FlexGroups or workgroup CIFS servers.
- branchcache - This property specifies that the share allows clients to request BranchCache hashes on the files within this share. This option is useful only if you specify *per-share* as the operating mode in the CIFS BranchCache configuration, and also specify the "oplocks" share property.
- access-based-enumeration - This property specifies that Access Based Enumeration is enabled on this share. ABE-filtered shared folders are visible to a user based on that individual user's access rights, preventing the display of folders or other shared resources that the user does not have rights to access.
- namespace-caching - This property specifies that the SMB clients connecting to this share can cache the directory enumeration results returned by the CIFS servers.
- encrypt-data - This property specifies that SMB encryption must be used when accessing this share. Clients that do not support encryption will not be able to access this share.
- show-previous-versions - This property specifies that the previous version can be viewed and restored from the client. This property is enabled by default.

**[`-symlink-properties {enable|hide|read-only|symlinks|symlinks-and-widelinks|disable|no-strict-security}`] - Symlink Properties**

This optional parameter specifies how the storage system presents UNIX symbolic links (symlinks) to CIFS clients. The default value for this parameter is "symlinks". The list can include one or more of the following:

- enable (DEPRECATED\*) - This property enables both local symlinks and wide links for read-write access. DFS advertisements are generated for both local symlinks and wide links even if the CIFS option `-is-advertise-dfs-enabled` is set to false.
- hide (DEPRECATED\*) - This property hides symlinks. DFS advertisements are generated if the CIFS option `-is-advertise-dfs-enabled` is set to true.
- read-only (DEPRECATED\*) - This property enables symlinks for read-only access.
- symlinks - This property enables local symlinks for read-write access. DFS advertisements are not generated even if the CIFS option `-is-advertise-dfs-enabled` is set to true.
- symlinks-and-widelinks – This property enables both local symlinks and wide links for read-write access. DFS advertisements are generated for both local symlinks and wide links even if the CIFS option `-is-advertise-dfs-enabled` is set to false.
- disable - This property disables symlinks and wide links. DFS advertisements are not generated even if the CIFS option `-is-advertise-dfs-enabled` is set to true.
- no-strict-security - This property enables clients to follow symlinks outside share boundaries.



\* The *enable*, *hide*, and *read-only* parameters are deprecated and may be removed in a future release of Data ONTAP.



The `no_strict_security` setting does not apply to wide links.

**[`-file-umask <Octal Integer>`] - File Mode Creation Mask**

This optional parameter specifies the default UNIX umask for new files created on the share.

### **[-dir-umask <Octal Integer>] - Directory Mode Creation Mask**

This optional parameter specifies the default UNIX umask for new directories created on the share.

### **[-comment <text>] - Share Comment**

This optional parameter specifies a text comment for the share that is made available to Windows clients. The comment can be up to 256 characters long. If there is a space in the descriptive remark or the path, you must enclose the entire string in quotation marks (for example, "This is engineering's share.").

### **[-attribute-cache-ttl <[<integer>d] [<integer>h] [<integer>m] [<integer>s]>] - File Attribute Cache Lifetime**

This optional parameter specifies the lifetime for the attribute cache share property, which you specify as the value of the -share-properties parameter.



This value is useful only if you specify attributecache as a share property.

### **[-offline-files {none|manual|documents|programs}] - Offline Files**

This optional parameter allows Windows clients to cache data on this share. The actual caching behavior depends upon the Windows client. The value can be one of the following:

- none - Disallows Windows clients from caching any files on this share.
- manual - Allows users on Windows clients to manually select files to be cached.
- documents - Allows Windows clients to cache user documents that are used by the user for offline access.
- programs - Allows Windows clients to cache programs that are used by the user for offline access and may use those files in an offline mode even if the share is available.

### **[-vscan-fileop-profile {no-scan|standard|strict|writes-only}] - Vscan File-Operations Profile**

This optional parameter controls which operations trigger virus scans. The value can be one of the following:

- no-scan: Virus scans are never triggered for this share.
- standard: Virus scans can be triggered by open, close, and rename operations. This is the default profile.
- strict: Virus scans can be triggered by open, read, close, and rename operations.
- writes-only: Virus scans can be triggered only when a file that has been modified is closed.

### **[-max-connections-per-share <integer>] - Maximum Tree Connections on Share**

This optional parameter specifies the maximum number of simultaneous connections on the new share. This limit is at the node level, not the Vserver or cluster level. The default for this parameter is 4294967295. The value 4294967295 indicates no limit. The allowed range for this parameter is (1 through 4294967295).

### **[-force-group-for-create <text>] - UNIX Group for File Create**

This optional parameter specifies that all files that CIFS users create in a specific share belong to the same group (also called the "force-group"). The "force-group" must be a predefined group in the UNIX group database. This setting has no effect unless the security style of the volume is UNIX or mixed security style. If "force-group" has been specified for a share, the following becomes true for the share:

- Primary GID of the CIFS users who access this share is temporarily changed to the GID of the "force-

group".

- All files in this share that CIFS users create belong to the same "force-group", regardless of the primary GID of the file owner.

## Examples

The following example creates a CIFS share named SALES\_SHARE on a Vserver named vs1. The path to the share is /sales.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name SALES_SHARE  
-path /sales -symlink-properties enable
```

The following example creates a CIFS share named SALES\_SHARE on a Vserver named vs1. The path to the share is /sales and the share uses opportunistic locks (client-side caching), the share can be browsed by Windows clients, and a notification is generated when a change occurs.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name SALE -share  
-properties browsable, changenotify, oplocks, show-previous-versions
```

The following example creates a CIFS share named DOCUMENTS on a Vserver named vs1. The path to the share is /documents and the share uses opportunistic locks (client-side caching), a notification is generated when a change occurs, and the share allows clients to ask for BranchCache hashes for files in the share.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name DOCUMENTS  
path /documents -share-properties branchcache, changenotify, oplocks
```

The following example creates a CIFS share named DOCUMENTS on a Vserver named vs1. The path to the share is /documents and the share uses opportunistic locks (client-side caching), a notification is generated when a change occurs, and the share allows clients to cache (client-side caching) user documents on this share.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name DOCUMENTS  
-path /documents -share-properties changenotify, oplocks -offline-files  
documents
```

The following example creates a home directory share on a Vserver named vs1. The path to the share has a %d and %w combination.

```
cluster1::> vserver cifs share create -share-name %d%w -path %d/%w -share
-properties homedirectory -vserver vs1
```

The following example creates a home directory share on a Vserver vs1 to be used with the home directory option s is-home-dirs-access-for-admin-enabled and/or is-home-dirs-access-for-public-enabled . The path to the share has a %d and %w combination.

```
cluster1::> vserver cifs share create -share-name ~%d~%w -path %d/%w
-share-properties homedirectory -vserver vs1
```

## vserver cifs share delete

Delete a CIFS share

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs share delete` command deletes a CIFS share.

### Parameters

**-vserver <vserver name> - Vserver**

This parameter specifies the Vserver from which you want to delete a CIFS share.

**-share-name <Share> - Share**

This parameter specifies the name of the CIFS share you want to delete.

### Examples

The following example deletes a CIFS share named share1 from a Vserver named vs1.

```
cluster1::> vserver cifs share delete -vserver vs1 -share-name share1
```

## vserver cifs share modify

Modify a CIFS share

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs share modify` command modifies a CIFS share.

## Parameters

### **-vserver <vserver name> - Vserver**

This parameter specifies the CIFS-enabled Vserver containing the CIFS share you want to modify.

### **-share-name <Share> - Share**

This parameter specifies the name of the CIFS share that you want to create. A share name can be up to 80 characters long. If this is a home directory share (designated as such by specifying the *homedirectory* on the `-share-properties` parameter), you can include `%w` (Windows user name), `%u` (UNIX user name) and `%d` (Windows domain name) variables in any combination with this parameter to generate shares dynamically, with the resultant share names based on the authenticating user's Windows user name, UNIX user name, and/or Windows domain name.

### **[-path <text>] - Path**

This parameter specifies the path to the CIFS share. This path must exist in a volume. A directory path name can be up to 256 characters long. If there is a space in the path name, you must enclose the entire string in quotation marks (for example, `"/new volume/mount here"`). If this is a *homedirectory* share as specified by value of *home directory* on the `-share-properties` parameter, a dynamic path name must be specified using `%w` (Windows user name), `%u` (UNIX user name), or `%d` (domain name) variables or any of their combination as a part of the value of this parameter. If this is a *continuously-available* share as specified by value of *continuously-available* on the `-share-properties` parameter, the path must not be within a FlexGroup because this property is not supported for FlexGroups.

