23.4 BrickStor SP Cluster Upgrade Guide

Terms of Use and Copyright and Trademark Notices

The copyright in the Documentation is owned by RackTop Systems and is protected by copyright and other intellectual property laws of the United States and other countries. Without limiting the rights of this copyright, no part of the Documentation may be modified, used in a compilation or otherwise incorporated into another work, or with or into any other documentation or user manuals, or be used to create derivative works, without the express prior written permission of RackTop Systems. RackTop Systems reserves the right to change the terms at any time, and your continued use of the Documentation shall be deemed an acceptance of those terms. RackTop Systems, the RackTop Systems logo, BrickStor, CyberConverged, and certain other trademarks and logos are trademarks or registered trademarks of RackTop Systems, Inc. in the United States and other countries. Other company, product and service names may be trademarks or service marks of others.

© 2023 RackTop Systems, Inc. All rights reserved.

Disclaimers

The Documentation and any information available from it may include inaccuracies or typographical errors. RackTop Systems may change the documentation from time to time. RackTop Systems makes no representations or warranties about the accuracy or suitability of any RackTop Systems-controlled website, the Documentation and/or any product information. RackTop Systems-controlled websites, the Documentation and all product information are provided "as is" and RackTop Systems disclaims any and all express and implied warranties, including but not limited to warranties of title and the implied warranties of merchantability and/or fitness for a particular purpose. In no event shall RackTop Systems be liable to you for any direct, indirect, incidental, special, exemplary, punitive, or consequential damages (including but not limited to procurement of substitute goods or services, loss of data, loss of profits, and/or business interruptions), arising out of or in any way related to RackTop Systems-controlled websites or the documentation, no matter how caused and/or whether based on contract, strict liability, negligence or other tortuous activity, or any other theory of liability, even if RackTop Systems is advised of the possibility of such damages. Because some states/jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitations may not apply to you.

Important Notice:

This Document is being provided as a RackTop Systems, Inc. provides this document "as is" without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. RackTop Systems, Inc. does not assume responsibility for the use of or inability to use the product as a result of providing this information.

Copyright ©2023 RackTop Systems, Inc. All Rights Reserved. BrickStor is a registered trademark of RackTop Systems, Inc. Intel and Seagate are trademarks of their respective companies.

Date Prepared: January 2023

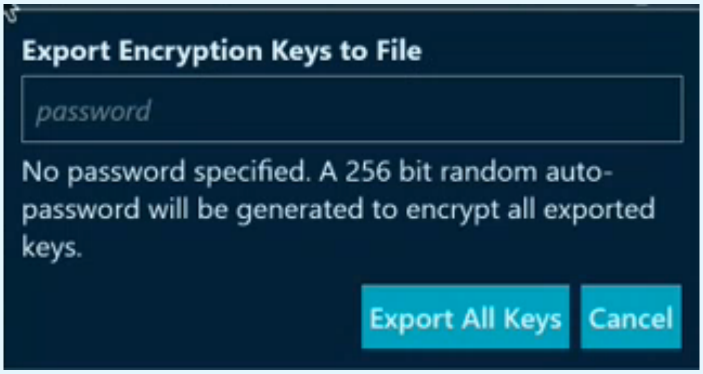
Updating the BrickStor SP Operating System

BrickStor SP Upgrade Prerequisite

When upgrading BrickStor SP it is always recommended to ensure that any encryption keys are exported and backed up. Follow these steps if using encrypted datasets or have encrypted storage pools.

- Navigate to the **Encryption** Tab.
- Click the **Resync Encryption Keys with Peers Button**.
- Click the **Export All Encryption Keys** button.
    - A prompt denoting the entrance of a password will present. Once entered, click the **Export All Keys** button.

NOTE: We recommend that a password be provided, rather than the automatically generated password.



Export Encryption Keys to File

No password specified. A 256 bit random auto-password will be generated to encrypt all exported keys.

-
    - A Windows File Explorer window will present a default file name. The file name will default to:

      NODENAME_YEAR_MONTH_DAY-#OFKEYS_keys

    - Click the **Save** button.

- A prompt denoting successful key export will present showing the Encrypted Key File, as well as the Key Report File.

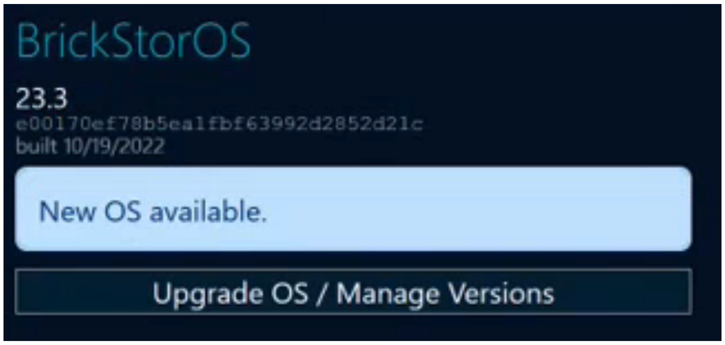
BrickStor SP OS Upgrade Procedure

The following steps will outline the process by which the BrickStor SP Manager and OS is updated (for the purposes of this example, the example cluster consists of a Node A, Node B, and a Witness. Node A is considered the Passive Node, and Node B is considered the Active Node. If the system is running two Active Nodes, consider Node A to be the Active Node carrying the lower serving load):

NOTE: If at any point the upgrade process is inhibited, contact the support team.

