



Data and configuration migration process

ONTAP 7-Mode Transition

NetApp
May 31, 2021

This PDF was generated from https://docs.netapp.com/us-en/ontap-7mode-transition/copy-based/concept_how_you_transition_a_stand_alone_volume.html on May 31, 2021. Always check docs.netapp.com for the latest.

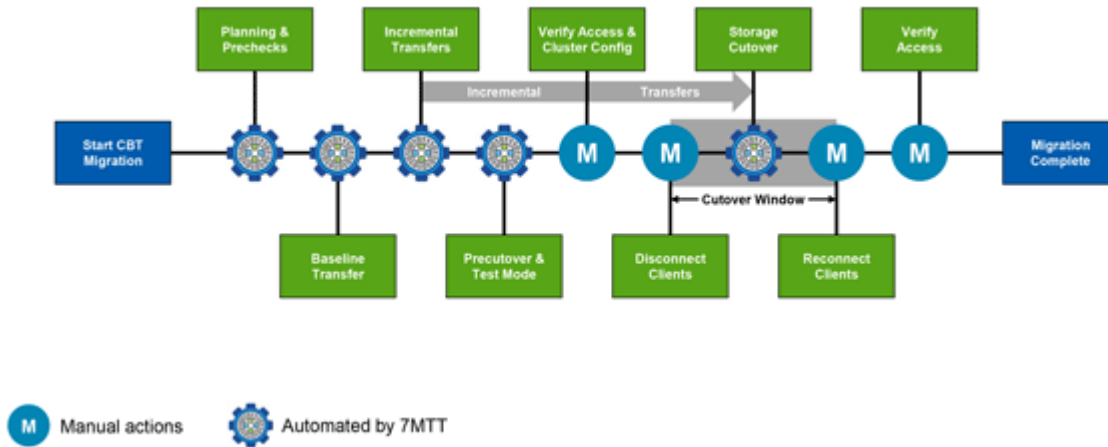
Table of Contents

- Data and configuration migration process 1
 - Preparation..... 1
 - Baseline data copy..... 1
 - Apply configuration (precutover) 2
 - Storage cutover 2
 - Chain of Custody verification for SnapLock volumes..... 2
 - How you transition a stand-alone volume 3
 - How you transition volumes in a SnapMirror relationship 8

Data and configuration migration process

The data and configuration migration process using the 7-Mode Transition Tool consists of the following phases: preparation, baseline data copy, apply configuration (precutover), and storage cutover. If you have SnapLock volumes for Chain of Custody verification, Chain of Custody verification is additional phase after the cutover.

The following image shows the different phases in the migration process:



Preparation

In this phase, prechecks are run to verify feature functionality. The process checks the 7-Mode storage systems to verify that the volumes and configuration are ready to be migrated to ONTAP. It checks that the cluster is configured properly and can support the transition. Any errors must be resolved before continuing with the transition. Although the tool allows you to continue without resolving warnings, you must understand the impact of the warnings before proceeding with the transition. You can run the prechecks multiple times to verify that all of the errors have been resolved.

Although the precheck step and assessment steps performed during the assessment appear to be similar, there are differences. The precheck step is a more detailed test that is focused on the specific storage systems that have been identified as the migration source (7-Mode) and destination (ONTAP) systems. The assessment step only evaluates the migration source systems, checking feature and functionality differences with ONTAP.

Baseline data copy

New volumes are created on the SVM, a SnapMirror relationship is established between the 7-Mode and ONTAP volumes, and a baseline transfer is performed. After the baseline is complete, incremental transfers are automatically run according to a user-defined data copy schedule. Clients and servers accessing the source storage remain online while this step is completed.

Copying data requires CPU, memory, and storage access, which results in additional resources being used on the source storage system. It is a best practice to schedule data copy activity to occur during off-peak times (preferably, CPU usage should be around 50%).

Apply configuration (precutover)

This phase includes SnapMirror incremental transfers; configuration information is applied to the ONTAP system, SVM, and volumes. Optionally, you can also test the ONTAP volumes that are being transitioned before storage cutover.