### **[-symlink-properties {enable|hide|read-only|symlinks|symlinks-and-widelinks|disable|no-strict-security}] - Symlink Properties**

This optional parameter specifies how the storage system presents UNIX symbolic links (symlinks) to CIFS clients. The list can include one or more of the following:

- `enable` (DEPRECATED\*) - This property enables both local symlinks and wide links for read-write access. DFS advertisements are generated for both local symlinks and wide links even if the CIFS option `-is-advertise-dfs-enabled` is set to `false`.
- `hide` (DEPRECATED\*) - This property hides symlinks. DFS advertisements are generated if the CIFS option `-is-advertise-dfs-enabled` is set to `true`.
- `read-only` (DEPRECATED\*) - This property enables symlinks for read-only access.
- `symlinks` - This property enables local symlinks for read-write access. DFS advertisements are not generated even if the CIFS option `-is-advertise-dfs-enabled` is set to `true`.
- `symlinks-and-widelinks` - This property enables both local symlinks and wide links for read-write access. DFS advertisements are generated for both local symlinks and wide links even if the CIFS option `-is-advertise-dfs-enabled` is set to `false`.
- `disable` - This property disables symlinks and wide links. DFS advertisements are not generated even if the CIFS option `-is-advertise-dfs-enabled` is set to `true`.
- `no-strict-security` - This property enables clients to follow symlinks outside share boundaries.



The `read_only` setting does not apply to wide links.



\* The *enable*, *hide*, and *read-only* parameters are deprecated and may be removed in a future release of Data ONTAP.



The `no_strict_security` setting does not apply to wide links.

### **[`-file-umask` <Octal Integer>] - File Mode Creation Mask**

This optional parameter specifies the default UNIX umask for new files created on the share.

### **[`-dir-umask` <Octal Integer>] - Directory Mode Creation Mask**

This optional parameter specifies the default UNIX umask for new directories created on the share.

### **[`-comment` <text>] - Share Comment**

This optional parameter specifies a text comment for the share that is made available to Windows clients. The comment can be up to 256 characters long. If there is a space in the descriptive remark or the path, you must enclose the entire string in quotation marks (for example, "This is engineering's share.").

### **[`-attribute-cache-ttl` <[<integer>d] [<integer>h] [<integer>m] [<integer>s]>] - File Attribute Cache Lifetime**

This optional parameter specifies the lifetime for the attribute cache share property, which you specify as the value of the `-share-properties` parameter.



This value is useful only if you specify `attributecache` as a share property.

### **[`-offline-files` {`none`|`manual`|`documents`|`programs`}] - Offline Files**

This optional parameter allows Windows clients to cache data on this share. The actual caching behavior depends upon the Windows client. The value can be one of the following:

- `none` - Disallows Windows clients from caching any files on this share.
- `manual` - Allows users on Windows clients to manually select files to be cached.
- `documents` - Allows Windows clients to cache user documents that are used by the user for offline access.
- `programs` - Allows Windows clients to cache programs that are used by the user for offline access and may use those files in an offline mode even if the share is available.

### **[`-vscan-fileop-profile` {`no-scan`|`standard`|`strict`|`writes-only`}] - Vscan File-Operations Profile**

This optional parameter controls which operations trigger virus scans. The value can be one of the following:

- `no-scan`: Virus scans are never triggered for this share.
- `standard`: Virus scans can be triggered by open, close, and rename operations. This is the default profile.
- `strict`: Virus scans can be triggered by open, read, close, and rename operations.
- `writes-only`: Virus scans can be triggered only when a file that has been modified is closed.

### **[`-max-connections-per-share` <integer>] - Maximum Tree Connections on Share**

This optional parameter specifies a maximum number of simultaneous connections to the share. This limit is at the node level, not the Vserver or cluster level. The default for this parameter is 4294967295. The



value 4294967295 indicates no limit. The allowed range for this parameter is (1 through 4294967295).

### **[`-force-group-for-create <text>`] - UNIX Group for File Create**

This optional parameter specifies that all files that CIFS users create in a specific share belong to the same group (also called the "force-group"). The "force-group" must be a predefined group in the UNIX group database. This setting has no effect unless the security style of the volume is UNIX or mixed security style. You can disable this option by passing a null string "".

## **Examples**

The following example modifies a CIFS share named SALES\_SHARE on a Vserver named vs1. The share uses opportunistic locks. The file mask is set to 644 and the directory mask to 777.

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name SALES_SHARE
-symlink-properties hide -file-umask 644 -dir-umask 777
```

The following example modifies a CIFS share named DOCUMENTS on a Vserver named vs1. This triggers a virus scan on write-only files in the share.

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name DOCUMENTS
-vscan-fileop-profile writes-only
```

The following example modifies a CIFS share named DOCUMENTS on a Vserver vs1. The share allows client to cache (client-side caching) user documents on this share.

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name DOCUMENTS
-offline-files documents
```

The following example modifies a CIFS share named DOCUMENTS on a Vserver named vs1. The optional parameter "force-group-for-create" can be disabled by passing the null string as parameter to "force-group-for-create" option.

```
cluster1::> cifs share modify -vserver vs1 -share-name DOCUMENTS -force
-group-for-create ""
```

The following example modifies the symlink property of all the shares on all the Vserver to "enable".

```
cluster1::> vserver cifs share modify -vserver * -share-name * -symlink
-properties enable
```

## **vserver cifs share show**

Display CIFS shares

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs share show` command displays information about CIFS shares. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following information about all CIFS shares:

- Vserver name
- CIFS share name
- Path
- Share properties
- Comment

You can specify additional parameters to display only information that matches those parameters. For example, to display information only about CIFS shares that use dynamic shares, run the command with the ``-share-properties dynamicshare`` parameter.

## Parameters

**{ [-fields <fieldname>,...]**

If you specify this parameter, the command only displays the fields that you specify.

**| [-shadowcopy ]**

If you specify this parameter, the command displays information only about CIFS shadow copy shares.

**| [-umask ]**

If you specify this parameter, the command displays file and directory masks for CIFS shares.

**| [-instance ] }**

If you specify this parameter, the command displays detailed information about all CIFS shares.

**[-vserver <vserver name>] - Vserver**

If you specify this parameter, the command displays information only about CIFS shares on the specified CIFS-enabled Vserver.

**[-share-name <Share>] - Share**

If you specify this parameter, the command displays information only about the CIFS share or shares that match the specified name.

**[-cifs-server <NetBIOS>] - CIFS Server NetBIOS Name**

If you specify this parameter, the command displays information only about the CIFS share or shares that use the CIFS-enabled Vserver with the specified CIFS server name.

**[-path <text>] - Path**

If you specify this parameter, the command displays information only about the CIFS share or shares that have the specified path.

**[-share-properties <share properties>,...] - Share Properties**

If you specify this parameter, the command displays information only about the CIFS share or shares that have the specified share properties.

**[-symlink-properties {enable|hide|read-only|symlinks|symlinks-and-widelinks|disable|no-strict-security}] - Symlink Properties**

If you specify this parameter, the command displays information only about the CIFS share or shares that have the specified symbolic link properties.

**[-file-umask <Octal Integer>] - File Mode Creation Mask**

If you specify this parameter, the command displays information only about the CIFS share or shares that use the specified file mask.

**[-dir-umask <Octal Integer>] - Directory Mode Creation Mask**

If you specify this parameter, the command displays information only about the CIFS share or shares that use the specified directory mask.

**[-comment <text>] - Share Comment**

If you specify this parameter, the command displays information only about the CIFS share or shares that have the specified comment.

**[-acl <text>,...] - Share ACL**

If you specify this parameter, the command displays information only about the CIFS share or shares that have the specified ACL.

**[-attribute-cache-ttl <[<integer>d] [<integer>h] [<integer>m] [<integer>s]>] - File Attribute Cache Lifetime**

If you specify this parameter, the command displays information only about the CIFS share or shares that have the specified attribute-cache-ttl for attribute cache.

**[-volume <volume name>] - Volume Name**

If you specify this parameter, the command displays information only about the CIFS shares that are present in this volume.

**[-offline-files {none|manual|documents|programs}] - Offline Files**

If you specify this parameter, the command displays information only about the CIFS shares that have the specified Offline Files properties.

**[-vscan-fileop-profile {no-scan|standard|strict|writes-only}] - Vscan File-Operations Profile**

If you specify this parameter, the command displays information only about the CIFS shares that have the specified Vscan fileop profile.

**[-max-connections-per-share <integer>] - Maximum Tree Connections on Share**

If you specify this parameter, the command displays information only about the CIFS shares that have the specified maximum connections per share configured.

## **[`-force-group-for-create <text>`] - UNIX Group for File Create**

This optional parameter displays information about the CIFS shares that have the specified "force-group" parameter configured.

## **Examples**

The following example displays information about all CIFS shares:

```
cluster1::> vserver cifs share show
Vserver      Share      Path      Properties Comment  ACL
-----
vs1          ROOTSHARE  /          oplocks   Share   CNC \
             browsable mapped
             Everyone /
             changenoti to top   Full
             fy      of      Control
             Vserver
             global
             namespac
             e
vs1          admin$     /          browsable -      -
vs1          c$        /          oplocks   -
BUILTIN\Administrators /          browsable
             changenoti Full
             fy      Control
vs1          ipc$      /          browsable -      -
4 entries were displayed.
```

The following example displays information about a CIFS share named SALES\_SHARE on a Vserver named vs1.