Upgrade Node A

1. To begin the upgrade process of the BrickStor SP Manager, first navigate to the **System** tab of Node A.
    a. In the **Systems** tab, click the **Upgrade OS/ Manage Upgrade Versions** button. This will take you to the OS Upgrade screen (shown below).



BrickStorOS

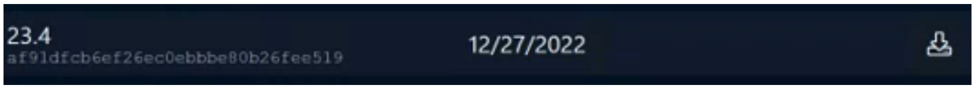
23.3

e00170ef78b5ea1fbf63992d2852d21c

built 10/19/2022

New OS available.

    b. In the OS Upgrade Screen, navigate to the new version (in this case, 23.4).
    c. Click the **Download** icon to the right of the release version of the desired upgrade (shown below).

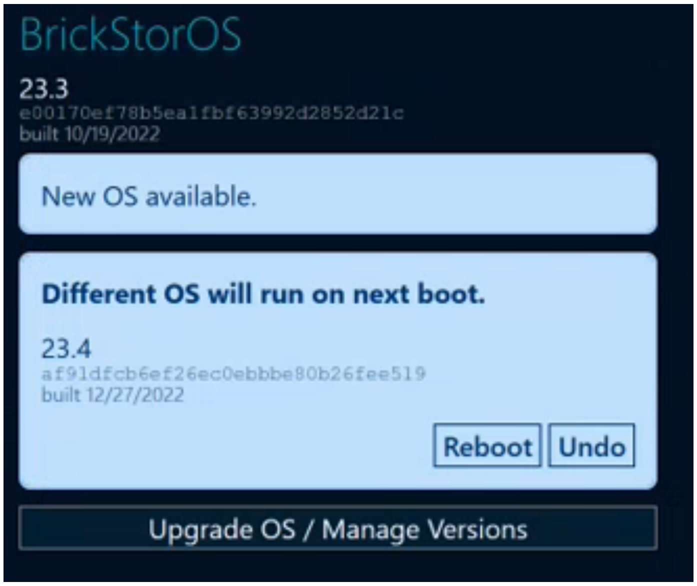


23.4

af91dfcb6ef26ec0ebbbe80b26fee519

12/27/2022

    d. A prompt displaying the downloading of the release version will present, as well as a progress bar.
    e. Once download is complete, click **Activate**.
    f. Navigate to the **System** tab.
        a. A message stating that a **Different OS will run on next boot** will present (shown below).
        b. Click **Reboot**.



BrickStorOS

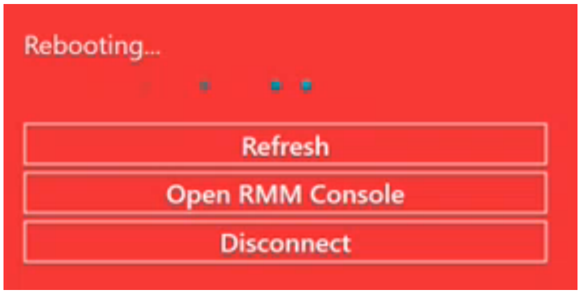
23.3
e00170ef78b5ea1fbf63992d2852d21c
built 10/19/2022

New OS available.

Different OS will run on next boot.

23.4
af91dfcb6ef26ec0ebbbe80b26fee519
built 12/27/2022

   c. A window will present on the right-side of the screen showing the active changes to the system. This will display the changes that will occur to the system when rebooting.
   d. Click the **checkbox** to acknowledge the warning.
      i. Click **Commit (1) Change(s).**
   e. A prompt will ask if you want to migrate resources and disable node



Rebooting...

