What else should I check before I revert?

ONTAP 9

NetApp
January 18, 2023

Table of Contents

What else should I check before I revert?

Pre-revert checks

Depending on your environment, you need to consider certain factors before revert. Get started by reviewing the table below to see what special considerations you need to consider.

Ask yourself…	If your answer is yes, then do this…
Is my cluster running SnapMirror?	• Review considerations for reverting systems with SnapMirror Synchronous relationships • Review reversion requirements for SnapMirror and SnapVault relationships
Is my cluster running SnapLock?	Set autocommit periods
Do I have Split FlexClone volumes?	Reverse physical block sharing
Do I have FlexGroup volumes?	Disable qtree functionality
Do I have CIFS servers in workgroup mode?	Move or delete CIFS servers in workgroup mode
Do I have deduplicated volumes?	Verify volume contains enough free space
Do I have Snapshot copies?	Prepare Snapshop copies
Am I reverting to ONTAP 8.3.x?	Identify user accounts that use SHA-2 hash function
Is anti-ransomware protection configured for ONTAP 9.11.1 or later?	Check anti-ransomware licensing
Is S3 multiprotocol access configured for 9.12.1 or later?	Remove S3 NAS bucket configuration

MetroCluster pre-revert checks

Depending on your MetroCluster configuration, you need to consider certain factors before revert. Get started by reviewing the table below to see what special considerations you need to consider.

Ask yourself…	If your answer is yes, then do this…
Do I have a two- or four-node MetroCluster configuration?	Disable automatic unplanned switchover
Do I have a four- or eight-node MetroCluster IP or fabric-attached configuration running ONTAP 9.12.1 or later?	Disable IPsec

SnapMirror

Considerations for reverting systems 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.

Reversion 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 reversion 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.

Set autocommit periods for SnapLock volumes before reverting

To revert from ONTAP 9, the value of the autocommit period for SnapLock volumes must be set in hours, not days. Before attempting to revert, you must check the autocommit value for your SnapLock volumes and modify it from days to hours, if necessary.

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`

Reverse physical block sharing in split FlexClone volumes

If you have split a FlexClone volume from its parent volume, you must undo the sharing of any physical block between the clone and its parent volume before reverting from ONTAP 9.4 or later to an earlier version of ONTAP.

This task is applicable only for AFF systems when split has been run on any of the FlexClone volumes.

1. Log in to the advanced privilege level: `set -privilege advanced`
2. Identify the split FlexClone volumes with shared physical blocks: `volume clone sharing-by-split show`

```
cluster1::> volume clone sharing-by-split show
Node            Vserver   Volume        Aggregate
--------------- --------- ------------- -------------
node1           vs1       vol_clone1    aggr1
node2           vs2       vol_clone2    aggr2
2 entries were displayed.
```

3. Undo the physical block sharing in all of the split FlexClone volumes across the cluster: `volume clone sharing-by-split undo start-all`
4. Verify that there are no split FlexClone volumes with shared physical blocks: `volume clone sharing-by-split show`

```
cluster1::> volume clone sharing-by-split show
This table is currently empty.
```

Disable qtree functionality in FlexGroup volumes before reverting

Qtrees for FlexGroup volumes are not supported prior to ONTAP 9.3. You must disable the qtree functionality on FlexGroup volumes before reverting from ONTAP 9.3 to an earlier version of ONTAP.

The qtree functionality is enabled either when you create a qtree or if you modify the security-style and oplock-mode attributes of the default qtree.

1. Identify and delete all of the non-default qtrees in each FlexGroup volume that are enabled with the qtree functionality:
   a. Log in to the advanced privilege level: `set -privilege advanced`
   b. Verify if any FlexGroup volume is enabled with the qtree functionality.

