# Manage file access using NFS

ONTAP 9

NetApp
June 27, 2023

# Table of Contents

# Manage file access using NFS

## Enable or disable NFSv3

You can enable or disable NFSv3 by modifying the `-v3` option. This allows file access for clients using the NFSv3 protocol. By default, NFSv3 is enabled.

**Step**

1. Perform one of the following actions:

| If you want to… | Enter the command… |
|---|---|
| Enable NFSv3 | `vserver nfs modify -vserver vserver_name -v3 enabled` |
| Disable NFSv3 | `vserver nfs modify -vserver vserver_name -v3 disabled` |

## Enable or disable NFSv4.0

You can enable or disable NFSv4.0 by modifying the `-v4.0` option. This allows file access for clients using the NFSv4.0 protocol. In ONTAP 9.9.1, NFSv4.0 is enabled by default; in earlier releases, it is disabled by default.

**Step**

1. Perform one of the following actions:

| If you want to… | Enter the following command… |
|---|---|
| Enable NFSv4.0 | `vserver nfs modify -vserver vserver_name -v4.0 enabled` |
| Disable NFSv4.0 | `vserver nfs modify -vserver vserver_name -v4.0 disabled` |

## Enable or disable NFSv4.1

You can enable or disable NFSv4.1 by modifying the `-v4.1` option. This allows file access for clients using the NFSv4.1 protocol. In ONTAP 9.9.1, NFSv4.1 is enabled by default; in earlier releases, it is disabled by default.

**Step**

1. Perform one of the following actions:

| If you want to… | Enter the following command… |
| --- | --- |
| Enable NFSv4.1 | `vserver nfs modify -vserver vserver_name -v4.1 enabled` |
| Disable NFSv4.1 | `vserver nfs modify -vserver vserver_name -v4.1 disabled` |

# Manage NFSv4 storepool limits

Beginning with ONTAP 9.13, administrators can enable their NFSv4 servers to deny resources to NFSv4 clients when they have reached per client storepool resource limits. When clients consume too many NFSv4 storepool resources this can lead to other NFSv4 clients getting blocked due to unavailability of NFSv4 storepool resources.

Enabling this feature also allows customers to view the active storepool resource consumption by each client. This makes it easier to identify clients exhausting system resources, and makes it possible to impose per client resource limits.

## View storepool resources consumed

The `vserver nfs storepool show` command shows the number of storepool resources consumed. A storepool is a pool of resources used by NFSv4 clients.

### Step

1. As an administrator, run the `vserver nfs storepool show` command to display the storepool information of NFSv4 clients.

### Example

This example displays the storepool information of NFSv4 clients.

```
cluster1::*> vserver nfs storepool show

Node: node1

Vserver: vs1

Data-Ip: 10.0.1.1

Client-Ip Protocol IsTrunked OwnerCount OpenCount DelegCount LockCount

-------------- --------- --------- ---------- ---------- ----------
---------

10.0.2.1          nfs4.1     true    2 1 0 4

10.0.2.2          nfs4.2     true    2 1 0 4

2 entries were displayed.
```

## Enable or disable storepool limit controls

Administrators can use the following commands to enable or disable storepool limit controls.

**Step**

1. As an administrator, perform one of the following actions:

| If you want to… | Enter the following command… |
| --- | --- |
| Enable storepool limit controls | `vserver nfs storepool config modify -limit-enforce enabled` |
| Disable storepool limit controls | `vserver nfs storepool config modify -limit-enforce disabled` |

## View a list of blocked clients

If the storepool limit is enabled, administrators can see which clients have been blocked upon reaching their per client resource threshold. Administrators can use the following command to see which clients have been marked as blocked clients.

**Steps**

1. Use the `vserver nfs storepool blocked-client show` command to display the NFSv4 blocked client list.

### Remove a client from the blocked client list

Clients that reach their per client threshold will be disconnected and added to the block-client cache. Administrators can use the following command to remove the client from the block client cache. This will allow the client to connect to the ONTAP NFSV4 server.

**Steps**

1. Use the `vserver nfs storepool blocked-client flush -client-ip <ip address>` command to flush the storepool blocked client cache.
2. Use the `vserver nfs storepool blocked-client show` command to verify the client has been removed from the block client cache.

**Example**

This example displays a blocked client with the IP address "10.2.1.1" being flushed from all the nodes.

```
cluster1::*>vserver nfs storepool blocked-client flush -client-ip 10.2.1.1

cluster1::*>vserver nfs storepool blocked-client show

Node: node1

Client IP
----------
10.1.1.1

1 entries were displayed.
```

# Enable or disable pNFS

pNFS improves performance by allowing NFS clients to perform read/write operations on storage devices directly and in parallel, bypassing the NFS server as a potential bottleneck. To enable or disable pNFS (parallel NFS), you can modify the `-v4.1-pnfs` option.

| If the ONTAP release is… | The pNFS default is… |
|---|---|
| 9.8 or later | disabled |
| 9.7 or earlier | enabled |

**What you'll need**

NFSv4.1 support is required to be able to use pNFS.

If you want to enable pNFS, you must first disable NFS referrals. They cannot both be enabled at the same time.

If you use pNFS with Kerberos on SVMs, you must enable Kerberos on every LIF on the SVM.

**Step**

1. Perform one of the following actions:

| If you want to… | Enter the command… |
| --- | --- |
| Enable pNFS | `vserver nfs modify -vserver vserver_name -v4.1-pnfs enabled` |
| Disable pNFS | `vserver nfs modify -vserver vserver_name -v4.1-pnfs disabled` |

# Control NFS access over TCP and UDP

You can enable or disable NFS access to storage virtual machines (SVMs) over TCP and UDP by modifying the `-tcp` and `-udp` parameters, respectively. This enables you to control whether NFS clients can access data over TCP or UDP in your environment.

**About this task**

These parameters only apply to NFS. They do not affect auxiliary protocols. For example, if NFS over TCP is disabled, mount operations over TCP still succeed. To completely block TCP or UDP traffic, you can use export policy rules.

> You must turn off the SnapDiff RPC Server before you disable TCP for NFS to avoid a command failed error. You can disable TCP by using the command `vserver snapdiff-rpc-server off -vserver vserver name`.

**Step**

1. Perform one of the following actions:

| If you want NFS access to be… | Enter the command… |
| --- | --- |
| Enabled over TCP | `vserver nfs modify -vserver vserver_name -tcp enabled` |
| Disabled over TCP | `vserver nfs modify -vserver vserver_name -tcp disabled` |
| Enabled over UDP | `vserver nfs modify -vserver vserver_name -udp enabled` |
| Disabled over UDP | `vserver nfs modify -vserver vserver_name -udp disabled` |

# Control NFS requests from nonreserved ports

You can reject NFS mount requests from nonreserved ports by enabling the `-mount -rootonly` option. To reject all NFS requests from nonreserved ports, you can enable the `-nfs-rootonly` option.

**About this task**

By default, the option `-mount-rootonly` is `enabled`.

By default, the option `-nfs-rootonly` is `disabled`.

These options do not apply to the NULL procedure.

**Step**

1. Perform one of the following actions:

| If you want to… | Enter the command… |
|---|---|
| Allow NFS mount requests from nonreserved ports | `vserver nfs modify -vserver vserver_name -mount -rootonly disabled` |
| Reject NFS mount requests from nonreserved ports | `vserver nfs modify -vserver vserver_name -mount -rootonly enabled` |
| Allow all NFS requests from nonreserved ports | `vserver nfs modify -vserver vserver_name -nfs -rootonly disabled` |
| Reject all NFS requests from nonreserved ports | `vserver nfs modify -vserver vserver_name -nfs -rootonly enabled` |

# Handle NFS access to NTFS volumes or qtrees for unknown UNIX users

If ONTAP cannot identify UNIX users attempting to connect to volumes or qtrees with NTFS security style, it therefore cannot explicitly map the user to a Windows user. You can configure ONTAP to either deny access to such users for stricter security or map them to a default Windows user to ensure a minimum level of access for all users.

**What you'll need**

A default Windows user must be configured if you want to enable this option.

**About this task**

If a UNIX user tries to access volumes or qtrees with NTFS security style, the UNIX user must first be mapped to a Windows user so that ONTAP can properly evaluate the NTFS permissions. However, if ONTAP cannot look up the name of the UNIX user in the configured user information name service sources, it cannot explicitly map the UNIX user to a specific Windows user. You can decide how to handle such unknown UNIX users in the following ways:

- Deny access to unknown UNIX users.

  This enforces stricter security by requiring explicit mapping for all UNIX users to gain access to NTFS volumes or qtrees.

- Map unknown UNIX users to a default Windows user.

This provides less security but more convenience by ensuring that all users get a minimum level of access to NTFS volumes or qtrees through a default Windows user.