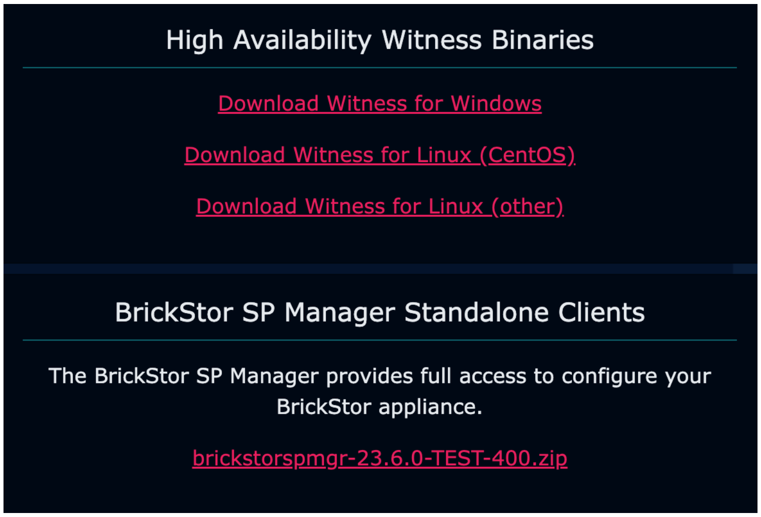
      i. Click **Yes**.
   f. Once the node has rebooted, ensure that it is **enabled**.

NOTE: Node A must be manually re-enabled **before** upgrading Node B by clicking the **play button** next to Node A on the HA tab in the BrickStor SP Manager.

      i. Verify this via navigating to node B.
      ii. Click the **HA** tab.
      iii. Ensure that HA is enabled.
      iv. Exit the running instance of the BrickStor SP Manager Client.

Upgrade Node B

2. **Repeat steps a - e** on Node B to upgrade the second node.
3. Navigate to the BrickStor SP web interface.
   a. Entering the IP of the BrickStor SP Node A into an internet browser search bar.
   b. Log in to the website with the admin Username and Password of Node A.
   c. Download and install the standalone BrickStor SP Manager client.
   d. From the Witness system, download the **High Availability Witness Binaries** (this will be used in the Witness Upgrade Procedure and Confd Upgrade Procedure).



High Availability Witness Binaries

Download Witness for Windows

Download Witness for Linux (CentOS)

Download Witness for Linux (other)

BrickStor SP Manager Standalone Clients

The BrickStor SP Manager provides full access to configure your BrickStor appliance.

brickstorspmgr-23.6.0-TEST-400.zip

4. Launch the standalone BrickStor SP Manager client (downloaded in step 3c).
    a. The BrickStor SP Manager will automatically load the credentials of the system.
    b. Select **Node A**, verify that the cluster is running (the homepage will display that the HA system requires an upgrade).

Witness Upgrade Procedure (Windows)

The following steps will outline the process to upgrade the Witness:

1. Log in as administrator.
2. Navigate to Windows Services and locate **RackTop High Availability Service**.
    a. Right-click on RackTop High Availability Service and click **Stop** to stop the service from running.
3. Navigate to the location of the downloaded .zip file in the Windows File Explorer.
4. Extract the .zip file using default system processes.
5. Once located, **right-click on hiavd.exe** and click **Copy**.
6. Navigate to the location of the outdated hiavd.exe on the system.
    a. This will be in either c:\racktop or C:\Program Files\Racktop\BrickStor\
7. Locate hiavd.exe and **right-click** it.
8. Click **Paste**.
9. Confirm the replacement of the file.
10. Navigate to Windows Services.
    a. Refresh the list of services.
    b. Locate **RackTop High Availability Service.**
    c. **Right-click** RackTop High Availability Service.
    d. Click **Run**.
11. On the BrickStor SP Manager, click the **refresh** button on the top right of the screen to ensure the Witness has been upgraded (The HA tab will display green LEDs, and the warning message denoting a version mismatch will disappear within 30 seconds).

Confd Upgrade Procedure (Windows)

The following steps will outline the process to upgrade confd:

1. Navigate to the location of the downloaded confd.exe file in the Windows File Explorer (the same directory as the hiavd.exe file).
2. Once located, **right-click on confd.exe** and click **Run As Administrator**.
3. A command prompt window will present.
    a. Enter **1** to install. Press **Return**.
    b. Enter **0** for instance number. Press **Return**.
    c. Enter **y** to confirm the installation. Press **Return**.
    d. Enter **y** to confirm the update. Press **Return**.
    e. Enter **y** as response to backup query. Press **Return**.
    f. Enter **y** to start the confd service after installation. Press **Return**.
    g. Press **Return** to exit and close the window.
4. Navigate to the Windows File Explorer and locate the new **confadm.exe**.
    a. **Right-click** the confadm.exe file.
    b. Click **Copy**.
5. Navigate to **C:\Program Files\RackTop\BrickStor\confd\00**.
    a. **Right-click** the existing confadm.exe.
    b. Click **Paste**.
6. Navigate to Windows Services.
    a. Refresh the list of services.
    b. Verify the new confd service is running.
7. Open a command prompt and cd to **C:\Program Files\RackTop\BrickStor\confd\00**.
8. Enter **confadm member show status** to confirm the cluster is healthy by assessing that all three nodes are online and communicating.