Although a majority of the configuration is applied, some actions are deferred to storage cutover: for example, applying quotas.

The 7-Mode IP addresses selected for the transition are created in the administrative down state. The new IP addresses selected for the transition are created in the administrative up state. These new IP addresses can be used to verify data access during precutover testing.

It is a best practice to run the apply configuration (precutover) phase a few days or weeks before the planned cutover window. This activity helps to verify that all of the configurations are applied properly and whether any changes are required.



Although incremental updates are not required, it is a best practice to perform an incremental transfer as close to the storage cutover as possible to minimize the time that clients are disconnected.

Storage cutover

At a high level during storage cutover, clients are disconnected, a final data transfer is performed, the SnapMirror relationship is broken, and clients are manually reconnected.

Disconnecting clients or servers from the source storage volume prevents additional writes from being performed while the final copy is being executed. Before disconnecting clients, it is a best practice to perform an incremental update to minimize the downtime.

Storage access must be disconnected only for the volumes that are being migrated. Access to storage can be discontinued from the storage side or the client side. The best practice is to discontinue connectivity from the storage side. For example, if a CIFS client is accessing a volume named “user01” on a 7-Mode storage system, you can use the `cifs terminate -v user01` command to disable access to all of the CIFS shares on the volume (discontinuing client access from the storage side). The IP addresses, mount points, or even share names might change as a result of the migration, and therefore client access might be discontinued from the client side as well. As long as clients cannot write any new data to the storage container that is being migrated, you can use either or both of these methods for discontinuing access.

After clients are disconnected, the 7-Mode Transition Tool executes a final copy so that both the source and destination datasets are at parity. The 7-Mode Transition Tool configures the data LIFs on the SVM. Some configuration changes that were not transitioned during precutover, such as applying SAN configurations and quotas, are also applied to the SVM at this time.

After storage cutover is complete, you can manually reconnect the clients and validate data access. Validating data access involves verifying that clients are accessing the ONTAP system properly and that all permissions are working as expected.

Chain of Custody verification for SnapLock volumes

You can trigger the Chain of Custody operation for the SnapLock volumes in the project after the transition is complete. This operation is not mandatory and is required only if Chain of Custody verification is essential for the transition of SnapLock volumes. You can perform this operation for all SnapLock volumes in the project or

for a subset of SnapLock volumes in the project. The Chain of Custody verification is supported for both compliance and enterprise SnapLock volumes. The Chain of Custody verification is supported only for read-write SnapLock volumes, and is not supported for read-only SnapLock volumes.



The Chain of Custody verification is not supported for SnapLock volume that have file names with non-ASCII characters.

The verification workflow is supported only in the 7-Mode Transition Tool GUI and is not supported in the CLI workflow.

The Chain of Custody verification operation performs the following:

- Enumerates all of the WORM files from 7-Mode volumes
- Calculates the fingerprint for each WORM file enumerated previously on both 7-Mode volumes and transitioned ONTAP volumes
- Generates a report with details about the number of files with matched and unmatched fingerprints, and the reason for the mismatch

Fingerprint data for all WORM files is stored in an ONTAP volume provided during the planning phase.



Based on the number of files on the 7-Mode volumes, the Chain of Custody verification process can take a significant amount of time (days or weeks).

How you transition a stand-alone volume

Transitioning a stand-alone volume includes different phases: preparation, data copy, apply configuration (precutover), and storage cutover. After completing transition, you must perform some post-transition steps before resuming client access. Understanding what occurs during each phase helps you manage your transition efficiently.

