



Perform ONTAP version specific pre-revert checks

ONTAP 9

NetApp
December 21, 2024

Table of Contents

- Perform ONTAP version specific pre-revert checks 1
 - Pre-revert tasks required for your ONTAP version..... 1
 - Any ONTAP 9 version 2
 - ONTAP 9.16.1 8
 - ONTAP 9.14.1 9
 - ONTAP 9.12.1 9
 - ONTAP 9.11.1..... 11
 - ONTAP 9.6 11

Perform ONTAP version specific pre-revert checks

Pre-revert tasks required for your ONTAP version

Depending upon your ONTAP version, you might need to perform additional preparatory tasks before you begin the revert process.

If you are reverting from ...	Do the following before you start the revert process...
Any ONTAP 9 version	<ul style="list-style-type: none">• Terminate SMB sessions that are not continuously available.• Review reversion requirements for SnapMirror and SnapVault relationships.• Verify deduplicated volumes have enough free space.• Prepare snapshots.• Set the autocommit period for SnapLock volumes to hours.• If you have a Metrocluster configuration, disable automatic unplanned switchover.
ONTAP 9.16.1	<ul style="list-style-type: none">• If you have TLS configured for NVMe/TCP connections, disable the TLS configuration on the NVME hosts.• If you have extended qtree performance monitoring enabled, disable it.• If you are using CORS to access your ONTAP s3 buckets, remove the CORS configuration.
ONTAP 9.14.1	<p>If you have enabled trunking for client connections, disable trunking on any NFSv4.1 servers.</p>
ONTAP 9.12.1	<ul style="list-style-type: none">• If you have configured S3 client access for NAS data, remove the S3 NAS bucket configuration.• If you are running the NVMe protocol and have configured in-band authentication, disable in-band authentication.• If you have a Metrocluster configuration, disable IPsec.
ONTAP 9.11.1	<p>If you have configured Autonomous Ransomware Protection (ARP), check the ARP licensing.</p>
ONTAP 9.6	<p>If you have SnapMirror synchronous relationships, prepare the relationships for revert.</p>

Any ONTAP 9 version

Terminate certain SMB sessions before reverting ONTAP

Before you revert an ONTAP cluster from any version of ONTAP 9, you should identify and gracefully terminate any SMB sessions that are not continuously available.

Continuously available SMB shares, which are accessed by Hyper-V or Microsoft SQL Server clients using the SMB 3.0 protocol, do not need to be terminated before upgrading or downgrading.

Steps

1. Identify any established SMB sessions that are not continuously available:

```
vserver cifs session show -continuously-available No -instance
```

This command displays detailed information about any SMB sessions that have no continuous availability. You should terminate them before proceeding with the ONTAP downgrade.

```
cluster1::> vserver cifs session show -continuously-available No
-instance

                Node: node1
                Vserver: vs1
                Session ID: 1
                Connection ID: 4160072788
Incoming Data LIF IP Address: 198.51.100.5
                Workstation IP address: 203.0.113.20
                Authentication Mechanism: NTLMv2
                Windows User: CIFS\user1
                UNIX User: nobody
                Open Shares: 1
                Open Files: 2
                Open Other: 0
                Connected Time: 8m 39s
                Idle Time: 7m 45s
                Protocol Version: SMB2_1
                Continuously Available: No
1 entry was displayed.
```

2. If necessary, identify the files that are open for each SMB session that you identified:

```
vserver cifs session file show -session-id session_ID
```

```

cluster1::> vserver cifs session file show -session-id 1

Node:      node1
Vserver:   vs1
Connection: 4160072788
Session:   1
File      File      Open Hosting
Continuously
ID        Type        Mode Volume          Share              Available
-----
-----
1         Regular    rw   vol10              homedirshare       No
Path:    \TestDocument.docx
2         Regular    rw   vol10              homedirshare       No
Path:    \file1.txt
2 entries were displayed.

```

ONTAP revert requirements for SnapMirror and SnapVault relationships

The `system node revert-to` command notifies you of any SnapMirror and SnapVault relationships that need to be deleted or reconfigured for the revert process to be completed. However, you should be aware of these requirements before you begin the reversion.

- All SnapVault and data protection mirror relationships must be quiesced and then broken.

After the reversion is completed, you can resynchronize and resume these relationships if a common Snapshot copy exists.

