



Special configurations

ONTAP 9

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/us-en/ontap/upgrade/concept_special_configurations_post_checks.html on April 24, 2024. Always check docs.netapp.com for the latest.

Table of Contents

- Special configurations 1
 - Special considerations after an ONTAP upgrade..... 1
 - Verify your networking configuration after an ONTAP upgrade from ONTAP 9.7x or earlier 1
 - Remove EMS LIF service from network service policies 3
 - Verify networking and storage status for MetroCluster configurations after an ONTAP upgrade 5
 - Verify the SAN configuration after an upgrade..... 8
 - Reconfigure KMIP server connections after an upgrade from ONTAP 9.2 or earlier..... 9
 - Relocate moved load-sharing mirror source volumes after an ONTAP upgrade 10
 - Change in user accounts that can access the Service Processor 10

Special configurations

Special considerations after an ONTAP upgrade

If your cluster is configured with any of the following features you might need to perform additional steps after you upgrade your ONTAP software.

Ask yourself...	If your answer is yes, then do this...
Did I upgrade from ONTAP 9.7 or earlier to ONTAP 9.8 or later?	Verify your network configuration Remove the EMS LIF service from network service policies that do not provide reachability to the EMS destination
Is my cluster in a MetroCluster configuration?	Verify your networking and storage status
Do I have a SAN configuration?	Verify your SAN configuration
Did I upgrade from ONTAP 9.3 or earlier, and am using NetApp Storage Encryption?	Reconfigure KMIP server connections
Do I have load-sharing mirrors?	Relocate moved load-sharing mirror source volumes
Do I have user accounts for Service Processor (SP) access that were created prior to ONTAP 9.9.1?	Verify the change in accounts that can access the Service Processor

Verify your networking configuration after an ONTAP upgrade from ONTAP 9.7x or earlier

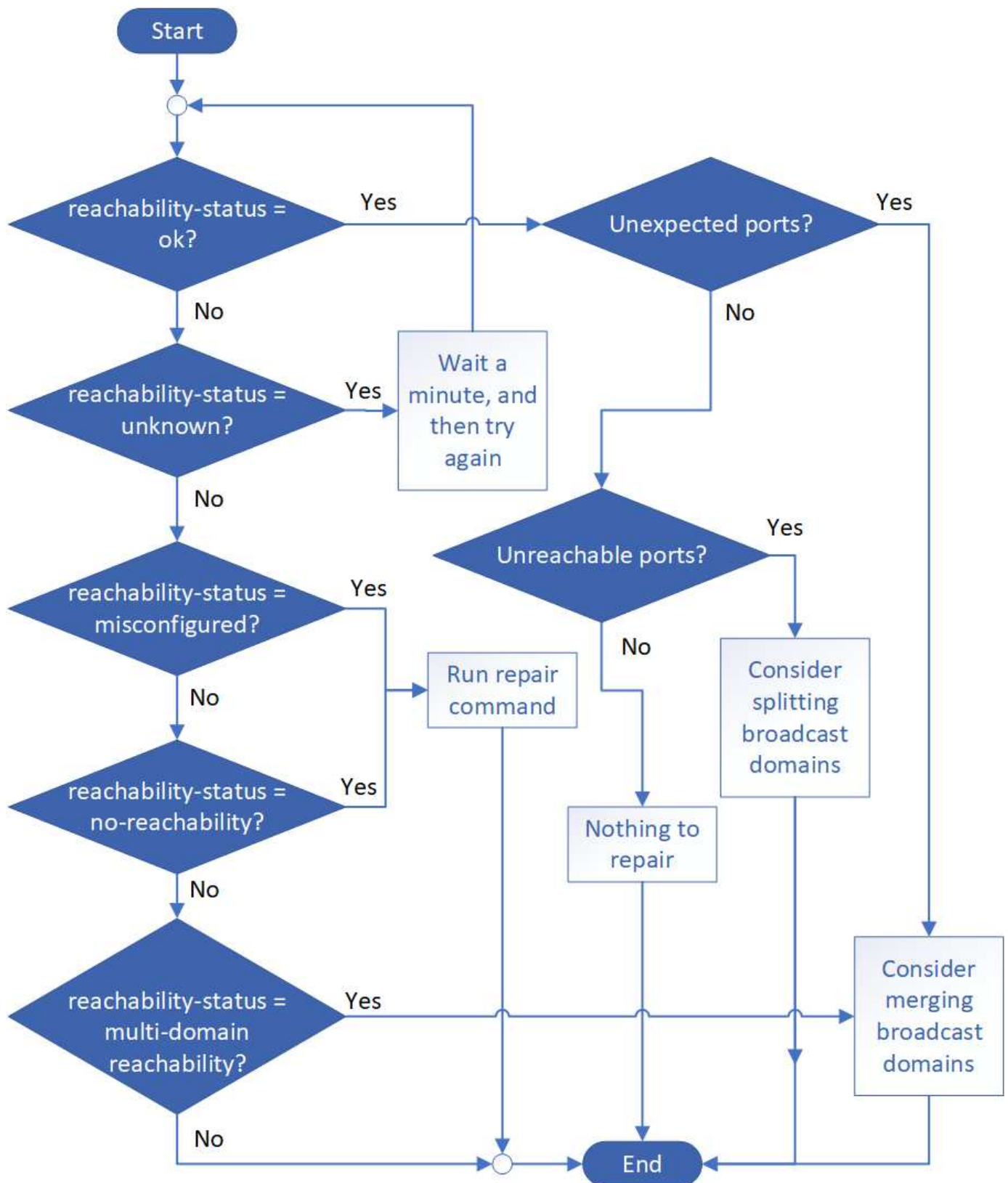
After you upgrade from ONTAP 9.7x or earlier to ONTAP 9.8 or later, you should verify your network configuration. After the upgrade, ONTAP automatically monitors layer 2 reachability.