Phase	Steps
Preparation	<ol style="list-style-type: none">1. Gathering information2. Performing the precheck3. Creating data copy schedules
Data copy	<ol style="list-style-type: none">1. Creating the ONTAP volumes as read-only2. Creating a transition peer relationship3. Establishing a SnapMirror relationship4. Performing a baseline transfer5. Performing scheduled incremental updates

Phase	Steps
Precutover	<ol style="list-style-type: none"> 1. Breaking the SnapMirror relationship 2. Applying configurations to the SVM 3. Configuring data LIFs on the SVM 4. Testing data and configurations (manual and only for precutover RW) 5. Resynchronizing ONTAP volumes with corresponding 7-Mode volumes
Storage cutover	<ol style="list-style-type: none"> 1. Disconnecting client access (manual) 2. Performing a final SnapMirror update 3. Breaking the SnapMirror relationship 4. Removing 7-Mode IP addresses and setting the data LIFs to the up state on the SVM 5. Taking the source volume offline <p>After cutover, performing post-transition steps and enabling client access (manual)</p>
Chain of Custody verification for SnapLock volumes	<ol style="list-style-type: none"> 1. Enumerating all of the WORM files from 7-Mode volumes 2. Calculating the fingerprint for each WORM file on the 7-Mode volumes (enumerated in the previous step) and calculating the fingerprint for the corresponding WORM file on the transitioned ONTAP volumes 3. Generating a report with details about the number of files with matched and unmatched fingerprints, and the reason for the mismatch

Preparation phase

In this phase, information about the 7-Mode system and the cluster, volumes, and IP addresses is collected. The 7-Mode Transition Tool performs the following tasks in this phase:

1. Collects and adds 7-Mode storage system and volume information.
2. Runs the transition precheck.
3. Collects and adds cluster, SVM, and aggregate information.
4. Collects IP addresses that must be configured on the SVM:
 - Selects the IP addresses that exist on the 7-Mode system.
 - Specifies new IP addresses that must be configured on the SVM. NOTE: Transitioning of iSCSI and FC LIFs (SAN) is not supported by the tool. You must manually configure SAN LIFs on the SVM before transition.
5. Creates data copy schedules for baseline copy and incremental updates.

6. If the project contains SnapLock volumes, collects information about the read-write SnapLock volumes for which Chain of Custody verification is required and the details of the ONTAP volume that stores the fingerprint data that is generated during the Chain of Custody verification operation.



The Chain of Custody verification operation is supported only for volumes with file names that have only ASCII characters.

7. Plans configuration transition by selecting the 7-Mode configurations that must be transitioned to the target SVM and target volumes.

You should not modify the objects (volumes, IP addresses, system information, and so on) on the controller after fixing the errors and warnings that are reported during the precheck.

Data copy phase

In this phase, data from the 7-Mode volumes is copied to the ONTAP volumes. The 7-Mode Transition Tool performs the following tasks in this phase:

1. Creates the ONTAP volumes with read-only access.
2. Set up a transition peer relationship between the 7-Mode system and the SVM.
3. Establishes a transition SnapMirror relationship (relationship of type TDP) between the 7-Mode volumes and ONTAP volumes.
4. Completes the baseline data copy transfer based on schedule inputs.
5. Performs scheduled incremental updates to the ONTAP volumes.

Apply configuration (precutover) phase

It is a best practice to run precutover operation a few days or weeks before the planned cutover window. This activity is to verify whether all the configurations are applied properly and whether any changes are required.

In this phase, configurations from the 7-Mode volumes are copied to ONTAP volumes.

There are two modes for the apply configuration (precutover) phase: **precutover read-only** and **precutover read/write**.

The precutover read/write mode is not supported when the project contains:

- SAN volumes and the target cluster is running Data ONTAP 8.3.1 or earlier

In this situation, the following configurations are not applied in the apply configuration (precutover) phase. Instead, they are applied during the cutover phase.

- SAN configurations
- Snapshot Schedule configurations
- SnapLock Compliance volumes

If the project contains SnapLock Compliance volumes, then the Snapshot Schedule configurations are not applied in the apply configuration (precutover) phase. Instead, these configurations are applied during the cutover phase.

[Considerations for transitioning of SnapLock Compliance volumes](#)

If the target cluster is running Data ONTAP 8.3.1 or earlier, and you want to run the apply configuration (precutover) operation in read/write mode for NAS volumes, then you must create separate projects for the NAS volumes and SAN volumes. This action is required because the precutover read/write mode is not supported if you have SAN volumes in your project.