```

cluster1::> vserver cifs share show -vserver vs1 -share-name SALES_SHARE
                Vserver: vs1
                Share: SALES_SHARE
    CIFS Server NetBIOS Name: WINDATA
                Path: /sales
    Share Properties: oplocks
                    browsable
    Symlink Properties: enable
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
                Share Comment: -
                Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                Offline Files: manual
    Vscan File-Operations Profile: standard

```

## vserver cifs share access-control create

Create an access control list

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs share access-control create` command adds a user or group to a CIFS share's ACL.

### Parameters

**-vserver <vserver name> - Vserver**

This parameter specifies the name of the Vserver containing the CIFS share.

**-share <Share> - Share Name**

This parameter specifies the name of the CIFS share.

**-user-or-group <TextNoCase> - User/Group Name**

This parameter specifies the user or group to add to the CIFS share's access control list. If you specify the user name, you must include the user's domain using the format "domain\username". The user-or-group parameter is case-insensitive text.

**[-user-group-type {windows|unix-user|unix-group}] - User or Group Type**

This parameter specifies the type of the user or group to add to the CIFS share's access control list. The default type is windows. The user-group-type can be one of the following:

- windows
- unix-user

- unix-group

### **-permission <access rights> - Access Type**

This parameter specifies the permissions for the user or group. The permissions can be one of the following:

- No\_access
- Read
- Change
- Full\_Control

## **Examples**

The following example adds the windows group "Everyone" with "Full\_Control" permission to the access control list of the share "vol3".

```
vs1::> vsserver cifs share access-control create -share vol3 -user-or-group
Everyone -user-group-type windows -permission Full_Control
```

The following example adds the unix-user "pcuser" and unix-group "daemon" with "read" permission to the access control list of the share "vol3".

```
vs1::> vsserver cifs share access-control create -share vol3 -user-or-group
pcuser -user-group-type unix-user -permission read
vs1::> vsserver cifs share access-control create -share vol3 -user
-or-group daemon -user-group-type unix-group -permission read
```

## **vsserver cifs share access-control delete**

Delete an access control list

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### **Description**

The `vsserver cifs share access-control delete` command deletes a user or group from a CIFS share's ACL.

### **Parameters**

#### **-vsserver <vsserver name> - Vserver**

This parameter specifies the name of the Vserver containing the CIFS share.

#### **-share <Share> - Share Name**

This parameter specifies the name of the CIFS share.

### **-user-or-group <TextNoCase> - User/Group Name**

This parameter specifies the user or group to delete from the CIFS share's access control list. If you specify a user name, you must include the user's domain using the format "domain\username". The user-or-group parameter is case-insensitive text.

### **[-user-group-type {windows|unix-user|unix-group}] - User or Group Type**

This parameter specifies the type of the user or group to delete from the CIFS share's access control list. The default type is windows. The user-group-type can be one of the following:

- windows
- unix-user
- unix-group

## **Examples**

The following example deletes the group "Everyone" for the access control list of share "vol3".

```
vs1::> vsriver cifs share access-control delete -share vol3 -user-or-group
Everyone
```

# **vserver cifs share access-control modify**

Modify an access control list

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## **Description**

The `vserver cifs share access-control modify` command modifies the permissions of a user or group in a CIFS share's ACL.

## **Parameters**

### **-vserver <vserver name> - Vserver**

This parameter specifies the name of the Vserver containing the CIFS share whose ACL you want to modify.

### **-share <Share> - Share Name**

This parameter specifies the name of the CIFS share whose ACL you want to modify.

### **-user-or-group <TextNoCase> - User/Group Name**

This parameter specifies the user or group to modify. If you specify the user name, you must include the user's domain using the format "domain\username". The user-or-group parameter is case-insensitive text.

### **[-user-group-type {windows|unix-user|unix-group}] - User or Group Type**

This parameter specifies the type of the user or group to modify. The default type is windows. The user-group-type can be one of the following:

- windows
- unix-user
- unix-group

### **[`-permission <access rights>`] - Access Type**

This parameter specifies the permissions for the user or group. The permissions can be one of the following:

- No\_access
- Read
- Change
- Full\_Control

## **Examples**

The following example modifies the access control list for a share named "vol3". It changes the permission for the windows group "Everyone" to "Full\_Control".

```
vs1::*> vsserver cifs share access-control modify -share vol3 -user-or
-group Everyone -user-group-type windows -permission Full_Control
```

The following example modifies the access control list for a share named "vol3". It changes the permission for the unix-user "pcuser" and unix-group "daemon" to "change".

```
vs1::> vsserver cifs share access-control modify -share vol3 -user-or-group
pcuser -user-group-type unix-user -permission change
vs1::> vsserver cifs share access-control modify -share vol3 -user
-or-group daemon -user-group-type unix-group -permission change
```

## **vserver cifs share access-control show**

Display access control lists on CIFS shares

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### **Description**

The `vserver cifs share access-control show` command displays the ACLs of CIFS shares.

### **Parameters**

**{ [`-fields <fieldname>`,...]**

If you specify the `-fields <fieldname>`, ... parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.



**[ `-instance` ] }**

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[ `-vserver <vserver name>` ] - Vserver**

This optional parameter specifies the name of the Vserver containing the share for which you want to display the access control list.

**[ `-share <Share>` ] - Share Name**

This optional parameter specifies the name of the CIFS share for which you want to display the access control list.

**[ `-user-or-group <TextNoCase>` ] - User/Group Name**

If you specify this optional parameter, the command displays only access control lists for the CIFS shares that have ACLs matching the specified user or group.

**[ `-user-group-type {windows|unix-user|unix-group}` ] - User or Group Type**

If you specify this optional parameter, the command displays only access control lists for the CIFS shares that have ACLs matching the specified user-group-type. The user-group-type can be one of the following:

- windows
- unix-user
- unix-group

**[ `-permission <access rights>` ] - Access Type**

If you specify this optional parameter, the command displays only access control lists for the CIFS shares that have ACLs matching the specified permission. The permissions can be one of the following:

- No\_access
- Read
- Change
- Full\_Control

**[ `-winsid <windows sid>` ] - Windows SID**

If you specify this optional parameter, the command displays only access control lists for the CIFS shares that have ACLs matching the specified Windows SID.

**[ `-access-mask <Hex Integer>` ] - Access mask**

If you specify this optional parameter, the command displays only access control lists for the CIFS shares that have ACLs matching the specified access rights.

## Examples

The following example displays all the ACLs for shares in Vserver vs1.

