Configure a new NFS server and exports for trunking

ONTAP 9

NetApp
June 04, 2024

This PDF was generated from https://docs.netapp.com/us-en/ontap/nfs-trunking/create-server-task.html on June 04, 2024. Always check docs.netapp.com for the latest.

Table of Contents

Configure a new NFS server and exports for trunking . . . 1
- Create a trunking-enabled NFS server . . . 1
- Prepare your network for trunking . . . 2
- Export data for client access . . . 3
- Create client mounts . . . 4

Configure a new NFS server and exports for trunking

Create a trunking-enabled NFS server

Beginning with ONTAP 9.14.1, trunking can be enabled on NFS servers. NFSv4.1 is enabled by default when NFS servers are created.

Before you begin

The SVM must be:

- backed by sufficient storage for client data requirements.
- enabled for NFS.
- dedicated to NFS trunking. No other clients should be configured on it.

Steps

1. If a suitable SVM does not exist, create one:

   ```
   vserver create -vserver svm_name -rootvolume root_volume_name -aggregate
   aggregate_name -rootvolume-security-style unix -language C.UTF-8
   ```

2. Verify the configuration and status of the newly created SVM:

   ```
   vserver show -vserver svm_name
   ```

   Learn more about creating an SVM.

3. Create the NFS server:

   ```
   vserver nfs create -vserver svm_name -v3 disabled -v4.0 disabled -v4.1 enabled
   -v4.1-trunking enabled -v4-id-domain my_domain.com
   ```

4. Verify that NFS is running:

   ```
   vserver nfs status -vserver svm_name
   ```

5. Verify that NFS is configured as desired:

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

   Learn more about NFS server configuration.

After you finish

Configure the following services as needed:

- DNS
- LDAP
- Kerberos

Prepare your network for trunking

To take advantage of NFSv4.1 trunking, the LIFs in a trunking group must reside on the same node and have home ports on the same node. The 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. Having at least two NICs installed can offer a performance benefit, but it is not required.

You can have multiple failover groups, but the failover group for trunking should 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 should know the port names associated with the NICs if you want 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 status
   ```

2. Create the failover group:

   ```
   network interface failover-groups create -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. If needed, create LIFs for members of the trunking group:

   ```
   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 also 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, not with the `-subnet` option.
- When you assign IP addresses, you may 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 every LIF 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 ??? -home
-node cluster1_01 -home-port e0c -address 192.0.2.0
```

Learn more about LIF creation.

4. Verify the LIFs were created:

```
network interface show
```

5. Verify the configured IP address is reachable:

To verify an…	Use…
IPv4 address	`network ping`
IPv6 address	`network ping6`

Export data for client access

To provide client access to data shares, you must create one or more volumes, and the volume must have export policies with at least one rule.

Client export requirements:

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

- 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. Create an export policy:

   ```
   vserver export-policy create -vserver svm_name -policyname policy_name
   ```

   The policy name can be up to 256 characters long.

2. Verify that the export policy was created:

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

   Example

   The following commands create and verify the creation of an export policy named exp1 on the SVM named vs1:

   ```
   vs1::> vserver export-policy create -vserver vs1 -policyname exp1
   ```

3. Create an export rule and add it to an existing export policy:

   ```
   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
   ```

   The `-clientmatch` parameter should identify the trunking-capable Linux or VMware clients that will mount the export.

   Learn more about creating export rules.

4. Create the volume with a junction point:

   ```
   volume create -vserver svm_name -volume volume_name -aggregate aggregate_name
   -size {integer[KB|MB|GB|TB|PB]} -security-style unix -user user_name_or_number
   -group group_name_or_number -junction-path junction_path -policy
   export_policy_name
   ```

   Learn about creating volumes.

5. Verify that the volume was created with the desired junction point:

   ```
   volume show -vserver svm_name -volume volume_name -junction-path
   ```

Create client mounts

Linux and VMware clients that support trunking can mount volumes or data shares from an ONTAP NFSv4.1 server that is enabled for trunking.

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

group.

Learn about supported clients.

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=16

mount lif2_ip:/vol-test /mnt/test2 -o vers=4.1,max_connect=16
```

The version (`vers`) value should be `4.1` or later.

The `max_connect` value corresponds 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 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.