If the project contains SnapLock Compliance volumes, and you want to run the apply configuration (precutover) operation in read/write mode for non-SnapLock Compliance volumes, then you must create separate projects for SnapLock Compliance volumes and non-SnapLock Compliance volumes. This action is required because the precutover read/write mode is not supported if you have SnapLock Compliance volumes in your project.

The tool performs the following steps in the **precutover read-only mode**:

1. Performs an incremental update from 7-Mode volumes to ONTAP volumes.
2. Breaks the SnapMirror relationship between 7-Mode volumes and ONTAP volumes.



For SnapLock Compliance volumes, the SnapMirror relationship between the 7-Mode volume and ONTAP volumes is not broken. The SnapMirror relationship is not broken because the SnapMirror resynchronization operation between 7-Mode and ONTAP volumes is not supported for SnapLock Compliance volumes.

3. Collects configurations from 7-Mode volumes, and applies the configurations to the ONTAP volumes and the SVM.
4. Configures the data LIFs on the SVM:
 - Existing 7-Mode IP addresses are created on the SVM in the administrative down state.
 - New IP addresses are created on the SVM in the administrative up state.
5. Resynchronizes the SnapMirror relationship between 7-Mode volumes and ONTAP volumes

The tool performs the following steps in the **precutover read/write mode**:

1. Performs an incremental update from 7-Mode volumes to ONTAP volumes.
2. Breaks the SnapMirror relationship between 7-Mode volumes and ONTAP volumes.
3. Collects configurations from 7-Mode volumes, and applying the configurations to the ONTAP volumes and the SVM.
4. Configures the data LIFs on the SVM:
 - Existing 7-Mode IP addresses are created on the SVM in the administrative down state.
 - New IP addresses are created on the SVM in the administrative up state.
5. Makes the ONTAP volumes available for read/write access.

After you apply the configuration, the ONTAP volumes are available for read/write access so that read/write data access can be tested on these volumes during apply configuration (precutover) testing. You can manually verify the configurations and data access in ONTAP.

6. Resynchronizes the ONTAP volumes when "finish testing" operation is triggered manually.

Storage cutover phase

The 7-Mode Transition Tool performs the following tasks in this phase:

1. Optional: Performs an on-demand SnapMirror update to reduce the downtime after cutover.
2. Manual: Disconnect client access from the 7-Mode system.
3. Performs a final SnapMirror update from 7-Mode volumes to ONTAP volumes.
4. Breaks and deletes the SnapMirror relationship between the 7-Mode volumes to ONTAP volumes, making the ONTAP volumes read/write.

If the selected volume is a SnapLock Compliance volume and the volume is the destination of a SnapMirror relationship, then the SnapMirror relationship between the 7-Mode volume and the ONTAP volume is deleted without a SnapMirror break operation. This action is performed to ensure that secondary ONTAP SnapLock Compliance volumes 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.

5. Applies Snapshot schedules configuration if:
 - The target cluster is running clustered Data ONTAP 8.3.0 or 8.3.1 and project contains SAN volumes.
 - The project contains SnapLock compliance volumes.
6. Applies SAN configurations, if the target cluster is running Data ONTAP 8.3.1 or earlier.
7. Applies quota configurations, if any.
8. Removes the existing 7-Mode IP addresses selected for transition from the 7-Mode system and brings the data LIFs on the SVM to the administrative up state.



SAN LIFs are not transitioned by the 7-Mode Transition Tool.

9. Optional: Takes the 7-Mode volumes offline.

Chain of Custody verification process for SnapLock volumes

You must perform the Chain of Custody verification operation. The tool performs the following operations when a Chain of Custody verification is initiated:

1. Enumerates all of the WORM files from 7-Mode volumes.
2. Calculates the fingerprint for each WORM file on the 7-Mode volumes (enumerated in the previous step) and calculates the fingerprint for the corresponding WORM file on the transitioned ONTAP volumes.
3. Generates a report with details about the number of files with matched and unmatched fingerprints, and the reason for the mismatch.



- The Chain of Custody verification operation is supported only for read-write SnapLock volumes that have file names with only ASCII characters.
- This operation can take a significant amount of time based on the number of files on the 7-Mode SnapLock volumes.