```

vs1::> vsserver cifs share access-control show
      Share      User/Group      User/Group  Access
Vserver  Name          Name           Type
Permission
-----
vs1      vol3          CIFSQA\administrator  windows    Read
vs1      vol3          Everyone         windows
Full_Control
vs1      vol3          pcuser           unix-user   Read
vs1      vol3          daemon           unix-group  Read

```

## vsserver cifs share properties add

Add to the list of share properties

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vsserver cifs share properties add` command adds share properties to the list of share properties of an existing CIFS share. You can add one or more share properties. You can add additional share properties at any time by rerunning this command. Any share properties that you have previously specified will remain in effect and newly added properties are appended to the existing list of share properties.

### Parameters

#### **-vsserver <vserver name> - Vserver**

This parameter specifies the name of the Vserver containing the CIFS share whose share properties you want to add.

#### **-share-name <Share> - Share**

This parameter specifies the name of the CIFS share.

#### **-share-properties <share properties>,... - Share Properties**

This parameter specifies the list of share properties you want to add to the CIFS share. The share properties can be one or more of the following:

- **oplocks** - This property specifies that the share uses opportunistic locks, also known as client-side caching. This is a default initial property for all shares; however, some applications do not work well when oplocks are enabled. In particular, database applications such as Microsoft Access are vulnerable to corruption when oplocks are enabled. An advantage of shares is that a single path can be shared multiple times, with each share having different properties. For instance, if a path named `/dept/finance` contains both a database and other types of files, you can create two shares to it, one with oplocks disabled for safe database access and one with oplocks enabled for client-side caching.
- **browsable** - This property allows Windows clients to browse the share. This is a default initial property for all shares.

- `showsnapshot` - This property specifies that Snapshot copies can be viewed and traversed by clients.
- `changenotify` - This property specifies that the share supports ChangeNotify requests. This is a default initial property for all shares.
- `attributecache` - This property enables the file attribute caching on the CIFS share in order to provide faster access of attributes over SMB 1.0.



For certain workloads, stale file attribute data could be delivered to a client.

- `continuously-available` - This property permits SMB clients that support it to open files in a persistent manner. Files opened this way are protected from disruptive events, such as failover and giveback. This option is not supported for FlexGroups or workgroup CIFS servers.
- `branchcache` - This property specifies that the share allows clients to request BranchCache hashes on the files within this share. This option is useful only if you specify "per-share" as the operating mode in the CIFS BranchCache configuration, and also specify the "`oplocks`" share property.
- `access-based-enumeration` - This property specifies that Access Based Enumeration(ABE) is enabled on this share. ABE-filtered shared folders are visible to a user based on that individual user's access rights, preventing the display of folders or other shared resources that the user does not have rights to access.
- `namespace-caching` - This property specifies that the SMB clients connecting to this share can cache the directory enumeration results returned by the CIFS servers.
- `encrypt-data` - This property specifies that SMB encryption must be used when accessing this share. Clients that do not support encryption will not be able to access this share.
- `show-previous-versions` - This property specifies that the previous version can be viewed and restored from the client. This property is enabled by default.



The `oplock`, `browsable`, `changenotify` and `show-previous-versions` share properties are assigned to a share by default. If you have removed them from a share, you can use the `vserver cifs share properties add` command to add these properties to the share.

## Examples

The following example adds the "`showsnapshot`" and "`changenotify`" properties to a share named "sh1".

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name sh1
-share-properties showsnapshot,changenotify
```

## vserver cifs share properties remove

Remove from the list of share properties

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs share properties remove` command removes share properties from the list of share properties of an existing CIFS share. You can remove one or more share properties. You can remove additional share properties at any time by rerunning this command. Any existing share properties that you do

not remove remain in effect.

## Parameters

### **-vserver <vserver name> - Vserver**

This parameter specifies the name of the Vserver containing the CIFS share whose share properties you want to remove.

### **-share-name <Share> - Share**

This parameter specifies the name of the CIFS share.

### **-share-properties <share properties>,... - Share Properties**

This parameter specifies the list of share properties you want to remove from the CIFS share. The share properties can be one or more of the following:

- **oplocks** - This property specifies that the share uses opportunistic locks, also known as client-side caching. Oplocks are enabled on shares by default; however, some applications do not work well when oplocks are enabled. In particular, database applications such as Microsoft Access are vulnerable to corruption when oplocks are enabled. An advantage of shares is that a single path can be shared multiple times, with each share having different properties. For instance, if a path named */dept/finance* contains both a database and other types of files, you can create two shares to it, one with oplocks disabled for safe database access and one with oplocks enabled for client-side caching.
- **browsable** - This property allows Windows clients to browse the share.
- **showsnapshot** - This property specifies that Snapshot copies can be viewed and traversed by clients.
- **changenotify** - This property specifies that the share supports ChangeNotify requests. This is a default initial property for all shares.
- **attributecache** - This property enables the file attribute caching on the CIFS share in order to provide faster access of attributes over SMB 1.0.



For certain workloads, stale file attribute data could be delivered to a client.

- **continuously-available** - This property permits SMB clients that support it to open files in a persistent manner. Files opened this way are protected from disruptive events, such as failover and giveback. This option is not supported for FlexGroups or workgroup CIFS servers.
- **branchcache** - This property specifies that the share allows clients to request BranchCache hashes on the files within this share. This option is useful only if you specify "per-share" as the operating mode in the CIFS BranchCache configuration, and also specify the "*oplocks*" share property.
- **access-based-enumeration** - This property specifies that Access Based Enumeration(ABE) is enabled on this share. ABE-filtered shared folders are visible to a user based on that individual user's access rights, preventing the display of folders or other shared resources that the user does not have rights to access.
- **namespace-caching** - This property specifies that the SMB clients connecting to this share can cache the directory enumeration results returned by the CIFS servers.
- **encrypt-data** - This property specifies that SMB encryption must be used when accessing this share. Clients that do not support encryption will not be able to access this share.
- **show-previous-versions** - This property specifies that the previous version can be viewed and restored from the client. This property is enabled by default.

## Examples

The following example removes "showsnapshot" and "changenotify" properties to a share named "sh1".

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name sh1 -share-properties showsnapshot,changenotify
```

## vserver cifs share properties show

Display share properties

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs share properties show` command displays the CIFS share properties.

### Parameters

**{ [-fields <fieldname>,...]**

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

**| [-instance ] }**

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver name>] - Vserver**

This optional parameter specifies the name of the Vserver containing the CIFS share for which you want to display share properties.

**[-share-name <Share>] - Share**

If you specify this parameter, the command displays share properties only for the CIFS share that you specify.

**[-share-properties <share properties>,...] - Share Properties**

If you specify this parameter, the command displays share properties only for CIFS shares using the properties you specify. The share properties can be one or more of the following:

- `homedirectory` - This property specifies that the share and path names are dynamic. Specify this value for a home directory share. In a home directory share, the share's name and path can be generated by substituting `%w` and `%d` variables with the corresponding user's name and domain, respectively, specified as the value of the `-share-name` and `-path` parameters. For instance, if a dynamic share is defined with a name of `%d%w_`, a user logged on as `barbara` from a domain named `FIN` sees the share as `FIN_barbara`. Using the `homedirectory` value specifies that the share and path names are dynamically expanded.
- `oplocks` - This property specifies that the share uses opportunistic locks, also known as client-side caching.
- `browsable` - This property allows Windows clients to browse the share.

- showsnapshot - This property specifies that Snapshot copies can be viewed and traversed by clients.
- changenotify - This property specifies that the share supports Change Notify requests.
- attributecache - This property enables the file attribute caching on the CIFS share in order to provide faster access of attributes over SMB 1.0.



For certain workloads, stale file attribute data could be delivered to a client.

- continuously-available - This property permits SMB clients that support it to open files in a persistent manner. Files opened this way are protected from disruptive events, such as failover and giveback. This attribute is not supported for FlexGroups and workgroup CIFS servers.
- branchcache - This property specifies that the share allows clients to request BranchCache hashes on the files within this share. This option is useful only if you specify "per-share" as the operating mode in the CIFS BranchCache configuration, and also specify the "*oplocks*" share property.
- shadowcopy - This property specifies that the share is pointing to a shadow copy. This attribute cannot be added nor removed from a share.
- access-based-enumeration - This property specifies that Access Based Enumeration is enabled on this share. ABE-filtered shared folders are visible to a user based on that individual user's access rights, preventing the display of folders or other shared resources that the user does not have rights to access.
- namespace-caching - This property specifies that the SMB clients connecting to this share can cache the directory enumeration results returned by the CIFS servers.
- encrypt-data - This property specifies that SMB encryption must be used when accessing this share. Clients that do not support encryption will not be able to access this share.
- show-previous-versions - This property specifies that the previous version can be viewed and restored from the client. This property is enabled by default.

## Examples

The following example displays share properties for shares in Vserver vs1.

```
cluster1::> vs1 cifs share properties show
Vserver      Share      Properties
-----
vs1          abc        oplocks
              browsable
              changenotify
              show-previous-versions
vs1          admin$     browsable
vs1          ipc$       browsable
vs1          sh1        oplocks
              browsable
              changenotify
              show-previous-versions

4 entries were displayed.
```

## vserver cifs superuser create

Adds superuser permissions to a CIFS account

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

### Description

The `vserver cifs superuser create` command elevates the privileges of the specified domain account in this Vserver to superuser. With superuser privileges, Data ONTAP bypasses some of the security checks. This command is not supported for workgroup CIFS servers.

### Parameters

**-vserver <vserver name> - Vserver (privilege: advanced)**

Vserver name.

**-domain <CIFS domain> - Domain (privilege: advanced)**

The domain name of accountname.

**-accountname <CIFS account> - User (privilege: advanced)**

The domain account to which you want to give superuser privileges.

### Examples

The following example shows how to elevate ExampleUser in EXAMPLE domain to superuser for a Vserver vs1.