**Steps**

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Perform one of the following actions:

| If you want the default Windows user for unknown UNIX users… | Enter the command… |
|---|---|
| Enabled | `vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user enabled` |
| Disabled | `vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user disabled` |

3. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

# Considerations for clients that mount NFS exports using a nonreserved port

The `-mount-rootonly` option must be disabled on a storage system that must support clients that mount NFS exports using a nonreserved port even when the user is logged in as root. Such clients include Hummingbird clients and Solaris NFS/IPv6 clients.

If the `-mount-rootonly` option is enabled, ONTAP does not allow NFS clients that use nonreserved ports, meaning ports with numbers higher than 1,023, to mount NFS exports.

# Perform stricter access checking for netgroups by verifying domains

By default, ONTAP performs an additional verification when evaluating client access for a netgroup. The additional check ensures that the client's domain matches the domain configuration of the storage virtual machine (SVM). Otherwise, ONTAP denies client access.

**About this task**

When ONTAP evaluates export policy rules for client access and an export policy rule contains a netgroup, ONTAP must determine whether a client's IP address belongs to the netgroup. For this purpose, ONTAP converts the client's IP address to a host name using DNS and obtains a fully qualified domain name (FQDN).

If the netgroup file only lists a short name for the host and the short name for the host exists in multiple

domains, it is possible for a client from a different domain to obtain access without this check.

To prevent this, ONTAP compares the domain that was returned from DNS for the host against the list of DNS domain names configured for the SVM. If it matches, access is allowed. If it does not match, access is denied.

This verification is enabled by default. You can manage it by modifying the `-netgroup-dns-domain -search` parameter, which is available at the advanced privilege level.

**Steps**

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Perform the desired action:

| If you want domain verification for netgroups to be… | Enter… |
|---|---|
| Enabled | `vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search enabled` |
| Disabled | `vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search disabled` |

3. Set the privilege level to admin:

   ```
   set -privilege admin
   ```

# Modify ports used for NFSv3 services

The NFS server on the storage system uses services such as mount daemon and Network Lock Manager to communicate with NFS clients over specific default network ports. In most NFS environments the default ports work correctly and do not require modification, but if you want to use different NFS network ports in your NFSv3 environment, you can do so.

**What you'll need**

Changing NFS ports on the storage system requires that all NFS clients reconnect to the system, so you should communicate this information to your users in advance of making the change.

**About this task**

You can set the ports used by the NFS mount daemon, Network Lock Manager, Network Status Monitor, and NFS quota daemon services for each storage virtual machine (SVM). The port number change affects NFS clients accessing data over both TCP and UDP.

Ports for NFSv4 and NFSv4.1 cannot be changed.

**Steps**

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Disable access to NFS:

   ```
   vserver nfs modify -vserver vserver_name -access false
   ```

3. Set the NFS port for the specific NFS service:

   ```
   vserver nfs modify -vserver vserver_namenfs_port_parameterport_number
   ```

   | NFS port parameter | Description | Default port |
   |---|---|---|
   | `-mountd-port` | NFS mount daemon | 635 |
   | `-nlm-port` | Network Lock Manager | 4045 |
   | `-nsm-port` | Network Status Monitor | 4046 |
   | `-rquotad-port` | NFS quota daemon | 4049 |

   Besides the default port, the allowed range of port numbers is 1024 through 65535. Each NFS service must use a unique port.

4. Enable access to NFS:

   ```
   vserver nfs modify -vserver vserver_name -access true
   ```

5. Use the `network connections listening show` command to verify the port number changes.
6. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

**Example**

The following commands set the NFS Mount Daemon port to 1113 on the SVM named vs1:

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -access false

vs1::*> vserver nfs modify -vserver vs1 -mountd-port 1113

vs1::*> vserver nfs modify -vserver vs1 -access true

vs1::*> network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- -------------------------------  ----------------
Node: cluster1-01
Cluster          cluster1-01_clus_1:7700          TCP/ctlopcp
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
vs1              data1:4045                       UDP/nlm-v4
vs1              data1:1113                       TCP/mount
vs1              data1:1113                       UDP/mount
...
vs1::*> set -privilege admin
```

# Commands for managing NFS servers

There are specific ONTAP commands for managing NFS servers.

| If you want to… | Use this command… |
|---|---|
| Create an NFS server | `vserver nfs create` |
| Display NFS servers | `vserver nfs show` |
| Modify an NFS server | `vserver nfs modify` |
| Delete an NFS server | `vserver nfs delete` |

| | |
|---|---|
| Hide the `.snapshot` directory listing under NFSv3 mount points<br><br>Explicit access to the `.snapshot` directory will still be allowed even if the option is enabled. | `vserver nfs` commands with the `-v3-hide-snapshot` option enabled |

See the man page for each command for more information.

# Troubleshoot name service issues

When clients experience access failures due to name service issues, you can use the `vserver services name-service getxxbyyy` command family to manually perform various name service lookups and examine the details and results of the lookup to help with troubleshooting.

**About this task**

- For each command, you can specify the following:
  - Name of the node or storage virtual machine (SVM) to perform the lookup on.

    This enables you to test name service lookups for a specific node or SVM to narrow the search for a potential name service configuration issue.
  - Whether to show the source used for the lookup.

    This enables you to check whether the correct source was used.
- ONTAP selects the service for performing the lookup based on the configured name service switch order.
- These commands are available at the advanced privilege level.

**Steps**

1. Perform one of the following actions:

| To retrieve the… | Use the command… |
|---|---|
| IP address of a host name | `vserver services name-service getxxbyyy getaddrinfo` `vserver services name-service getxxbyyy gethostbyname` (IPv4 addresses only) |
| Members of a group by group ID | `vserver services name-service getxxbyyy getgrbygid` |
| Members of a group by group name | `vserver services name-service getxxbyyy getgrbyname` |

| | |
|---|---|
| List of groups a user belongs to | `vserver services name-service getxxbyyy getgrlist` |
| Host name of an IP address | `vserver services name-service getxxbyyy getnameinfo` `vserver services name-service getxxbyyy gethostbyaddr` (IPv4 addresses only) |
| User information by user name | `vserver services name-service getxxbyyy getpwbyname` You can test name resolution of RBAC users by specifying the `-use-rbac` parameter as `true`. |
| User information by user ID | `vserver services name-service getxxbyyy getpwbyuid`<br>You can test name resolution of RBAC users by specifying the `-use-rbac` parameter as `true`. |
| Netgroup membership of a client | `vserver services name-service getxxbyyy netgrp` |
| Netgroup membership of a client using netgroup-by-host search | `vserver services name-service getxxbyyy netgrpbyhost` |

The following example shows a DNS lookup test for the SVM vs1 by attempting to obtain the IP address for the host acast1.eng.example.com:

```
cluster1::*> vserver services name-service getxxbyyy getaddrinfo -vserver
vs1 -hostname acast1.eng.example.com -address-family all -show-source true
Source used for lookup: DNS
Host name: acast1.eng.example.com
Canonical Name: acast1.eng.example.com
IPv4: 10.72.8.29
```

The following example shows a NIS lookup test for the SVM vs1 by attempting to retrieve user information for a user with the UID 501768:

```
cluster1::*> vserver services name-service getxxbyyy getpwbyuid -vserver
vs1 -userID 501768 -show-source true
Source used for lookup: NIS
pw_name: jsmith
pw_passwd: $1$y8rA4XX7$/DDOXAvc2PC/IsNFozfIN0
pw_uid: 501768
pw_gid: 501768
pw_gecos:
pw_dir: /home/jsmith
pw_shell: /bin/bash
```

The following example shows an LDAP lookup test for the SVM vs1 by attempting to retrieve user information for a user with the name ldap1:

```
cluster1::*> vserver services name-service getxxbyyy getpwbyname -vserver
vs1 -username ldap1 -use-rbac false -show-source true
Source used for lookup: LDAP
pw_name: ldap1
pw_passwd: {crypt}JSPM6yc/ilIX6
pw_uid: 10001
pw_gid: 3333
pw_gecos: ldap1 user
pw_dir: /u/ldap1
pw_shell: /bin/csh
```

The following example shows a netgroup lookup test for the SVM vs1 by attempting to find out whether the client dnshost0 is a member of the netgroup lnetgroup136:

```
cluster1::*> vserver services name-service getxxbyyy netgrp -vserver vs1
-netgroup lnetgroup136 -client dnshost0 -show-source true
Source used for lookup: LDAP
dnshost0 is a member of lnetgroup136
```

1. Analyze the results of the test you performed and take the necessary action.

| If the… | Check the… |
|---|---|
| Host name or IP address lookup failed or yielded incorrect results | DNS configuration |
| Lookup queried an incorrect source | Name service switch configuration |

| | |
|---|---|
| User or group lookup failed or yielded incorrect results | Name service switch configuration Source configuration (local files, NIS domain, LDAP client)<br><br>Network configuration (for example, LIFs and routes) |
| Host name lookup failed or timed out, and the DNS server does not resolve DNS short names (for example, host1) | DNS configuration for top-level domain (TLD) queries. You can disable TLD queries using the `-is-tld-query-enabled false` option to the `vserver services name-service dns modify` command. |

**Related information**

NetApp Technical Report 4668: Name Services Best Practices Guide

# Verify name service connections

Beginning with ONTAP 9.2, you can check DNS and LDAP name servers to verify that they are connected to ONTAP. These commands are available at the admin privilege level.

**About this task**

You can check for a valid DNS or LDAP name service configuration on an as-needed basis using the name service configuration checker. This validation check can be initiated at the command line or in System Manager.

For DNS configurations, all servers are tested and need to be working for the configuration to be considered valid. For LDAP configurations, as long as any server is up, the configuration is valid. The name service commands apply the configuration checker unless the `skip-config-validation` field is true (the default is false).

**Step**

1. Use the appropriate command to check a name service configuration. The UI displays the status of the configured servers.

| To check… | Use this command… |
|---|---|
| DNS configuration status | `vserver services name-service dns check` |
| LDAP configuration status | `vserver services name-service ldap check` |

```
cluster1::> vserver services name-service dns check -vserver vs0

Vserver         Name Server     Status  Status Details
--------------  --------------- ------- -------------------------
 vs0            10.11.12.13     up      Response time (msec): 55
 vs0            10.11.12.14     up      Response time (msec): 70
 vs0            10.11.12.15     down    Connection refused.
+-------------------------------------------------------------+
```

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                                |
| Client Configuration Name: c1                               |
| LDAP Status: up                                             |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                              |
```

Configuration validation is successful if at least one of the configured servers (name-servers/ldap-servers) is reachable and providing the service. A warning is shown if some of the servers are not reachable.

# Commands for managing name service switch entries

You can manage name service switch entries by creating, displaying, modifying, and deleting them.

| If you want to… | Use this command… |
|---|---|
| Create a name service switch entry | `vserver services name-service ns-switch create` |
| Display name service switch entries | `vserver services name-service ns-switch show` |
| Modify a name service switch entry | `vserver services name-service ns-switch modify` |
| Delete a name service switch entry | `vserver services name-service ns-switch delete` |

See the man page for each command for more information.

**Related information**

NetApp Technical Report 4668: Name Services Best Practices Guide

# Commands for managing name service cache

You can manage name service cache by modifying the time to live (TTL) value. The TTL

value determines how long name service information is persistent in cache.

| If you want to modify the TTL value for… | Use this command… |
|---|---|
| Unix users | `vserver services name-service cache unix-user settings` |
| Unix groups | `vserver services name-service cache unix-group settings` |
| Unix netgroups | `vserver services name-service cache netgroups settings` |
| Hosts | `vserver services name-service cache hosts settings` |
| Group membership | `vserver services name-service cache group-membership settings` |

**Related information**

ONTAP 9 Commands

# Commands for managing name mappings

There are specific ONTAP commands for managing name mappings.

| If you want to… | Use this command… |
|---|---|
| Create a name mapping | `vserver name-mapping create` |
| Insert a name mapping at a specific position | `vserver name-mapping insert` |
| Display name mappings | `vserver name-mapping show` |
| Exchange the position of two name mappings<br>NOTE: A swap is not allowed when name-mapping is configured with an ip-qualifier entry. | `vserver name-mapping swap` |
| Modify a name mapping | `vserver name-mapping modify` |
| Delete a name mapping | `vserver name-mapping delete` |

| | |
|---|---|
| Validate the correct name mapping | `vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1` |

See the man page for each command for more information.

# Commands for managing local UNIX users

There are specific ONTAP commands for managing local UNIX users.

| If you want to… | Use this command… |
|---|---|
| Create a local UNIX user | `vserver services name-service unix-user create` |
| Load local UNIX users from a URI | `vserver services name-service unix-user load-from-uri` |
| Display local UNIX users | `vserver services name-service unix-user show` |
| Modify a local UNIX user | `vserver services name-service unix-user modify` |
| Delete a local UNIX user | `vserver services name-service unix-user delete` |

See the man page for each command for more information.

# Commands for managing local UNIX groups

There are specific ONTAP commands for managing local UNIX groups.

| If you want to… | Use this command… |
|---|---|
| Create a local UNIX group | `vserver services name-service unix-group create` |
| Add a user to a local UNIX group | `vserver services name-service unix-group adduser` |
| Load local UNIX groups from a URI | `vserver services name-service unix-group load-from-uri` |
| Display local UNIX groups | `vserver services name-service unix-group show` |
| Modify a local UNIX group | `vserver services name-service unix-group modify` |
| Delete a user from a local UNIX group | `vserver services name-service unix-group deluser` |

| | |
|---|---|
| Delete a local UNIX group | `vserver services name-service unix-group delete` |

See the man page for each command for more information.

# Limits for local UNIX users, groups, and group members

ONTAP introduced limits for the maximum number of UNIX users and groups in the cluster, and commands to manage these limits. These limits can help avoid performance issues by preventing administrators from creating too many local UNIX users and groups in the cluster.

There is a limit for the combined number of local UNIX user groups and group members. There is a separate limit for local UNIX users. The limits are cluster-wide. Each of these new limits is set to a default value that you can modify up to a preassigned hard limit.

| Database | Default limit | Hard limit |
|---|---|---|
| Local UNIX users | 32,768 | 65,536 |
| Local UNIX groups and group members | 32,768 | 65,536 |

# Manage limits for local UNIX users and groups

There are specific ONTAP commands for managing limits for local UNIX users and groups. Cluster administrators can use these commands to troubleshoot performance issues in the cluster believed to be related to excessive numbers of local UNIX users and groups.

**About this task**

These commands are available to the cluster administrator at the advanced privilege level.

**Step**

1. Perform one of the following actions:

| If you want to… | Use the command… |
|---|---|
| Display information about local UNIX user limits | `vserver services unix-user max-limit show` |
| Display information about local UNIX group limits | `vserver services unix-group max-limit show` |
| Modify local UNIX user limits | `vserver services unix-user max-limit modify` |

| If you want to… | Use the command… |
| --- | --- |
| Modify local UNIX group limits | `vserver services unix-group max-limit modify` |

See the man page for each command for more information.

# Commands for managing local netgroups

You can manage local netgroups by loading them from a URI, verifying their status across nodes, displaying them, and deleting them.

| If you want to… | Use the command… |
| --- | --- |
| Load netgroups from a URI | `vserver services name-service netgroup load` |
| Verify the status of netgroups across nodes | `vserver services name-service netgroup status`<br><br>Available at the advanced privilege level and higher. |
| Display local netgroups | `vserver services name-service netgroup file show` |
| Delete a local netgroup | `vserver services name-service netgroup file delete` |

See the man page for each command for more information.

# Commands for managing NIS domain configurations

There are specific ONTAP commands for managing NIS domain configurations.

| If you want to… | Use this command… |
| --- | --- |
| Create a NIS domain configuration | `vserver services name-service nis-domain create` |
| Display NIS domain configurations | `vserver services name-service nis-domain show` |
| Display binding status of a NIS domain configuration | `vserver services name-service nis-domain show-bound` |
| Display NIS statistics | `vserver services name-service nis-domain show-statistics` Available at the advanced privilege level and higher. |
| Clear NIS statistics | `vserver services name-service nis-domain clear-statistics` Available at the advanced privilege level and higher. |

| | |
|---|---|
| Modify a NIS domain configuration | `vserver services name-service nis-domain modify` |
| Delete a NIS domain configuration | `vserver services name-service nis-domain delete` |
| Enable caching for netgroup-by-host searches | `vserver services name-service nis-domain netgroup-database config modify` Available at the advanced privilege level and higher. |

See the man page for each command for more information.

# Commands for managing LDAP client configurations

There are specific ONTAP commands for managing LDAP client configurations.

> SVM administrators cannot modify or delete LDAP client configurations that were created by cluster administrators.

| If you want to… | Use this command… |
|---|---|
| Create an LDAP client configuration | `vserver services name-service ldap client create` |
| Display LDAP client configurations | `vserver services name-service ldap client show` |
| Modify an LDAP client configuration | `vserver services name-service ldap client modify` |
| Change the LDAP client BIND password | `vserver services name-service ldap client modify-bind-password` |
| Delete an LDAP client configuration | `vserver services name-service ldap client delete` |

See the man page for each command for more information.