Post-transition steps

After the storage cutover phase finishes successfully and the transition is completed, you must perform some post-transition manual tasks:

1. Perform the required steps to configure features that were not transitioned or were partially transitioned, as listed in the precheck report.

For example, IPv6 and FPolicy must be configured manually after transition.

2. For SAN transition, reconfigure the hosts.

[SAN host transition and remediation](#)

3. Ensure that the SVM is ready to serve data to the clients by verifying the following:
 - The volumes on the SVM are online and read/write.
 - The IP addresses are up and reachable on the SVM.
4. Redirect client access to the ONTAP volumes.

Related information

[Migrating data and configuration from 7-Mode volumes](#)

How you transition volumes in a SnapMirror relationship

If you want to transition 7-Mode volumes that are in a SnapMirror relationship, the secondary volumes must be transitioned first. Then, a volume SnapMirror relationship is established between the 7-Mode primary volumes and ONTAP secondary volumes.

After transitioning the primary volumes, the 7-Mode Transition Tool establishes a volume SnapMirror relationship between ONTAP primary and secondary volumes.



The 7-Mode Transition Tool does not automatically transition SnapLock Compliance volumes that are in a SnapMirror relationship. All SnapLock Compliance volumes that are in a SnapMirror relationship must be transitioned as stand-alone volumes. After the primary and secondary SnapLock Compliance volumes are transitioned to ONTAP, you must manually perform the SnapMirror resynchronization operation between these volumes.

You can perform precheck, baseline copy, incremental transfers, and apply configuration (precutover) on the secondary and primary projects simultaneously; however, the storage cutover for the secondary project must be performed first.

Preparation phase

In this phase, the 7-Mode system, cluster, volumes, and IP addresses are selected. The 7-Mode Transition Tool performs the following tasks in this phase:

1. Adds 7-Mode storage system and volume information
2. Gathers information about 7-Mode source volumes and SnapMirror relationships:
 - For transitioning a secondary volume, collecting information about the 7-Mode primary system
 - For transitioning a primary volume, collecting information about the 7-Mode secondary system
3. Runs the transition precheck
4. Adds cluster, SVM, and aggregate information
5. Collects IP addresses that must be configured on the SVM:
 - Selecting IP addresses that exist on the 7-Mode system

- Specifying new IP addresses that must be configured on the SVM



Transitioning iSCSI and FC LIFs (SAN) is not supported by the tool. You must manually configure the SAN LIFs on the SVM before transition.

6. Creates the data copy schedules for baseline and incremental transfers.
7. If the project contains SnapLock volumes, collects information about the read-write SnapLock volumes for which Chain of Custody verification is required and details about the ONTAP volume that stores the fingerprint data generated during the Chain of Custody verification operation.



The SnapLock Chain of Custody verification is supported only for read/write 7-Mode SnapLock volumes. It is not supported for read-only volumes. The SnapLock Chain of Custody verification is not supported for SnapLock volumes containing files that have names with non-ASCII characters.

8. Plans the configuration transition by selecting the 7-Mode configurations that must be transitioned to target SVM and target volumes.

You must not modify the objects (volumes, IP addresses, system information, and so on) on the controller after fixing errors and warnings that are reported by the precheck.

Data copy phase

In this phase, data from the 7-Mode volumes is copied to the ONTAP volumes. The 7-Mode Transition Tool performs the following tasks in this phase:

1. Creates the ONTAP volumes with read-only access
2. Set up a transition peer relationship between the 7-Mode system and the SVM
3. Establishes a SnapMirror relationship between the 7-Mode volumes and ONTAP volumes
4. Completes the baseline data transfer based on schedule inputs
5. Performs scheduled SnapMirror data copy updates to the ONTAP volumes

Apply configuration (precutover) phase

It is a best practice to run **Apply configuration** a few days or weeks before the planned cutover window. This precheck enables you to have enough time to verify that all of the configurations are applied properly and whether any changes are required.

In this phase, configurations from the 7-Mode volumes are copied to the ONTAP volumes.

There are two modes for the apply configuration (precutover) phase: precutover read-only and precutover read/write.