```
vs1::> vserver cifs superuser create -domain EXAMPLE -accountname  
ExampleUser -vserver vs1
```

## vserver cifs superuser delete

Deletes superuser permissions from a CIFS account

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

### Description

The `vserver cifs superuser delete` command removes the superuser privileges for the specified domain account in this Vserver. With superuser privileges, Data ONTAP bypasses some of the security checks.

### Parameters

**-vserver <vserver name> - Vserver (privilege: advanced)**

Vserver name.

**-domain <CIFS domain> - Domain (privilege: advanced)**

The domain name of accountname.

**-accountname <CIFS account> - User (privilege: advanced)**

The domain account name you want to remove superuser privileges.

## Examples

The following example shows how to remove superuser privileges for ExampleUser in EXAMPLE domain for a Vserver vs1.

```
vs1::> vsriver cifs superuser delete -domain EXAMPLE -accountname
ExampleUser -vsriver vs1
```

## vsvriver cifs superuser show

Display superuser permissions for CIFS accounts

**Availability:** This command is available to *cluster* and *Vsvriver* administrators at the *advanced* privilege level.

### Description

The `vsvriver cifs superuser show` command displays all account names with superuser privileges. The command output depends on the parameter or parameters specified with the command. If you do not specify any parameters, the command displays the following superuser information for all CIFS servers:

- Vsvriver name
- CIFS server NetBIOS name
- Domain
- Account Name

### Parameters

**{ [-fields <fieldname>,...]**

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

**| [-instance ] }**

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vsriver <vsriver name>] - Vsvriver (privilege: advanced)**

If you specify this parameter, the command displays superuser information of only the specified Vservers.

**[-domain <CIFS domain>] - Domain (privilege: advanced)**

If you specify this parameter, the command displays superuser information of only for accounts that are in the specified domain.



### **[`-accountname <CIFS account>`] - User (privilege: advanced)**

If you specify this parameter, the command displays superuser information of only the CIFS servers with the specified superuser account.

### **[`-cifs-server <NetBIOS>`] - CIFS Server NetBIOS Name (privilege: advanced)**

If you specify this parameter, the command displays superuser information of only the Vservers with specified CIFS server name.

## Examples

The following example displays superuser information of all Vservers.

```
vs1::> vserver cifs superuser show
```

Vserver	CIFS Server	Domain	Account Name
vs1	SMB_SERVER1	CIFSDOMAIN	ADMINISTRATOR
vs2	SMB_SERVER2	CIFSDOMAIN	ADMINISTRATOR

## vserver cifs symlink create

Create a symlink path mapping

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs symlink create` command creates a symbolic link mapping for CIFS. A mapping consists of a Vserver name, a UNIX (NFS) path, a CIFS share name, and a CIFS path. You can also specify a CIFS server name and whether the CIFS symbolic link is a local link, a free link (obsolete), or wide link. A local symbolic link maps to the local CIFS share. A free symbolic link can map anywhere on the local server. A wide symbolic link maps to any CIFS share on the network. If the target share is a Home Directory, then the `-home-directory` field must be set to true for correct processing.

### Parameters

#### **`-vserver <vserver name>` - Vserver**

This parameter specifies the Vserver on which you want to create the mapping.

#### **`-unix-path <text>` - UNIX Path**

This parameter specifies the UNIX (NFS) path for the mapping.



It must begin and end with a forward slash (/).

#### **[`-share-name <Share>`] - CIFS Share**

This parameter specifies the CIFS share for the mapping.

### **-cifs-path <TextNoCase> - CIFS Path**

This parameter specifies the CIFS path for the mapping. Note that this value is specified by using a UNIX-style path.



It must begin and end with a forward slash (/).

### **[-cifs-server <TextNoCase>] - Remote NetBIOS Server Name**

This parameter specifies a new CIFS server DNS name, IP address, or NetBIOS name for the mapping.

### **[-locality {local|widelink}] - Local or Wide Symlink**

This parameter specifies whether the CIFS symbolic link is a local link, a free link (obsolete), or wide link. A local symbolic link maps to the local CIFS share. A free symbolic link can map anywhere on the local server. A wide symbolic link maps to any CIFS share on the network. The default setting is `local`. The free link option is obsolete.

### **[-home-directory {true|false}] - Home Directory**

This parameter specifies whether the target share is a home directory. The default value is `false`.



This field must be set to `true` when the target share is a Home Directory for correct processing.

## **Examples**

The following example creates a symbolic link mapping on a Vserver named `vs1`. It has the UNIX path `/sales/`, the CIFS share name `SALES_SHARE`, and the CIFS path `/mycompany/sales/`.

```
cluster1::> vsserver cifs symlink create -vserver vs1
-unix-path /sales/ -share-name SALES_SHARE -cifs-path "/mycompany/sales/"
```

The following example creates a symbolic link mapping on a Vserver named `vs1`. It has the UNIX path `/example/`, the CIFS share name `EXAMPLE_SHARE`, the CIFS path `/mycompany/example/`, the CIFS server IP address, and is a wide link.

```
cluster1::> vsserver cifs symlink create -vserver vs1 -unix-path /example/
-share-name EXAMPLE_SHARE
-cifs-path "/mycompany/example/" -cifs-server CIFSSEVER1 -locality
widelink
```

## **vserver cifs symlink delete**

Delete a symlink path mapping

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs symlink delete` command deletes a symbolic link mapping for CIFS.

## Parameters

**-vserver <vserver name> - Vserver**

This specifies the Vserver on which the symbolic link mapping is located.

**-unix-path <text> - UNIX Path**

This specifies the UNIX (NFS) path of the mapping that you want to delete.

## Examples

The following example deletes a symbolic link mapping to a UNIX path `/example/` from a Vserver named `vs1`:

```
cluster1::> vserver cifs symlink delete -vserver vs1 -unix-path /example/
```

## vserver cifs symlink modify

Modify a symlink path mapping

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs symlink modify` command modifies the CIFS share name, CIFS path, CIFS server name, or locality of a symbolic link mapping. It can also be used to modify the value of `-home-directory` field.

## Parameters

**-vserver <vserver name> - Vserver**

This parameter specifies the Vserver on which the symbolic link mapping is located.

**-unix-path <text> - UNIX Path**

This parameter specifies the UNIX (NFS) path of the mapping that you want to modify.



It must begin and end with a forward slash (/).

**[-share-name <Share>] - CIFS Share**

This parameter specifies a new CIFS share name for the mapping.

**[-cifs-path <TextNoCase>] - CIFS Path**

This parameter specifies a new CIFS path for the mapping. Note that this value is specified by using a UNIX-style path.



It must begin and end with a forward slash (/).

### **[-cifs-server <TextNoCase>] - Remote NetBIOS Server Name**

This parameter specifies a new CIFS server DNS name, IP address, or NetBIOS name for the mapping.

### **[-locality {local|widelink}] - Local or Wide Symlink**

This parameter specifies a new locality for the mapping. A local symbolic link maps to the local CIFS share. A free symbolic link can map anywhere on the local server. A wide symbolic link maps to any CIFS share on the network. The default setting is `local`. The free link option is obsolete.

### **[-home-directory {true|false}] - Home Directory**

This parameter specifies whether the new target share is a home directory.



This field must be set to true when the target share is a Home Directory for correct processing.

## **Examples**

The following example modifies the symbolic link mapping to a UNIX path `/example/` on a Vserver named `vs1`. The mapping is modified to use the CIFS path `/mycompany/example/`.

```
cluster1::> vsserver cifs symlink modify -vsserver vs1 -unix-path /example/
-cifs-path "/mycompany/example/"
```

The following example modifies the symbolic link mapping to a UNIX path `/example/` on a Vserver named `vs1`. The mapping is modified to use the CIFS share name `EXAMPLE_SHARE`, the CIFS path `/mycompany/example/`, on the CIFS server `cifs.example.com`, and to be a wide link.