Step

1. Verify each port has reachability to its expected broadcast domain:

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

The command output contains reachability results. Use the following decision tree and table to understand the reachability results (reachability-status) and determine what, if anything, to do next.



reachability-status	Description
---------------------	-------------

ok	<p>The port has layer 2 reachability to its assigned broadcast domain.</p> <p>If the reachability-status is "ok", but there are "unexpected ports", consider merging one or more broadcast domains. For more information, see Merge broadcast domains.</p> <p>If the reachability-status is "ok", but there are "unreachable ports", consider splitting one or more broadcast domains. For more information, see Split broadcast domains.</p> <p>If the reachability-status is "ok", and there are no unexpected or unreachable ports, your configuration is correct.</p>
misconfigured-reachability	<p>The port does not have layer 2 reachability to its assigned broadcast domain; however, the port does have layer 2 reachability to a different broadcast domain.</p> <p>You can repair the port reachability. When you run the following command, the system will assign the port to the broadcast domain to which it has reachability:</p> <pre>network port reachability repair -node -port</pre> <p>For more information, see Repair port reachability.</p>
no-reachability	<p>The port does not have layer 2 reachability to any existing broadcast domain.</p> <p>You can repair the port reachability. When you run the following command, the system will assign the port to a new automatically created broadcast domain in the Default IPspace:</p> <pre>network port reachability repair -node -port</pre> <p>For more information, see Repair port reachability.</p>
multi-domain-reachability	<p>The port has layer 2 reachability to its assigned broadcast domain; however, it also has layer 2 reachability to at least one other broadcast domain.</p> <p>Examine the physical connectivity and switch configuration to determine if it is incorrect or if the port's assigned broadcast domain needs to be merged with one or more broadcast domains.</p> <p>For more information, see Merge broadcast domains or Repair port reachability.</p>
unknown	<p>If the reachability-status is "unknown", then wait a few minutes and try the command again.</p>

After you repair a port, you need to check for and resolve displaced LIFs and VLANs. If the port was part of an interface group, you also need to understand what happened to that interface group. For more information, see [Repair port reachability](#).