- SnapVault relationships must not contain the following SnapMirror policy types:

- `async-mirror`

You must delete any relationship that uses this policy type.

- `MirrorAndVault`

If any of these relationships exist, you should change the SnapMirror policy to `mirror-vault`.

- All load-sharing mirror relationships and destination volumes must be deleted.
- SnapMirror relationships with FlexClone destination volumes must be deleted.
- Network compression must be disabled for each SnapMirror policy.
- The `all_source_snapshot` rule must be removed from any `async-mirror` type SnapMirror policies.



The Single File Snapshot Restore (SFSR) and Partial File Snapshot Restore (PFSR) operations are deprecated on the root volume.

- Any currently running single file and Snapshot restore operations must be completed before the reversion can proceed.

You can either wait for the restore operation to finish, or you can abort it.

- Any incomplete single file and Snapshot restore operations must be removed by using the `snapmirror restore` command.

Verify free space for deduplicated volumes before reverting ONTAP

Before you revert an ONTAP cluster from any version of ONTAP 9, you must ensure that the volumes contain sufficient free space for the revert operation.

The volume must have enough space to accommodate the savings that were achieved through the inline detection of blocks of zeros. See the Knowledge Base article [How to see space savings from deduplication, compression, and compaction in ONTAP 9](#).

If you have enabled both deduplication and data compression on a volume that you want to revert, then you must revert data compression before reverting deduplication.

Steps

1. View the progress of the efficiency operations that are running on the volumes:

```
volume efficiency show -fields vserver,volume,progress
```

2. Stop all active and queued deduplication operations:

```
volume efficiency stop -vserver <svm_name> -volume <volume_name> -all
```

3. Set the privilege level to advanced:

```
set -privilege advanced
```

4. Downgrade the efficiency metadata of a volume to the target version of ONTAP:

```
volume efficiency revert-to -vserver <svm_name> -volume <volume_name>  
-version <version>
```

The following example reverts the efficiency metadata on volume VolA to ONTAP 9.x.

```
volume efficiency revert-to -vserver vs1 -volume VolA -version 9.x
```



The volume efficiency revert-to command reverts volumes that are present on the node on which this command is executed. This command does not revert volumes across nodes.

5. Monitor the progress of the downgrade:

```
volume efficiency show -vserver <svm_name> -op-status Downgrading
```

6. If the revert does not succeed, display the instance to see why the revert failed.

```
volume efficiency show -vserver <svm_name> -volume <volume_name> -  
instance
```

7. After the revert operation is complete, return to the admin privilege level:

```
set -privilege admin
```

Learn more about [Logical storage management](#).

Prepare Snapshots before reverting an ONTAP cluster

Before you revert an ONTAP cluster from any version of ONTAP 9, you must disable all Snapshot copy policies and delete any Snapshot copies that were created after upgrading to the current release.

If you are reverting in a SnapMirror environment, you must first have deleted the following mirror relationships:

- All load-sharing mirror relationships
- Any data protection mirror relationships that were created in ONTAP 8.3.x
- All data protection mirror relationships if the cluster was re-created in ONTAP 8.3.x

Steps

1. Disable Snapshot copy policies for all data SVMs:

```
volume snapshot policy modify -vserver * -enabled false
```

2. Disable Snapshot copy policies for each node's aggregates:

a. Identify the node's aggregates:

```
run -node <nodename> -command aggr status
```

b. Disable the Snapshot copy policy for each aggregate:

```
run -node <nodename> -command aggr options aggr_name nosnap on
```

c. Repeat this step for each remaining node.

3. Disable Snapshot copy policies for each node's root volume:

a. Identify the node's root volume:

```
run-node <node_name> -command vol status
```

You identify the root volume by the word **root** in the **Options** column of the `vol status` command output.

```
vs1::> run -node node1 vol status

      Volume State           Status           Options
      vol0 online            raid_dp, flex   root, nvfail=on
                        64-bit
```

b. Disable the Snapshot copy policy on the root volume:

```
run -node <node_name> vol options root_volume_name nosnap on
```

c. Repeat this step for each remaining node.

4. Delete all Snapshot copies that were created after upgrading to the current release:

a. Set the privilege level to advanced:

```
set -privilege advanced
```

b. Disable the snapshots:

```
snapshot policy modify -vserver * -enabled false
```

c. Delete the node's newer-version Snapshot copies:

```
volume snapshot prepare-for-revert -node <node_name>
```

This command deletes the newer-version Snapshot copies on each data volume, root aggregate, and root volume.