```
cluster1::> vsserver cifs symlink modify -vsserver vs1 -unix-path /example/
-share-name EXAMPLE_SHARE -cifs-path "/mycompany/example/" -cifs-server
cifs.example.com
-locality widelink
```

## **vsserver cifs symlink show**

Show symlink path mappings

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### **Description**

The `vsserver cifs symlink show` command displays the following information about symbolic link mappings for CIFS:

- Vserver
- UNIX (NFS) path

- The DNS name, IP address, or NetBIOS name of the CIFS server
- CIFS share name
- CIFS path
- Whether the locality of the CIFS server is a local, free, or wide link. (A local symbolic link maps to the local CIFS share. A free symbolic link can map anywhere on the local server. A wide symbolic link maps to any CIFS share on the network. The free link option is deprecated and may be removed in a future release of Data ONTAP.)

## Parameters

**{ [-fields <fieldname>,...]**

If you specify the -fields <fieldname>, ... parameter, the command only displays the fields that you specify.

**| [-instance ] }**

If you specify the -instance parameter, the command displays detailed information about all entries.

**[-vserver <vserver name>] - Vserver**

If you specify this parameter, the command displays information about symbolic link mappings on the specified Vserver.

**[-unix-path <text>] - UNIX Path**

If you specify this parameter, the command displays information only about the symbolic link mapping that uses the specified UNIX (NFS) path.

**[-share-name <Share>] - CIFS Share**

If you specify this parameter, the command displays information only about the symbolic link mapping or mappings that use the specified CIFS share.

**[-cifs-path <TextNoCase>] - CIFS Path**

If you specify this parameter, the command displays information only about the symbolic link mapping that uses the specified CIFS path.

**[-cifs-server <TextNoCase>] - Remote NetBIOS Server Name**

If you specify this parameter, the command displays information only about the symbolic link mapping that uses the specified CIFS server.

**[-locality {local|widelink}] - Local or Wide Symlink**

If you specify this parameter, the command displays information only about the symbolic link mappings that have the specified locality.

**[-home-directory {true|false}] - Home Directory**

If you specify this parameter, the command displays information only about the symbolic link mappings that have the target share as a home directory (if true) or as a static CIFS share (if false).

## Examples

The following example displays information about all symbolic link mappings for CIFS:

```

cluster1::> vserver cifs symlink show
Vserver      Unix Path  CIFS Server      CIFS Share  CIFS Path
Locality
-----
-----
vs1          /hr/      192.0.2.160     HR_SHARE    /mycompany/hr/
widelink
vs1          /sales/   WINDATA          SALES_SHARE /mycompany/sales/
local
vs1          /web/     cifs.example.com WEB_SHARE    /mycompany/web/
widelink
3 entries were displayed.

```

The following example displays information about all symbolic link mappings that are wide links:

```

cluster1::> vserver cifs symlink show -locality widelink
Vserver      Unix Path  CIFS Server      CIFS Share  CIFS Path
Locality
-----
-----
vs1          /hr/      192.0.2.160     HR_SHARE    /mycompany/hr/
widelink
vs1          /web/     cifs.example.com WEB_SHARE    /mycompany/web/
widelink
2 entries were displayed.

```

## vserver cifs users-and-groups remove-stale-records

Delete the Stale CIFS local users-and-groups records for the specified vserver

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

### Description

The `vserver cifs users-and-groups remove-stale-records` command removes Stale local users and groups entries associated with old CIFS server.

### Parameters

**-vserver <vserver> - Vserver (privilege: advanced)**

The command deletes Stale local users and groups entries associated with the specified Vserver.

### Examples

The following example displays the syntax of the command.

```
cluster1::*> vserver cifs users-and-groups remove-stale-records -vserver
vs1
```

## vserver cifs users-and-groups update-names

Update the names of Active Directory users and groups

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *advanced* privilege level.

### Description

The `vserver cifs users-and-groups update-names` command updates the names of Active Directory users and groups that are registered in local databases on the cluster and reports the status of the update operations. This is done so that objects that were renamed in the Active Directory can be properly displayed and configured in the local databases.

### Parameters

**-vserver <vserver name> - Vserver (privilege: advanced)**

If you specify this parameter, the command will only be performed within the scope of the Vserver that matches the specified Vserver name.

**{ [-display-failed-only {true|false}] - Display Only Failures (privilege: advanced)**

If you set this parameter to true, the command displays only the Active Directory users and groups that failed to update. If set to false, the command displays only the Active Directory users and groups that successfully updated.

**| [-suppress-all-output {true|false}] - Suppress All Output (privilege: advanced) }**

If you set this parameter to true, the command does not display information about the status of the updates of Active Directory users and groups. To display information about the status of the updates, set this parameter to false or do not specify this parameter in the command.

### Examples

The following example updates the names of Active Directory users and groups associated with Vserver "vs1". In the last case, there is a dependent chain of names that needs to be updated.

```

cluster1::*> vserver cifs users-and-groups update-names -vserver vs1
Vserver:          vs1
  SID:            S-1-5-21-123456789-234565432-987654321-12345
  Domain:        EXAMPLE1
  Out-of-date Name: dom_user1
  Updated Name:   dom_user2
  Status:        Successfully updated
Vserver:          vs1
  SID:            S-1-5-21-123456789-234565432-987654322-23456
  Domain:        EXAMPLE2
  Out-of-date Name: dom_user1
  Updated Name:   dom_user2
  Status:        Successfully updated
Vserver:          vs1
  SID:            S-1-5-21-123456789-234565432-987654321-123456
  Domain:        EXAMPLE1
  Out-of-date Name: dom_user3
  Updated Name:   dom_user4
  Status:        Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                  to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                  to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                  to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                  to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

```

## vserver cifs users-and-groups local-group add-members

Add members to a local group

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs users-and-groups local-group add-members` command adds members to a local group.

### Parameters



**-vserver <vserver name> - Vserver**

This specifies the name of the Vserver.

**-group-name <CIFS name> - Group Name**

This specifies the name of the local group.

**-member-names <CIFS name>, ... - Names of Users or Active Directory Groups to be Added**

This specifies the list of local users, Active Directory users, or Active Directory groups to be added to a particular local group.

## Examples

The following example adds a local user "CIFS\_SERVER\loc\_usr1" and an Active Directory group "CIFS\_SERVER\dom\_grp2" to the local group "CIFS\_SERVER\g1".

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1 -group-name CIFS_SERVER\g1 -member-names
CIFS_SERVER\loc_usr1,AD_DOMAIN\dom_grp2
```

## vserver cifs users-and-groups local-group create

Create a local group

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs users-and-groups local-group create` command creates a local group and optionally sets the description of that local group. The group name must meet the following criteria:

- The group name length must not exceed 256 characters.
- The group name cannot be terminated by a period.
- The group name cannot include commas.
- The group name cannot include any of the following printable characters: " , / \ [ ] , : | < > + = ; , ? \* , @
- The group name cannot include characters in the ASCII range 1-31, which are non-printable.

### Parameters

**-vserver <vserver name> - Vserver**

This specifies the name of the Vserver.

**-group-name <CIFS name> - Group Name**

This specifies the name of the local group.

**[-description <TextNoCase>] - Description**

This specifies a description for this local group. If the description contains a space, enclose the parameter in quotation marks.

## Examples

The following example creates a local group "CIFS\_SERVER\g1" associated with Vserver "vs1".

```
cluster1::> vserver cifs users-and-groups local-group create -vserver vs1
-group-name CIFS_SERVER\g1
```

## vserver cifs users-and-groups local-group delete

Delete a local group

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs users-and-groups local-group delete` command deletes a local group. Removing a local group removes its membership records.

### Parameters

**-vserver <vserver name> - Vserver**

This specifies the name of the Vserver.

**-group-name <CIFS name> - Group Name**

This specifies the name of the local group to delete.

## Examples

The following example deletes the local group "CIFS\_SERVER\g1" associated with Vserver "vs1".

```
cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1
-group-name CIFS_SERVER\g1
```

## vserver cifs users-and-groups local-group modify

Modify a local group

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs users-and-groups local-group modify` command modifies the description of a local group.

## Parameters

**-vserver <vserver name> - Vserver**

This specifies the name of the Vserver.

**-group-name <CIFS name> - Group Name**

This specifies the name of the local group.

**[-description <TextNoCase>] - Description**

This specifies a description for this local group. If the description contains a space, enclose the parameter in quotation marks.

## Examples

The following example modifies the description of the local group "CIFS\_SERVER\g1" associated with Vserver "vs1".