      For ONTAP 9.6 or later, use: `volume show -is-qtree-caching-enabled true`

      For ONTAP 9.5 or earlier, use: `volume show -is-flexgroup-qtree-enabled true`

      ```
      cluster1::*> volume show -is-flexgroup-qtree-enabled true
      Vserver   Volume       Aggregate    State      Type       Size
      Available Used%
      --------- ------------ ------------ ---------- ---- ----------
      ---------- -----
      vs0       fg           -            online     RW        320MB
      220.4MB   31%
      ```

   c. Delete all of the non-default qtrees in each FlexGroup volume that are enabled with the qtree functionality: `volume qtree delete -vserver svm_name -volume volume_name -qtree qtree_name`

      If the qtree functionality is enabled because you modified the attributes of the default qtree and if you do not have any qtrees, you can skip this step.

      ```
      cluster1::*> volume qtree delete -vserver vs0 -volume fg -qtree
      qtree4
      WARNING: Are you sure you want to delete qtree qtree4 in volume fg
      vserver vs0?  {y|n}: y
      [Job 38] Job is queued: Delete qtree qtree4 in volume fg vserver vs0.
      ```

2. Disable the qtree functionality on each FlexGroup volume: `volume flexgroup qtree-disable -vserver svm_name -volume volume_name`

```
cluster1::*> volume flexgroup qtree-disable -vserver vs0 -volume fg
```

3. Identify and delete any Snapshot copies that are enabled with the qtree functionality.

   a. Verify if any Snapshot copies are enabled with the qtree functionality: `volume snapshot show -vserver vserver_name -volume volume_name -fields is-flexgroup-qtree-enabled`

```
cluster1::*> volume snapshot show -vserver vs0 -volume fg -fields is-
flexgroup-qtree-enabled
vserver volume snapshot is-flexgroup-qtree-enabled
------- ------ -------- --------------------------
vs0     fg     fg_snap1 true
vs0     fg     daily.2017-09-27_0010 true
vs0     fg     daily.2017-09-28_0010 true
vs0     fg     snapmirror.0241f354-a865-11e7-a1c0-
00a098a71764_2147867740.2017-10-04_124524 true
```

   b. Delete all of the Snapshot copies that are enabled with the qtree functionality: `volume snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot_name -force true -ignore-owners true`

   The Snapshot copies that must be deleted include regular Snapshot copies and the Snapshot copies taken for SnapMirror relationships. If you have created any SnapMirror relationship for the FlexGroup volumes with a destination cluster that is running ONTAP 9.2 or earlier, you must delete all of the Snapshot copies that were taken when the source FlexGroup volume was enabled for the qtree functionality.

```
cluster1::> volume snapshot delete -vserver vs0 -volume fg -snapshot
daily.2017-09-27_0010 -force true -ignore-owners true
```

Related information

FlexGroup volumes management

Identify and move SMB servers in workgroup mode

Before performing a revert, you must delete any SMB servers in workgroup mode or move them in to a domain. Workgroup mode is not supported on ONTAP versions prior to ONTAP 9.

1. Identify any SMB servers with a Authentication Style of workgroup: `vserver cifs show`
2. Move or delete the servers you identified:

If you are going to…	Then use this command….
Move the SMB server from the workgroup to an Active Directory domain:	`vserver cifs modify -vserver vserver_name -domain domain_name`
Delete the SMB server	`vserver cifs delete -vserver vserver_name`

3. If you deleted the SMB server, enter the username of the domain, then enter the user password.

Related information

SMB management

Verify deduplicated volumes have enough free space before reverting

Before reverting 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.

1. Use the volume efficiency show command with the -fields option to view the progress of the efficiency operations that are running on the volumes.

   The following command displays the progress of efficiency operations: `volume efficiency show -fields vserver,volume,progress`

2. Use the volume efficiency stop command with the -all option to stop all active and queued deduplication operations.

   The following command stops all active and queued deduplication operations on volume VolA: `volume efficiency stop -vserver vs1 -volume VolA -all`

3. Use the set -privilege advanced command to log in at the advanced privilege level.
4. Use the volume efficiency revert-to command with the -version option to downgrade the efficiency metadata of a volume to a specific version of ONTAP.