If any Snapshot copies cannot be deleted, the command fails and notifies you of any required actions you must take before the Snapshot copies can be deleted. You must complete the required actions and then rerun the `volume snapshot prepare-for-revert` command before proceeding to the next step.


```
cluster1::*> volume snapshot prepare-for-revert -node node1
```

```
Warning: This command will delete all Snapshot copies that have the  
format used by the current version of ONTAP. It will fail if any  
Snapshot copy polices are enabled, or  
if any Snapshot copies have an owner. Continue? {y|n}: y
```

d. Verify that the Snapshot copies have been deleted:

```
volume snapshot show -node nodename
```

e. If any newer-version Snapshot copies remain, force them to be deleted:

```
volume snapshot delete {-fs-version 9.0 -node nodename -is  
-constituent true} -ignore-owners -force
```

f. Repeat these steps for each remaining node.

g. Return to the admin privilege level:

```
set -privilege admin
```



You must perform these steps on both the clusters in MetroCluster configuration.

Set autocommit periods for SnapLock volumes before reverting ONTAP

Before you revert an ONTAP cluster from any version of ONTAP 9, the value of the autocommit period for SnapLock volumes must be set in hours, not days. You should check the autocommit value for your SnapLock volumes and modify it from days to hours, if necessary.

Steps

1. Verify that there are SnapLock volumes in the cluster that have unsupported autocommit periods:

```
volume snaplock show -autocommit-period *days
```

2. Modify the unsupported autocommit periods to hours

```
volume snaplock modify -vserver <vserver_name> -volume <volume_name>  
-autocommit-period value hours
```

Disable automatic unplanned switchover before reverting two-node and four-node MetroCluster configurations

Before reverting a two-node or four-node MetroCluster configuration running any version of ONTAP 9, you must disable automatic unplanned switchover (AUSO).

Step

1. On both the clusters in MetroCluster, disable automatic unplanned switchover:

```
metrocluster modify -auto-switchover-failure-domain auso-disabled
```

Related information

[MetroCluster management and disaster recovery](#)

ONTAP 9.16.1

Disable TLS on NVMe hosts before reverting from ONTAP 9.16.1

If you have TLS secure channel for NVMe/TCP connections configured on an NVMe host, you need to disable it before you revert your cluster from ONTAP 9.16.1.

Steps

1. Remove the TLS secure channel configuration from the host:

```
vserver nvme subsystem host unconfigure-tls-for-revert -vserver  
<svm_name> -subsystem <subsystem> -host-nqn <host_nqn>
```

This command removes the host from the subsystem, and then recreates the host in the subsystem without the TLS configuration.

2. Verify that TLS secure channel is removed from the host:

```
vserver nvme subsystem host show
```

Disable extended Qtree performance monitoring before reverting from ONTAP 9.16.1

Beginning with ONTAP 9.16.1, you can use the ONTAP REST API to access the extended qtree monitoring capabilities which includes latency metrics and historical statistics. If extended qtree monitoring is enabled on any qtrees, before you revert from 9.16.1, you must set `ext_performance_monitoring.enabled` to false.

Learn more about [reverting clusters with extended qtree performance monitoring](#).

Remove CORS configuration before reverting from ONTAP 9.16.1

If you are using Cross-Origin Resource Sharing (CORS) to access ONTAP S3 buckets, you must remove it before you revert from ONTAP 9.16.1.

Learn more about [reverting ONTAP clusters with using CORS](#).

ONTAP 9.14.1

Disable NFSv4.1 session trunking before reverting from ONTAP 9.14.1

If you have enabled trunking for client connections, you must disable trunking on any NFSv4.1 servers before reverting from ONTAP 9.14.1.

When you enter the `revert-to` command, you will see a warning message advising you to disable trunking before proceeding.

After reverting to an ONTAP 9.13.1, the clients using trunked connections fall back to using a single connection. Their data throughput will be affected, but there will be no disruption. The revert behavior is the same as modifying the NFSv4.1 trunking option for the SVM from enabled to disabled.

