vserver export-policy commands

ONTAP 9.15.1 commands

NetApp
December 18, 2024

Table of Contents

vserver export-policy commands . . . 1
- vserver export-policy check-access . . . 1
- vserver export-policy copy . . . 4
- vserver export-policy create . . . 5
- vserver export-policy delete . . . 6
- vserver export-policy rename . . . 6
- vserver export-policy show . . . 7
- vserver export-policy access-cache flush . . . 8
- vserver export-policy access-cache show-negative . . . 9
- vserver export-policy access-cache show-rules . . . 11
- vserver export-policy access-cache show . . . 15
- vserver export-policy access-cache config modify-all-vservers . . . 18
- vserver export-policy access-cache config modify . . . 19
- vserver export-policy access-cache config show-all-vservers . . . 20
- vserver export-policy access-cache config show . . . 21
- vserver export-policy cache flush . . . 23
- vserver export-policy config-checker show . . . 24
- vserver export-policy config-checker start . . . 25
- vserver export-policy config-checker stop . . . 26
- vserver export-policy config-checker rule delete . . . 27
- vserver export-policy config-checker rule show . . . 28
- vserver export-policy netgroup check-membership . . . 30
- vserver export-policy netgroup cache show . . . 31
- vserver export-policy netgroup queue show . . . 33
- vserver export-policy rule add-clientmatches . . . 35
- vserver export-policy rule create . . . 36
- vserver export-policy rule delete . . . 41
- vserver export-policy rule modify . . . 42
- vserver export-policy rule remove-clientmatches . . . 47
- vserver export-policy rule setindex . . . 48
- vserver export-policy rule show . . . 49

vserver export-policy commands

vserver export-policy check-access

Given a Volume And/or a Qtree, Check to See If the Client Is Allowed Access

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

Description

The `vserver export-policy check-access` command checks whether a specific client is allowed access to a specific export path. This enables you to test export policies to ensure they work as intended and to troubleshoot client access issues.

The command takes the volume name (and optionally the qtree name) as input and computes the export path for the volume/qtree. It evaluates the export policy rules that apply for each path component and displays the policy name, policy owner, policy rule index and access rights for that path component. If no export policy rule matches the specified client IP address access is denied and the policy rule index will be set to 0. The output gives a clear view on how the export policy rules are evaluated and helps narrow down the policy and (where applicable) the specific rule in the policy that grants or denies access.

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 Name

This parameter specifies the name of the Vserver in which the export policy resides.

-volume <volume name> - Volume Name

This parameter specifies the name of the volume that you want to check export access for. To check export access for a qtree use the -qtree parameter. The -qtree parameter is optional. If you specify the -qtree parameter, you must provide the name of the volume containing the qtree. If you do not specify the -qtree parameter, export access will be checked only for the volume.

-client-ip <IP Address> - Client IP Address

This parameter specifies the IP address of the client that you want to check export access for.

-authentication-method <authentication method> - Authentication Method

This parameter specifies the authentication method of the client that is attempting access. Possible values include the following:

- *sys* - The authentication method used by the client is AUTH_SYS.
- *krb5* - The authentication method used by the client is Kerberos v5.
- *krb5i* - The authentication method used by the client is Kerberos v5 with integrity service.

- *krb5p* - The authentication method used by the client is Kerberos v5 with privacy service.
- *ntlm* - The authentication method used by the client is CIFS NTLM.
- *none* - The authentication method used by the client is not explicitly listed in the list of values in the rorule.

-protocol <Client Access Protocol> - Protocol

This parameter specifies the protocol that the client is using when attempting to access the exported path. Possible values include the following:

- *nfs3* - The NFSv3 protocol
- *nfs4* - The NFSv4 protocol
- *cifs* - The CIFS protocol

-access-type {read|read-write|denied} - Access Rights to Check for

This parameter specifies the type of access you want to check for. Possible values are read for read-only access and read-write for read-write access.

[-qtree <qtree name>] - Name of the Qtree

This optional parameter specifies the qtree in the volume that is part of the exported path. If you specify this parameter, you must also provide the name of the volume the qtree belongs to.

[-path <text>] - Path

Selects the entries in the output that match the specified path value. This field describes the junction-path path component encountered when evaluating the export policies starting from the root ('/') of the Vserver.

[-policy <text>] - Export Policy

Selects the entries in the output that match the specified policy value. This field describes the export policy that is in effect for the path encountered so far when evaluating the export policies starting from the root ('/') of the Vserver.

[-policy-owner <text>] - Export Policy Owner

Selects the entries in the output that match the specified policy owner value. This field describes the owner of the export policy that is in effect for the path encountered so far when evaluating the export policies starting from the root ('/') of the vserver. The owner of the export policy could be a volume or a qtree.

[-policy-owner-type {volume|qtree}] - Type of Export Policy Owner

Selects the entries in the output that match the specified type of the owner of an export policy. Possible values include the following:

- *volume* - The owner of the export policy is a volume
- *qtree* - The owner of the export policy is a qtree

[-rule-index <integer>] - Export Policy Rule Index

Selects the entries in the output that match the specified export policy rule index. This field describes the rule index of the rule in the export policy that grants or denies access. If the value of the rule index is 0 it implies none of the client match strings provided in the rules of the export policy matched the specified IP address of the client.

[-access {read|read-write|denied}] - Access Rights

Selects the entries in the output that match the specified access value. This field describes the access rights to the path. Possible values include the following:

- *read* - Read access is granted
- *read-write* - Read-write access is granted
- *denied* - Requested access is denied

[-partial-rule-match {true|false}] - Did a Subset of the Rules Match?

Selects the entries in the output that match if a partially matched subset of rules in the export policy were used to grant access to the client.

[-clientmatch <text>] - Client Match Spec

Selects the entries in the output that match the specified clientmatch string. The clientmatch string denotes the string that resulted in a rule match for the specified client IP address.

[-security-style <security style>] - Security Style

Selects the entries in the output that match the specified security style value. Possible values are unix, ntfs and mixed.

Examples

The following examples of the `vserver export-policy check-access` command display various possible results for client export access checks.

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
10.22.32.42 -volume flex_vol -authentication-method sys -protocol nfs3
-access-type read
                                 Policy    Policy     Rule
Security
Path                 Policy      Owner     Owner Type Index Access
Style
-------------------- ---------- --------- ---------- ---- ----------
----------
/                    default     vs1_root  volume        1 read       mixed
/dir1                default     vs1_root  volume        1 read       mixed
/dir1/dir2           default     vs1_root  volume        1 read       mixed
/dir1/dir2/flex1     data        flex_vol  volume       10 read       mixed
4 entries were displayed.

cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
10.22.32.42 -volume flex_vol -authentication-method sys -protocol nfs3
-access-type read-write
                                 Policy    Policy     Rule
Security
Path                 Policy      Owner     Owner Type Index Access
Style
```

```
------------------- ---------- --------- ---------- ---- ----------
----------
/                   default    vs1_root  volume        1 read       mixed
/dir1               default    vs1_root  volume        1 read       mixed
/dir1/dir2          default    vs1_root  volume        1 read       mixed
/dir1/dir2/flex1    data       flex_vol  volume       10 read-write mixed
4 entries were displayed.

cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
10.22.32.42 -volume flex_vol -authentication-method sys -protocol nfs3
-access-type read-write -qtree qt1
                               Policy    Policy     Rule
Security
Path                Policy     Owner     Owner Type Index Access
Style
------------------- ---------- --------- ---------- ---- ----------
----------
/                   default    vs1_root  volume        1 read       mixed
/dir1               default    vs1_root  volume        1 read       mixed
/dir1/dir2          default    vs1_root  volume        1 read       mixed
/dir1/dir2/flex1    data       flex_vol  volume       10 read       mixed
/dir1/dir2/flex1/qt1 primarynames
                               qt1       qtree         0 denied     mixed
5 entries were displayed.

cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
10.22.32.42 -volume flex_vol -authentication-method ntlm -protocol cifs
-access-type read-write -qtree qt1
                               Policy    Policy     Rule
Security
Path                Policy     Owner     Owner Type Index Access
Style
------------------- ---------- --------- ---------- ---- ----------
----------
/                   default    vs1_root  volume        1 read       mixed
/dir1               default    vs1_root  volume        1 read       mixed
/dir1/dir2          default    vs1_root  volume        1 read       mixed
/dir1/dir2/flex1    data       flex_vol  volume       10 read       mixed
/dir1/dir2/flex1/qt1 primarynames
                               qt1       qtree           2 denied   mixed
5 entries were displayed.
```

vserver export-policy copy

Copy an export policy

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

Description

The `vserver export-policy copy` command creates a copy of an export policy on the same or a different Vserver. The command fails if an export policy with the specified new name already exists on the target Vserver.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the Vserver on which the export policy that you want to copy is located.

`-policyname <export policy name>` - Policy Name

This parameter specifies the export policy that you want to copy.

`-newvserver <vserver name>` - New Vserver

This parameter specifies the Vserver to which you want to copy the export policy.

`-newpolicyname <export policy name>` - New Export Policy Name

This parameter specifies the name of the new policy.

Examples

The following example copies an existing policy named read_only_expolicy located on a Vserver named vs0 to a new policy named default_expolicy located on a Vserver named vs1.

```
vs1::> vserver export-policy copy -vserver vs0 -policyname
read_only_expolicy -newvserver vs1 -newpolicyname default_expolicy
```

vserver export-policy create

Create a rule set

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

Description

The `vserver export-policy create` command creates an export policy. You can use the vserver export-policy rule create command to add rules to a policy. Each cluster has an empty default export policy with the ID 0. This default export policy does not contain any rules. You cannot delete the default export policy, but you can rename or modify it.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the Vserver on which you want to create the export policy.

-policyname <export policy name> - Policy Name

This parameter specifies the export policy that you want to create.

Examples

The following example creates an export policy named read_only_expolicy on a Vserver named vs0:

```
vs1::> vserver export-policy create -vserver vs0 -policyname
read_only_expolicy
```

Related Links

- vserver export-policy rule create

vserver export-policy delete

Delete a rule set

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

Description

The `vserver export-policy delete` command deletes an export policy. You cannot delete the default policy (named `default`) for a Vserver unless you delete the Vserver.

Parameters

-vserver <vserver name> - Vserver

This parameter specifies the Vserver on which the export policy that you want to delete is located.

-policyname <export policy name> - Policy Name

This parameter specifies the export policy that you want to delete.

Examples

The following example deletes an export policy named test_expolicy from a Vserver named vs0:

```
vs1::> vserver export-policy delete -vserver vs0 -policyname test_expolicy
```

vserver export-policy rename

Rename an export policy

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

Description

The `vserver export-policy rename` command renames an export policy.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the Vserver on which the export policy is located.

`-policyname <export policy name>` - Policy Name

This parameter specifies the export policy that you want to rename.

`-newpolicyname <export policy name>` - New Export Policy Name

This parameter specifies the new name of the export policy.

Examples

The following example renames an export policy named user_expolicy with the name read_only_expolicy on a Vserver named vs0:

```
vs1::> vserver export-policy rename -vserver vs0 -policyname user_expolicy
-newpolicyname read_only_expolicy
```

vserver export-policy show

Display a list of rule sets

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

Description

The `vserver export-policy show` command displays the following information:

- Vserver name
- Export policy name
- Policy ID (diagnostic privilege level only)

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 entries.

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

If you specify this parameter, the command displays a list of export policies that are located on the Vserver

that you specify.

[-policyname <export policy name>] - Policy Name

If you specify this parameter, the command displays only the export policy or sets that match the specified name.

Examples

The following example displays a list of all export policies:

```
vs1::> vserver export-policy show
VServer          Policy Name
---------------  -------------------
vs0              default_expolicy
vs0              read_only_expolicy
vs1              default_expolicy
vs1              test_expolicy
4 entries were displayed.
```

vserver export-policy access-cache flush

Flush an entry from the access cache

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

Description

The `vserver export-policy access-cache flush` command can be used to remove all entries in the access cache that belong to the specified export policy. The command can also be used to remove the access cache entry for a specific IP address belonging to an export policy. You must provide the name of the node that hosts the access cache and the name of the Vserver that owns the export policy. This command differs from the vserver export-policy cache flush command. The vserver export-policy cache flush command allows you to flush all access cache entries across all export policies in a Vserver. In contrast the `vserver export-policy access-cache flush` command gives you the granularity to flush a specific access cache entry or the granularity to flush all access cache entries for a specific export policy.

This command is useful to clear out a negative access cache entry. A negative cache entry is one where a client IP address experiences an access denied error due to stale export policy rule information present in the cache entry. Data ONTAP maintains several caches in the kernel and userspace to speed access to exports. A negative cache entry can get created in the access cache if a client tries to access an export path before the export rules or the name server settings or the caches in management gateway have been updated to grant access to that client. The negative cache entry will remain in the access cache until the TTL for the entry expires and the entry is refreshed. You can use the `export-policy access-cache config show ` command to find out the refresh intervals and timeouts for the access cache. If you know that the caches in userspace have the latest information for the client and don’t want to wait until the TTL for the access cache entry expires then you can use this command to remove the access cache entry in the kernel and force the cache entry to get re-populated with the latest information that will allow the client to access the export path.

You can use the `vserver export-policy access-cache entry show` and `vserver export-policy access-cache entry show-rules` commands to examine the contents of an entry in the access

cache before removing it using the flush command.

Parameters

-vserver <vserver name> - Vserver

This parameter specifies the name of the Vserver on which you want to flush the access cache entry.

-node <nodename> - Node

This parameter specifies the node on which you want to flush the access cache entry.

-policy <text> - Export Policy Name

This parameter specifies the name of the export policy that is effective for the exported path that the client is trying to access.

[-address <IP Address>] - IP Address

This parameter is optional. It specifies the IP address of the client whose access cache entry you want to remove. If this parameter is not specified all access cache entries belonging to the specified export policy will be removed.

Examples

The following example flushes the access cache entry for client IP address '1.2.3.4' in volume 'flex1' having export policy 'testpol' in a Vserver named 'vs1' on node 'vsim1':

```
cluster1::*> vserver export-policy access-cache flush -vserver vs1 -node
vsim1 -policy testpol -address 1.2.3.4
Successfully removed access cache entry for IP address "1.2.3.4" belonging
to export policy "testpol" in Vserver "vs1" on node "vsim1".

cluster1::*> vserver export-policy access-cache flush -vserver vs1 -node
vsim1 -policy testpol

Warning: This command removes all access cache entries for export policy
"testpol" in Vserver "vs1" on node "vsim1". Do you want to continue?
{y|n}: y

Successfully removed 1 access cache entry for export policy "testpol" in
Vserver "vs1" on node "vsim1".
```

Related Links

- vserver export-policy cache flush

vserver export-policy access-cache show-negative

Display information about the negative access cache entry

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

Description

The `vserver export-policy access-cache show-negative` command can be used to display the contents of access cache having negative polarity of the specified node for a particular client IP address belonging to an export policy in a Vserver.

The command will display information such as the age, policy name and client IP address of the negative access cache entry.

If you are interested in finding out more details about the access cache then you can use the vserver export-policy access-cache show command.

If the client IP address for which access is denied is not cached in the access cache then the command will display an error message stating that this table is current empty.

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 Name

This parameter specifies the node on which you want to examine the access cache entry.Use an exact value. Queries are not supported.

[-vserver <vserver>] - Vserver

This parameter specifies the name of the Vserver on which you want to see the access cache entry. Use an exact value. Queries are not supported.

[-policy <text>] - Export Policy Name

This parameter specifies the name of the export policy that is in effect on the export path that the client is trying to access.Use an exact value. Queries are not supported.

[-client-ip <IP Address>] - Client IP Address

This parameter specifies the IP address of the client whose access cache entry you want to examine.Use an exact value. Queries are not supported.

[-age <[<integer>h][<integer>m][<integer>s]>] - Age of Entry

Selects the access cache entries that match the specified age of the entry. This field describes the age of the access cache entry.

Examples

The following example shows the contents of the access cache entry having negative polarity:

```
cluster1::*> vserver export-policy access-cache show-negative
     Node: vikash2-vsim1
  Vserver: vs12
Policy Name      IP Address         Age of Entry
-------------    ---------------    ------------
default          1.1.1.1            16s
default          1.1.1.2            17s
default          1.1.1.3            18s
3 entries were displayed.
```

Related Links

- vserver export-policy access-cache show

vserver export-policy access-cache show-rules

Display information about the export policy rules in the access cache entry

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

Description

The `vserver export-policy access-cache show-rules` command is used in conjunction with the vserver export-policy access-cache show command. The vserver export-policy access-cache show command displays the state and contents of an access cache entry on the specified node for a particular client IP address belonging to an export policy in a Vserver. The command lists the rule indexes of the export policy rules that matched. If you are interested in finding out the security settings for each policy rule that matched then you can use the ` vserver export-policy access-cache show-rules` command. You can use the -instance switch to get a more detailed listing. Do note that the security settings of the rules cached in the access cache entry match the security settings of the rules that can be obtained by running the vserver export-policy rule show command with the corresponding rule index.

If the client IP address is not cached in access cache then the command will display an error message stating that the entry does not exist.

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> - Node

This parameter specifies the node on which you want to examine the export policy rule details in the access cache entry.

-vserver <vserver name> - Vserver

This parameter specifies the name of the Vserver on which you want to see the policy rule details in the access cache entry.

-policy <export policy name> - Policy Name

This parameter specifies the name of the export policy that is in effect on the export path that the client is trying to access.

-address <IP Address> - IP Address

This parameter specifies the IP address of the client whose access cache entry you want to examine in greater detail.

[-ruleindex <integer>] - Entry Policy Rule Index

This optional parameter specifies the index number of the export rule of a specific policy.

[-protocol <Client Access Protocol>,…] - Access Protocol

This optional parameter specifies the list access protocols of export rules.

[-rorule <authentication method>,…] - RO Access Rule

This parameter specifies the security type for read-only access to volumes that use the export rule.

[-rwrule <authentication method>,…] - RW Access Rule

This parameter specifies the security type for read-write access to volumes that use the export rule.

[-superuser <authentication method>,…] - Superuser Security Types

This parameter specifies a security type for superuser access to files.

[-anon-uid <integer>] - Anonymous User ID

This parameter specifies an anonymous user ID that the user credentials are mapped to.

[-anon-gid <integer>] - Anonymous User Primary GID

This parameter specifies an anonymous User Primary GID.

[-anon-gid-list <integer>,…] - Anonymous User GID List

This parameter specifies an anonymous User Primary GID list.

[-protocol-flags {allow-suid|allow-dev}] - Protocol Flags

This parameter specifies protocol flags such as allow-suid and allow-dev.

[-ntfs-unix-security-ops {ignore|fail}] - NTFS Unix Security Options

This parameter specifies whether UNIX-type permissions changes on NTFS (Windows) volumes are prohibited (fail) or allowed (ignore).

[-chown-mode {restricted|unrestricted}] - Change Ownership Mode

This parameter specifies a change ownership mode.

[-clientmatch <text>] - Client Match String

This parameter specifies the client or clients to which the export rule applies.

[-anonuser <text>] - Anonymous Username or ID

This parameter specifies a UNIX user ID or user name that the user credentials are mapped to.

Examples

The following example shows the contents of the access cache entry for client IP address '1.2.3.4' in volume 'flex1' having export policy 'testpol' in a Vserver named 'vs1' on node 'vsim1'. This entry has two export policy rules with rule indexes 1 and 2 that matched and are cached in the entry. To examine what the rule settings are in each of these rules we can use the show-rules variant of the command.

```
cluster1::*>vserver export-policy access-cache show -vserver vs1 -node
vsim1 -policy testpol -address 1.2.3.4
Node: vsim1
                            Vserver: vs1
                        Policy Name: testpol
                         IP Address: 1.2.3.4
           Access Cache Entry Flags: -
                        Result Code: 0
                  Failure Type Code: 0
     Number of Matched Policy Rules: 2
List of Matched Policy Rule Indexes: 1, 2
                       Age of Entry: 5s

cluster1::*>vserver export-policy access-cache show-rules -vserver vs1
-node vsim1 -policy testpol -address 1.2.3.4
                                    Rule  Access   RO    RW    Super Anon
Node       Address         Policy   Index Protocol Rule  Rule  User  User
---------- --------------- -------- ----- -------- ----  ----  ----- -----
vsim1      1.2.3.4         testpol  1     any      any   any   none  65534
vsim1      1.2.3.4         testpol  2     nfs3     never never sys   123
2 entries were displayed.

cluster1::*>vserver export-policy access-cache show-rules -vserver vs1
-node vsim1 -policy testpol -address 1.2.3.4 -instance
Vserver: vs1
                      Node: vsim1
                Policy Name: testpol
                 IP Address: 1.2.3.4
           Export Policy ID: 12884901890
   Entry Policy Rule Index: 1
            Access Protocol: any
             RO Access Rule: any
             RW Access Rule: any
  Superuser Security Types: none
          Anonymous User ID: 65534
```

```
            Protocol Flags: allow-suid, allow-dev
NTFS Unix Security Options: fail
     Change Ownership Mode: restricted
Vserver: vs1
                      Node: vsim1
               Policy Name: testpol
                IP Address: 1.2.3.4
             Export Policy: testpol
          Export Policy ID: 12884901890
   Entry Policy Rule Index: 2
           Access Protocol: nfs3
            RO Access Rule: never
            RW Access Rule: never
  Superuser Security Types: sys
         Anonymous User ID: 123
            Protocol Flags: allow-suid
NTFS Unix Security Options: ignore
     Change Ownership Mode: restricted
2 entries were displayed.

cluster1::*> vserver export-policy rule show -vserver vs1 -policyname
testpol -ruleindex 1
                                    Vserver: vs1
                                Policy Name: testpol
                                 Rule Index: 1
                             Access Protocol: any
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                              RO Access Rule: any
                              RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                    Superuser Security Types: none
                Honor SetUID Bits in SETATTR: true
                   Allow Creation of Devices: true

cluster1::*> vserver export-policy rule show -vserver vs1 -policyname
testpol -ruleindex 2
                                    Vserver: vs1
                                Policy Name: testpol
                                 Rule Index: 2
                             Access Protocol: nfs3
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                              RO Access Rule: never
                              RW Access Rule: never
User ID To Which Anonymous Users Are Mapped: testu1
                    Superuser Security Types: sys
                Honor SetUID Bits in SETATTR: true
```