   The following command 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. Use the volume efficiency show command with the -op-status option to monitor the progress of the downgrade.

The following command monitors and displays the status of the downgrade: `volume efficiency show -vserver vs1 -op-status Downgrading`

6. If the revert does not succeed, use the volume efficiency show command with the -instance option to see why the revert failed.

   The following command displays detailed information about all fields: `volume efficiency show -vserver vs1 -volume vol1 - instance`

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

   Logical storage management

Prepare Snapshot copies before reverting

Before reverting to an earlier ONTAP release, 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

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 by using the run-nodenodenameaggr status command.
   b. Disable the Snapshot copy policy for each aggregate: `run -node nodename 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 by using the run-nodenodenamevol status command.

      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 nodename 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 nodename`

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`

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`

e. Repeat this step c for each remaining node.

f. Return to the admin privilege level: `set -privilege admin`

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

Identify user accounts that use SHA-2 hash function

If you are reverting from ONTAP 9.1 or ONTAP 9.0 to ONTAP 8.3.x, SHA-2 account users can no longer be authenticated with their passwords. Before you revert, you should identify the user accounts that use the SHA-2 hash function, so that after reverting, you can have them reset their passwords to use the encryption type (MD5) that is supported by the release you revert to.

1. Change to the privilege setting to advanced: `set -privilege advanced`
2. Identify the user accounts that use the SHA-2 has function: `security login show -vserver * -username * -application * -authentication-method password -hash-function !md5`
3. Retain the command output for use after the revert.

During the revert, you will be prompted to run the advanced command `security login password-prepare-to-downgrade` to reset your own password to use the MD5 hash function. If your password is not encrypted with MD5, the command prompts you for a new password and encrypts it with MD5, enabling your credential to be authenticated after the revert.

Check Autonomous Ransomware Protection licensing before reverting from ONTAP 9.11.1 or later

If you have configured Autonomous Ransomware Protection (ARP) and you revert from ONTAP 9.11.1 or later to ONTAP 9.10.1 or earlier, 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. However, 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.

Remove S3 NAS bucket configuration before reverting from ONTAP 9.12.1 or later

If you have configured S3 client access for NAS data and you revert from ONTAP 9.12.1 or later to ONTAP 9.11.1 or earlier, you must remove the NAS bucket configuration, and you must remove any name mappings (S3 users to Windows or Unix users) before reverting.

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.

System Manager

1. Remove a S3 NAS bucket configuration.
   Click **Storage > Buckets**, click ⋮ for each configured S3 NAS bucket, then click **Delete**.
2. Remove local name mappings for UNIX or Windows clients (or both).
   a. Click **Storage > Buckets**, then select the S3/NAS-enabled storage VM.
   b. Select **Settings**, then click → in **Name Mapping** (under **Host Users and Groups**).
   c. In the **S3 to Windows** or **S3 to UNIX tiles** (or both), click ⋮ for each configured mapping, then click **Delete**.

CLI

1. Remove S3 NAS bucket configuration.
   `vserver object-store-server bucket delete -vserver` *`svm_name`* `-bucket` *`s3_nas_bucket_name`*
2. Remove name mappings.
   `vserver name-mapping delete -vserver` *`svm_name`* `-direction s3-unix`
   `vserver name-mapping delete -vserver` *`svm_name`* `-direction s3-win`

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

Before reverting a two-node or four-node MetroCluster configuration, you must disable automatic unplanned switchover (AUSO).

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

Disable IPsec before reverting MetroCluster configurations

Before reverting a MetroCluster configuration, you must disable IPsec.

You cannot revert ONTAP in a MetroCluster configuration running ONTAP 9.12.1 with IPsec enabled. 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.

Copyright information

Trademark information