



Adapt existing NFS exports for trunking

ONTAP 9

NetApp
April 06, 2024

Table of Contents

- Adapt existing NFS exports for trunking 1
 - Adapting single-path exports overview 1
 - Enable trunking on the NFS server 1
 - Update your network for trunking 1
 - Modify data export for client access 3
 - Reestablish client mounts 4

Adapt existing NFS exports for trunking

Adapting single-path exports overview

You can adapt an existing single-path (non-trunked) NFSv4.1 export to use trunking. Trunking-capable clients can take advantage of improved performance as soon as trunking is enabled on the server, provided the server and client prerequisites have been satisfied.

Adapting a single-path export for trunking allows you to maintain exported data sets in their existing volumes and SVMs. To do so, you must enable trunking on the NFS server, update networking and export configuration, and remount the exported share on the clients.

Enabling trunking has the effect of restarting the server. VMware clients must then remount the exported datastores; Linux clients must remount exported volumes with the `max_connect` option.

Enable trunking on the NFS server

Trunking must be explicitly enabled on NFS servers. NFSv4.1 is enabled by default when NFS servers are created.

After enabling trunking, verify that the following services are configured as needed.

- [DNS](#)
- [LDAP](#)
- [Kerberos](#)

Steps

1. Enable trunking and ensure that NFSv4.1 is enabled:

```
vserver nfs create -vserver svm_name -v4.1 enabled -v4.1-trunking enabled
```

2. Verify that NFS is running: `vserver nfs status -vserver svm_name`
3. Verify that NFS is configured as desired:

```
vserver nfs show -vserver svm_name
```

Learn more about [NFS server configuration](#). .. If you are serving to Windows clients from this SVM, move the shares then delete the server. `vserver cifs show -vserver svm_name`

```
+ vserver cifs delete -vserver svm_name
```

Update your network for trunking

NFSv4.1 trunking requires the LIFs in a trunking group to reside on the same node and have home ports on the same node. All LIFs should be configured in a failover group on the same node.

About this task

A one-to-one mapping of LIFs and NICs yields the greatest performance gain, but is not required to enable trunking.

You can have multiple failover groups, but the failover group for trunking must include only those LIFS in the trunking group.

You should adjust the trunking failover group any time you add or remove connections (and underlying NICs) from a failover group.

Before you begin

- You must know the port names associated with the NICs to create a failover group.
- The ports must all be on the same node.

Steps

1. Verify the names and status of the network ports you plan to use:

```
network port show
```

2. Create a trunking failover group or modify an existing one for trunking:

```
network interface failover-groups create -vserver svm_name -failover-group  
failover_group_name -targets ports_list
```

```
network interface failover-groups modify -vserver svm_name -failover-group  
failover_group_name -targets ports_list
```



It is not a requirement to have a failover group, but it is strongly recommended.

- *svm_name* is the name of the SVM containing the NFS server.
- *ports_list* is the list of ports that will be added to the failover group.

Ports are added in the format *node_name:port_number*, for example, *node1:e0c*.

The following command creates failover group *fg3* for SVM *vs1* and adds three ports:

```
network interface failover-groups create -vserver vs1 -failover-group fg3  
-targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
```

Learn more about [failover groups](#).

3. Create additional LIFs for members of the trunking group as needed:

```
network interface create -vserver svm_name -lif lif_name -home-node node_name  
-home-port port_name -address IP_address -netmask IP_address [-service-policy  
policy] [-auto-revert {true|false}]
```

- *-home-node* - the node to which the LIF returns when the network interface *revert* command is run on the LIF.

You can specify whether the LIF should automatically revert to the home-node and home-port with the *-auto-revert* option.

- `-home-port` is the physical or logical port to which the LIF returns when the network interface revert command is run on the LIF.
- You can specify an IP address with the `-address` and `-netmask` options.
- When you assign IP addresses manually (without using a subnet), you might need to configure a default route to a gateway if there are clients or domain controllers on a different IP subnet. The network route create man page contains information about creating a static route within an SVM.
- `-service-policy` - the service policy for the LIF. If no policy is specified, a default policy will be assigned automatically. Use the `network interface service-policy show` command to review available service policies.
- `-auto-revert` - specify whether a data LIF is automatically reverted to its home node under circumstances such as startup, changes to the status of the management database, or when the network connection is made. **The default setting is false**, but you can set it to true depending on network management policies in your environment.

Repeat this step for each additional LIF needed in the trunking group.

The following command creates lif-A for the SVM vs1, on port e0c of the node cluster1_01:

```
network interface create -vserver vs1 -lif lif-A -service-policy default-
intercluster -home-node cluster1_01 -home-port e0c -address 192.0.2.0
```

Learn more about [LIF creation](#).

4. Verify that the LIFs were created:

```
network interface show
```

5. Verify that the configured IP address is reachable:

To verify an...	Use...
IPv4 address	<code>network ping</code>
IPv6 address	<code>network ping6</code>

Modify data export for client access

To enable clients to take advantage of trunking for existing data shares, you might have to modify export policies and rules, and the volumes to which they are attached. There are different export requirements for Linux clients and VMware datastores.

Client export requirements:

- Linux clients must have a separate mount and a separate mount point for each trunking connection (that is, for each LIF).

If you are upgrading to ONTAP 9.14.1 and you have already exported a volume, you can continue to use that volume in a trunking group.

- VMware clients require only a single mount point for an exported volume, with multiple LIFs specified.

VMware clients require root access in the export policy.

Steps

1. Verify that an existing export policy is in place:

```
vserver export-policy show
```

2. Verify that the existing export policy rules are appropriate for the trunking configuration:

```
vserver export-policy rule show -policyname policy_name
```

In particular, verify that the `-clientmatch` parameter correctly identifies the trunking-capable Linux or VMware clients that will mount the export.

If adjustments are necessary, modify the rule using the `vserver export-policy rule modify` command or create a new rule:

```
vserver export-policy rule create -vserver svm_name -policyname policy_name
-ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,..." }
-rorule security_type -rwrule security_type -superuser security_type -anon
user_ID
```

Learn more about [creating export rules](#).

3. Verify that existing exported volumes are online:

```
volume show -vserver svm_name
```

Reestablish client mounts

To convert non-trunked client connections to trunked connections, existing mounts on Linux and VMware clients must be unmounted and remounted using information about LIFs.

When entering mount commands on the clients, you must enter IP addresses for each LIF in the trunking group.

Learn about [supported clients](#).



Unmounting VMware clients is disruptive for any VMs on the datastore. An alternative would be to create a new datastore enabled for trunking, and use **storage vmotion** to move your VMs from the old datastore to the new one. See your VMware documentation for details.

Linux client requirements

A separate mount point is required for each connection in the trunking group.

Mount the exported volumes with commands similar to the following:

```
mount lif1_ip:/vol-test /mnt/test1 -o vers=4.1,max_connect=2
```

```
mount lif2_ip:/vol-test /mnt/test2 -o vers=4.1,max_connect=2
```

The `vers` value should be 4.1 or later.

The `max_connect` value should correspond to the number of connections in the trunking group.

VMware client requirements

A mount statement is required that includes an IP address for each connection in the trunking group.

Mount the exported datastore with a command similar to the following:

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

The `-H` values should correspond to the connections in the trunking group.

Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

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