```
                    Allow Creation of Devices: false
```

Related Links

- vserver export-policy access-cache show
- vserver export-policy rule show

vserver export-policy access-cache show

Display information about the access cache entry

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

Description

The `vserver export-policy access-cache show` command can be used to display the contents of an access cache entry of the specified node for a particular client IP address belonging to an export policy in a Vserver.

The command will display information such as the flags of the access cache entry, the age of the entry, any errors that were encountered when looking up the export policy rules from the management gateway, and the number of policy rules from the export policy that matched the specified client IP address. If an error is encountered when looking up the export policy rules from the management gateway process, the first rule index in the export policy that encountered the error is displayed. The client match string or the anon string in the rule that caused the rule evaluation to fail is also displayed. A more detailed view of the output of this command is available if you specify the -instance switch to the command.

The command output lists the rule indexes of the policy rules that matched. If you are interested in finding out the security settings for each policy rule that matched then you can use the vserver export-policy access-cache show-rules command.

If the client IP address is not cached in the access cache then the command will display an error message stating that the entry does not exist.

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> - Node

This parameter specifies the node on which you want to examine the access cache entry.

-vserver <vserver name> - Vserver

This parameter specifies the name of the Vserver on which you want to see the access cache entry.

-policy <export policy name> - Policy Name

This parameter specifies the name of the export policy that is in effect on the export path that the client is trying to access.

-address <IP Address> - IP Address

This parameter specifies the IP address of the client whose access cache entry you want to examine.

[-flags {pending|refreshing|is-abandoned|is-queued-for-update|is-updating|has-usable-data}] - Access Cache Entry Flags

Selects the access cache entries that match the specified flags value. The flags describe the internal state of the access cache entry. The access cache entry could be in 'pending' state. This denotes the initial state of the access cache entry when a client first tries to access the exported mount point and the rules in the export policy are being matched against the IP address of the client. The 'refreshing' state denotes that the access cache entry is being refreshed. The 'abandoned' state denotes that the access cache entry has been cleared as a result of a cache flush operation. If the access cache entry has been successfully evaluated this field will not be set to any value.

[-result <integer>] - Result Code

Selects the access cache entries that match the specified result value. This field describes the error code of the error encountered when matching the IP address of the client against the rules specified in the export policy. If all rules were evaluated successfully this field will be set to 0.

[-first-unresolved-index <integer>] - First Unresolved Rule Index

Selects the access cache entries that match the specified unresolved rule index value. This field describes the rule index of the first rule in the export policy that could not be evaluated successfully when matching the IP address of the client against the rules specified in the export policy. If all rules were evaluated successfully this field will not be set to any value.

[-unresolved-clientmatch <text>] - Unresolved Clientmatch

Selects the access cache entries that match the specified unresolved client match value. This field describes the client match string that caused the rule evaluation to fail at the displayed rule index. Client match strings that denote a netgroup, hostname or a domain name can fail in evaluation if there are problems in contacting the name servers configured to serve them. If all rules were evaluated successfully this field will not be set to any value.

[-num-rules <integer>] - Number of Matched Policy Rules

Selects the access cache entries that match the specified number of matched export rules. This field describes the number of rules in the export policy that were matched successfully against the IP address of the client. If the number of matched rules is 0 and the 'result' field is also 0 then the client will experience an access denied error during mount. If the number of matched rules is non-zero and the 'result' field is 0 then access is granted or denied based on the ro, rw, superuser and other security settings in the matched rules. If the number of matched rules is 0 and the 'result' field has a non-zero value in it the client will experience a hang until the error that caused the rule evaluation to fail is resolved. If the number of matched rules is non-zero and the 'result' field has a non-zero value then this represents a situation where an error was encountered that stopped the match of rules in the export policy against the IP address of the client. The rules that have matched so far are used to make access decisions. (Note that the match of rules follows an ordering precedence determined by the rule index). Access may be granted if the security settings in the rules that have matched so far allow access. The security settings in the partial subset of matched rules are never used to deny access because they represent an incomplete set of matched export rules. Instead the client will experience a hang until the error that caused the rule evaluation to fail is resolved.

[-ruleindex-list <integer>,…] - List of Matched Policy Rule Indexes

Selects the access cache entries that match the specified list of matched rule indexes. This field describes a comma separated list of the indexes of the rules in the export policy that matched the IP address of the client. If no rules match the IP address of the client or an error was encountered in the client match process then this field will not be set to any value.

[-age <[<integer>h][<integer>m][<integer>s]>] - Age of Entry

Selects the access cache entries that match the specified age of the entry. This field describes the age of the access cache entry.

[-polarity {positive|negative|init}] - Access Cache Entry Polarity

Selects the access cache entries that match the specified polarity of the entry. The polarity of an access cache entry can be positive or negative. A positive polarity denotes that access is granted to the client IP address. A negative polarity denotes that access is denied to the client IP address.

[-duration-since-last-use <[<integer>h][<integer>m][<integer>s]>] - Time Elapsed since Last Use for Access Check

Selects the access cache entries that match the specified time duration since the entry was last used for access determination.

[-duration-since-last-update-attempt <[<integer>h][<integer>m][<integer>s]>] - Time Elapsed since Last Update Attempt

Selects the access cache entries that match the specified time duration since the access cache entry was last updated.

[-last-update-attempt-result <integer>] - Result of Last Update Attempt

Selects the access cache entries that match the specified result obtained when the access cache entry was last updated.

[-clientmatch-list <text>,…] - List of Client Match Strings

Selects the access cache entries that match the specified list of clientmatch strings that matched the specified client IP address.

Examples

The following example shows the contents of the access cache entry for client IP address '10.22.33.32' in volume 'flex1' having export policy 'testpol' in a Vserver named 'vs1' on node 'vsim1':

```
cluster1::*> vserver export-policy access-cache show -vserver vs1 -policy
testpol -node vsim1 -address 10.22.33.32
Node: vsim1
                                        Vserver: vs1
                                    Policy Name: testpol
                                     IP Address: 10.22.33.32
                           Access Cache Entry Flags: has-usable-data
                                    Result Code: 0
                        First Unresolved Rule Index: -
                             Unresolved Clientmatch: -
                    Number of Matched Policy Rules: 1
                List of Matched Policy Rule Indexes: 20
                                  Age of Entry: 77s
                      Access Cache Entry Polarity: positive
            Time Elapsed since Last Update Attempt: 8s
      Time Elapsed since Last Use for Access Check: 3s
                    Result of Last Update Attempt: 7208
                     List of Client Match Strings: 0.0.0.0/0
```

Related Links

- vserver export-policy access-cache show-rules

vserver export-policy access-cache config modify-all-vservers

Modify exports access cache configuration for all Vservers

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

Description

The `vserver export-policy access-cache config modify-all-vservers` command modifies access cache timeout values for all Vservers. Modifying these values from any node updates the values on all the nodes in the cluster. The modified values persist across reboots.

> This command is not supported in a cluster with effective cluster version of Data ONTAP 9.0.0 or later. The access cache settings are modified on a per-Vserver basis starting Data ONTAP 9.0.0. See the vserver export-policy access-cache config modify command.

Parameters

`[-ttl-positive <integer>]` - TTL For Positive Entries (Secs)

This parameter specifies the duration after which positive access cache entries will be refreshed when the client accesses.

[-ttl-negative <integer>] - TTL For Negative Entries (Secs)

This parameter specifies the duration after which negative access cache entries will be refreshed when the client accesses.

[-harvest-timeout <integer>] - Harvest Timeout (Secs)

This parameter specifies the time period after which Data ONTAP deletes unused entries in the access cache.

[-isDnsTTLEnabled {true|false}] - Is Dns TTL Enabled

This parameter specifies the dns TTL is enabled or not.

Examples

The following command sets the positive TTL value to 36000 seconds, the negative TTL value to 3600 seconds, and the harvest timeout value to 43200 seconds for all Vservers in a cluster where the effective cluster version is earlier than Data ONTAP 9.0.0.

```
cluster1::*> vserver export-policy access-cache config modify-all-vservers
-ttl-positive 36000 -ttl-negative 3600 -harvest-timeout 43200
-isDnsTTLEnabled false

cluster1::*> vserver export-policy access-cache config show-all-vservers
     TTL For Positive Entries (secs): 36000
     TTL For Negative Entries (secs): 3600
               Harvest Timeout (secs): 43200
                   Is Dns TTL Enabled: false
```

Related Links

- vserver export-policy access-cache config modify

vserver export-policy access-cache config modify

Modify exports access cache configuration

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

Description

The `vserver export-policy access-cache config modify` command modifies access cache timeout values per Vserver. Modifying these values from any node updates the values on all the nodes in the cluster. The modified values persist across reboots.

Parameters

-vserver <vserver name> - Vserver

This parameter specifies the Vserver name for which the timeout values need to be modified.

[-ttl-positive <integer>] - TTL For Positive Entries (Secs)

This parameter specifies the duration after which positive access cache entries will be refreshed upon client access. The value is specified in seconds. The default value is 3600 seconds. Valid values range from 300 seconds to 86400 seconds.

[-ttl-negative <integer>] - TTL For Negative Entries (Secs)

This parameter specifies the duration after which negative access cache entries will be refreshed upon client access. The value is specified in seconds. The default value is 3600 seconds. Valid values range from 60 seconds to 86400 seconds.

[-harvest-timeout <integer>] - Harvest Timeout (Secs)

This parameter specifies the time period after which Data ONTAP deletes unused entries in the access cache. The value is specified in seconds. The default value is 86400 seconds. Valid values range from 60 seconds to 2592000 seconds.

[-isDnsTTLEnabled {true|false}] - Is Dns TTL Enabled

This parameter specifies the dns TTL is enabled or not. If dns TTL is enable then access cache will use ttl returned from dns lookup, in case dns lookup doesn’t return TTL then it will use default ttl value.

Examples

The following command sets the positive TTL value to 36000 seconds, the negative TTL value to 3600 seconds, and the harvest timeout value to 43200 seconds for Vserver 'vs0':

```
cluster1::*> vserver export-policy access-cache config modify -ttl
-positive 36000 -ttl-negative 3600 -harvest-timeout 43200 -isDnsTTLEnabled
false

cluster1::*> vserver export-policy access-cache config show -vserver vs0
Vserver: vs0
    TTL For Positive Entries (secs): 36000
    TTL For Negative Entries (secs): 3600
TTL For Entries with Failure (secs): 1
             Harvest Timeout (secs): 43200
                 Is Dns TTL Enabled: false
```

vserver export-policy access-cache config show-all-vservers

Display exports access cache configuration for all Vservers

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

Description

The `vserver export-policy access-cache config show-all-vservers` command displays the timeout attributes related to the exports access cache. The access cache maintains export rules applicable to a client that is accessing the volume or qtree. Data ONTAP obtains the access cache timeout values from the

node where you run the command. The command output displays the following timeout parameters and their values:

- TTL for Positive Entries: This is the TTL for positive entries in the access cache. During client access, if the TTL for the access cache entry that is allowing access has expired, that access cache entry will be refreshed. While the refresh is in progress, client access will be evaluated with the existing information in the access cache entry.
- TTL for Negative Entries: This is the TTL for negative entries in the access cache. During client access, if the TTL for the access cache entry that is denying access has expired, that access cache entry will be refreshed. While the refresh is in progress, client access will be evaluated with the existing information in the access cache entry.
- Harvest Timeout: If Data ONTAP does not use an entry that is stored in the access cache for this period of time, it deletes the entry.

This command is not supported in a cluster with effective cluster version of Data ONTAP 9.0.0 or later. The access cache settings are stored on a per-Vserver basis starting Data ONTAP 9.0.0. See the vserver export-policy access-cache config show command.

Examples

The following command displays the exports access cache timeout values for all Vservers in a cluster where the effective cluster version is earlier than Data ONTAP 9.0.0:

```
cluster1::*> vserver export-policy access-cache config show-all-vservers
     TTL For Positive Entries (secs): 36000
     TTL For Negative Entries (secs): 3600
              Harvest Timeout (secs): 43200
```

Related Links

- vserver export-policy access-cache config show

vserver export-policy access-cache config show

Display exports access cache configuration

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

Description

The `vserver export-policy access-cache config show` command displays the timeout attributes related to the exports access cache. The access cache maintains export rules applicable to a client that is accessing the volume or qtree. The command output displays the following timeout parameters and their values for each Vserver:

- TTL for Positive Entries: This is the TTL for positive entries in the access cache. During client access, if the TTL for the access cache entry that is allowing access has expired, that access cache entry will be refreshed. While the refresh is in progress, client access will be evaluated with the existing information in the access cache entry.

- TTL for Negative Entries: This is the TTL for negative entries in the access cache. During client access, if the TTL for the access cache entry that is denying access has expired, that access cache entry will be refreshed. While the refresh is in progress, client access will be evaluated with the existing information in the access cache entry.
- TTL for Entries with Failure: This is the TTL for access cache entries for which a failure was encountered while trying to get matching rules.
- Harvest Timeout: If Data ONTAP does not use an entry that is stored in the access cache for this period of time, it deletes the entry.

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 timeout values for the specified Vserver.

[-ttl-positive <integer>] - TTL For Positive Entries (Secs)

If this parameter is specified, the command displays the timeout values for Vservers whose ttl-positive matches the provided value.

[-ttl-negative <integer>] - TTL For Negative Entries (Secs)

If this parameter is specified, the command displays the timeout values for Vservers whose ttl-negative matches the provided value.

[-harvest-timeout <integer>] - Harvest Timeout (Secs)

If this parameter is specified, the command displays the timeout values for Vservers whose harvest-timeout matches the provided value.

[-isDnsTTLEnabled {true|false}] - Is Dns TTL Enabled

If this parameter is specified, the command displays the isDnsTTLEnabled value.

Examples

The following command displays the exports access cache timeout values for all Vservers in the cluster:

```
cluster1::*> vserver export-policy access-cache config show
Vserver  TTL Positive  TTL Negative TTL Failure Harvest Timeout
isDnsTTLEnabled
               (secs)        (secs)      (secs)          (secs)
-------- ------------ ------------ ----------- --------------- --------
vs0               300           60           1            3600 false
vs1             36000         3600           5            3600 false
2 entries were displayed.
```

vserver export-policy cache flush

Flush the Export Caches

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

Description

The `vserver export-policy cache flush` command clears out the contents of the export policy caches for a Vserver. You might need to flush the caches to allow the changes to immediately take effect for your NFS clients because of:

- A change to your export policy rules.
- Modifying a host name record in a name server (i.e., local hosts or DNS).
- Modifying a PTR record in a DNS server (i.e., reverse DNS lookup).
- Modifying the entries in a netgroup in a name server (i.e., local netgroup, LDAP, or NIS).
- Recovering from a network outage that resulted in a netgroup being partially expanded.

To flush the caches, you must specify the following items:

- Vserver: either a specific Vserver or use "*" to flush all of them.

You can optionally specify the following items:

- Node: if flushing the *access* cache, you can also specify which node to flush it on.
- Cache to flush: by default all but *showmount* will be flushed.

Note that the *showmount* cache is not used to determine NFS client access and as such is only flushable explicitly.

Parameters

-vserver <vserver name> - Vserver

This parameter specifies the name of the Vserver on which you want to flush the caches.

[-node <nodename>] - Node

This parameter specifies the node on which you want to flush the *access* cache.

[-cache {all|access|host|id|name|netgroup|showmount|ip}] - Cache Name

This parameter specifies the name of the cache which you want to flush. Possible values include the following:

- *all* - All caches but *showmount* . This is the default.
- *access* - The export-policy rules access cache.
- *host* - The host name to IP cache.
- *id* - The ID to credential cache.
- *ip* - The IP to host name cache.
- *name* - The name to ID cache.
- *netgroup* - The netgroup cache.
- *showmount* - The showmount caches.

Examples

The following example flushes the access cache on a Vserver named vs0:

```
cluster1::> vserver export-policy cache flush -vserver vs0 -cache access
```

vserver export-policy config-checker show

Show the status of export policy configuration checker jobs

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

Description

The `vserver export-policy config-checker show` command displays status information about export policy configuration checker job. This command displays the following information:

- Vserver name
- Export policy name
- Export policy configuration checker job state
- Export policy rule checked count
- Export policy rule being checked rule index
- Export policy rule with issue count

This command output will only be available after running the export policy configuration checker job.

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 entries.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays export policy configuration checker job state information for Vservers that match the specified value.

[-policy <export policy name>] - Policy Name

If you specify this parameter, the command displays export policy configuration checker job state information for policy that match the specified value.

[-rules-checked <integer>] - Number of Rules Checked

If you specify this parameter, the command displays export policy configuration checker job state information that have the specified rules-checked count matching.

[-rule-being-checked <integer>] - Rule Being Checked

If you specify this parameter, the command displays export policy configuration checker job state information that have the specified rule-being-checked index matching.

[-rules-with-issues <integer>] - Number of Rules with Issues

If you specify this parameter, the command displays export policy configuration checker job state information that have the specified rules-with-issues count matching.

[-state {Initial|Queued|Running|Waiting|Pausing|Paused|Quitting|Success|Failure|Reschedule|Error|Quit|Dead|Unknown|Restart|Dormant}] - Job State

If you specify this parameter, the command displays export policy configuration checker job state information that have the specified state matching.

Examples

The following example displays an export policy configuration checker job state information for vserver vs2 and policy default:

```
cluster1::> vserver export-policy config-checker show -vserver vs2 -policy
default
Job       Rules     Rule Index    Rules With
Vserver    Policy     State     Checked   Being Checked Issues
---------- ---------- --------- --------- ------------- -------------
vs2        default    Running   1         2             1
```

vserver export-policy config-checker start

Start export policy configuration checker job

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

Description

The `vserver export-policy config-checker start` command invokes background job, which will check export policy configuration and if issue found in rules then error entry is created for each affected rule in export policy configuration checker error rule list.

Export policy configuration checker only validates hostname, netgroup and anonymous user related configuration.

Parameters

`-vserver <vserver name>` - Vserver

If you specify this parameter, the export policy configuration checker job will be triggered for specified Vserver.

`[-policy <export policy name>]` - Export Policy Name

If you specify this parameter, the export policy configuration checker job will be triggered for specified policy.

Examples

The following example start a export policy configuration checker job for vserver vs2 and policy default:

```
cluster1::> vserver export-policy config-checker start -vserver vs2
-policy default
          [Job 644] Job is queued: Export Policy configuration checker.
```

vserver export-policy config-checker stop

Stop export policy configuration checker job

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

Description

The `vserver export-policy config-checker stop` command stops running export policy configuration checker job.

Export policy configuration checker stop command only works if the keys provided are same as the keys provided at the time of starting export policy configuration checker job.

Parameters

`-vserver <vserver name>` - Vserver

If you specify this parameter, the command stops export policy configuration checker job, if any export policy configuration checker job is running for the specified Vserver.

[-policy <export policy name>] - Export Policy Name

If you specify this parameter, the command stops export policy configuration checker job, if any export policy configuration checker job is running for the specified policy.

Examples

The following example stop an export policy configuration checker job for Vserver vs2 and policy default:

```
cluster1::> vserver export-policy config-checker stop -vserver vs2 -policy
default
```

vserver export-policy config-checker rule delete

Delete error entries for rules from export policy configuration checker error rule list

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

Description

The `vserver export-policy config-checker rule delete` command deletes error rule entries from export policy configuration checker error rule list. You can delete a specific error entry rule by specifying its rule index number.

Parameters

-node {<nodename>|local} - Node

This parameter specifies the node on which the export policy configuration error rule entries are stored.

-vserver <vserver name> - Vserver

This parameter specifies the Vserver which contains the export policy.

-policy <export policy name> - Policy Name

This parameter specifies the export policy from which you want to delete an error rule entry.

-rule-index <integer> - Rule Index

This parameter specifies the index number of the error rule entry that you want to delete. You can use the vserver export-policy config-checker rule show command to view a list of rules with their index numbers.

Examples

The following example deletes an error rule entry from config-checker error rule list, with the index number 1 from an export policy named default on a Vserver named vs34:

```
cluster1::>vserver export-policy config-checker rule delete -node node-
vsim3 -vserver vs34 -policy test -rule-index 1
  (vserver export-policy config-checker rule delete)
1 entry was deleted.
```

Related Links

- vserver export-policy config-checker rule show

vserver export-policy config-checker rule show

Show error entries for rules in export policy configuration checker job

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

Description

The `vserver export-policy config-checker rule show` command displays information about error related to configuration in export policy rules. If a rule has any issues the configuration checker job will log information about such errors on the node where the job runs. The command displays the following information:

- Node name
- Vserver name
- Export policy name
- Export policy rule index number
- Export policy rule error

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 entries.

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

If you specify this parameter, the command displays detailed error information for node that matches the specified value.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the command displays detailed error information for Vservers that match the specified value.

[-policy <export policy name>] - Policy Name

If you specify this parameter, the command displays detailed error information for policy that match the specified value.

[-rule-index <integer>] - Rule Index

If you specify this parameter, the command displays detailed error information for rule-index that match the specified value.

[-error <text>] - Error Details

If you specify this parameter, the command displays rule index information for error that match the specified value. The complete error string needs to be specified within "{}".

Examples

The following example displays information about error related to export rules:

```
cluster1::> vserver export-policy config-checker rule show -node node-
vsim3 -vserver vs34 -policy test
  (vserver export-policy config-checker rule show)
                        Rule
Node       Vserver      Policy    Index     Error
---------- ------------ --------- ---------
---------------------------------
node-vsim3
           vs34         test      1         DNS lookup for host "h1"
failed
           vs34         test      2         Entry not found for "UserName:
testuser", DNS lookup for host "h2" failed
2 entries were displayed.
```

```
cluster1::> vserver export-policy config-checker rule show -node node-
vsim3 -vserver vs34 -policy test -rule-index 1
  (vserver export-policy config-checker rule show)
Node: node-vsim3
      Vserver: vs34
  Policy Name: test
   Rule Index: 1
Error Details: DNS lookup for host "h1" failed
```

```
cluster1::> vserver export-policy config-checker rule show -node node-
vsim3 -vserver vs34 -policy test -error  {DNS lookup for host "h1" failed}
  (vserver export-policy config-checker rule show)
                          Rule
Node       Vserver      Policy    Index     Error
---------- ------------ --------- ---------
-----------------------------------
node-vsim3
           vs34         test      1         DNS lookup for host "h1"
failed
```

vserver export-policy netgroup check-membership

Check to see if the client is a member of the netgroup

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

Description

The `vserver export-policy netgroup check-membership` command determines if the client IP address is a member of the netgroup. The netgroup must be configured as clientmatch in atleast one of the export-policy rules configured in the vserver. Data ONTAP can determine the membership information only after it has fully loaded the netgroup into the cache. Until then, while the reverse lookup scan algorithm might find a match, both DNS round robin and DNS aliases prevent ruling out non-matches. You can use the vserver export-policy netgroup queue show command to monitor the loading of the netgroup.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the name of the Vserver whose netgroup you want to check for client membership.

`-netgroup <text>` - Name of the Netgroup

This parameter specifies the name of the netgroup that you want to check for client membership.

`-client-ip <IP Address>` - Client Address

This parameter specifies the IP address of the client whose netgroup membership you want to check.

Examples

The following examples of the `vserver export-policy netgroup check-membership` command display various possible results for client membership checks.

