Support for transitioning SnapLock volumes

ONTAP 7-Mode Transition

NetApp
February 11, 2024

This PDF was generated from https://docs.netapp.com/us-en/ontap-7mode-transition/copy-based/concept_considerations_for_transitioning_of_snaplock_enterprise_volumes.html on February 11, 2024. Always check docs.netapp.com for the latest.

Table of Contents

Support for transitioning SnapLock volumes . . . 1
Considerations for transitioning of SnapLock Enterprise volumes . . . 1
Considerations for transitioning of SnapLock Compliance volumes . . . 1
Considerations for transitioning of SnapLock Audit volumes . . . 2
Considerations for transitioning of 7-Mode SnapLock options . . . 2
Considerations for using Chain of Custody verification for 7-Mode SnapLock volumes . . . 2

Support for transitioning SnapLock volumes

The 7-Mode Transition Tool supports the transition of SnapLock volumes to target clusters running any ONTAP 9.0 release except 9.6.

The SnapLock Enterprise and SnapLock Compliance volumes are supported for transition to target clusters that are running any ONTAP release except 9.6. However, SnapLock Compliance volume transition is not supported to the target clusters that are in MetroCluster configurations.

Considerations for transitioning of SnapLock Enterprise volumes

The 7-Mode Transition Tool supports the transition of stand-alone SnapLock Enterprise volumes and SnapLock Enterprise volumes that are in a SnapMirror relationship.

The workflow for transitioning SnapLock Enterprise volumes is the same as for FlexVol volumes.

SnapMirror relationships are preserved during the transition.

> The 7-Mode Transition Tool only supports like-to-like transition for SnapMirror relationships of SnapLock Enterprise volumes. That is, both the source and destination volumes must be SnapLock Enterprise volumes.

Considerations for transitioning of SnapLock Compliance volumes

The 7-Mode Transition Tool supports the transition of standalone SnapLock Compliance volumes and SnapLock Compliance volumes that are in a SnapMirror relationship.

The workflow for transitioning standalone SnapLock Compliance volumes is the same as for transitioning FlexVol volumes.

The transition of SnapMirror relationships for SnapLock Compliance volumes is not automated by the 7-Mode Transition Tool. You must transition the primary and secondary SnapLock Compliance volumes as stand-alone volumes, and then manually resynchronize the relationships.

You can include the SnapLock Compliance volumes (both stand-alone and the volumes that are in SnapMirror relationships) as a standalone volume in stand-alone, primary, and secondary projects.

The precutover read/write mode is not supported for projects with SnapLock Compliance volumes. It is a best practice to create separate projects for SnapLock Compliance volumes and non-SnapLock Compliance volumes because the precutover read/write mode is not supported if SnapLock Compliance volumes are included in the project.

During the cutover operation, if the selected volume is a SnapLock Compliance volume and it is the destination of a SnapMirror relationship, then the SnapMirror relationship between the 7-Mode volume and the ONTAP volume is deleted without SnapMirror break operation. This action enables the secondary ONTAP SnapLock Compliance volumes to remain in read-only mode. The secondary ONTAP SnapLock Compliance volumes must be in read-only mode for the resynchronization operation to be successful between the primary and secondary SnapLock Compliance volumes.

See How to transition the 7-Mode SnapLock Compliance volumes with SnapMirror relationship to clustered Data ONTAP

Considerations for transitioning of SnapLock Audit volumes

The 7-Mode Transition Tool supports the transition of SnapLock Audit volumes. The workflow to transition SnapLock Audit volumes is the same as the transition of SnapLock Compliance volumes.

After you transition audit volumes to the ONTAP, you must manually designate the transitioned audit volume as SnapLock Audit volume for the target SVM.

In ONTAP, the audit volumes are configured at an SVM level. In Data ONTAP operating in 7-Mode, an audit volume serves as a consolidated repository for all of the volumes in the controller across the vFiler units.

SnapLock Audit volumes are a type of SnapLock Compliance volume. The transition of SnapLock Audit volumes is not supported if the target cluster is in a MetroCluster configuration.

See How to configure audit volume in clustered Data ONTAP for the transitioned SnapLock volumes

Considerations for transitioning of 7-Mode SnapLock options

The 7-Mode Transition Tool supports the transition of a few 7-Mode options that are related to SnapLock volumes.

Data ONTAP operating in 7-Mode has the following options that are related to SnapLock volumes:

- `snaplock.autocommit_period`

  This option is at a volume level in ONTAP, and is transitioned to ONTAP during the transition.

- `snaplock.compliance.write_verify`

  This option is not applicable in ONTAP.

- `snaplock.log.default_retention`
- `snaplock.log.maximum_size`

Although the `snaplock.log.default_retention` and `snaplock.log.maximum_size` options are supported in ONTAP, the settings configured in these options are not transitioned by the 7-Mode Transition Tool. You must manually set these options for audit volumes after the transition is completed.

Considerations for using Chain of Custody verification for 7-Mode SnapLock volumes

You should be aware of the considerations for using Chain of Custody verification for 7-Mode SnapLock volumes.

- The SnapLock Chain of Custody verification must be performed only if it is a requirement for the transition of SnapLock volumes.

  You can perform the Chain of Custody verification for all or a subset of SnapLock volumes in the project.

- The SnapLock Chain of Custody verification can take a significant amount of time based on the number of files on the 7-Mode SnapLock volumes.
- The Chain of Custody verification is supported only for read/write 7-Mode SnapLock volumes

  The Chain of Custody verification is not supported for read-only volumes.

- The Chain of Custody verification is not supported for SnapLock volumes containing files that have names with non-ASCII characters.

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.