



Verify the node3 installation

ONTAP Systems

Barb Einarsen, Amanda Stroman, Paula Carrigan
May 10, 2021

Table of Contents

Verify the node3 installation	1
Restore network configuration on node3	2

Verify the node3 installation

You must verify that the physical ports from node1 map correctly to the physical ports on node3. This will allow node3 to communicate with other nodes in the cluster and with the network after the upgrade.

About this task

Capture information about the ports on the new nodes from the [Hardware Universe](#). You will use the information later in this section.

Physical port layout might vary, depending on the model of the nodes. When the new node boots up, ONTAP will try to determine which ports should host cluster LIFs in order to automatically come into quorum.

If the physical ports on node1 do not map directly to the physical ports on node3, the subsequent section [Restore network configuration on node3](#) must be used to repair the network connectivity.

After you install and boot node3, you must verify that it is installed correctly. You must wait for node3 to join quorum and then resume the relocation operation.

At this point in the procedure, the operation will have paused as node3 joins quorum.

Steps

1. Verify that node3 has joined quorum by using the following command:

```
cluster show -node node3 -fields health
```

The output of the `health` field should be `true`.

2. Verify that node3 is part of the same cluster as node2 and that it is healthy by using the following command:

```
cluster show
```

3. Switch to advanced privilege mode by using the following command:

```
set advanced
```

4. Check the status of the controller replacement operation and verify that it is in a paused state and in the same state that it was in before node1 was halted to perform the physical tasks of installing new controllers and moving cables by using the following commands:

```
system controller replace show
```

```
system controller replace show-details
```

5. If you are working on a MetroCluster system, verify that the replaced controller is configured correctly for the MetroCluster configuration; the MetroCluster configuration should be in a healthy state. See [Verify the health of the MetroCluster configuration](#).

Reconfigure the intercluster LIFs on MetroCluster node node3, and check cluster peering to restore communication between the MetroCluster nodes before proceeding to Step 6.

Check the MetroCluster node status by using the following command:

```
metrocluster node show
```

6. Resume the controller replacement operation by using the following command.

```
system controller replace resume
```

7. Controller replacement will pause for intervention with the following message:

```
Cluster::*> system controller replace show
Node           Status           Error-Action
-----
Node1(now node3) Paused-for-intervention Follow the instructions
given in
Step Details
Node2           None
Step Details:
-----
To complete the Network Reachability task, the ONTAP network
configuration must be manually adjusted to match the new physical
network configuration of the hardware. This includes:

1. Re-create the interface group, if needed, before restoring VLANs. For
detailed commands and instructions, refer to the "Re-creating VLANs,
ifgrps, and broadcast domains" section of the upgrade controller
hardware guide for the ONTAP version running on the new controllers.
2. Run the command "cluster controller-replacement network displaced-
vls show" to check if any VLAN is displaced.
3. If any VLAN is displaced, run the command "cluster controller-
replacement network displaced-vls restore" to restore the VLAN on the
desired port.

2 entries were displayed.
```



In this guide, the section *Re-creating VLANs, ifgrps, and broadcast domains* has been renamed *Restore network configuration on node3*.

8. With the controller replacement in a paused state, proceed to the next section of this document to restore network configuration on the node.

Restore network configuration on node3

After you confirm that node3 is in quorum and can communicate with node2, verify that node1's VLANs, interface groups, and broadcast domains are seen on node3. Also, verify that all node3 network ports are configured in their correct broadcast domains.

About this task

For more information on creating and re-creating VLANs, interface groups, and broadcast domains, see the [ONTAP 9 Network Management Guide](#).

Steps

1. List all the physical ports that are on upgraded node1 (referred to as node3) by using the following command:

```
network port show -node node3
```

All physical network ports, VLAN ports and interface group ports on the node are displayed. From this output, you can see any physical ports that have been moved into the **Cluster** broadcast domain by ONTAP. You can use this output to aid in deciding which ports should be used as interface group member ports, VLAN base ports or standalone physical ports for hosting LIFs.

2. List the broadcast domains on the cluster by using the following command:

```
broadcast-domain show
```

3. List network port reachability of all ports on node3 by using the following command:

```
network port reachability show
```

You should see output like the following example:

```
clusterA::*> reachability show -node node1_node3
(network port reachability show)
Node          Port          Expected Reachability  Reachability Status

node1_node3
    a0a        Default:Default    no-reachability
    a0a-822     Default:822        no-reachability
    a0a-823     Default:823        no-reachability
    e0M         Default:Mgmt         ok
    e0a         Cluster:Cluster   misconfigured-

reachability
    e0b         Cluster:Cluster   no-reachability
    e0c         Cluster:Cluster   no-reachability
    e0d         Cluster:Cluster   no-reachability
    e0e         Cluster:Cluster   ok
    e0e-822     -                    no-reachability
    e0e-823     -                    no-reachability
    e0f         Default:Default    no-reachability
    e0f-822     Default:822        no-reachability
    e0f-823     Default:823        no-reachability
    e0g         Default:Default    misconfigured-

reachability
    e0h         Default:Default    ok
    e0h-822     Default:822        ok
    e0h-823     Default:823        ok

18 entries were displayed.
```

In the above example, node1_node3 is just booted after controller replacement. Some ports do not have reachability to their expected broadcast domains and must be repaired.