Steps

1. Disable trunking on the NFSv4.1 server:

```
vserver nfs modify -vserver _svm_name_ -v4.1-trunking disabled
```

2. Verify that NFS is configured as desired:

```
vserver nfs show -vserver _svm_name_
```

ONTAP 9.12.1

Remove S3 NAS bucket configuration before reverting from ONTAP 9.12.1

If you have configured S3 client access for NAS data, you should use the ONTAP command line interface (CLI) to remove the NAS bucket configuration and to remove any name mappings (S3 users to Windows or Unix users) before reverting from ONTAP 9.12.1.

About this task

The following tasks are completed in the background during the revert process.

- Remove all partially completed singleton object creations (that is, all entries in hidden directories).
- Remove all hidden directories; there might be one on for each volume that is accessible from the root of the export mapped from the S3 NAS bucket.

- Remove the upload table.
- Delete any default-unix-user and default-windows-user values for all configured S3 servers.

Steps

1. Remove S3 NAS bucket configuration:

```
vserver object-store-server bucket delete -vserver <svm_name> -bucket <s3_nas_bucket_name>
```

2. Remove name mappings for UNIX:

```
vserver name-mapping delete -vserver <svm_name> -direction s3-unix
```

3. Remove name mappings for Windows:

```
vserver name-mapping delete -vserver <svm_name> -direction s3-win
```

4. Remove the S3 protocols from the SVM:

```
vserver remove-protocols -vserver <svm_name> -protocols s3
```

Disable NVMe in-band authentication before reverting from ONTAP 9.12.1

If you are running the NVME protocol, you must disable in-band authentication before you revert your cluster from ONTAP 9.12.1. If in-band authentication using DH-HMAC-CHAP is not disabled, revert will fail.

Steps

1. Remove the host from the subsystem to disable DH-HMAC-CHAP authentication:

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem <subsystem> -host-nqn <host_nqn>
```

2. Verify that the DH-HMAC-CHAP authentication protocol is removed from the host:

```
vserver nvme subsystem host show
```

3. Add the host back to the subsystem without authentication:

```
vserver nvme subsystem host add vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

Disable IPsec in MetroCluster configurations before reverting from ONTAP 9.12.1

Before reverting a MetroCluster configuration from ONTAP 9.12.1, you must disable IPsec.

A check is performed before revert to ensure there are no IPsec configurations within the MetroCluster configuration. You must remove any IPsec configurations present and disable IPsec before continuing with the revert. Reverting ONTAP is blocked if IPsec is enabled, even when you have not configured any user policies.

ONTAP 9.11.1

Check Autonomous Ransomware Protection licensing before reverting from ONTAP 9.11.1

If you have configured Autonomous Ransomware Protection (ARP) and you revert from ONTAP 9.11.1 to ONTAP 9.10.1, you might experience warning messages and limited ARP functionality.

In ONTAP 9.11.1, the Anti-ransomware license replaced the Multi-Tenant Key Management (MTKM) license. If your system has the Anti_ransomware license but no MT_EK_MGMT license, you will see a warning during revert that ARP cannot be enabled on new volumes upon revert.

The volumes with existing protection will continue to work normally after revert, and ARP status can be displayed using the ONTAP CLI. System Manager cannot show ARP status without the MTKM license.

Therefore, if you want ARP to continue after reverting to ONTAP 9.10.1, be sure the MTKM license is installed before reverting. [Learn about ARP licensing.](#)

ONTAP 9.6

Considerations for reverting systems from ONTAP 9.6 with SnapMirror synchronous relationships

You must be aware of the considerations for SnapMirror synchronous relationships before reverting from ONTAP 9.6 to ONTAP 9.5.

Before reverting, you must take the following steps if you have SnapMirror synchronous relationships:

- You must delete any SnapMirror synchronous relationship in which the source volume is serving data using NFSv4 or SMB.

ONTAP 9.5 does not support NFSv4 and SMB.

- You must delete any SnapMirror synchronous relationships in a mirror-mirror cascade deployment.

A mirror-mirror cascade deployment is not supported for SnapMirror synchronous relationships in ONTAP 9.5.

- If the common Snapshot copies in ONTAP 9.5 are not available during revert, you must initialize the SnapMirror synchronous relationship after reverting.

After two hours of upgrade to ONTAP 9.6, the common Snapshot copies from ONTAP 9.5 are automatically replaced by the common Snapshot copies in ONTAP 9.6. Therefore, you cannot resynchronize the SnapMirror synchronous relationship after reverting if the common Snapshot copies from ONTAP 9.5 are not available.

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.