```
cluster1::*> vserver export-policy netgroup check-membership -vserver vs1
-netgroup  mercury -client-ip 172.17.16.72
Client 172.17.16.72 is a member of netgroup "mercury" for Vserver "vs1"
with state "reverse lookup scan".

cluster1::*> vserver export-policy netgroup check-membership -vserver vs1
-netgroup  mercury -client-ip 172.17.16.72
Client 172.17.16.72 is a member of netgroup "mercury" for Vserver "vs1"
with state "cache".

cluster1::*> vserver export-policy netgroup check-membership -vserver vs1
-netgroup  mercury -client-ip 172.17.16.14
Client 172.17.16.14 is not a member of netgroup "mercury" for Vserver
"vs1".

cluster1::*> vserver export-policy netgroup check-membership -vserver vs1
-netgroup  big -client-ip 172.17.16.69
Cannot yet determine the membership of client 172.17.16.69 in netgroup
"big" for Vserver "vs1". Try again when the netgroup is loaded in the
cache.

cluster1::*> vserver export-policy netgroup check-membership -vserver vs1
-netgroup  big -client-ip 172.17.16.69
Client 172.17.16.72 is a member of netgroup "big" for Vserver "vs1" with
state "cache".

cluster1::*> vserver export-policy netgroup check-membership -vserver vs1
-netgroup  big -client-ip 2002:c65f:e228:0:0:0:0:0
Cannot yet determine the membership of client 2002:c65f:e228:: in netgroup
"big" for Vserver "vs1". Try again when the netgroup is loaded in the
cache.
```

Related Links

- vserver export-policy netgroup queue show

vserver export-policy netgroup cache show

Show the Netgroup Cache

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

Description

The `vserver export-policy netgroup cache show` command displays the contents of the export policy netgroup cache for a Vserver. Entries shown here correspond to the caches used to evaluate client

membership in a netgroup. To show the netgroup cache, you must specify the following item:

- Vserver: The name of the Vserver whose netgroup cache you want to display.

The following information is displayed per cache entry:

- Vserver name: The name of the Vserver.
- Netgroup name: The name of the netgroup.
- State of the cache entry: The state of the cache entry. There are four possible values:
- initializing: The cache entry is being populated for the first time.
- ready: Processing of the cache entry is complete and it is ready to be used.
- not-found: The netgroup could not be found.
- abandoned: The cache entry has been abandoned.
- Total number of hosts in the netgroup cache: The number of host names retrieved from the name service in mapping the netgroup to a list of hosts.
- How long it took to expand the netgroup: How long it took to expand the netgroup the last time in the queue.
- Entry is refreshing: If the entry is a complete miss or refresh.
- Next refresh time: When the next refresh is scheduled to take place.
- Netgroup by host state: Boolean state indicating if netgroup-by-host feature is used for resolving netgroup membership check.
- Number of IP addresses cached: Number of client IP addresses that are matched for the netgroup. The count includes both positive and negative results.

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 the netgroup cache information only if the Vserver name matches the specified value.

[-netgroup <text>] - Name of the Netgroup

If you specify this parameter, the command displays the netgroup cache information only if the netgroup name matches the specified value.

[-cache-state {initializing|ready|not-found|abandoned}] - State of the Cache Entry

If you specify this parameter, the command displays the netgroup cache information only if the netgroup cache state matches the specified value.

[-total-hosts <integer>] - Total Number of Hosts in the Netgroup

If you specify this parameter, the command displays the netgroup cache information only if the netgroup record's count of host names matches the specified value.

[-expansion-duration <[[<hours>:]<minutes>:]<seconds>>] - Expansion Duration

If you specify this parameter, the command displays the netgroup cache information only if the netgroup record expansion time matches the specified value.

[-is-refreshing {true|false}] - Is Entry Refreshing?

If you specify this parameter, the command displays the netgroup cache information only if the netgroup record refreshing state matches the specified value.

[-time-next-refresh <Date>] - Next Refresh Time

If you specify this parameter, the command displays the netgroup cache information only if the time of the next scheduled refresh matches the specified value.

[-num-ip-addrs-cache <integer>] - Number of Cached IP Addresses

If you specify this parameter, the command displays the netgroup cache information only if the number of cached IP addresses matches the specified value.

Examples

The following example displays the netgroup cache for the Vserver vs1 and the netgroup netgroup1:

```
cluster1::> vserver export-policy netgroup cache show -vserver vs1
-netgroup netgroup1
Vserver  Netgroup   State
    -------- ---------- ------------
    vs1      netgroup1  Ready
```

vserver export-policy netgroup queue show

Show the Netgroup Processing Queue

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

Description

The `vserver export-policy netgroup queue show` command displays the ongoing processing of the netgroup cache for a node. Entries shown here are not used to evaluate client membership in a netgroup. The following information is displayed per queue entry:

- Vserver name: The name of the Vserver.
- Netgroup name: The name of the netgroup.
- Age of entry in the queue: How long the entry has been in the queue.
- Queue state: The state of the entry in the queue. There are three possible values:
- running: The entry is currently being processed.

- waiting: The entry is waiting to be processed.
- retrying: The entry is waiting to be reprocessed.

```
 Note that as the `vserver export-policy netgroup queue show` command is
not atomic. Several queue entries might show up in the 'running' state.
* Number of times retried in the queue: The number of times was the
entry was taken off of the netgroup processing queue and added back on
it.
* Total number of hosts in the netgroup: The number of host names
retrieved from the name service in mapping the netgroup to a list of
hosts.
```

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 the netgroup cache information only if the Vserver name matches the specified value.

[-netgroup <text>] - Name of the Netgroup

If you specify this parameter, the command displays the netgroup cache information only if the netgroup name matches the specified value.

[-queue-state {waiting|running|retrying}] - State of Entry in the Queue

If you specify this parameter, the command displays the netgroup cache information only if the netgroup queue state matches the specified value.

[-age <[[<hours>:]<minutes>:]<seconds>>] - Age of Entry in the Queue

If you specify this parameter, the command displays the netgroup cache information only if the age of when the netgroup record was put on the netgroup processing queue matches the specified value.

[-retries-on-queue <integer>] - Number of Retries on the Queue

If you specify this parameter, the command displays the netgroup cache information only if, during a refresh, the number of times the netgroup record has been put back on the netgroup processing queue matches the specified value.

[-total-hosts <integer>] - Total Number of Hosts in the Netgroup

If you specify this parameter, the command displays the netgroup cache information only if the netgroup record’s count of hosts matches the specified value.

Examples

The following example displays the netgroup queue:

```
cluster1::> vserver export-policy netgroup queue show
                                        Age on     Total
    Vserver    Netgroup   State          Queue     Hosts
    ---------- ---------- --------- --------- ---------
    testvs1    test-netgr retrying     0:0:47     12441
    testvs1    test       waiting     0:01:35         -
```

vserver export-policy rule add-clientmatches

Add list of clientmatch strings to an existing rule

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

Description

The `vserver export-policy rule add-clientmatches` command adds a list of strings to the clientmatch field of a specified export rule in a policy. This command only operates on the clientmatch field; to modify other fields in a rule use the `vserver export-policy modify` command.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the Vserver on which the export policy is located.

`-policyname <export policy name>` - Policy Name

This parameter specifies the name of the export policy containing the export rule to which you want to add additional clientmatch strings.

`-ruleindex <integer>` - Rule Index

This parameter specifies the index number of the export rule to which you want to add additional clientmatch strings. To view a list of rules with their index numbers, use the vserver export-policy rule show command.

`-clientmatches <text>` - List of Clientmatch Strings to Add

This parameter specifies list of the match strings specifying the client or clients to add to the export rule. Duplicate match strings will not be created and the list may not contain duplicates entries. Match strings from the clientmatches list are added to the clientmatch field if the match string is not identical to one of the strings already in the clientmatch field. The maximum number of clientmatches that can be created is 4096. You can specify the match string in any of the following formats:

- As a hostname; for instance, host1
- As an IPv4 address; for instance, 10.1.12.24
- As an IPv6 address; for instance, fd20:8b1e:b255:4071::100:1

- As an IPv4 address with a subnet mask expressed as a number of bits; for instance, 10.1.12.0/24
- As an IPv6 address with a subnet mask expressed as a number of bits; for instance, fd20:8b1e:b255:4071::/64
- As an IPv4 address with a network mask; for instance, 10.1.16.0/255.255.255.0
- As a netgroup, with the netgroup name preceded by the @ character; for instance, @eng
- As a domain name preceded by the . character; for instance, .example.com

Note: Entering an IP address range, such as 10.1.12.10-10.1.12.70, is not allowed. Entries in this format are interpreted as a text string and treated as a hostname.

Examples

The following example adds match strings "2.2.2.2" and "3.3.3.3" to the clientmatch field of the export rule with index number 3 in an export policy named default_expolicy on a Vserver named vs0.

