Special considerations

ONTAP 9

NetApp
February 02, 2026

Table of Contents

Special considerations

Check for specific ONTAP configurations before an upgrade

Certain cluster configurations require you to take specific actions before you begin an ONTAP software upgrade. For example, if you have a SAN configuration, you should verify that each host is configured with the correct number of direct and indirect paths before you begin the upgrade.

Review the following table to determine what additional steps you might need to take.

Before you upgrade ONTAP, ask yourself…	If your answer is yes, then do this…
Is my cluster currently in a mixed version state?	Check mixed version requirements
Do I have a MetroCluster configuration?	Review specific upgrade requirements for MetroCluster configurations
Do I have a SAN configuration?	Verify the SAN host configuration
Does my cluster have SnapMirror relationships defined?	Verify compatibility of ONTAP versions for SnapMirror relationships
Do I have DP-type SnapMirror relationships defined, and am I upgrading to ONTAP 9.12.1 or later?	Convert existing DP-type relationships to XDP
Am I using SnapMirror S3, and am I upgrading to ONTAP 9.12.1 or later?	Verify licensing for SnapMirror S3 configurations
Do I have long-term retention snapshots enabled on the middle volume of a cascade?	Disable long-term retention snapshots in middle volumes of cascade topologies
Am I using NetApp Storage Encryption with external key management servers?	Delete any existing key management server connections
Do I have netgroups loaded into SVMs?	Verify that the netgroup file is present on each node
Did I create an SVM and am I upgrading from ONTAP 9.12.1 or earlier to a later version?	Assign an explicit value to the v4.2-xattrs option
Do I have LDAP clients using SSLv3?	Configure LDAP clients to use TLS
Am I using session-oriented protocols?	Review adverse effects of session-oriented protocols
Is SSL FIPS mode enabled on a cluster where administrator accounts authenticate with an SSH public key?	Verify SSH host key algorithm support
Does my Autonomous Ransomware Protection have an active warning?	Respond to Autonomous Ransomware Protection warnings of abnormal activity

Verify compatibility of ONTAP versions for mixed version clusters

In a mixed version ONTAP cluster, nodes run two different major ONTAP versions for a

short time. For example, a cluster with nodes running ONTAP 9.8 and 9.12.1 or ONTAP 9.9.1 and 9.13.1 is a mixed version cluster. Clusters with nodes running different patch levels within the same version, like ONTAP 9.9.1P1 and 9.9.1P5, are not mixed version clusters.

ⓘ Mixed version clusters are not supported for Cloud Volumes ONTAP.

NetApp supports mixed version ONTAP clusters for limited periods of time and in specific scenarios.

The following are the most common scenarios in which an ONTAP cluster will be in a mixed version state:

- ONTAP software upgrades in large clusters

    It can take several days or weeks to upgrade all the nodes in a large cluster. The cluster enters and remains in a mixed version state until all the nodes are upgraded.

- ONTAP software upgrades required when you plan to add new nodes to a cluster

    You might add new nodes to your cluster to expand its capacity, or you might add new nodes as part of the process of completely replacing your controllers. In either case, you need might need to enter a mixed version state to enable the migration of your data from existing controllers to the new nodes in your new system.

For optimal cluster operation, the length of time that the cluster is in a mixed version state should be as short as possible. The maximum length of time a cluster is eligible for support in a mixed version state depends on the lowest ONTAP version in the cluster.

If the lowest version of ONTAP running in the mixed version cluster is…	Then you can remain in a mixed version state for a maximum of…
ONTAP 9.8 or later	90 days
ONTAP 9.7 or earlier	7 days

While the cluster is in a mixed version state, you should not enter any commands that alter the cluster operation or configuration except those that are required for the upgrade or data migration process. For example, activities such as (but not limited to) LIF migration, planned storage failover operations, or large-scale object creation or deletion should not be performed until upgrade and data migration are complete.