4. Repair the reachability for each of the ports on node3 with a reachability status other than **ok**. Run the following command, first on any physical ports, then on any VLAN ports, one at a time:

```
network port reachability repair -node <node_name> -port <port_name>
```

You should see output like the following sample:

```
Cluster ::> reachability repair -node node1_node3 -port e0h
```

```
Warning: Repairing port "node1_node3: e0h" may cause it to move into a
different broadcast domain, which can cause LIFs to be re-homed away
from the port. Are you sure you want to continue? {y|n}:
```

A warning message, as shown above, is expected for ports with a reachability status that might be different

from the reachability status of the broadcast domain where it is currently located. Review the connectivity of the port and answer **y** or **n** as appropriate.

Verify that all physical ports have their expected reachability by using the following command:

```
network port reachability show
```

As the reachability repair is performed, ONTAP attempts to place the ports in the correct broadcast domains. However, if a port's reachability cannot be determined and does not belong to any of the existing broadcast domains, ONTAP will create new broadcast domains for these ports.

5. If interface group configuration does not match the new controller physical port layout, modify it by using the following steps.
 - a. You must first remove physical ports that should be interface group member ports from their broadcast domain membership. You can do this by using the following command:

```
network port broadcast-domain remove-ports -broadcast-domain <broadcast-domain_name> -ports <node_name:port_name>
```

- b. Add a member port to an interface group by using the following command:

```
network port ifgrp add-port -node <node_name> - ifgrp <ifgrp> -port <port_name>
```

- c. The interface group is automatically added to the broadcast domain about a minute after the first member port is added.
 - d. Verify that the interface group was added to the appropriate broadcast domain by using the following command:

```
network port reachability show -node <node_name> -port <ifgrp>
```

If the interface group's reachability status is not **ok**, assign it to the appropriate broadcast domain by using the following command:

```
network port broadcast-domain add-ports -broadcast-domain <broadcast_domain_name> -ports <node:port>
```

6. Assign appropriate physical ports to the **Cluster** broadcast domain by using the following steps:
 - a. Determine which ports have reachability to the **Cluster** broadcast domain by using the following command:

```
network port reachability show -reachable-broadcast-domains Cluster:Cluster
```

- b. Repair any port with reachability to the **Cluster** broadcast domain, if its reachability status is not **ok** by using the following command:

```
network port reachability repair -node <node_name> -port <port_name>
```

7. Move the remaining physical ports into their correct broadcast domains by using one of the following commands:

```
network port reachability repair -node <node_name> -port <port_name>
```

```
network port broadcast-domain remove-port
```

```
network port broadcast-domain add-port
```

Verify that there are no unreachable or unexpected ports present. Check the reachability status for all physical ports by using the following command and examining the output to ensure the status is **ok**:

```
network port reachability show -detail
```

8. Restore any VLANs that might have become displaced by using the following steps:

a. List displaced VLANs by using the following command:

```
displaced- vlans show
```

Output like the following should display:

```
Cluster::*> displaced-vlans show
(cluster controller-replacement network displaced-vlans show)
      Original
Node      Base Port   VLANs
Node1     a0a         822, 823
          e0e         822, 823
2 entries were displayed.
```

b. Restore VLANs that were displaced from their previous base ports by using the following command:

```
displaced- vlans restore
```

The following is an example of restoring VLANs that have been displaced from interface group a0a back onto the same interface group:

```
Cluster::*> displaced-vlans restore -node node1_node3 -port a0a
-destination-port a0a
```

The following is an example of restoring displaced VLANs on port e0e to e0h:

```
Cluster::*> displaced-vlans restore -node node1_node3 -port e0e
-destination-port e0h
```

When a VLAN restore is successful, the displaced VLANs are created on the specified destination port. The VLAN restore fails if the destination port is a member of an interface group, or if the destination port is down.

Wait about one minute for newly restored VLANs to be placed into their appropriate broadcast domains.

c. Create new VLAN ports as needed for VLAN ports that are not in the `displaced- vlans show` output but should be configured on other physical ports.

9. Delete any empty broadcast domains after all port repairs have been completed by using the following command:

```
broadcast-domain delete -broadcast-domain <broadcast_domain_name>
```

10. Verify port reachability by using the following command:

```
network port reachability show
```

When all ports are correctly configured and added to the correct broadcast domains, the `network port reachability show` command should report the reachability status as `ok` for all connected ports, and the status as `no-reachability` for ports with no physical connectivity. If any port reports a status other than these two, perform the reachability repair and add or remove ports from their broadcast domains as instructed in [Step 4](#).

11. Verify that all ports have been placed into broadcast domains by using the following command:

```
network port show
```

12. Verify that all ports in the broadcast domains have the correct maximum transmission unit (MTU) configured by using the following command:

```
network port broadcast-domain show
```

13. Restore LIF home ports, specifying the Vserver(s) and LIF(s) home ports, if any, that need to be restored by using the following steps:

- a. List any LIFs that are displaced by using the following command:

```
displaced-interface show
```

- b. Restore LIF home nodes and home ports by using the following command:

```
displaced-interface    restore-home-node    -node    <node_name>    -vserver  
<vserver_name> - lif-name <LIF_name>
```

14. Verify that all LIFs have a home port and are administratively up by using the following command:

```
network interface show -fields home- port,status-admin
```

Copyright Information

Copyright © 2021 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

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.