```
cluster1::> vserver export-policy rule add-clientmatches -vserver vs0
-policyname default_expolicy -ruleindex 3 -clientmatches "2.2.2.2,3.3.3.3"
```

Related Links

- vserver export-policy rule show

vserver export-policy rule create

Create a rule

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

Description

The `vserver export-policy rule create` command creates an export rule and adds it to a policy. To create an export rule, you must specify the following items:

- Vserver
- Export policy
- Clients that match the rule
- Read-only access rule
- Read-write access rule

You can optionally specify the following items:

- Index number; that is, the location of the export rule in the policy
- Access protocol
- Anonymous ID
- Superuser security type

- Whether suid access is enabled
- Whether creation of devices is enabled
- Whether UNIX-type permissions changes on NTFS (Windows) volumes are prohibited or allowed when the request originates from an NFS client (advanced privilege and higher only)
- Whether ownership changes are restricted or not (advanced privilege and higher only)

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the Vserver on which the export policy is located.

`-policyname <export policy name>` - Policy Name

This parameter specifies the name of the export policy to which you want to add the new export rule. The export policy must already exist. To create an export policy, see the vserver export-policy create command.

`[-ruleindex <integer>]` - Rule Index

This optional parameter specifies the index number of the export rule that you want to create. If you specify an index number that already matches a rule, the index number of the existing rule is incremented, as are the index numbers of all subsequent rules, either to the end of the list or to an open space in the list. If you do not specify an index number, the new rule is placed at the end of the policy's list. Valid values are values from 1 to 4294967295.

`[-protocol <Client Access Protocol>,…]` - Access Protocol

This optional parameter specifies the list of access protocols for which you want to apply the export rule. Possible values include the following:

- *`any`* - Any current or future access protocol
- *`nfs`* - Any current or future version of NFS
- *`nfs3`* - The NFSv3 protocol
- *`nfs4`* - The NFSv4 protocol
- *`cifs`* - The CIFS protocol

You can specify a comma-separated list of multiple access protocols for an export rule. If you specify the protocol as any, you cannot specify any other protocols in the list. If you do not specify this parameter, the value defaults to *`any`* . If you enable NFSv4, you will not be able to apply the policy to which this rule belongs to a FlexGroup, as FlexGroups do not support NFSv4 protocol access.

`-clientmatch <text>` - List of Client Match Hostnames, IP Addresses, Netgroups, or Domains

This parameter specifies list of the match strings specifying the client or clients to which the export rule applies. Duplicate match strings in the same rule are not allowed. The maximum number of clientmatches that can be created is 4096. You can specify the match string in any of the following formats:

- As a hostname; for instance, host1
- As an IPv4 address; for instance, 10.1.12.24
- As an IPv6 address; for instance, fd20:8b1e:b255:4071::100:1
- As an IPv4 address with a subnet mask expressed as a number of bits; for instance, 10.1.12.0/24

- As an IPv6 address with a subnet mask expressed as a number of bits; for instance, fd20:8b1e:b255:4071::/64
- As an IPv4 address with a network mask; for instance, 10.1.16.0/255.255.255.0
- As a netgroup, with the netgroup name preceded by the @ character; for instance, @eng
- As a domain name preceded by the . character; for instance, .example.com

Note: Entering an IP address range, such as 10.1.12.10-10.1.12.70, is not allowed. Entries in this format are interpreted as a text string and treated as a hostname.

`-rorule <authentication method>,…` - RO Access Rule

This parameter specifies the security type for read-only access to volumes that use the export rule. Possible values include the following:

- *`sys`* - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume if the security type of that incoming request is AUTH_SYS. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes sys.
- *`krb5`* - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume if the security type of that incoming request is Kerberos v5. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes krb5.
- *`krb5i`* - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume if the security type of that incoming request is Kerberos v5 with integrity service. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes krb5i.
- *`krb5p`* - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume if the security type of that incoming request is Kerberos v5 with privacy service. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes krb5p.
- *`ntlm`* - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume if the security type of that incoming request is CIFS NTLM. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes ntlm.
- *`any`* - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume regardless of the security type of that incoming request. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) remains the same as the security type of the incoming request.

  If the security type of the incoming request is AUTH_NONE, read access will be granted to that incoming request as an anonymous user.

- *`none`* - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume as an anonymous user if the security type of that incoming request is not explicitly listed in the list of values in the rorule. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes none.
- *`never`* - For an incoming request from a client matching the clientmatch criteria, do not allow any access to the volume regardless of the security type of that incoming request.

You can specify a comma-separated list of multiple security types for an export rule. If you specify the security type as *`any`* or *`never`* , you cannot specify any other security types.

For an incoming request from a client matching the clientmatch criteria, if the security type doesn't match any of the values listed in rorule (as explained above), access will be denied to that incoming request.

-rwrule <authentication method>,… - RW Access Rule

This parameter specifies the security type for read-write access to volumes that use the export rule. Possible values include the following:

- *sys* - For an incoming request from a client matching the clientmatch criteria, allow write access to the volume if the effective security type (determined from rorule) of that incoming request is AUTH_SYS.
- *krb5* - For an incoming request from a client matching the clientmatch criteria, allow write access to the volume if the effective security type (determined from rorule) of that incoming request is Kerberos v5.
- *krb5i* - For an incoming request from a client matching the clientmatch criteria, allow write access to the volume if the effective security type (determined from rorule) of that incoming request is Kerberos v5 with integrity service.
- *krb5p* - For an incoming request from a client matching the clientmatch criteria, allow write access to the volume if the effective security type (determined from rorule) of that incoming request is Kerberos v5 with privacy service.
- *ntlm* - For an incoming request from a client matching the clientmatch criteria, allow write access to the volume if the effective security type (determined from rorule) of that incoming request is CIFS NTLM.
- *any* - For an incoming request from a client matching the clientmatch criteria, allow write access to the volume regardless of the effective security type (determined from rorule) of that incoming request.

  If the effective security type (determined from rorule) of the incoming request is none, write access will be granted to that incoming request as an anonymous user.

- *none* - For an incoming request from a client matching the clientmatch criteria, allow write access to the volume as an anonymous user if the effective security type (determined from rorule) of that incoming request is none.
- *never* - For an incoming request from a client matching the clientmatch criteria, do not allow write access to the volume regardless of the effective security type (determined from rorule) of that incoming request.

You can specify a comma-separated list of multiple security types for an export rule. If you specify the security type as *any* or *never* , you cannot specify any other security types.

For an incoming request from a client matching the clientmatch criteria, if the effective security type (determined by rorule) doesn't match any of the values listed in rwrule (as explained above), write access will be denied to that incoming request.

[-anon <text>] - User ID To Which Anonymous Users Are Mapped

This parameter specifies a UNIX user ID or user name that the user credentials are mapped to when evaluation of rorule or superuser parameters result in user being mapped to the anonymous user. The default setting of this parameter is 65534, which is normally associated with the user name "nobody" or "nfsnobody" in Linux environments. NetApp appliances use 65534 as the user "pcuser", which is generally used for multiprotocol operations. Because of this difference, if using local files and NFSv4, the name string for users mapped to 65534 might not match. This discrepancy might cause files to be written as the user specified in the /etc/idmapd.conf file on the client (Linux) or /etc/default/nfs file (Solaris), particularly when using multiprotocol (CIFS and NFS) on the same datasets. The following notes apply to the use of this

parameter:

- To disable access by any client with a user ID of 0, specify a value of 65535 which is associated with the user nobody.

[-superuser <authentication method>,…] - Superuser Security Types

This parameter specifies a security type for superuser access to files. The default setting of this parameter is *none* . Possible values include the following:

- *sys* - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow superuser access to the volume if the effective security type (determined from rorule) of that incoming request is AUTH_SYS.
- *krb5* - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow superuser access to the volume if the effective security type (determined from rorule) of that incoming request is Kerberos v5.
- *krb5i* - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow superuser access to the volume if the effective security type (determined from rorule) of that incoming request is Kerberos v5 with integrity service.
- *krb5p* - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow superuser access to the volume if the effective security type (determined from rorule) of that incoming request is Kerberos v5 with privacy service.
- *ntlm* - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow superuser access to the volume if the effective security type (determined from rorule) of that incoming request is CIFS NTLM.
- *any* - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow superuser access to the volume regardless of the effective security type (determined by rorule) of that incoming request.

  If the effective security type (determined from rorule) of the incoming request is none, access will be granted to that incoming request as an anonymous user.

- *none* - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow access to the volume as an anonymous user if the effective security type (determined from rorule) of that incoming request is none.

You can specify a comma-separated list of multiple security types for superuser access. If you specify the security type as *any* , you cannot specify any other security types.

For an incoming request from a client matching the clientmatch criteria and with the user ID 0, if the effective security type doesn't match any of the values listed in superuser (as explained above), the user ID is mapped to anonymous user.

[-allow-suid {true|false}] - Honor SetUID Bits in SETATTR

This parameter specifies whether set user ID (suid) and set group ID (sgid) access is enabled by the export rule. The default setting is `true` .

[-allow-dev {true|false}] - Allow Creation of Devices

This parameter specifies whether the creation of devices is enabled by the export rule. The default setting is `true` .

[-ntfs-unix-security-ops {ignore|fail}] - NTFS Unix Security Options (privilege: advanced)

This parameter specifies whether UNIX-type permissions changes on NTFS (Windows) volumes are prohibited (fail) or allowed (ignore) when the request originates from an NFS client. The default setting is `fail`.

[-chown-mode {restricted|unrestricted}] - Change Ownership Mode (privilege: advanced)

This parameter specifies who is allowed to change the ownership mode of a file. The default setting is `restricted`. The allowed values are:

- restricted - Only root may change the ownership of the file.
- unrestricted - Non-root users may change file ownership provided the on-disk permissions allow the operation.

Examples

The following example creates an export rule with index number 1 in an export policy named read_only_expolicy on a Vserver named vs0. The rule matches all clients in the domains named example.com or example.net. The rule enables all access protocols. It enables read-only access by any matching client and requires authentication by AUTH_SYS, NTLM, or Kerberos 5 for read-write access. Clients with the UNIX user ID zero are mapped to user ID 65534 (which normally maps to the user name nobody). It does not enable suid and sgid access or the creation of devices.

```
cluster1::> vserver export-policy rule create -vserver vs0 -policyname
read_only_expolicy -ruleindex 1
-protocol any -clientmatch ".example.com,.example.net" -rorule any -rwrule
"ntlm,krb5,sys" -anon 65534 -allow-suid false
-allow-dev false
```

Related Links

- vserver export-policy create

vserver export-policy rule delete

Delete a rule

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

Description

The `vserver export-policy rule delete` command deletes an export rule from a policy. You can specify the export rule by specifying its index number in the policy. When you delete a rule, the other rules in the policy are not automatically renumbered or reordered. You can use the vserver export-policy rule setindex command to reorder the rules in a rule set.

Parameters

-vserver <vserver name> - Vserver

This parameter specifies the Vserver which contains the export policy.

-policyname <export policy name> - Policy Name

This parameter specifies the export policy from which you want to delete a rule.

-ruleindex <integer> - Rule Index

This parameter specifies the index number of the rule that you want to delete. You can use the vserver export-policy rule show command to view a list of rules with their index numbers.

Examples

The following example deletes an export rule with the index number 5 from an export policy named rs1 on a Vserver named vs0:

```
cluster1::> vserver export-policy rule delete -vserver vs0
-policyname read_only_expolicy -ruleindex 5
```

Related Links

- vserver export-policy rule setindex
- vserver export-policy rule show

vserver export-policy rule modify

Modify a rule

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

Description

The `vserver export-policy rule modify` command modifies a specified export rule in a policy. This command cannot change the position of a rule in a policy; to reorder rules in a policy, use the vserver export-policy rule setindex command. Duplicate match strings in the same rule are not allowed. You can use this command to change the following attributes of an export rule:

- Access protocol
- Client match specification
- Read-only access rule
- Read-write access rule
- Anonymous ID
- Superuser security type
- Whether suid access is enabled
- Whether creation of devices is enabled
- Whether UNIX-type permissions changes on NTFS (Windows) volumes are prohibited or allowed when the request originates from an NFS client (advanced privilege and higher only)

- Whether ownership changes are restricted or not (advanced privilege and higher only)

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the Vserver on which the export policy is located.

`-policyname <export policy name>` - Policy Name

This parameter specifies the name of the export policy containing the export rule that you want to modify.

`-ruleindex <integer>` - Rule Index

This parameter specifies the index number of the export rule that you want to modify. To view a list of rules with their index numbers, use the vserver export-policy rule show command.

`[-protocol <Client Access Protocol>,…]` - Access Protocol

This optional parameter specifies the list of access protocols for which you want to apply the export rule. Possible values include the following:

- *any* - Any current or future access protocol
- *nfs* - Any current or future version of NFS
- *nfs3* - The NFSv3 protocol
- *nfs4* - The NFSv4 protocol
- *cifs* - The CIFS protocol

You can specify a comma-separated list of multiple access protocols for an export rule. If you specify the protocol as any, you cannot specify any other protocols in the list. If you do not specify this parameter, the value defaults to *any* . If you enable NFSv4, you will not be able to apply the policy to which this rule belongs to a FlexGroup, as FlexGroups do not support NFSv4 protocol access.

`[-clientmatch <text>]` - List of Client Match Hostnames, IP Addresses, Netgroups, or Domains

This parameter specifies list of the match strings specifying the client or clients to which the export rule applies. The maximum number of clientmatches that can be created is 4096. You can specify the match string in any of the following formats:

- As a hostname; for instance, host1
- As an IPv4 address; for instance, 10.1.12.24
- As an IPv6 address; for instance, fd20:8b1e:b255:4071::100:1
- As an IPv4 address with a subnet mask expressed as a number of bits; for instance, 10.1.12.0/24
- As an IPv6 address with a subnet mask expressed as a number of bits; for instance, fd20:8b1e:b255:4071::/64
- As an IPv4 address with a network mask; for instance, 10.1.16.0/255.255.255.0
- As a netgroup, with the netgroup name preceded by the @ character; for instance, @eng
- As a domain name preceded by the . character; for instance, .example.com

Note: Entering an IP address range, such as 10.1.12.10-10.1.12.70, is not allowed. Entries in this format are interpreted as a text string and treated as a hostname.

[-rorule <authentication method>,…] - RO Access Rule

This parameter modifies the security type for read-only access to volumes that use the export rule. Possible values include the following:

- *sys* - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume if the security type of that incoming request is AUTH_SYS. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes sys.
- *krb5* - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume if the security type of that incoming request is Kerberos v5. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes krb5.
- *krb5i* - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume if the security type of that incoming request is Kerberos v5 with integrity service. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes krb5i.
- *krb5p* - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume if the security type of that incoming request is Kerberos v5 with privacy service. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes krb5p.
- *ntlm* - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume if the security type of that incoming request is CIFS NTLM. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes ntlm.
- *any* - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume regardless of the security type of that incoming request. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) remains the same as the security type of the incoming request.

  If the security type of the incoming request is AUTH_NONE, read access will be granted to that incoming request as an anonymous user.

- *none* - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume as an anonymous user if the security type of that incoming request is not explicitly listed in the list of values in the rorule. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes none.
- *never* - For an incoming request from a client matching the clientmatch criteria, do not allow any access to the volume regardless of the security type of that incoming request.

You can specify a comma-separated list of multiple security types for an export rule. If you specify the security type as *any* or *never* , you cannot specify any other security types.

For an incoming request from a client matching the clientmatch criteria, if the security type doesn't match any of the values listed in rorule (as explained above), access will be denied to that incoming request.

[-rwrule <authentication method>,…] - RW Access Rule

This parameter modifies the security type for read-write access to volumes that use the export rule. Possible values include the following:

- *sys* - For an incoming request from a client matching the clientmatch criteria, allow write access to the volume if the effective security type (determined from rorule) of that incoming request is AUTH_SYS.

- *krb5* - For an incoming request from a client matching the clientmatch criteria, allow write access to the volume if the effective security type (determined from rorule) of that incoming request is Kerberos v5.
- *krb5i* - For an incoming request from a client matching the clientmatch criteria, allow write access to the volume if the effective security type (determined from rorule) of that incoming request is Kerberos v5 with integrity service.
- *krb5p* - For an incoming request from a client matching the clientmatch criteria, allow write access to the volume if the effective security type (determined from rorule) of that incoming request is Kerberos v5 with privacy service.
- *ntlm* - For an incoming request from a client matching the clientmatch criteria, allow write access to the volume if the effective security type (determined from rorule) of that incoming request is CIFS NTLM.
- *any* - For an incoming request from a client matching the clientmatch criteria, allow write access to the volume regardless of the effective security type (determined from rorule) of that incoming request.

  If the effective security type (determined from rorule) of the incoming request is none, write access will be granted to that incoming request as an anonymous user.

- *none* - For an incoming request from a client matching the clientmatch criteria, allow write access to the volume as an anonymous user if the effective security type (determined from rorule) of that incoming request is none.
- *never* - For an incoming request from a client matching the clientmatch criteria, do not allow write access to the volume regardless of the effective security type (determined from rorule) of that incoming request.

You can specify a comma-separated list of multiple security types for an export rule. If you specify the security type as *any* or *never* , you cannot specify any other security types.

For an incoming request from a client matching the clientmatch criteria, if the effective security type (determined by rorule) doesn't match any of the values listed in rwrule (as explained above), write access will be denied to that incoming request.

[-anon <text>] - User ID To Which Anonymous Users Are Mapped

This parameter specifies a UNIX user ID or user name that the user credentials are mapped to when evaluation of rorule or superuser parameters result in user being mapped to the anonymous user. The default setting of this parameter is 65534, which is normally associated with the user name "nobody" or "nfsnobody" in Linux environments. NetApp appliances use 65534 as the user "pcuser", which is generally used for multiprotocol operations. Because of this difference, if using local files and NFSv4, the name string for users mapped to 65534 might not match. This discrepancy might cause files to be written as the user specified in the /etc/idmapd.conf file on the client (Linux) or /etc/default/nfs file (Solaris), particularly when using multiprotocol (CIFS and NFS) on the same datasets. The following notes apply to the use of this parameter:

- To disable access by any client with a user ID of 0, specify a value of 65535 which is associated with the user nobody.

[-superuser <authentication method>,…] - Superuser Security Types

This parameter specifies a security type for superuser access to files. The default setting of this parameter is *none* . Possible values include the following:

- *sys* - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow superuser access to the volume if the effective security type (determined from rorule) of that

incoming request is AUTH_SYS.

- *krb5* - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow superuser access to the volume if the effective security type (determined from rorule) of that incoming request is Kerberos v5.
- *krb5i* - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow superuser access to the volume if the effective security type (determined from rorule) of that incoming request is Kerberos v5 with integrity service.
- *krb5p* - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow superuser access to the volume if the effective security type (determined from rorule) of that incoming request is Kerberos v5 with privacy service.
- *ntlm* - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow superuser access to the volume if the effective security type (determined from rorule) of that incoming request is CIFS NTLM.
- *any* - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow superuser access to the volume regardless of the effective security type (determined by rorule) of that incoming request.

  If the effective security type (determined from rorule) of the incoming request is none, access will be granted to that incoming request as an anonymous user.

- *none* - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow access to the volume as an anonymous user if the effective security type (determined from rorule) of that incoming request is none.

You can specify a comma-separated list of multiple security types for superuser access. If you specify the security type as *any* , you cannot specify any other security types.

For an incoming request from a client matching the clientmatch criteria and with the user ID 0, if the effective security type doesn't match any of the values listed in superuser (as explained above), the user ID is mapped to anonymous user.

[-allow-suid {true|false}] - Honor SetUID Bits in SETATTR

This parameter specifies whether set user ID (suid) and set group ID (sgid) access is enabled by the export rule. The default setting is `true` .

[-allow-dev {true|false}] - Allow Creation of Devices

This parameter specifies whether the creation of devices is enabled by the export rule. The default setting is `true` .

[-ntfs-unix-security-ops {ignore|fail}] - NTFS Unix Security Options (privilege: advanced)

This parameter specifies whether UNIX-type permissions changes on NTFS (Windows) volumes are prohibited (with value *fail*) or allowed (with value *ignore*) when the request originates from an NFS client. The default setting is `fail` . This parameter is only used if you set the NTFS UNIX security option for the Vserver to `use_export_policy` ; otherwise, it has no effect.

[-chown-mode {restricted|unrestricted}] - Change Ownership Mode (privilege: advanced)

This parameter specifies who is authorized to change the ownership mode of a file. The default setting is `restricted` . This parameter is only used if you set the change ownership mode option for the Vserver to `use_export_policy` ; otherwise, it has no effect. The allowed values are :

- restricted - Only root user can change the ownership of the file.
- unrestricted - Non-root users may change file ownership provided the on-disk permissions allow the operation.

Examples

The following example modifies the export rule with index number 3 in an export policy named default_expolicy on a Vserver named vs0. The rule is modified to match any clients in the netgroups named group1 or group2 to enable NFSv2 and CIFS support, to enable read-only access by any matching client, to require authentication by NTLM or Kerberos 5 for read-write access, and to enable suid and sgid access.

```
cluster1::> vserver export-policy rule modify -vserver vs0 -policyname
default_expolicy -ruleindex 3 -protocol "nfs2,cifs"
-clientmatch "@group1, @group2" -rorule any -rwrule "ntlm,krb5" -allow
-suid true
```

Related Links

- vserver export-policy rule setindex
- vserver export-policy rule show

vserver export-policy rule remove-clientmatches

Remove list of clientmatch strings from an existing rule

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

Description

The `vserver export-policy rule remove-clientmatches` command removes a list of strings from the clientmatch field of a specified export rule in a policy. This command only operates on the clientmatch field; to modify other fields in a rule use the `vserver export-policy modify` command.

Parameters

`-vserver <vserver name>` - Vserver

This parameter specifies the Vserver on which the export policy is located.

`-policyname <export policy name>` - Policy Name

This parameter specifies the name of the export policy containing the export rule from which you want to remove clientmatch strings.

`-ruleindex <integer>` - Rule Index

This parameter specifies the index number of the export rule from which you want to remove clientmatch strings. To view a list of rules with their index numbers, use the vserver export-policy rule show command.

`-clientmatches <text>` - List of Clientmatch Strings to Remove

This parameter specifies list of the match strings specifying the client or clients to remove from the export rule. Match strings are removed from the clientmatch field if the match string is identical to one of the elements in the clientmatches list. If all match strings are removed from the clientmatch field the entire export rule is deleted. You can specify the match string in any of the following formats:

- As a hostname; for instance, host1
- As an IPv4 address; for instance, 10.1.12.24
- As an IPv6 address; for instance, fd20:8b1e:b255:4071::100:1
- As an IPv4 address with a subnet mask expressed as a number of bits; for instance, 10.1.12.0/24
- As an IPv6 address with a subnet mask expressed as a number of bits; for instance, fd20:8b1e:b255:4071::/64
- As an IPv4 address with a network mask; for instance, 10.1.16.0/255.255.255.0
- As a netgroup, with the netgroup name preceded by the @ character; for instance, @eng
- As a domain name preceded by the . character; for instance, .example.com

Note: Entering an IP address range, such as 10.1.12.10-10.1.12.70, is not allowed. Entries in this format are interpreted as a text string and treated as a hostname.

Examples

The following example removes match strings "2.2.2.2" and "3.3.3.3" from the clientmatch field of the export rule with index number 3 in an export policy named default_expolicy on a Vserver named vs0.