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver vs1
-group-name CIFS_SERVER\g1 -description "Example Description"
```

## vserver cifs users-and-groups local-group remove-members

Remove members from a local group

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs users-and-groups local-group remove-members` command removes members from a local group.

### Parameters

**-vserver <vserver name> - Vserver**

This specifies the name of the Vserver.

**-group-name <CIFS name> - Group Name**

This specifies the name of the local group.

**-member-names <CIFS name>, ... - Names of Users or Active Directory Groups to be Removed**

This specifies the list of local users, Active Directory users, or Active Directory groups to be removed from a particular local group.

### Examples

The following example removes the local users "CIFS\_SERVER\u1" and "CIFS\_SERVER\u2" from the local group "CIFS\_SERVER\g1".

```
cluster1::> vsserver cifs users-and-groups local-group remove-members
-vsserver vs1 -group-name CIFS_SERVER\g1 -member-names
CIFS_SERVER\u1,CIFS_SERVER\u2
```

## vserver cifs users-and-groups local-group rename

Rename a local group

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs users-and-groups local-group rename` command renames a local group. The new group name must remain in the same domain as the old group name. The new group name must meet the following criteria:

- The group name length must not exceed 256 characters.
- The group name cannot be terminated by a period.
- The group name cannot include commas.
- The group name cannot include any of the following printable characters: ", /, \, [, ], :, |, <, >, +, =, ;, ?, \*, @
- The group name cannot include characters in the ASCII range 1-31, which are non-printable.

### Parameters

**-vserver <vserver name> - Vserver**

This specifies the name of the Vserver.

**-group-name <CIFS name> - Group Name**

This specifies the local group's name.

**-new-group-name <CIFS name> - New Group Name**

This specifies the local group's new name.

### Examples

The following example renames the local group "CIFS\_SERVER\g\_old" to "CIFS\_SERVER\g\_new" on Vserver "vs1".

```
cluster1::> vserver cifs users-and-groups local-group rename -group-name
CIFS_SERVER\g_old -new-group-name CIFS_SERVER\g_new -vserver vs1
```

## vserver cifs users-and-groups local-group show-members

Display local groups' members

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs users-and-groups local-group show-members` command displays members of a local group. The members can be local or Active Directory users or groups.

## Parameters

**{ [-fields <fieldname>,...]**

If you specify the `-fields <fieldname>`, ... parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

**| [-instance ] }**

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver name>] - Vserver**

If this parameter is specified, the command displays group members of local groups that match the specified Vserver name.

**[-group-name <CIFS name>] - Group Name**

If this parameter is specified, the command displays group members of local groups that match the specified group name.

**[-member <CIFS name>,...] - Member Name**

If this parameter is specified, the command displays group members that match the specified member name. The name can be that of a local user, Active Directory user, or Active Directory group.

## Examples

The following example displays members of local groups associated with Vserver "vs1".

```
cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
Vserver          Group Name          Members
-----
vs1              BUILTIN\Administrators  CIFS_SERVER\Administrator
                  AD_DOMAIN\Domain Admins
                  AD_DOMAIN\dom_grp1
                  BUILTIN\Users          AD_DOMAIN\Domain Users
                  AD_DOMAIN\dom_usr1
                  CIFS_SERVER\g1          CIFS_SERVER\u1
6 entries were displayed.
```

## vserver cifs users-and-groups local-group show

Display local groups

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs users-and-groups local-group show` command displays local groups.

## Parameters

**{ [-fields <fieldname>,...]**

If you specify the `-fields <fieldname>`, ... parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

**| [-instance ] }**

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver name>] - Vserver**

If this parameter is specified, the command displays information only about local groups that match the specified Vserver name.

**[-group-name <CIFS name>] - Group Name**

If this parameter is specified, the command displays information only about local groups that match the specified group name.

**[-description <TextNoCase>] - Description**

If this parameter is specified, the command displays information only about local groups that match the specified description.

## Examples

The following example displays all local groups associated with Vserver "vs1".

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver          Group Name          Description
-----
vs1              BUILTIN\Administrators  Built-in Administrators
group
vs1              BUILTIN\Backup Operators  Backup Operators group
vs1              BUILTIN\Power Users      Restricted administrative
privileges
vs1              BUILTIN\Users            All users
vs1              CIFS_SERVER\g1
vs1              CIFS_SERVER\g2
6 entries were displayed.
```

# vserver cifs users-and-groups local-user create

Create a local user

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs users-and-groups local-user create` command creates a local user and optionally sets the attributes for that local user. The command prompts for the local user's password. + + + The user name must meet the following criteria: +

- The user name length must not exceed 20 characters.
- The user name cannot be terminated by a period.
- The user name cannot include commas.
- The user name cannot include any of the following printable characters: ", /, \, [, ], :, |, <, >, +, =, ;, ?, \*, @
- The user name cannot include characters in the ASCII range 1-31, which are non-printable.

The password must meet the following criteria:

- The password must be at least six characters in length.
- The password must not contain user account name.
- The password must contain characters from three of the following four categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Special characters: ~, !, @, #, 0, ^, , \*, \_ , -, +, =, ` , \, |, (, ), [ , ] , : , ; , " , ' , < , > , , , . , ? , /

## Parameters

**-vserver <vserver name> - Vserver**

This specifies the name of the Vserver.

**-user-name <CIFS name> - User Name**

This specifies the user name.

**[-full-name <TextNoCase>] - Full Name**

This specifies the user's full name. If the full name contains a space, enclose the full name within double quotation marks.

**[-description <TextNoCase>] - Description**

This specifies a description for this local user. If the description contains a space, enclose the parameter in quotation marks.

**[-is-account-disabled {true|false}] - Is Account Disabled**

This specifies whether the user account is enabled or disabled. Set this parameter to true to disable the account. Set this parameter to false to enable the account. If this parameter is not specified, the default is to

enable the user account.

## Examples

The following example creates a local user "CIFS\_SERVER\u1" associated with Vserver "vs1".

```
cluster1::> vsserver cifs users-and-groups local-user create -vsserver vs1
-user-name CIFS_SERVER\u1
```

Enter the password:

Confirm the password:

## vsserver cifs users-and-groups local-user delete

Delete a local user

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vsserver cifs users-and-groups local-user delete` command deletes a local user. Upon deletion, all membership entries for this local user are deleted.

### Parameters

**-vsserver <vsserver name> - Vserver**

This specifies the name of the Vserver.

**-user-name <CIFS name> - User Name**

This specifies the user name.

## Examples

The following example deletes the local user "CIFS\_SERVER\u1" associated with Vserver "vs1".



```

cluster1::> vserver cifs users-and-groups local-user show-membership
(vserver cifs users-and-groups local-user show-membership)
Vserver          User Name                      Membership
-----
vs1              CIFS_SERVER\Administrator      BUILTIN\Administrators
                CIFS_SERVER\u1                CIFS_SERVER\g1
2 entries were displayed.

cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\u1

cluster1::> vserver cifs users-and-groups local-user show-membership
Vserver          User Name                      Membership
-----
vs1              CIFS_SERVER\Administrator      BUILTIN\Administrators

```

## vserver cifs users-and-groups local-user modify

Modify a local user

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs users-and-groups local-user modify` command modifies attributes of a local user.

### Parameters

**-vserver <vserver name> - Vserver**

This specifies the name of the Vserver.

**-user-name <CIFS name> - User Name**

This specifies the user name.

**[-full-name <TextNoCase>] - Full Name**

This specifies the user's full name. If the full name contains a space in the name, enclose it within double quotation marks

**[-description <TextNoCase>] - Description**

This specifies a description for this local user. If the description contains a space, enclose the parameter in quotation marks.

**[-is-account-disabled {true|false}] - Is Account Disabled**

This specifies if the user account is enabled or disabled. Set this parameter to true to disable the account. Set this parameter to false to enable the account.

## Examples

The following example modifies the full name of the local user "CIFS\_SERVER\u1".

```
cluster1::> vsserver cifs users-and-groups local-user modify -user-name
CIFS_SERVER\u1 -full-name "John Smith" -vsserver vs1
```

## vsserver cifs users-and-groups local-user rename

Rename a local user

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vsserver cifs users-and-groups local-user rename` command renames a local user. The new user name must remain in the same domain as the old user name. + The new user name must meet the following criteria:

- The user name length must not exceed 20 characters.
- The user name cannot be terminated by a period.
- The user name cannot include commas.
- The user name cannot include any of the following printable characters: ", /, \, [, ], :, |, <, >, +, =, ;, ?, \*, @
- The user name cannot include characters in the ASCII range 1-31, which are non-printable.

