# Upgrading or downgrading the firmware on a Brocade FC switch

## ONTAP MetroCluster

Ivana Devine
April 12, 2021

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

# Table of Contents

Upgrading or downgrading the firmware on a Brocade FC switch . . . . . 1

# Upgrading or downgrading the firmware on a Brocade FC switch

To upgrade or downgrade the firmware on a Brocade FC switch, you must use the Brocade-specific commands to disable the switch, perform and verify the firmware change, and reboot and reenable the switch.

- You must have the firmware files.
- The system must be properly cabled.
- All paths to the storage shelves must be available.
- The disk shelf stacks must be stable.
- The FC switch fabric must be healthy.
- No failed components can be present in the system.
- The system must be operating normally.
- You must have the admin password and access to an FTP or SCP server.

The switch fabric is disabled during a firmware upgrade or downgrade, and the MetroCluster configuration relies on the second fabric to continue operation.

This task must be performed on each of the switch fabrics in succession so that all switches are running the same firmware version.

This procedure is nondisruptive and takes approximately one hour to complete.

**Steps**

1. Log in to each of the switches in the fabric.

   The examples in the following steps use the switch `FC_switch_A_1`.

2. Disable each of the switches in the fabric:

   **`switchCfgPersistentDisable`**

   If this command is not available, then run the `switchDisable` command.

   ```
   FC_switch_A_1:admin> switchCfgPersistentDisable
   ```

3. Download the desired firmware version:

   **`firmwareDownload`**

   When prompted for the file name, you must specify the subdirectory or relative path to the firmware file.

   You can run the `firmwareDownload` command at the same time on both switches, but you must allow the firmware to download and commit properly before moving to the next step.

```
FC_switch_A_1:admin> firmwaredownload
Server Name or IP Address: 10.64.203.188
User Name: test
File Name: v7.3.1b
Network Protocol(1-auto-select, 2-FTP, 3-SCP, 4-SFTP) [1]: 2
Password:
Server IP: 10.64.203.188, Protocol IPv4
Checking system settings for firmwaredownload...
System settings check passed.
```

4. Verify that the firmware was downloaded and committed to both partitions:

   **`firmwareShow`**

   The following example shows that the firmware download is complete as both images are updated:

```
FC_switch_A_1:admin> firmwareShow
Appl     Primary/Secondary Versions

------------------------------------------

FOS      v7.3.1b

         v7.3.1b
```

5. Reboot the switches:

   **`reboot`**

   Some firmware versions automatically perform an haReboot operation after the firmware download is finished. The reboot in this step is required even if the haReboot has been performed.

```
FC_switch_A_1:admin> reboot
```

6. Check whether the new firmware is for an intermediate firmware level or for a final specified release.

   If the download is for the intermediate firmware level, then perform the previous two steps until the specified release is installed.

7. Enable the switches:

   **`switchCfgPersistentEnable`**

   If this command is not available, then the switch should be in the `enabled` state after the `reboot` command is executed.

```
FC_switch_A_1:admin> switchCfgPersistentEnable
```

8. Verify that the switches are online and that all of the devices are properly logged in:

   **switchShow**

```
FC_switch_A_1:admin> switchShow
```

9. Verify that the buffer usage information for a port group or all of the port groups in the switch is displayed properly:

   **portbuffershow**

```
FC_switch_A_1:admin> portbuffershow
```

10. Verify that the current configuration of a port is displayed properly:

    **portcfgshow**

```
FC_switch_A_1:admin> portcfgshow
```

    Verify the port settings, such as speed, mode, trunking, encryption, and compression, in the Inter-Switch Link (ISL) output. Verify that the port settings were not affected by the firmware download.

11. Verify the operation of the MetroCluster configuration in ONTAP:

    a. Check whether the system is multipathed:
    **node run -node *node-name* sysconfig -a**

    b. Check for any health alerts on both clusters:
    **system health alert show**

    c. Confirm the MetroCluster configuration and that the operational mode is normal:
    **metrocluster show**

    d. Perform a MetroCluster check:
    **metrocluster check run**

    e. Display the results of the MetroCluster check:
    **metrocluster check show**

    f. Check for any health alerts on the switches (if present):
    **storage switch show**

    g. Run Config Advisor.

    NetApp Downloads: Config Advisor

    h. After running Config Advisor, review the tool's output and follow the recommendations in the output to address any issues discovered.

12. Wait 15 minutes before repeating this procedure for the second switch fabric.

## 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.