Mixed version clusters supported for ONTAP software upgrades

You can enter a mixed version state with any ONTAP version supported for a direct upgrade from your lowest current release. For example, if you are running ONTAP 9.11.1, you can enter a mixed version state with nodes running ONTAP 9.15.1. You cannot enter a mixed version state with nodes running ONTAP 9.11.1 and ONTAP 9.16.1. ONTAP 9.16.1 is not supported for direct upgrade from ONTAP 9.11.1.

ⓘ ONTAP patch (P) release versions have no impact on compatibility for mixed version clusters. For example, if you are running ONTAP 9.11.1P6, your current ONTAP release for mixed-version cluster compatibility is ONTAP 9.11.1. Or, if you are running ONTAP 9.12.1 and you want to upgrade to ONTAP 9.15.1P2, your target ONTAP release for mixed-version cluster compatibility is ONTAP 9.15.1.

To upgrade to an ONTAP version that is not supported for a direct upgrade from your current release, you must

perform a multi-stage upgrade. In a multi-stage upgrade, you first enter a mixed version state with the highest release supported for a direct upgrade from your current release. You complete that upgrade; then you perform a separate upgrade to your target release. For example, if your lowest current release is ONTAP 9.10.1 and you want to upgrade to ONTAP 9.16.1, you first enter a mixed version state to upgrade all your nodes to ONTAP 9.14.1; then you perform a separate upgrade from ONTAP 9.14.1 to ONTAP 9.16.1. Learn more about multi-stage upgrades and supported upgrade paths.

A mixed version cluster can contain only two major ONTAP releases. For example, you can have a mixed version cluster with nodes running ONTAP 9.13.1 and 9.15.1; or with nodes running ONTAP 9.13.1 and 9.16.1. You cannot have a mixed version cluster with nodes running ONTAP 9.13.1, 9.15.1 and 9.16.1.

If your current ONTAP release is…	And your target ONTAP release is…	Mixed version state for upgrade is…
9.17.1	9.18.1	Supported
9.16.1	9.18.1	Supported
	9.17.1	Supported
9.15.1	9.18.1	Supported
	9.17.1	Supported
	9.16.1	Supported
9.14.1	9.18.1	Supported
	9.17.1	Supported
	9.16.1	Supported
	9.15.1	Supported
9.13.1	9.18.1	Not supported
	9.17.1	Supported
	9.16.1	Supported
	9.15.1	Supported
	9.14.1	Supported
9.12.1	9.17.1 or later	Not supported
	9.16.1	Supported
	9.15.1	Supported
	9.14.1	Supported
	9.13.1	Supported
9.11.1	9.16.1 or later	Not supported
	9.15.1	Supported
	9.14.1	Supported
	9.13.1	Supported
	9.12.1	Supported

If your current ONTAP release is…	And your target ONTAP release is…	Mixed version state for upgrade is…
9.10.1	9.15.1 or later	Not supported
	9.14.1	Supported
	9.13.1	Supported
	9.12.1	Supported
	9.11.1	Supported
9.9.1	9.14.1 or later	Not supported
	9.13.1	Supported
	9.12.1	Supported
	9.11.1	Supported
	9.10.1	Supported
9.8	9.13.1 or later	Not supported
	9.12.1	Supported
	9.11.1	Supported
	9.10.1	Supported
	9.9.1	Supported

Adding new nodes to an ONTAP cluster

If you plan to add new nodes to your cluster, and those nodes require a minimum version of ONTAP that's later than the version currently running in your cluster, you need to perform any supported software upgrades on the existing nodes in your cluster before adding the new nodes. Ideally, you would upgrade all existing nodes to the minimum version of ONTAP required by the nodes you plan to add to the cluster. However, if this is not possible because some of your existing nodes don't support the later version of ONTAP, you'll need to enter a mixed version state for a limited amount of time as part of your upgrade process.

Steps

1. Upgrade the nodes that do not support the minimum ONTAP version required by your new controllers to the highest ONTAP version they support.