Remove EMS LIF service from network service policies

If you have Event Management System (EMS) messages set up before you upgrade from ONTAP 9.7 or earlier to ONTAP 9.8 or later , after the upgrade, your EMS messages

might not be delivered.

During the upgrade, management-ems, which is the EMS LIF service, is added to all existing service policies. This allows EMS messages to be sent from any of the LIFs associated with any of the service policies. If the selected LIF does not have reachability to the event notification destination, the message is not delivered.

To prevent this, after the upgrade, you should remove the EMS LIF service from the network service policies that do not provide reachability to the destination.

Steps

1. Identify the LIFs and associated network service policies through which EMS messages can be sent:

```
network interface show -fields service-policy -services management-ems
```

vserver	lif	service-policy
cluster-1	cluster_mgmt	
		default-management
cluster-1	node1-mgmt	
		default-management
cluster-1	node2-mgmt	
		default-management
cluster-1	inter_cluster	
		default-intercluster

4 entries were displayed.

2. Check each LIF for connectivity to the EMS destination:

```
network ping -lif lif_name -vserver svm_name -destination  
destination_address
```

Perform this on each node.

Examples

```
cluster-1::> network ping -lif node1-mgmt -vserver cluster-1  
-destination 10.10.10.10  
10.10.10.10 is alive  
  
cluster-1::> network ping -lif inter_cluster -vserver cluster-1  
-destination 10.10.10.10  
no answer from 10.10.10.10
```

3. Enter advanced privilege level:

```
set advanced
```

4. For the LIFs that do not have reachability, remove the management-ems LIF service from the corresponding service policies:

```
network interface service-policy remove-service -vserver svm_name  
-policy service_policy_name -service management-ems
```

5. Verify that the management-ems LIF is now only associated with the LIFs that provide reachability to the EMS destination:

```
network interface show -fields service-policy -services management-ems
```

Related Links

[LIFs and service policies in ONTAP 9.6 and later](#)

Verify networking and storage status for MetroCluster configurations after an ONTAP upgrade

After you upgrade an ONTAP cluster in a MetroCluster configuration, you should verify the status of the LIFs, aggregates, and volumes for each cluster.

1. Verify the LIF status:

```
network interface show
```

In normal operation, LIFs for source SVMs must have an admin status of up and be located on their home nodes. LIFs for destination SVMs are not required to be up or located on their home nodes. In switchover, all LIFs have an admin status of up, but they do not need to be located on their home nodes.

```

cluster1::> network interface show

```

Current Is	Logical	Status	Network	Current	
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	
Cluster					
	cluster1-a1_clus1	up/up	192.0.2.1/24	cluster1-01	e2a
true					
	cluster1-a1_clus2	up/up	192.0.2.2/24	cluster1-01	e2b
true					
cluster1-01					
	clus_mgmt	up/up	198.51.100.1/24	cluster1-01	e3a
true					
	cluster1-a1_inet4_intercluster1	up/up	198.51.100.2/24	cluster1-01	e3c
true					
	...				

27 entries were displayed.

2. Verify the state of the aggregates:

```
storage aggregate show -state !online
```

This command displays any aggregates that are *not* online. In normal operation, all aggregates located at the local site must be online. However, if the MetroCluster configuration is in switchover, root aggregates at the disaster recovery site are permitted to be offline.

This example shows a cluster in normal operation:

```

cluster1::> storage aggregate show -state !online
There are no entries matching your query.