# Commands for managing LDAP configurations

There are specific ONTAP commands for managing LDAP configurations.

| If you want to… | Use this command… |
|---|---|
| Create an LDAP configuration | `vserver services name-service ldap create` |
| Display LDAP configurations | `vserver services name-service ldap show` |
| Modify an LDAP configuration | `vserver services name-service ldap modify` |

| | |
|---|---|
| Delete an LDAP configuration | `vserver services name-service ldap delete` |

See the man page for each command for more information.

# Commands for managing LDAP client schema templates

There are specific ONTAP commands for managing LDAP client schema templates.

SVM administrators cannot modify or delete LDAP client schemas that were created by cluster administrators.

| If you want to… | Use this command… |
|---|---|
| Copy an existing LDAP schema template | `vserver services name-service ldap client schema copy` Available at the advanced privilege level and higher. |
| Display LDAP schema templates | `vserver services name-service ldap client schema show` |
| Modify an LDAP schema template | `vserver services name-service ldap client schema modify` Available at the advanced privilege level and higher. |
| Delete an LDAP schema template | `vserver services name-service ldap client schema delete` Available at the advanced privilege level and higher. |

See the man page for each command for more information.

# Commands for managing NFS Kerberos interface configurations

There are specific ONTAP commands for managing NFS Kerberos interface configurations.

| If you want to… | Use this command… |
|---|---|
| Enable NFS Kerberos on a LIF | `vserver nfs kerberos interface enable` |
| Display NFS Kerberos interface configurations | `vserver nfs kerberos interface show` |
| Modify an NFS Kerberos interface configuration | `vserver nfs kerberos interface modify` |
| Disable NFS Kerberos on a LIF | `vserver nfs kerberos interface disable` |

See the man page for each command for more information.

# Commands for managing NFS Kerberos realm configurations

There are specific ONTAP commands for managing NFS Kerberos realm configurations.

| If you want to… | Use this command… |
|---|---|
| Create an NFS Kerberos realm configuration | `vserver nfs kerberos realm create` |
| Display NFS Kerberos realm configurations | `vserver nfs kerberos realm show` |
| Modify an NFS Kerberos realm configuration | `vserver nfs kerberos realm modify` |
| Delete an NFS Kerberos realm configuration | `vserver nfs kerberos realm delete` |

See the man page for each command for more information.

# Commands for managing export policies

There are specific ONTAP commands for managing export policies.

| If you want to… | Use this command… |
|---|---|
| Display information about export policies | `vserver export-policy show` |
| Rename an export policy | `vserver export-policy rename` |
| Copy an export policy | `vserver export-policy copy` |
| Delete an export policy | `vserver export-policy delete` |

See the man page for each command for more information.

# Commands for managing export rules

There are specific ONTAP commands for managing export rules.

| If you want to… | Use this command… |
|---|---|

| | |
|---|---|
| Create an export rule | `vserver export-policy rule create` |
| Display information about export rules | `vserver export-policy rule show` |
| Modify an export rule | `vserver export-policy rule modify` |
| Delete an export rule | `vserver export-policy rule delete` |

If you have configured multiple identical export rules matching different clients, be sure to keep them in sync when managing export rules.

See the man page for each command for more information.

# Configure the NFS credential cache

## Reasons for modifying the NFS credential cache time-to-live

ONTAP uses a credential cache to store information needed for user authentication for NFS export access to provide faster access and improve performance. You can configure how long information is stored in the credential cache to customize it for your environment.

There are several scenarios when modifying the NFS credential cache time-to-live (TTL) can help resolve issues. You should understand what these scenarios are as well as the consequences of making these modifications.

### Reasons

Consider changing the default TTL under the following circumstances:

| Issue | Remedial action |
|---|---|
| The name servers in your environment are experiencing performance degradation due to a high load of requests from ONTAP. | Increase the TTL for cached positive and negative credentials to reduce the number of requests from ONTAP to name servers. |
| The name server administrator made changes to allow access to NFS users that were previously denied. | Decrease the TTL for cached negative credentials to reduce the time NFS users have to wait for ONTAP to request fresh credentials from external name servers so they can get access. |
| The name server administrator made changes to deny access to NFS users that were previously allowed. | Reduce the TTL for cached positive credentials to reduce the time before ONTAP requests fresh credentials from external name servers so the NFS users are now denied access. |

#### Consequences

You can modify the length of time individually for caching positive and negative credentials. However, you should be aware of both the advantages and disadvantages of doing so.

| If you… | The advantage is… | The disadvantage is… |
|---|---|---|
| Increase the positive credential cache time | ONTAP sends requests for credentials to name servers less frequently, reducing the load on name servers. | It takes longer to deny access to NFS users that previously were allowed access but are not anymore. |
| Decrease the positive credential cache time | It takes less time to deny access to NFS users that previously were allowed access but are not anymore. | ONTAP sends requests for credentials to name servers more frequently, increasing the load on name servers. |
| Increase the negative credential cache time | ONTAP sends requests for credentials to name servers less frequently, reducing the load on name servers. | It takes longer to grant access to NFS users that previously were not allowed access but are now. |
| Decrease the negative credential cache time | It takes less time to grant access to NFS users that previously were not allowed access but are now. | ONTAP sends requests for credentials to name servers more frequently, increasing the load on name servers. |

## Configure the time-to-live for cached NFS user credentials

You can configure the length of time that ONTAP stores credentials for NFS users in its internal cache (time-to-live, or TTL) by modifying the NFS server of the storage virtual machine (SVM). This enables you to alleviate certain issues related to high load on name servers or changes in credentials affecting NFS user access.

#### About this task

These parameters are available at the advanced privilege level.

#### Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Perform the desired action:

| If you want to modify the TTL for cached… | Use the command… |
|---|---|

| | |
|---|---|
| Positive credentials | `vserver nfs modify -vserver vserver_name -cached -cred-positive-ttl time_to_live`<br><br>The TTL is measured in milliseconds. The default is 24 hours (86,400,000 milliseconds). The allowed range for this value is 1 minute (60000 milliseconds) through 7 days (604,800,000 milliseconds). |
| Negative credentials | `vserver nfs modify -vserver vserver_name -cached -cred-negative-ttl time_to_live`<br><br>The TTL is measured in milliseconds. The default is 2 hours (7,200,000 milliseconds). The allowed range for this value is 1 minute (60000 milliseconds) through 7 days (604,800,000 milliseconds). |

3. Return to the admin privilege level:

   `set -privilege admin`

# Manage export policy caches

## Flush export policy caches

ONTAP uses several export policy caches to store information related to export policies for faster access. Flushing export policy caches manually (`vserver export-policy cache flush`) removes potentially outdated information and forces ONTAP to retrieve current information from the appropriate external resources. This can help resolve a variety of issues related to client access to NFS exports.

### About this task

Export policy cache information might be outdated due to the following reasons:

- A recent change to export policy rules
- A recent change to host name records in name servers
- A recent change to netgroup entries in name servers
- Recovering from a network outage that prevented netgroups from being fully loaded

### Steps

1. If you do not have name service cache enabled, perform one of the following actions in advance privilege mode:

| If you want to flush… | Enter the command… |
|---|---|
| All export policy caches (except for showmount) | `vserver export-policy cache flush -vserver vserver_name` |

| If you want to flush… | Enter the command… |
| --- | --- |
| The export policy rules access cache | `vserver export-policy cache flush -vserver vserver_name -cache access` You can include the optional `-node` parameter to specify the node on which you want to flush the access cache. |
| The host name cache | `vserver export-policy cache flush -vserver vserver_name -cache host` |
| The netgroup cache | `vserver export-policy cache flush -vserver vserver_name -cache netgroup` Processing of netgroups is resource intensive. You should only flush the netgroup cache if you are trying to resolve a client access issue that is caused by a stale netgroup. |
| The showmount cache | `vserver export-policy cache flush -vserver vserver_name -cache showmount` |

2. If name service cache is enabled, perform one of the following actions:

| If you want to flush… | Enter the command… |
| --- | --- |
| The export policy rules access cache | `vserver export-policy cache flush -vserver vserver_name -cache access` You can include the optional `-node` parameter to specify the node on which you want to flush the access cache. |
| The host name cache | `vserver services name-service cache hosts forward-lookup delete-all` |
| The netgroup cache | `vserver services name-service cache netgroups ip-to-netgroup delete-all` `vserver services name-service cache netgroups members delete-all` Processing of netgroups is resource intensive. You should only flush the netgroup cache if you are trying to resolve a client access issue that is caused by a stale netgroup. |
| The showmount cache | `vserver export-policy cache flush -vserver vserver_name -cache showmount` |

## Display the export policy netgroup queue and cache

ONTAP uses the netgroup queue when importing and resolving netgroups and it uses the netgroup cache to store the resulting information. When troubleshooting export policy netgroup related issues, you can use the `vserver export-policy netgroup queue show` and `vserver export-policy netgroup cache show` commands to display the status of the netgroup queue and the contents of the netgroup cache.