The precutover read/write mode is not supported when the project contains the following:

- SAN volumes and the target cluster is running Data ONTAP 8.3.1 or earlier

In this situation, the following configurations are not applied in the apply configuration (precutover) phase, instead they are applied during the cutover phase:

- SAN configurations

- Snapshot schedule configurations
- SnapLock Compliance volumes

If the project contains SnapLock Compliance volumes, then the Snapshot schedule configurations are not applied in the apply configuration (precutover) phase. Instead, these configurations are applied during the cutover phase.

Considerations for transitioning of SnapLock Compliance volumes.

If the target cluster is running Data ONTAP 8.3.1 or earlier and you want to run the apply configuration (precutover) operation in read/write mode for NAS volumes, then you must create separate projects for the NAS and SAN volumes. This action is required because the apply configuration (precutover) read/write mode is not supported if you have SAN volumes in your project.

If the project contains SnapLock Compliance volumes and you want to run the apply configuration (precutover) operation in read/write mode for non-SnapLock Compliance volumes, then you must create separate projects for SnapLock Compliance volumes and non-SnapLock Compliance volumes. This action is required because the apply configuration (precutover) read/write mode is not supported if you have SnapLock Compliance volumes in your project.

The following steps are performed by the tool in the **precutover read-only mode**:

1. Performs an incremental update from 7-Mode volumes to ONTAP volumes
2. Breaks the SnapMirror relationship between 7-Mode volumes and ONTAP volumes



For SnapLock Compliance volumes, the SnapMirror relationship between the 7-Mode volume and ONTAP volumes is not broken. This is because the SnapMirror resynchronization operation between 7-Mode and ONTAP volumes is not supported for SnapLock Compliance volumes.

3. Collects configurations from 7-Mode volumes and applying the configurations to the ONTAP volumes and SVM
4. Configures the data LIFs on the SVM:
 - Existing 7-Mode IP addresses are created on the SVM in the administrative down state.
 - New IP addresses are created on the SVM in the administrative up state.
5. Resynchronizes the SnapMirror relationship between 7-Mode volumes and ONTAP volumes

The following steps are performed in the **precutover read/write mode**:

1. Performs an incremental update from 7-Mode volumes to ONTAP volumes
2. Breaks the SnapMirror relationship between 7-Mode volumes and ONTAP volumes
3. Collects configurations from 7-Mode volumes and applying the configurations to the ONTAP volumes and SVM
4. Configures the data LIFs on the SVM:
 - Existing 7-Mode IP addresses are created on the SVM in the administrative down state.
 - New IP addresses are created on the SVM in the administrative up state.
5. Tests the read/write data access on the ONTAP volumes during apply configuration (precutover) testing

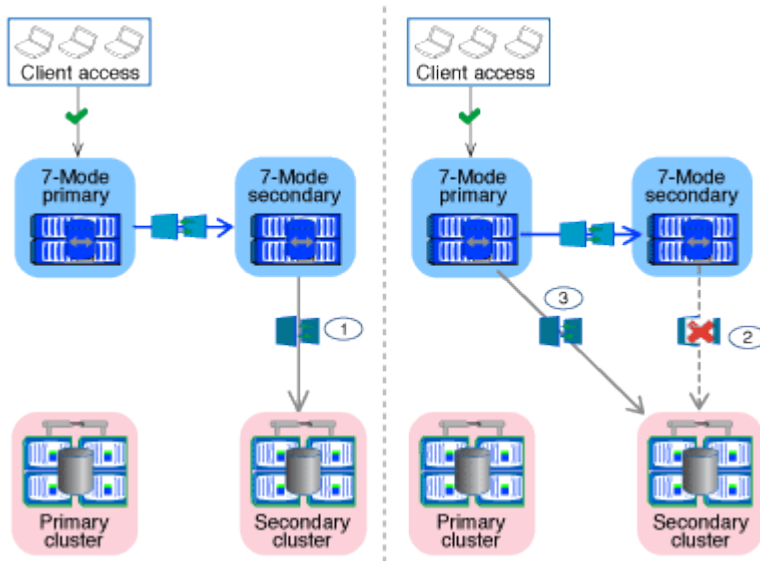
These ONTAP volumes will be available for read/write access after you apply the configuration. After you apply the configuration, the ONTAP volumes are available for read/write access so that read/write data access can be tested on these volumes during apply configuration (precutover) testing.