```

This example shows a cluster in switchover, in which the root aggregates at the disaster recovery site are

offline:

```
cluster1::> storage aggregate show -state !online
Aggregate      Size Available Used% State   #Vols  Nodes      RAID
Status
-----
-----
aggr0_b1
      0B      0B    0% offline    0 cluster2-01
raid_dp,
mirror
degraded
aggr0_b2
      0B      0B    0% offline    0 cluster2-02
raid_dp,
mirror
degraded
2 entries were displayed.
```

3. Verify the state of the volumes:

```
volume show -state !online
```

This command displays any volumes that are *not* online.

If the MetroCluster configuration is in normal operation (it is not in switchover state), the output should show all volumes owned by the cluster's secondary SVMs (those with the SVM name appended with "-mc").

Those volumes come online only in the event of a switchover.

This example shows a cluster in normal operation, in which the volumes at the disaster recovery site are not online.

```
cluster1::> volume show -state !online
(volume show)
Vserver   Volume      Aggregate    State    Type    Size
Available Used%
-----
vs2-mc    vol1        aggr1_b1     -        RW      -
-         -
vs2-mc    root_vs2    aggr0_b1     -        RW      -
-         -
vs2-mc    vol2        aggr1_b1     -        RW      -
-         -
vs2-mc    vol3        aggr1_b1     -        RW      -
-         -
vs2-mc    vol4        aggr1_b1     -        RW      -
-         -
5 entries were displayed.
```

4. Verify that there are no inconsistent volumes:

```
volume show -is-inconsistent true
```

See the Knowledge Base article [Volume Showing WAFL Inconsistent](#) on how to address the inconsistent volumes.

Verify the SAN configuration after an upgrade

After an ONTAP upgrade, in a SAN environment, you should verify that each initiator that was connected to a LIF before the upgrade has successfully reconnected to the LIF.

1. Verify that each initiator is connected to the correct LIF.

You should compare the list of initiators to the list you made during the upgrade preparation.

For...	Enter...
iSCSI	<pre>iscsi initiator show -fields igroup,initiator-name,tpgroup</pre>
FC	<pre>fcp initiator show -fields igroup,wwpn,lif</pre>

Reconfigure KMIP server connections after an upgrade from ONTAP 9.2 or earlier

After you upgrade from ONTAP 9.2 or earlier to ONTAP 9.3 or later, you need to reconfigure any external key management (KMIP) server connections.

Steps

1. Configure the key manager connectivity:

```
security key-manager setup
```

2. Add your KMIP servers:

```
security key-manager add -address key_management_server_ip_address
```

3. Verify that KMIP servers are connected:

```
security key-manager show -status
```

4. Query the key servers:

```
security key-manager query
```

5. Create a new authentication key and passphrase:

```
security key-manager create-key -prompt-for-key true
```

The passphrase must have a minimum of 32 characters.

6. Query the new authentication key:

```
security key-manager query
```

7. Assign the new authentication key to your self-encrypting disks (SEDs):

```
storage encryption disk modify -disk disk_ID -data-key-id key_ID
```



Make sure you are using the new authentication key from your query.

8. If needed, assign a FIPS key to the SEDs:

```
storage encryption disk modify -disk disk_id -fips-key-id  
fips_authentication_key_id
```

If your security setup requires you to use different keys for data authentication and FIPS 140-2 authentication, you should create a separate key for each. If that is not the case, you can use the same authentication key for FIPS compliance that you use for data access.

Relocate moved load-sharing mirror source volumes after an ONTAP upgrade

After you upgrade ONTAP, you need to move load-sharing mirror source volumes back to their pre-upgrade locations.

Steps

1. Identify the location to which you are moving the load-sharing mirror source volume by using the record you created before moving the load-sharing mirror source volume.
2. Move the load-sharing mirror source volume back to its original location:

```
volume move start
```

Change in user accounts that can access the Service Processor

If you created user accounts in ONTAP 9.8 or earlier that can access the Service Processor (SP) with a non-admin role and you upgrade to ONTAP 9.9.1 or later, any non-admin value in the `-role` parameter is modified to `admin`.

For more information, see [Accounts that can access the SP](#).

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.