**Step**

1. Perform one of the following actions:

| To display the export policy netgroup… | Enter the command… |
|---|---|
| Queue | `vserver export-policy netgroup queue show` |
| Cache | `vserver export-policy netgroup cache show -vserver vserver_name` |

See the man page for each command for more information.

## Check whether a client IP address is a member of a netgroup

When troubleshooting NFS client access issues related to netgroups, you can use the `vserver export-policy netgroup check-membership` command to help determine whether a client IP is a member of a certain netgroup.

**About this task**

Checking netgroup membership enables you to determine whether ONTAP is aware that a client is or is not member of a netgroup. It also lets you know whether the ONTAP netgroup cache is in a transient state while refreshing netgroup information. This information can help you understand why a client might be unexpectedly granted or denied access.

**Step**

1. Check the netgroup membership of a client IP address: `vserver export-policy netgroup check-membership -vserver vserver_name -netgroup netgroup_name -client-ip client_ip`

   The command can return the following results:

   - The client is a member of the netgroup.

     This was confirmed through a reverse lookup scan or a netgroup-by-host search.

   - The client is a member of the netgroup.

     It was found in the ONTAP netgroup cache.

   - The client is not a member of the netgroup.

- The membership of the client cannot yet be determined because ONTAP is currently refreshing the netgroup cache.

  Until this is done, membership cannot be explicitly ruled in or out. Use the `vserver export-policy netgroup queue show` command to monitor the loading of the netgroup and retry the check after it is finished.

**Example**

The following example checks whether a client with the IP address 172.17.16.72 is a member of the netgroup mercury on the SVM vs1:

```
 cluster1::> vserver export-policy netgroup check-membership -vserver vs1
-netgroup  mercury -client-ip 172.17.16.72
```

## Optimize access cache performance

You can configure several parameters to optimize the access cache and find the right balance between performance and how current the information stored in the access cache is.

**About this task**

When you configure the access cache refresh periods, keep the following in mind:

- Higher values mean entries stay longer in the access cache.

  The advantage is better performance because ONTAP spends less resources on refreshing access cache entries. The disadvantage is that if export policy rules change and access cache entries become stale as a result, it takes longer to update them. As a result, clients that should get access might get denied, and clients that should get denied might get access.

- Lower values mean ONTAP refreshes access cache entries more often.

  The advantage is that entries are more current and clients are more likely to be correctly granted or denied access. The disadvantage is a decrease in performance because ONTAP spends more resources refreshing access cache entries.

**Steps**

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Perform the desired action:

| To modify the… | Enter… |
| --- | --- |
| Refresh period for positive entries | `vserver export-policy access-cache config modify-all-vservers -refresh -period-positive timeout_value` |

| To modify the… | Enter… |
| --- | --- |
| Refresh period for negative entries | `vserver export-policy access-cache config modify-all-vservers -refresh -period-negative timeout_value` |
| Timeout period for old entries | `vserver export-policy access-cache config modify-all-vservers -harvest -timeout timeout_value` |

3. Verify the new parameter settings:

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

4. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

# Manage file locks

## About file locking between protocols

File locking is a method used by client applications to prevent a user from accessing a file previously opened by another user. How ONTAP locks files depends on the protocol of the client.

If the client is an NFS client, locks are advisory; if the client is an SMB client, locks are mandatory.

Because of differences between the NFS and SMB file locks, an NFS client might fail to access a file previously opened by an SMB application.

The following occurs when an NFS client attempts to access a file locked by an SMB application:

- In mixed or NTFS volumes, file manipulation operations such as `rm`, `rmdir`, and `mv` can cause the NFS application to fail.
- NFS read and write operations are denied by SMB deny-read and deny-write open modes, respectively.
- NFS write operations fail when the written range of the file is locked with an exclusive SMB bytelock.

In UNIX security-style volumes, NFS unlink and rename operations ignore SMB lock state and allow access to the file. All other NFS operations on UNIX security-style volumes honor SMB lock state.

## How ONTAP treats read-only bits

The read-only bit is set on a file-by-file basis to reflect whether a file is writable (disabled) or read-only (enabled).

SMB clients that use Windows can set a per-file read-only bit. NFS clients do not set a per-file read-only bit because NFS clients do not have any protocol operations that use a per-file read-only bit.

ONTAP can set a read-only bit on a file when an SMB client that uses Windows creates that file. ONTAP can also set a read-only bit when a file is shared between NFS clients and SMB clients. Some software, when used by NFS clients and SMB clients, requires the read-only bit to be enabled.

For ONTAP to keep the appropriate read and write permissions on a file shared between NFS clients and SMB clients, it treats the read-only bit according to the following rules:

- NFS treats any file with the read-only bit enabled as if it has no write permission bits enabled.
- If an NFS client disables all write permission bits and at least one of those bits had previously been enabled, ONTAP enables the read-only bit for that file.
- If an NFS client enables any write permission bit, ONTAP disables the read-only bit for that file.
- If the read-only bit for a file is enabled and an NFS client attempts to discover permissions for the file, the permission bits for the file are not sent to the NFS client; instead, ONTAP sends the permission bits to the NFS client with the write permission bits masked.
- If the read-only bit for a file is enabled and an SMB client disables the read-only bit, ONTAP enables the owner's write permission bit for the file.
- Files with the read-only bit enabled are writable only by root.

Changes to file permissions take effect immediately on SMB clients, but might not take effect immediately on NFS clients if the NFS client enables attribute caching.

## How ONTAP differs from Windows on handling locks on share path components

Unlike Windows, ONTAP does not lock each component of the path to an open file while the file is open. This behavior also affects SMB share paths.

Because ONTAP does not lock each component of the path, it is possible to rename a path component above the open file or share, which can cause problems for certain applications, or can cause the share path in the SMB configuration to be invalid. This can cause the share to be inaccessible.

To avoid issues caused by renaming path components, you can apply Windows Access Control List (ACL) security settings that prevent users or applications from renaming critical directories.

Learn more about How to prevent directories from being renamed while clients are accessing them.

## Display information about locks

You can display information about the current file locks, including what types of locks are held and what the lock state is, details about byte-range locks, sharelock modes, delegation locks, and opportunistic locks, and whether locks are opened with durable or persistent handles.

### About this task

The client IP address cannot be displayed for locks established through NFSv4 or NFSv4.1.

By default, the command displays information about all locks. You can use command parameters to display information about locks for a specific storage virtual machine (SVM) or to filter the command's output by other criteria.

The `vserver locks show` command displays information about four types of locks:

- Byte-range locks, which lock only a portion of a file.
- Share locks, which lock open files.
- Opportunistic locks, which control client-side caching over SMB.
- Delegations, which control client-side caching over NFSv4.x.

By specifying optional parameters, you can determine important information about each lock type. See the man page for the command for more information.

**Step**

1. Display information about locks by using the `vserver locks show` command.

**Examples**

The following example displays summary information for an NFSv4 lock on a file with the path `/vol1/file1`. The sharelock access mode is write-deny_none, and the lock was granted with write delegation:

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1               lif1        nfsv4     share-level -
               Sharelock Mode: write-deny_none
                                                         delegation  -
               Delegation Type: write
```

The following example displays detailed oplock and sharelock information about the SMB lock on a file with the path `/data2/data2_2/intro.pptx`. A durable handle is granted on the file with a share lock access mode of write-deny_none to a client with an IP address of 10.3.1.3. A lease oplock is granted with a batch oplock level:

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/intro.pptx
                  Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
              Lock Protocol: cifs
                  Lock Type: share-level
    Node Holding Lock State: node3
                 Lock State: granted
   Bytelock Starting Offset: -
     Number of Bytes Locked: -
      Bytelock is Mandatory: -
      Bytelock is Exclusive: -
```

```
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                   Vserver: vs1
                    Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/test.pptx
                 Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
             Lock Protocol: cifs
                 Lock Type: op-lock
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

## Breaking locks

When file locks are preventing client access to files, you can display information about currently held locks, and then break specific locks. Examples of scenarios in which you might need to break locks include debugging applications.

#### About this task

The `vserver locks break` command is available only at the advanced privilege level and higher. The man page for the command contains detailed information.

**Steps**

1. To find the information you need to break a lock, use the `vserver locks show` command.

   The man page for the command contains detailed information.

2. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

3. Perform one of the following actions:

| If you want to break a lock by specifying… | Enter the command… |
|---|---|
| The SVM name, volume name, LIF name, and file path | `vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif` |
| The lock ID | `vserver locks break -lockid UUID` |

4. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

# How FPolicy first-read and first-write filters work with NFS

NFS clients experience high response time during high traffic of read/write requests when the FPolicy is enabled using an external FPolicy server with read/write operations as monitored events. For NFS clients, the use of first-read and first-write filters in the FPolicy reduces the number of FPolicy notifications and improves performance.

In NFS, the client does I/O on a file by fetching its handle. This handle might remain valid across reboots of the server and the client. Therefore, the client is free to cache the handle and send requests on it without retrieving handles again. In a regular session, lots of reads/write requests are sent to the file server. If notifications are generated for all these requests, it might result in the following issues:

- A larger load due to additional notification processing, and higher response time.
- A large number of notifications being sent to the FPolicy server even though the server unaffected by all of the notifications.

After receiving the first read/write request from a client for a particular file, a cache entry is created and the read/write count is incremented. This request is marked as the first-read/write operation, and an FPolicy event is generated. Before you plan and create your FPolicy filters for an NFS client, you should understand the basics of how FPolicy filters work.

- First-read: Filters the client read requests for first-read.

  When this filter is used for NFS events, the `-file-session-io-grouping-count` and `-file`

`-session-io-grouping-duration` settings determine the first-read request for which FPolicy is processed.

- First-write: Filters the client write requests for first-write.

  When this filter is used for NFS events, the `-file-session-io-grouping-count` and `-file -session-io-grouping-duration` settings determine the first-write request for which FPolicy processed.

The following options are added in NFS servers database.