6. Manual: Verifying the configurations and data access in ONTAP
7. Manual: Finish testing

The ONTAP volumes are resynchronized.

Storage cutover (secondary volumes) phase

The following illustration depicts the transition of a secondary volume:



Phase	Steps
Storage cutover (secondary volumes)	<ol style="list-style-type: none"> 1. Transitioning the secondary volumes 2. Breaking and deleting SnapMirror relationship between the secondary volumes 3. Establishing a DR relationship between the 7-Mode primary and ONTAP secondary volumes

The 7-Mode Transition Tool performs the following tasks in this phase:

1. Optional: Performs an on-demand SnapMirror update on the ONTAP secondary volumes
2. Manual: Disconnecting client access, if required
3. Performs a final SnapMirror update from the 7-Mode secondary volume to the ONTAP secondary volume
4. Breaks and deletes the SnapMirror relationship between the 7-Mode secondary volume and the ONTAP secondary volume, and making the destination volumes read/write
5. Applies the Snapshot schedules configuration, if the target cluster is running Data ONTAP 8.3.0 or 8.3.1 and the project contains SAN volumes
6. Applies SAN configurations, if the target cluster is running Data ONTAP 8.3.1 or earlier



All of the required igroups are created during this operation. For the secondary volumes, mapping LUNs to igroups is not supported during the cutover operation. You must manually map the secondary LUNs after completing the storage cutover operation of the primary volumes. However, for stand-alone volumes included in the secondary project, LUNs are mapped to the igroups during this operation.

7. Applies quota configurations, if any
8. Establishes a SnapMirror relationship between the volumes on the 7-Mode primary system and the ONTAP secondary volumes

The SnapMirror schedule that is used to update the SnapMirror relationships between the 7-Mode primary volumes and 7-Mode secondary volumes is applied to the SnapMirror relationships between the 7-Mode primary volumes and ONTAP secondary volumes.

9. Removes the existing 7-Mode IP addresses selected for transition from the 7-Mode system and bringing the data LIFs on the SVM to the administrative up state