```
cluster1::> vserver export-policy rule remove-clientmatches -vserver vs0
-policyname default_expolicy -ruleindex 3 -clientmatches "2.2.2.2,3.3.3.3"
```

Related Links

- vserver export-policy rule show

vserver export-policy rule setindex

Move a rule to a specified index

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

Description

The `vserver export-policy rule setindex` command modifies the index number of the specified export rule. If the new index number is already in use, the command reorders the list to accommodate it. If the existing index is given a higher index number (that is, later in the list), the command decrements the index numbers of rules between the moved rule and moved-to rule; otherwise, the command increments the index numbers between the moved-to rule and the existing rule.

You can use the vserver export-policy rule show command to view a list of rules with their index numbers.

Parameters

-vserver <vserver name> - Vserver

This parameter specifies the Vserver on which the export policy is located.

-policyname <export policy name> - Policy Name

This parameter specifies the export policy that contains the rule whose index number you want to modify.

-ruleindex <integer> - Rule Index

This parameter specifies the index number of the rule that you want to move.

-newruleindex <integer> - Index

This parameter specifies the new index number for the rule.

Examples

The following example changes the index number of a rule at index number 5 to index number 3 in an export policy named rs1 on a Vserver named vs0:

```
cluster1::> vserver export-policy rule setindex -vserver vs0
-policyname read_only_policy -ruleindex 5 -newruleindex 3
```

Related Links

- vserver export-policy rule show

vserver export-policy rule show

Display a list of rules

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

Description

The `vserver export-policy rule show` command displays information about export rules. 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:

- Vserver name
- Export policy name
- Export rule index number
- Access protocol
- Client match
- Read-only access rule
- Read-write access rule

To display detailed information about a specific export rule, run the command with the `-vserver` ,

`-policyname` , and `-ruleindex` parameters. The detailed view provides all of the information in the previous list and the following additional information:

- Anonymous ID
- Superuser security type
- Whether set user ID (suid) and set group ID (sgid) access is enabled
- Whether creation of devices is enabled
- NTFS security settings
- Change ownership mode

You can specify additional parameters to display only the information that matches those parameters. For example, to display information only about export rules that have a read-write rule value of never, run the command with the `-rwrule never` parameter.

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 entries.

[-vserver <vserver name>] - Vserver

If you specify this parameter, the `-policyname` parameter, and the `-ruleindex` parameter, the command displays detailed information about the specified export rule. If you specify this parameter by itself, the command displays information only about the export rules on the specified Vserver.

[-policyname <export policy name>] - Policy Name

If you specify this parameter, the `-vserver` parameter, and the `-ruleindex` parameter, the command displays detailed information about the specified export rule. If you specify this parameter by itself, the command displays information only about the export rules on the specified policy.

[-ruleindex <integer>] - Rule Index

If you specify this parameter, the `-vserver` parameter, and the `-policyname` parameter, the command displays detailed information about the specified export rule. If you specify this parameter by itself, the command displays information only about the export rules that have the specified index number.

[-protocol <Client Access Protocol>,…] - Access Protocol

If you specify this parameter, the command displays information only about the export rules that have the specified access protocol or protocols. Possible values include the following:

- *any* - Any current or future access protocol
- *nfs* - Any current or future version of NFS
- *nfs3* - The NFSv3 protocol
- *nfs4* - The NFSv4 protocol
- *cifs* - The CIFS protocol

You can specify a comma-separated list of multiple access protocols for an export rule. If you specify the protocol as any, you cannot specify any other protocols in the list.

[-clientmatch <text>] - List of Client Match Hostnames, IP Addresses, Netgroups, or Domains

If you specify this parameter, the command displays information only about the export rules that have a clientmatch list containing all of the strings in the specified client match. You can specify the match as a list of strings in any of the following formats:

- As a hostname; for instance, host1
- As an IPv4 address; for instance, 10.1.12.24
- As an IPv6 address; for instance, fd20:8b1e:b255:4071::100:1
- As an IPv4 address with a subnet mask expressed as a number of bits; for instance, 10.1.12.0/24
- As an IPv6 address with a subnet mask expressed as a number of bits; for instance, fd20:8b1e:b255:4071::/64
- As an IPv4 address with a network mask; for instance, 10.1.16.0/255.255.255.0
- As a netgroup, with the netgroup name preceded by the @ character; for instance, @eng
- As a domain name preceded by the . character; for instance, .example.com

[-rorule <authentication method>,…] - RO Access Rule

If you specify this parameter, the command displays information only about the export rule or rules that have the specified read-only rule. Possible values include the following:

- *sys* - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume if the security type of that incoming request is AUTH_SYS. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes sys.
- *krb5* - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume if the security type of that incoming request is Kerberos v5. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes krb5.
- *krb5i* - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume if the security type of that incoming request is Kerberos v5 with integrity service. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes krb5i.
- *krb5p* - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume if the security type of that incoming request is Kerberos v5 with privacy service. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes krb5p.
- *ntlm* - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume if the security type of that incoming request is CIFS NTLM. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes ntlm.
- *any* - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume regardless of the security type of that incoming request. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) remains the same as the security type of the incoming request.

If the security type of the incoming request is AUTH_NONE, read access will be granted to that incoming request as an anonymous user.

- *none* - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume as an anonymous user if the security type of that incoming request is not explicitly listed in the list of values in the rorule. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes none.
- *never* - For an incoming request from a client matching the clientmatch criteria, do not allow any access to the volume regardless of the security type of that incoming request.

You can specify a comma-separated list of multiple security types for an export rule. If you specify the security type as *any* or *never* , you cannot specify any other security types.

> For an incoming request from a client matching the clientmatch criteria, if the security type doesn't match any of the values listed in rorule (as explained above), access will be denied to that incoming request.

[-rwrule <authentication method>,…] - RW Access Rule

If you specify this parameter, the command displays information only about the export rule or rules that have the specified read-write rule. Possible values include the following:

- *sys* - For an incoming request from a client matching the clientmatch criteria, allow write access to the volume if the effective security type (determined from rorule) of that incoming request is AUTH_SYS.
- *krb5* - For an incoming request from a client matching the clientmatch criteria, allow write access to the volume if the effective security type (determined from rorule) of that incoming request is Kerberos 5.
- *krb5i* - For an incoming request from a client matching the clientmatch criteria, allow write access to the volume if the security type of that incoming request is Kerberos v5 with integrity service. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes krb5i.
- *krb5p* - For an incoming request from a client matching the clientmatch criteria, allow write access to the volume if the security type of that incoming request is Kerberos v5 with privacy service. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes krb5p.
- *ntlm* - For an incoming request from a client matching the clientmatch criteria, allow write access to the volume if the effective security type (determined from rorule) of that incoming request is CIFS NTLM.
- *any* - For an incoming request from a client matching the clientmatch criteria, allow write access to the volume regardless of the effective security type (determined from rorule) of that incoming request.

  > If the effective security type (determined from rorule) of the incoming request is none, write access will be granted to that incoming request as an anonymous user.

- *none* - For an incoming request from a client matching the clientmatch criteria, allow write access to the volume as an anonymous user if the effective security type (determined from rorule) of that incoming request is none.
- *never* - For an incoming request from a client matching the clientmatch criteria, do not allow write access to the volume regardless of the effective security type (determined from rorule) of that incoming request.

You can specify a comma-separated list of multiple security types for an export rule. If you specify the security type as *any* or *never* , you cannot specify any other security types.

For an incoming request from a client matching the clientmatch criteria, if the effective security type (determined by rorule) doesn't match any of the values listed in rwrule (as explained above), write access will be denied to that incoming request.

[-anon <text>] - User ID To Which Anonymous Users Are Mapped

If you specify this parameter, the command displays information only about the export rule or rules that have the specified anonymous ID.

[-superuser <authentication method>,…] - Superuser Security Types

If you specify this parameter, the command displays information only about the export rule or rules that have the specified superuser security type. Possible values include the following:

- *sys* - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow superuser access to the volume if the effective security type (determined from rorule) of that incoming request is AUTH_SYS.
- *krb5* - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow superuser access to the volume if the effective security type (determined from rorule) of that incoming request is Kerberos v5.
- *krb5i* - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume if the security type of that incoming request is Kerberos v5 with integrity service. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes krb5i.
- *krb5p* - For an incoming request from a client matching the clientmatch criteria, allow read access to the volume if the security type of that incoming request is Kerberos v5 with privacy service. The effective security type of the incoming request (to be used subsequently in evaluation of rwrule/superuser) becomes krb5p.
- *ntlm* - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow superuser access to the volume if the effective security type (determined from rorule) of that incoming request is CIFS NTLM.
- *any* - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow superuser access to the volume regardless of the effective security type (determined by rorule) of that incoming request.

  If the effective security type (determined from rorule) of the incoming request is none, access will be granted to that incoming request as an anonymous user.

- *none* - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow access to the volume as an anonymous user if the effective security type (determined from rorule) of that incoming request is none.
- *never* - For an incoming request from a client matching the clientmatch criteria and with the user ID 0, allow access to the volume as an anonymous user regardless of the effective security type (determined from rorule) of that incoming request.

  Only export rules that were created in an earlier release can have the superuser parameter set to the security type *never*

You can specify a comma-separated list of multiple security types for superuser access. If you specify the security type as *any* , you cannot specify any other security types.

For an incoming request from a client matching the clientmatch criteria and with the user ID 0, if the effective security type doesn't match any of the values listed in superuser (as explained above), the user ID is mapped to anonymous user.

[-allow-suid {true|false}] - Honor SetUID Bits in SETATTR

If you specify this parameter, the command displays information only about the export rule or rules that have the specified setting for set user ID (suid) and set group ID (sgid) access.

[-allow-dev {true|false}] - Allow Creation of Devices

If you specify this parameter, the command displays information only about the export rule or rules that have the specified setting for the creation of devices.

[-ntfs-unix-security-ops {ignore|fail}] - NTFS Unix Security Options (privilege: advanced)

If you have specified this parameter for a particular export policy rule, then the command displays information about the UNIX security options that apply to that export policy rule. The setting can either prohibit (with value *fail*) or allow (with value *ignore*) UNIX-type permissions changes on NTFS (Windows) volumes when the request originates from an NFS client. If the Vserver NTFS UNIX security option is set to fail or allow for the Vserver, then this parameter is overridden.

[-ntfs-unix-security-ops-vs {fail|ignore|use_export_policy}] - Vserver NTFS Unix Security Options (privilege: advanced)

If you specify this parameter, the command displays information about the UNIX security options that apply to all volumes in this Vserver. The setting can prohibit (with value *fail*) or allow (with value *ignore*) UNIX-type permissions changes on NTFS (Windows) volumes when the request originates from an NFS client, or you can set it to `use_export_policy` . If you set this parameter to `fail` or `allow` , this parameter overrides the individual UNIX security options set for the export policy rules. If you set this parameter to `use_export_policy` , the UNIX security options associated with the respective export policy rule is used.

[-chown-mode {restricted|unrestricted}] - Change Ownership Mode (privilege: advanced)

If you have specified this parameter for a particular export policy rule, then the command displays information about the change ownership mode that applies to that export-policy rule. The setting can either allow only the root (with value *restricted*) or all users (with value *unrestricted*) to change file ownership provided the on-disk permissions allow the operation. If the Vserver change ownership mode is set to restricted or unrestricted for the Vserver, then this parameter is overridden.

[-chown-mode-vs {restricted|unrestricted|use_export_policy}] - Vserver Change Ownership Mode (privilege: advanced)

If you specify this parameter, the command displays information about the change ownership mode that applies to all volumes in this Vserver. The setting can allow only the root (with value *restricted*) or all users (with value *unrestricted*) to change ownership of the files that they own, or you can set it to `use_export_policy` . If you set this parameter to `restricted` or `unrestricted` , this parameter overrides the individual change ownership mode set for the export policy rules. If you set this parameter to `use_export_policy` , the change ownership mode associated with the respective export policy rule is used.

Examples

The following example displays information about all export rules:

```
cluster1::> vserver export-policy rule show
       Policy             Rule    Access   Client                    RO
Vserver      Name               Index   Protocol Match
Rule
------------ ------------------ ------  -------- ------------------------
------
vs0          default_expolicy   1       any      0.0.0.0/0,::0/0
any
vs0          read_only_expolicy 2       any      0.0.0.0/0
any
vs1          default_expolicy   1       any      10.10.10.10,11.11.11.11
any
vs1          test_expolicy      1       any      0.0.0.0/0
any
4 entries were displayed.
```

Copyright information

Trademark information