```
file-session-io-grouping-count: Number of I/O Ops on a File to Be Clubbed
and Considered as One Session
for Event Generation
file-session-io-grouping-duration: Duration for Which I/O Ops on a File to
Be Clubbed and Considered as
One Session for Event Generation
```

# Modify the NFSv4.1 server implementation ID

The NFSv4.1 protocol includes a server implementation ID that documents the server domain, name, and date. You can modify the server implementation ID default values. Changing the default values can be useful, for example, when gathering usage statistics or troubleshooting interoperability issues. For more information, see RFC 5661.

**About this task**

The default values for the three options are as follows:

| Option | Option name | Default value |
|---|---|---|
| NFSv4.1 Implementation ID Domain | `-v4.1-implementation -domain` | netapp.com |
| NFSv4.1 Implementation ID Name | `-v4.1-implementation-name` | Cluster version name |
| NFSv4.1 Implementation ID Date | `-v4.1-implementation-date` | Cluster version date |

**Steps**

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Perform one of the following actions:

| If you want to modify the NFSv4.1 implementation ID… | Enter the command… |
|---|---|
| Domain | `vserver nfs modify -v4.1 -implementation-domain domain` |
| Name | `vserver nfs modify -v4.1 -implementation-name name` |
| Date | `vserver nfs modify -v4.1 -implementation-date date` |

3. Return to the admin privilege level:

   `set -privilege admin`

# Manage NFSv4 ACLs

## Benefits of enabling NFSv4 ACLs

There are many benefits to enabling NFSv4 ACLs.

The benefits of enabling NFSv4 ACLs include the following:

- Finer-grained control of user access for files and directories
- Better NFS security
- Improved interoperability with CIFS
- Removal of the NFS limitation of 16 groups per user

## How NFSv4 ACLs work

A client using NFSv4 ACLs can set and view ACLs on files and directories on the system. When a new file or subdirectory is created in a directory that has an ACL, the new file or subdirectory inherits all ACL Entries (ACEs) in the ACL that have been tagged with the appropriate inheritance flags.

When a file or directory is created as the result of an NFSv4 request, the ACL on the resulting file or directory depends on whether the file creation request includes an ACL or only standard UNIX file access permissions, and whether the parent directory has an ACL:

- If the request includes an ACL, that ACL is used.
- If the request includes only standard UNIX file access permissions but the parent directory has an ACL, the ACEs in the parent directory's ACL are inherited by the new file or directory as long as the ACEs have been tagged with the appropriate inheritance flags.

A parent ACL is inherited even if `-v4.0-acl` is set to `off`.

- If the request includes only standard UNIX file access permissions and the parent directory does not have an ACL, the client file mode is used to set standard UNIX file access permissions.
- If the request includes only standard UNIX file access permissions and the parent directory has a non-inheritable ACL, the new object is created only with mode bits.

> If the `-chown-mode` parameter has been set to `restricted` with commands in the `vserver nfs` or `vserver export-policy rule` families, file ownership can be changed by the superuser only, even if the on-disk permissions set with NFSv4 ACLs allow a non-root user to change the file ownership. For more information, see the relevant man pages.

## Enable or disable modification of NFSv4 ACLs

When ONTAP receives a `chmod` command for a file or directory with an ACL, by default the ACL is retained and modified to reflect the mode bit change. You can disable the `-v4 -acl-preserve` parameter to change the behavior if you want the ACL to be dropped instead.

**About this task**

When using unified security style, this parameter also specifies whether NTFS file permissions are preserved or dropped when a client sends a chmod, chgroup, or chown command for a file or directory.

The default for this parameter is enabled.

**Steps**

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Perform one of the following actions:

| If you want to… | Enter the following command… |
|---|---|
| Enable retention and modification of existing NFSv4 ACLs (default) | `vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled` |
| Disable retention and drop NFSv4 ACLs when changing mode bits | `vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled` |

3. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

## How ONTAP uses NFSv4 ACLs to determine whether it can delete a file

To determine whether it can delete a file, ONTAP uses a combination of the file's DELETE bit, and the containing directory's DELETE_CHILD bit. For more information, see the NFS 4.1 RFC 5661.

## Enable or disable NFSv4 ACLs

To enable or disable NFSv4 ACLs, you can modify the `-v4.0-acl` and `-v4.1-acl` options. These options are disabled by default.

### About this task

The `-v4.0-acl` or `-v4.1-acl` option controls the setting and viewing of NFSv4 ACLs; it does not control enforcement of these ACLs for access checking.

### Step

1. Perform one of the following actions:

| If you want to… | Then… |
|---|---|
| Enable NFSv4.0 ACLs | Enter the following command:<br><br>`vserver nfs modify -vserver vserver_name -v4.0-acl enabled` |
| Disable NFSv4.0 ACLs | Enter the following command:<br><br>`vserver nfs modify -vserver vserver_name -v4.0-acl disabled` |
| Enable NFSv4.1 ACLs | Enter the following command:<br><br>`vserver nfs modify -vserver vserver_name -v4.1-acl enabled` |
| Disable NFSv4.1 ACLs | Enter the following command:<br><br>`vserver nfs modify -vserver vserver_name -v4.1-acl disabled` |

## Modify the maximum ACE limit for NFSv4 ACLs

You can modify the maximum number of allowed ACEs for each NFSv4 ACL by modifying the parameter `-v4-acl-max-aces`. By default, the limit is set to 400 ACEs for each ACL. Increasing this limit can help ensure successful migration of data with ACLs containing over 400 ACEs to storage systems running ONTAP.

### About this task

Increasing this limit might impact performance for clients accessing files with NFSv4 ACLs.

### Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Modify the maximum ACE limit for NFSv4 ACLs:

   `vserver nfs modify -v4-acl-max-aces max_ace_limit`

   The valid range of

   `max_ace_limit` is `192` to `1024`.

3. Return to the admin privilege level:

   `set -privilege admin`

# Manage NFSv4 file delegations

## Enable or disable NFSv4 read file delegations

To enable or disable NFSv4 read file delegations, you can modify the `-v4.0-read-delegation`or `-v4.1-read-delegation` option. By enabling read file delegations, you can eliminate much of the message overhead associated with the opening and closing of files.

**About this task**

By default, read file delegations are disabled.

The disadvantage of enabling read file delegations is that the server and its clients must recover delegations after the server reboots or restarts, a client reboots or restarts, or a network partition occurs.

**Step**

1. Perform one of the following actions:

| If you want to… | Then… |
| --- | --- |
| Enable NFSv4 read file delegations | Enter the following command:<br><br>`vserver nfs modify -vserver vserver_name -v4.0 -read-delegation enabled` |
| Enable NFSv4.1 read file delegations | Enter the following command:<br><br>+<br>`vserver nfs modify -vserver vserver_name -v4.1 -read-delegation enabled` |
| Disable NFSv4 read file delegations | Enter the following command:<br><br>`vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled` |

| | |
|---|---|
| Disable NFSv4.1 read file delegations | Enter the following command:<br><br>`vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled` |

**Result**

The file delegation options take effect as soon as they are changed. There is no need to reboot or restart NFS.

## Enable or disable NFSv4 write file delegations

To enable or disable write file delegations, you can modify the `-v4.0-write -delegation`or `-v4.1-write-delegation` option. By enabling write file delegations, you can eliminate much of the message overhead associated with file and record locking in addition to opening and closing of files.

**About this task**

By default, write file delegations are disabled.

The disadvantage of enabling write file delegations is that the server and its clients must perform additional tasks to recover delegations after the server reboots or restarts, a client reboots or restarts, or a network partition occurs.

**Step**

1. Perform one of the following actions:

| If you want to… | Then… |
|---|---|
| Enable NFSv4 write file delegations | Enter the following command: `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation enabled` |
| Enable NFSv4.1 write file delegations | Enter the following command: `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation enabled` |
| Disable NFSv4 write file delegations | Enter the following command: `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation disabled` |
| Disable NFSv4.1 write file delegations | Enter the following command: `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation disabled` |

**Result**

The file delegation options take effect as soon as they are changed. There is no need to reboot or restart NFS.

# Configure NFSv4 file and record locking

## About NFSv4 file and record locking

For NFSv4 clients, ONTAP supports the NFSv4 file-locking mechanism, maintaining the state of all file locks under a lease-based model.

NetApp Technical Report 3580: NFSv4 Enhancements and Best Practices Guide Data ONTAP Implementation

## Specify the NFSv4 locking lease period

To specify the NFSv4 locking lease period (that is, the time period in which ONTAP irrevocably grants a lock to a client), you can modify the `-v4-lease-seconds` option. Shorter lease periods speed up server recovery while longer lease periods are beneficial for servers handling a very large amount of clients.

### About this task

By default, this option is set to `30`. The minimum value for this option is `10`. The maximum value for this option is the locking grace period, which you can set with the `locking.lease_seconds` option.

### Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Enter the following command:

   ```
   vserver nfs modify -vserver vserver_name -v4-lease-seconds number_of_seconds
   ```

3. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

## Specify the NFSv4 locking grace period

To specify the NFSv4 locking grace period (that is, the time period in which clients attempt to reclaim their locking state from ONTAP during server recovery), you can modify the `-v4-grace-seconds` option.

### About this task

By default, this option is set to `45`.

### Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Enter the following command:

```
vserver nfs modify -vserver vserver_name -v4-grace-seconds number_of_seconds
```

3. Return to the admin privilege level:

```
set -privilege admin
```

# How NFSv4 referrals work

When you enable NFSv4 referrals, ONTAP provides “intra-SVM” referrals to NFSv4 clients. Intra-SVM referral is when a cluster node receiving the NFSv4 request refers the NFSv4 client to another logical interface (LIF) on the storage virtual machine (SVM).

The NFSv4 client should access the path that received the referral at the target LIF from that point onward. The original cluster node provides such a referral when it determines that there exists a LIF in the SVM that is resident on the cluster node on which the data volume resides, thereby enabling the clients faster access to the data and avoiding extra cluster communication.

# Enable or disable NFSv4 referrals

You can enable NFSv4 referrals on storage virtual machines (SVMs) by enabling the options `-v4-fsid-change` and `-v4.0-referrals`or `-v4.1-referrals`. Enabling NFSV4 referrals can result in faster data access for NFSv4 clients that support this feature.

**What you’ll need**

If you want to enable NFS referrals, you must first disable parallel NFS. You cannot enable both at the same time.

**Steps**

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Perform one of the following actions:

| If you want to… | Enter the command… |
|---|---|
| Enable NFSv4 referrals | `vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.0-referrals enabled` |
| Disable NFSv4 referrals | `vserver nfs modify -vserver vserver_name -v4.0 -referrals disabled` |
| Enable NFSv4.1 referrals | `vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.1-referrals enabled` |

| | |
|---|---|
| Disable NFSv4.1 referrals | `vserver nfs modify -vserver vserver_name -v4.1 -referrals disabled` |

3. Return to the admin privilege level:

   `set -privilege admin`

# Display NFS statistics

You can display NFS statistics for storage virtual machines (SVMs) on the storage system to monitor performance and diagnose issues.

**Steps**

1. Use the `statistics catalog object show` command to identify the NFS objects from which you can view data.

   `statistics catalog object show -object nfs*`

2. Use the `statistics start` and optional `statistics stop` commands to collect a data sample from one or more objects.
3. Use the `statistics show` command to view the sample data.

**Example: Monitoring NFSv3 performance**

The following example shows performance data for the NFSv3 protocol.

The following command starts data collection for a new sample:

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

The following command shows data from the sample by specifying counters that show the number of successful read and write requests versus the total number of read and write requests:

```
vs1::> statistics show -sample-id nfs_sample -counter
read_total|write_total|read_success|write_success

Object: nfsv3
Instance: vs1
Start-time: 2/11/2013 15:38:29
End-time: 2/11/2013 15:38:41
Cluster: cluster1

    Counter                                     Value
    -------------------------- ----------------------------
    read_success                                40042
    read_total                                  40042
    write_success                              1492052
    write_total                                1492052
```

**Related information**

Performance monitoring setup

# Display DNS statistics

You can display DNS statistics for storage virtual machines (SVMs) on the storage system to monitor performance and diagnose issues.

**Steps**

1. Use the `statistics catalog object show` command to identify the DNS objects from which you can view data.

   ```
   statistics catalog object show -object external_service_op*
   ```

2. Use the `statistics start` and `statistics stop` commands to collect a data sample from one or more objects.
3. Use the `statistics show` command to view the sample data.

## Monitoring DNS statistics

The following examples show performance data for DNS queries. The following commands start data collection for a new sample:

```
vs1::*> statistics start -object external_service_op -sample-id
dns_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
dns_sample2
```

The following command displays data from the sample by specifying counters that display the number of DNS

queries sent versus the number of DNS queries received, failed, or timed out:

```
vs1::*> statistics show -sample-id dns_sample1 -counter
num_requests_sent|num_responses_received|num_successful_responses|num_time
outs|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:DNS:Query:10.72.219.109
Start-time: 3/8/2016 11:15:21
End-time: 3/8/2016 11:16:52
Elapsed-time: 91s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            0
    num_requests_sent                                               1
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

The following command displays data from the sample by specifying counters that display the number of times a specific error was received for a DNS query on the particular server:

```
vs1::*> statistics show -sample-id dns_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:DNS:Query:NXDOMAIN:10.72.219.109
Start-time: 3/8/2016 11:23:21
End-time: 3/8/2016 11:24:25
Elapsed-time: 64s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                             NXDOMAIN
    server_ip_address                                   10.72.219.109
3 entries were displayed.
```

**Related information**

Performance monitoring setup

# Display NIS statistics

You can display NIS statistics for storage virtual machines (SVMs) on the storage system to monitor performance and diagnose issues.

**Steps**

1. Use the `statistics catalog object show` command to identify the NIS objects from which you can view data.

   ```
   statistics catalog object show -object external_service_op*
   ```

2. Use the `statistics start` and `statistics stop` commands to collect a data sample from one or more objects.
3. Use the `statistics show` command to view the sample data.

## Monitoring NIS statistics

The following examples display performance data for NIS queries. The following commands start data collection for a new sample:

```
vs1::*> statistics start -object external_service_op -sample-id
nis_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
nis_sample2
```

The following command displays data from the sample by specifying counters that show the number of NIS queries sent versus the number of NIS queries received, failed, or timed out:

```
vs1::*> statistics show -sample-id nis_sample1 -counter
instance|num_requests_sent|num_responses_received|num_successful_responses
|num_timeouts|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:NIS:Query:10.227.13.221
Start-time: 3/8/2016 11:27:39
End-time: 3/8/2016 11:27:56
Elapsed-time: 17s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            1
    num_requests_sent                                               2
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

The following command displays data from the sample by specifying counters that show the number of times a specific error was received for a NIS query on the particular server:

```
vs1::*> statistics show -sample-id nis_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:NIS:Query:YP_NOTFOUND:10.227.13.221
Start-time: 3/8/2016 11:33:05
End-time: 3/8/2016 11:33:10
Elapsed-time: 5s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                           YP_NOTFOUND
    server_ip_address                                    10.227.13.221
3 entries were displayed.
```

**Related information**

Performance monitoring setup

# Support for VMware vStorage over NFS

ONTAP supports certain VMware vStorage APIs for Array Integration (VAAI) features in an NFS environment.

## Supported features

The following features are supported:

- Copy offload

  Enables an ESXi host to copy virtual machines or virtual machine disks (VMDKs) directly between the source and destination data store location without involving the host. This conserves ESXi host CPU cycles and network bandwidth. Copy offload preserves space efficiency if the source volume is sparse.

- Space reservation

  Guarantees storage space for a VMDK file by reserving space for it.

## Limitations

VMware vStorage over NFS has the following limitations:

- Copy offload operations can fail in the following scenarios:
  - While running wafliron on the source or destination volume because it temporarily takes the volume offline
  - While moving either the source or destination volume
  - While moving either the source or destination LIF
  - While performing takeover or giveback operations
  - While performing switchover or switchback operations
- Server-side copy can fail due to file handle format differences in the following scenario:

  You attempt to copy data from SVMs that have currently or had previously exported qtrees to SVMs that have never had exported qtrees. To work around this limitation, you can export at least one qtree on the destination SVM.

**Related information**

What VAAI offloaded operations are supported by Data ONTAP?

# Enable or disable VMware vStorage over NFS

You can enable or disable support for VMware vStorage over NFS on storage virtual machines (SVMs) by using the `vserver nfs modify` command.

**About this task**

By default, support for VMware vStorage over NFS is disabled.

**Steps**

1. Display the current vStorage support status for SVMs:

   ```
   vserver nfs show -vserver vserver_name -instance
   ```

2. Perform one of the following actions:

| If you want to… | Enter the following command… |
|---|---|
| Enable VMware vStorage support | `vserver nfs modify -vserver vserver_name -vstorage enabled` |
| Disable VMware vStorage support | `vserver nfs modify -vserver vserver_name -vstorage disabled` |

**After you finish**

You must install the NFS Plug-in for VMware VAAI before you can use this functionality. For more information, see *Installing the NetApp NFS Plug-in for VMware VAAI*.

**Related information**

NetApp Documentation: NetApp NFS Plug-in for VMware VAAI

# Enable or disable rquota support

ONTAP supports the remote quota protocol version 1 (rquota v1). The rquota protocol enables NFS clients to obtain quota information for users from a remote machine. You can enable rquota on storage virtual machines (SVMs) by using the `vserver nfs modify` command.

**About this task**

By default, rquota is disabled.

**Step**

1. Perform one of the following actions:

| If you want to… | Enter the following command… |
|---|---|
| Enable rquota support for SVMs | `vserver nfs modify -vserver vserver_name -rquota enable` |
| Disable rquota support for SVMs | `vserver nfs modify -vserver vserver_name -rquota disable` |

   For more information about quotas, see Logical storage management.

# NFSv3 and NFSv4 performance improvement by modifying the TCP transfer size

You can improve the performance of NFSv3 and NFSv4 clients connecting to storage systems over a high-latency network by modifying the TCP maximum transfer size.

When clients access storage systems over a high-latency network, such as a wide area network (WAN) or metro area network (MAN) with a latency over 10 milliseconds, you might be able to improve the connection performance by modifying the TCP maximum transfer size. Clients accessing storage systems in a low-latency network, such as a local area network (LAN), can expect little to no benefit from modifying these parameters. If the throughput improvement does not outweigh the latency impact, you should not use these parameters.

To determine whether your storage environment would benefit from modifying these parameters, you should first conduct a comprehensive performance evaluation of a poorly performing NFS client. Review whether the low performance is because of excessive round trip latency and small request on the client. Under these conditions, the client and server cannot fully use the available bandwidth because they spend the majority of their duty cycles waiting for small requests and responses to be transmitted over the connection.

By increasing the NFSv3 and NFSv4 request size, the client and server can use the available bandwidth more effectively to move more data per unit time; therefore, increasing the overall efficiency of the connection.

Keep in mind that the configuration between the storage system and the client might vary. The storage system and the client supports maximum size of 1 MB for transfer operations. However, if you configure the storage system to support 1 MB maximum transfer size but the client only supports 64 KB, then the mount transfer size is limited to 64 KB or less.

Before modifying these parameters, you must be aware that it results in additional memory consumption on the storage system for the period of time necessary to assemble and transmit a large response. The more high-latency connections to the storage system, the higher the additional memory consumption. Storage systems with high memory capacity might experience very little effect from this change. Storage systems with low memory capacity might experience noticeable performance degradation.

The successful use of these parameter relies on the ability to retrieve data from multiple nodes of a cluster. The inherent latency of the cluster network might increase the overall latency of the response. Overall latency tends to increase when using these parameters. As a result, latency sensitive workloads might show negative impact.

# Modify the NFSv3 and NFSv4 TCP maximum transfer size

You can modify the `-tcp-max-xfer-size` option to configure maximum transfer sizes for all TCP connections using the NFSv3 and NFSv4.x protocols.

**About this task**

You can modify these options individually for each storage virtual machine (SVM).

Beginning with ONTAP 9, the `v3-tcp-max-read-size` and `v3-tcp-max-write-size` options are obsolete. You must use the `-tcp-max-xfer-size` option instead.

**Steps**

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Perform one of the following actions:

| If you want to… | Enter the command… |
| --- | --- |
| Modify the NFSv3 or NFSv4 TCP maximum transfer size | `vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer_max_xfer_size` |

| Option | Range | Default |
| --- | --- | --- |
| `-tcp-max-xfer-size` | 8192 to 1048576 bytes | 65536 bytes |

> The maximum transfer size that you enter must be a multiple of 4 KB (4096 bytes). Requests that are not properly aligned negatively affect performance.

3. Use the `vserver nfs show -fields tcp-max-xfer-size` command to verify the changes.
4. If any clients use static mounts, unmount and remount for the new parameter size to take effect.

**Example**

The following command sets the NFSv3 and NFSv4.x TCP maximum transfer size to 1048576 bytes on the SVM named vs1:

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

# Configure the number of group IDs allowed for NFS users

By default, ONTAP supports up to 32 group IDs when handling NFS user credentials using Kerberos (RPCSEC_GSS) authentication. When using AUTH_SYS authentication, the default maximum number of group IDs is 16, as defined in RFC 5531. You can increase the maximum up to 1,024 if you have users who are members of more than the default number of groups.

**About this task**

If a user has more than the default number of group IDs in their credentials, the remaining group IDs are truncated and the user might receive errors when attempting to access files from the storage system. You should set the maximum number of groups, per SVM, to a number that represents the maximum groups in your environment.

The following table shows the two parameters of the `vserver nfs modify` command that determine the maximum number of group IDs in three sample configurations:

| Parameters | Settings | Resulting group IDs limit |
| --- | --- | --- |

| | | |
|---|---|---|
| `-extended-groups-limit`<br><br>`-auth-sys-extended-groups` | `32`<br><br>`disabled`<br><br>These are the default settings. | RPCSEC_GSS: 32<br><br>AUTH_SYS: 16 |
| `-extended-groups-limit`<br><br>`-auth-sys-extended-groups` | `256`<br><br>`disabled` | RPCSEC_GSS: 256<br><br>AUTH_SYS: 16 |
| `-extended-groups-limit`<br><br>`-auth-sys-extended-groups` | `512`<br><br>`enabled` | RPCSEC_GSS: 512<br><br>AUTH_SYS: 512 |

Some older NFS clients might not be compatible with AUTH_SYS extended groups.

**Steps**

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Perform the desired action:

| If you want to set the maximum number of allowed auxiliary groups… | Enter the command… |
|---|---|
| Only for RPCSEC_GSS and leave AUTH_SYS set to the default value of 16 | `vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups disabled` |
| For both RPCSEC_GSS and AUTH_SYS | `vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups enabled` |

3. Verify the `-extended-groups-limit` value and verify whether AUTH_SYS is using extended groups: `vserver nfs show -vserver vserver_name -fields auth-sys-extended-groups,extended-groups-limit`
4. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

**Example**

The following example enables extended groups for AUTH_SYS authentication and sets the maximum number of extended groups to 512 for both AUTH_SYS and RPCSEC_GSS authentication. These changes are made only for clients who access the SVM named vs1:

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -auth-sys-extended-groups enabled
-extended-groups-limit 512

vs1::*> vserver nfs show -vserver vs1 -fields auth-sys-extended-
groups,extended-groups-limit
vserver auth-sys-extended-groups extended-groups-limit
------- ------------------------ --------------------
vs1     enabled                  512

vs1::*> set -privilege admin
```

# Control root user access to NTFS security-style data

You can configure ONTAP to allow NFS clients access to NTFS security-style data and NTFS clients to access NFS security-style data. When using NTFS security style on an NFS data store, you must decide how to treat access by the root user and configure the storage virtual machine (SVM) accordingly.

**About this task**

When a root user accesses NTFS security-style data, you have two options:

- Map the root user to a Windows user like any other NFS user and manage access according to NTFS ACLs.
- Ignore NTFS ACLs and provide full access to root.

**Steps**

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Perform the desired action:

| If you want the root user to… | Enter the command… |
|---|---|
| Be mapped to a Windows user | `vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root disabled` |
| Bypass the NT ACL check | `vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root enabled` |

   By default, this parameter is disabled.

If this parameter is enabled but there is no name mapping for the root user, ONTAP uses a default SMB administrator credential for auditing.

3. Return to the admin privilege level:

```
set -privilege admin
```

## Copyright information



## Trademark information