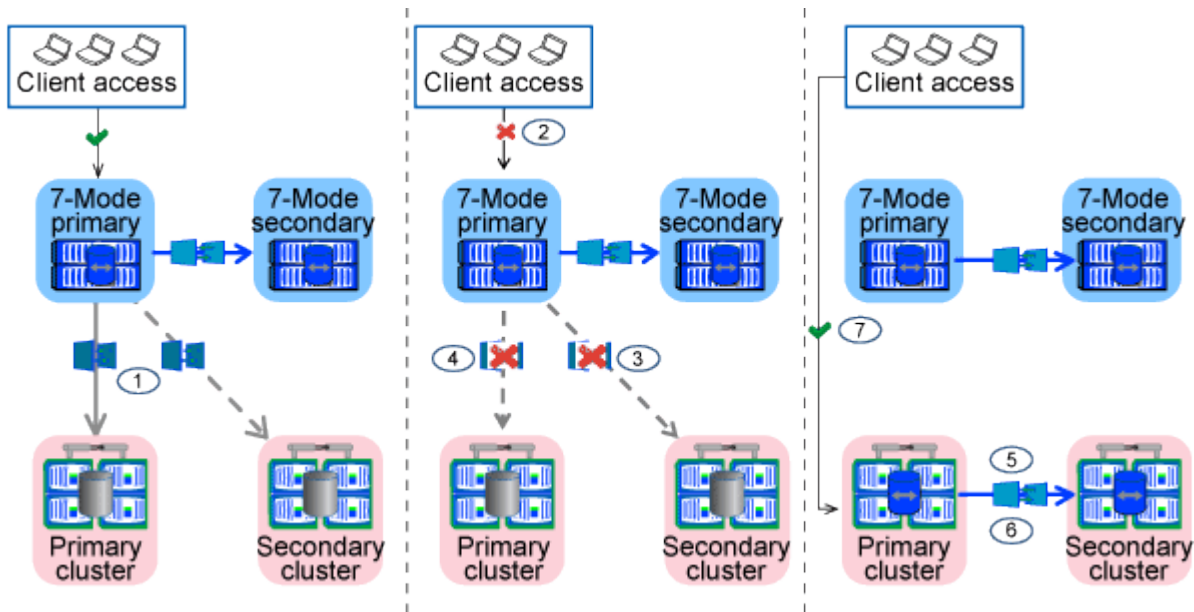


SAN LIFs are not transitioned by the 7-Mode Transition Tool.

10. Optional: Taking the 7-Mode volumes offline

Storage cutover (primary volumes) phase

The following illustration depicts the transition of a primary volume:



Phase	Steps
Storage cutover (primary volumes)	<ol style="list-style-type: none"> 1. Transitioning the primary volumes 2. Disconnecting clients from the 7-Mode system (storage cutover) 3. Breaking and deleting the DR relationship between the 7-Mode primary and ONTAP secondary volumes 4. Breaking and deleting SnapMirror relationship between the primary volumes 5. Setting up an SVM peer relationship between the ONTAP primary and secondary volumes 6. Resynchronizing the SnapMirror relationship between ONTAP volumes 7. Enabling client access to ONTAP volumes

The 7-Mode Transition Tool performs the following tasks in this phase:

1. Optional: Performs an on-demand SnapMirror update on the ONTAP secondary volumes
2. Manual: Disconnecting client access from the 7-Mode system
3. Performs a final incremental update from the 7-Mode primary volume and the ONTAP primary volume
4. Breaks and deletes the SnapMirror relationship between the 7-Mode primary volume and the ONTAP primary volume, and making the destination volumes read/write
5. Applies the Snapshot schedules configuration if the target cluster is running Data ONTAP 8.3.0 or 8.3.1 and the project contains SAN volumes
6. Applies SAN configurations, if the target cluster is running Data ONTAP 8.3.1 or earlier
7. Applies quota configurations, if any
8. Breaks and deletes the SnapMirror relationship between the 7-Mode primary volume and the ONTAP secondary volume
9. Setting up cluster peer and SVM peer relationships between the primary and secondary clusters
10. Setting up a SnapMirror relationship between the primary and secondary ONTAP volumes
11. Resynchronizes the SnapMirror relationship between the ONTAP volumes
12. Removes the existing 7-Mode IP addresses selected for transition from the 7-Mode system and bringing the data LIFs on the primary SVM to the administrative up state



SAN LIFs are not transitioned by the 7-Mode Transition Tool.

13. Optional: Taking the 7-Mode volumes offline

Chain of Custody verification process for SnapLock volumes

Perform the Chain of Custody verification operation.

1. Enumerates all of the WORM files from 7-Mode volumes

2. Calculates the fingerprint for each WORM file on the 7-Mode volumes (enumerated in the previous step) and calculates the fingerprint for the corresponding WORM file on the transitioned ONTAP volumes.
3. Generates a report with details about the number of files with matched and unmatched fingerprints, and the reason for the mismatch



- The Chain of Custody verification operation is supported only for read-write SnapLock volumes that have file names with only ASCII characters.
- This operation can take significant amount of time based on the number of files on the 7-Mode SnapLock volumes.

Post-transition steps

After the cutover phase is successfully and the transition is completed, you must perform the following post-transition tasks:

1. Perform any manual steps to transition features that were available on the 7-Mode system, but were not transitioned automatically to the SVM by the tool.
2. If the target cluster is running Data ONTAP 8.3.1 or earlier, you must map the secondary LUNs manually.
3. For SAN transitions, manually reconfigure the hosts.

[SAN host transition and remediation](#)

4. Ensure that the SVM is ready to serve data to the clients by verifying the following:
 - The volumes on the SVM are online and read/write.
 - The transitioned IP addresses are up and reachable on the SVM.
5. Redirect client access to the ONTAP volumes.

Related information

[Migrating data and configuration from 7-Mode volumes](#)

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.