Reconfiguring an FC switch layout configured before ONTAP 9.x

ONTAP MetroCluster

Ivana Devine, Martin Houser
April 21, 2021

This PDF was generated from https://docs.netapp.com/us-en/ontap-metrocluster/maintain/task_do_not_use_for_9_8_and_later_reconfigure_the_fc_switch_layout_for_ontap_9_1_or_later.html on September 24, 2021. Always check docs.netapp.com for the latest.

Table of Contents

Reconfiguring an FC switch layout configured before ONTAP 9.x . . . 1
- Sending a custom AutoSupport message prior to reconfiguring switches . . . 1
- Verifying the health of the MetroCluster configuration . . . 1
- Checking for MetroCluster configuration errors . . . 2
- Persistently disabling the switches . . . 3
- Determining the new cabling layout . . . 3
- Applying RCF files and recabling the switches . . . 4
- Persistently enable the switches . . . 4
- Verifying switchover, healing, and switchback . . . 5

Reconfiguring an FC switch layout configured before ONTAP 9.x

If your existing FC switch layout was configured prior to ONTAP 9.1, you must reconfigure the port layout and apply the latest Reference Configuration Files (RCFs). This procedure applies only to MetroCluster FC configurations.

You must identify the FC switches present in the fabric domain.

You need the admin password and access to an FTP or SCP server.

You must perform this task if your existing FC switch layout was configured prior to ONTAP 9.1. It is *not* required if you are upgrading from an existing switch layout that was configured for ONTAP 9.1 or later.

This procedure is nondisruptive and takes approximately four hours to complete (excluding rack and stack) when disks are zeroed.

Sending a custom AutoSupport message prior to reconfiguring switches

Before reconfiguring your switches, you should issue an AutoSupport message to notify NetApp technical support that maintenance is underway. Informing technical support that maintenance is underway prevents them from opening a case on the assumption that a disruption has occurred.

This task must be performed on each MetroCluster site.

Steps

1. Log in to the cluster.
2. Invoke an AutoSupport message indicating the start of the maintenance:

   `system node autosupport invoke -node * -type all -message MAINT=`*`maintenance-window-in-hours`*

   maintenance-window-in-hours specifies the length of the maintenance window, with a maximum of 72 hours. If the maintenance is completed before the time has elapsed, you can invoke an AutoSupport message indicating the end of the maintenance period:

   `system node autosupport invoke -node * -type all -message MAINT=end`

3. Repeat these steps on the partner site.

Verifying the health of the MetroCluster configuration

You should check the health of the MetroCluster configuration to verify proper operation.

Steps

1. Verify that the MetroCluster components are healthy:

metrocluster check run

```
cluster_A::*> metrocluster check run
```

The operation runs in the background.

2. After the `metrocluster check run` operation completes, run `metrocluster check show` to view the results.

   After approximately five minutes, the following results are displayed:

```
-----------
cluster_A::*> metrocluster check show

Last Checked On: 4/7/2019 21:15:05

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          warning
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

3. To check the status of the running MetroCluster check operation, use the command:

   metrocluster operation history show -job-id 38

4. Verify that there are no health alerts:

   system health alert show

Checking for MetroCluster configuration errors

You can use the Config Advisor tool available from the NetApp Support Site to check for common configuration errors.

Config Advisor is a configuration validation and health check tool. You can deploy it at both secure sites and non-secure sites for data collection and system analysis.

Support for Config Advisor is limited, and available only online.

1. Download the Config Advisor tool.

NetApp Downloads: Config Advisor

2. Run Config Advisor, reviewing the output and following its recommendations to address any issues.

Persistently disabling the switches

You must disable the switches in the fabric persistently so that you can modify its configuration.

You disable the switches by running the commands on the switch command line; the commands used for this are not ONTAP commands.

Steps

1. Persistently disable the switch:
   - For Brocade switches, use the `switchCfgPersistentDisable` command.
   - For Cisco switches, use the `suspend` command. The following command disables a Brocade switch persistently:

     ```
     FC_switch_A_1:admin> switchCfgPersistentDisable
     ```

     The following command disables a Cisco switch:

     ```
     vsan [vsna #] suspend
     ```

Determining the new cabling layout

You must determine the cabling for the new controller modules and any new disk shelves to the existing FC switches.

This task must be performed at each MetroCluster site.

Steps

1. Use the *Fabric-attached MetroCluster Installation and Configuration Guide* to determine the cabling layout for your switch type, using the port usage for an eight-node MetroCluster configuration.

   The FC switch port usage must match the usage described in the guide so that the Reference Configuration Files (RCFs) can be used.

   Fabric-attached MetroCluster installation and configuration

   > If your environment cannot be cabled in a way that RCFs can be used, then contact technical support. Do not use this procedure if the cabling cannot use RCFs.

Applying RCF files and recabling the switches

You must apply the appropriate reference configuration (RCF) files to reconfigure your switches to accommodate the new nodes. After you apply the RCF files, you can recable the switches.

The FC switch port usage must match the usage described in the *Fabric-attached MetroCluster Installation and Configuration Guide* so that the RCFs can be used.

Fabric-attached MetroCluster installation and configuration

Steps

1. Locate the RCF files for your configuration.

   You must use the RCF files that match your switch model.

2. Apply the RCF files, following the directions on the Download page and adjusting the ISL settings as needed.
3. Verify that the switch configuration is saved.
4. Cable both of the FC-to-SAS bridges to the FC switches, using the cabling layout you created in the “Determining the new cabling layout” section.
5. Verify that the ports are online:
   - For Brocade switches, use the `switchshow` command.
   - For Cisco switches, use the `show interface brief` command.
6. Cable the FC-VI ports from the controllers to the switches.
7. From the existing nodes, verify that the FC-VI ports are online:

   `metrocluster interconnect adapter show`

   `metrocluster interconnect mirror show`

Persistently enable the switches

You must enable the switches in the fabric persistently.

Steps

1. Persistently enable the switch:
   - For Brocade switches, use the `switchCfgPersistentenable` command.
   - For Cisco switches, use the no `suspend` command. The following command persistently enables a Brocade switch:

     ```
     FC_switch_A_1:admin> switchCfgPersistentenable
     ```

     The following command enables a Cisco switch:

```
vsan [vsna #]no suspend
```

Verifying switchover, healing, and switchback

You should verify the switchover, healing, and switchback operations of the MetroCluster configuration.

1. Use the procedures for negotiated switchover, healing, and switchback that are mentioned in the *MetroCluster Management and Disaster Recovery Guide*.

   MetroCluster management and disaster recovery

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.