### Parameters

**-vsserver <vsserver name> - Vserver**

This specifies the name of the Vserver.

**-user-name <CIFS name> - User Name**

This specifies the user name.

**-new-user-name <CIFS name> - New User Name**

This specifies the new user name.

## Examples

The following example renames the local user "CIFS\_SERVER\u\_old" to "CIFS\_SERVER\u\_new" on Vserver "vs1".

```
cluster1::> vsserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\u_old -new-user-name CIFS_SERVER\u_new -vsserver vs1
```

# vserver cifs users-and-groups local-user set-password

Set a password for a local user

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs users-and-groups local-user set-password` command sets the password for the specified local user. The password must meet the following criteria:

- The password must be at least six characters in length.
- The password must not contain user account name.
- The password must contain characters from three of the following four categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Special characters: ~, !, @, #, 0, ^, , , \*, \_ , - , + , = , ` , \ , | , ( , ) , [ , ] , : , ; , " , ' , < , > , , , . , ? , /

## Parameters

**-vserver <vserver name> - Vserver**

This specifies the name of the Vserver.

**-user-name <CIFS name> - User Name**

This specifies the user name.

## Examples

The following example sets the password for the local user "CIFS\_SERVER\u1" associated with Vserver "vs1".

```
cluster1::> vserver cifs users-and-groups local-user set-password -user  
-name CIFS_SERVER\u1 -vserver vs1
```

Enter the new password:

Confirm the new password:

+ + The following example attempts to set the password but fails because the password did not meet password complexity requirements.

```
cluster1::> vserver cifs users-and-groups local-user set-password -user
-name CIFS_SERVER\u1 -vserver vs1
```

Enter the new password:

Confirm the new password:

```
Error: command failed: The password does not meet the password complexity
requirements. Refer to the man page for details.
```

## vserver cifs users-and-groups local-user show-membership

Display local users' membership information

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs users-and-groups local-user show-membership` command displays the membership of local users.

### Parameters

**{ [-fields <fieldname>,...]**

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

**| [-instance ] }**

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver name>] - Vserver**

If this parameter is specified, the command displays local user membership information for local users that are associated with the specified Vserver.

**[-user-name <CIFS name>] - User Name**

If this parameter is specified, the command displays local user membership information for a local user that matches the specified user name.

**[-membership <CIFS name>,...] - Local Group That This User is a Member of**

If this parameter is specified, the command displays local user membership information for the local group of which this local user is a member.

### Examples

The following example displays the membership information of all local users; user "CIFS\_SERVER\Administrator" is a member of "BUILTIN\Administrators" group, and "CIFS\_SERVER\u1" is a member of "CIFS\_SERVER\g1" group.

```

cluster1::> vserver cifs users-and-groups local-user show-membership
Vserver          User Name          Membership
-----
vs1              CIFS_SERVER\Administrator  BUILTIN\Administrators
                CIFS_SERVER\u1          CIFS_SERVER\g1
2 entries were displayed.

```

## vserver cifs users-and-groups local-user show

Display local users

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs users-and-groups local-user show` command displays local users and their attributes.

### Parameters

**{ [-fields <fieldname>,...]**

If you specify the `-fields <fieldname>`, ... parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

**| [-instance ] }**

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver name>] - Vserver**

If this parameter is specified, the command displays information only about local users that match the specified Vserver name.

**[-user-name <CIFS name>] - User Name**

If this parameter is specified, the command displays information only about local users that match the specified user name.

**[-full-name <TextNoCase>] - Full Name**

If this parameter is specified, the command displays information only about local users that match the specified full name.

**[-description <TextNoCase>] - Description**

If this parameter is specified, the command displays information only about local users that match the specified description.

**[-is-account-disabled {true|false}] - Is Account Disabled**

If this parameter is specified, the command displays information only about local users that match the status specified.

## Examples

The following example displays information about all local users.

```
cluster1::> vserver cifs users-and-groups local-user show
Vserver      User Name                               Full Name                               Description
-----
vs1          CIFS_SERVER\Administrator             James Raynor                             Built-in
administrator account
vs1          CIFS_SERVER\u1                         Sarah Kerrigan
2 entries were displayed.
```

## vserver cifs users-and-groups privilege add-privilege

Add local privileges to a user or group

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs users-and-groups privilege add-privilege` command adds privileges to a local or Active Directory user or group.

### Parameters

**-vserver <vserver name> - Vserver**

This specifies the name of the Vserver.

**-user-or-group-name <CIFS name> - User or Group Name**

This specifies the name of the local or Active Directory user or group.

**-privileges <Privilege>,... - Privileges**

This specifies the list of privileges to be associated with this user or group.

### Examples

The following example adds the privileges "SeTcbPrivilege" and "SeTakeOwnershipPrivilege" to the user "CIFS\_SERVER\u1".

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\u1 -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege
```

# vserver cifs users-and-groups privilege remove-privilege

Remove privileges from a user or group

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `vserver cifs users-and-groups privilege remove-privilege` command removes privileges from a local or Active Directory user or group. This command creates a new or modifies an existing privilege entry.

## Parameters

**-vserver <vserver name> - Vserver**

This specifies the name of the Vserver.

**-user-or-group-name <CIFS name> - User or Group Name**

This specifies the name of the local or Active Directory user or group.

**-privileges <Privilege>,... - Privileges**

This specifies the list of privileges to be removed from this user or group.

## Examples

The following example removes the previously added "SeTcbPrivilege" and "SeTakeOwnershipPrivilege" privileges from the user "CIFS\_SERVER\u1".

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver      User or Group Name      Privileges
-----
vs1          CIFS_SERVER\u1          SeTcbPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\u1 -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show
Vserver      User or Group Name      Privileges
-----
vs1          CIFS_SERVER\u1          -
```

+ + The following example removes "SeBackupPrivilege" from the group "BUILTIN\Administrators".

```

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators -privileges
SeBackupPrivilege

cluster1::> vserver cifs users-and-groups privilege show
Vserver          User or Group Name          Privileges
-----
vs1              BUILTIN\Administrators     SeRestorePrivilege
                                                SeSecurityPrivilege
                                                SeTakeOwnershipPrivilege

```

## vserver cifs users-and-groups privilege reset-privilege

Reset local privileges for a user or group

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs users-and-groups privilege reset-privilege` command resets privileges of a local or Active Directory user or group.

### Parameters

**-vserver <vserver name> - Vserver**

This specifies the name of the Vserver.

**-user-or-group-name <CIFS name> - User or Group Name**

This specifies the name of the local or Active Directory user or group.

### Examples

The following example resets the privileges for the local user "CIFS\_SERVER\u1". This operation removes the privilege entry, if any, associated with the local user "CIFS\_SERVER\u1".



```

cluster1::> vserver cifs users-and-groups privilege show
Vserver          User or Group Name          Privileges
-----
vs1              CIFS_SERVER\ul              SeTakeOwnershipPrivilege
                                   SeRestorePrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\ul

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.

```

+ + The following example resets the privileges for the group "BUILTIN\Administrators", effectively removing the privilege entry.

```

cluster1::> vserver cifs users-and-groups privilege show
Vserver          User or Group Name          Privileges
-----
vs1              BUILTIN\Administrators      SeRestorePrivilege
                                   SeSecurityPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.

```

## vserver cifs users-and-groups privilege show

Display privileges

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `vserver cifs users-and-groups privilege show` command displays privilege overrides assigned to local or Active Directory users or groups.

### Parameters

```
{ [-fields <fieldname>,...]
```

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified

field or fields. You can use '-fields ?' to display the fields to specify.

**[ [-instance ] ] }**

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[ -vserver <vserver name> ] - Vserver**

If this parameter is specified, the command displays information only about privilege overrides assigned to local or Active Directory users or groups that match the specified Vserver name.

**[ -user-or-group-name <CIFS name> ] - User or Group Name**

If this parameter is specified, the command displays information only about privilege overrides assigned to local or Active Directory users or groups that match the specified user name or group name.

**[ -privileges <Privilege>, ... ] - Privileges**

If this parameter is specified, the command displays information only about privilege overrides assigned to local or Active Directory users or groups that match the specified privileges.

## Examples

The following example displays all privileges explicitly associated with local or Active Directory users or groups for Vserver "vs1".

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver          User or Group Name          Privileges
-----
vs1              BUILTIN\Administrators     SeTakeOwnershipPrivilege
                                                SeRestorePrivilege
```

## Copyright information

Copyright © 2024 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## 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.