   For example, if you have a FAS8080 running ONTAP 9.5 and you are adding a new C-Series platform running ONTAP 9.12.1, you should upgrade your FAS8080 to ONTAP 9.8 (which is the highest ONTAP version it supports).

2. Add the new nodes to your cluster.

3. Migrate the data from the nodes being removed from the cluster to the newly added nodes.

4. Remove the unsupported nodes from the cluster.

5. Upgrade the cluster to the same ONTAP version and patch level running on the new nodes or to the latest recommended patch release for the ONTAP version running on the new nodes.

6. Verify that all nodes are running the same ONTAP version.

   a. Show the ONTAP version running on the cluster:

   ```
   version
   ```

   b. Show the ONTAP version running on each node of the cluster:

   ```
   version *
   ```

   If there is a difference between the ONTAP version reported in the output for the `version *` (cluster) and `version` (individual nodes) commands, update all nodes to the same ONTAP and patch version by running a cluster image update.

For details on data migration see:

- Create an aggregate and move volumes to the new nodes
- Setting up new iSCSI connections for SAN volume moves
- Moving volumes with encryption

Check ONTAP upgrade requirements for MetroCluster configurations

Before you upgrade your ONTAP software on a MetroCluster configuration, your clusters must meet certain requirements.

- Both clusters must be running the same version of ONTAP.

  You can verify the ONTAP version by using the version command.

- If you're performing a major ONTAP upgrade, the MetroCluster configuration must be in normal mode.

- If you're performing a patch ONTAP upgrade, the MetroCluster configuration can be in either normal or switchover mode.

- For all configurations except two-node clusters, you can nondisruptively upgrade both clusters at the same time.

  For nondisruptive upgrade in two-node clusters, the clusters must be upgraded one node at a time.

- The aggregates in both clusters must not be in resyncing RAID status.

  During MetroCluster healing, the mirrored aggregates are resynchronized. You can verify if the MetroCluster configuration is in this state by using the `storage aggregate plex show -in -progress true` command. If any aggregates are being synchronized, you should not perform an upgrade until the resynchronization is complete.

  Learn more about `storage aggregate plex show` in the ONTAP command reference.

- Negotiated switchover operations will fail while the upgrade is in progress.

  To avoid issues with upgrade or revert operations, do not attempt an unplanned switchover during an upgrade or revert operation unless all nodes on both clusters are running the same version of ONTAP.

Configuration requirements for MetroCluster normal operation

- The source SVM LIFs must be up and located on their home nodes.

  Data LIFs for the destination SVMs are not required to be up or to be on their home nodes.

- All aggregates at the local site must be online.
- All root and data volumes owned by the local cluster's SVMs must be online.

Configuration requirements for MetroCluster switchover

- All LIFs must be up and located on their home nodes.
- All aggregates must be online, except for the root aggregates at the DR site.

  Root aggregates at the DR site are offline during certain phases of switchover.

- All volumes must be online.

Related information

Verifying networking and storage status for MetroCluster configurations

Verify SAN host configuration before an ONTAP upgrade

Upgrading ONTAP in a SAN environment changes which paths are direct. Before you upgrade a SAN cluster, you should verify that each host is configured with the correct number of direct and indirect paths, and that each host is connected to the correct LIFs.

Steps

1. On each host, verify that a sufficient number of direct and indirect paths are configured, and that each path is active.

   Each host must have a path to each node in the cluster.

2. Verify that each host is connected to a LIF on each node.

   You should record the list of initiators for comparison after the upgrade. If you are running ONTAP 9.11.1 or later, use System Manager to view the connection status as it gives a much clearer display than CLI.

System Manager

1. In System Manager, click **Hosts > SAN Initiator Groups**.

   The page displays a list of initiator groups (igroups). If the list is large, you can view additional pages of the list by clicking the page numbers at the lower right corner of the page.

   The columns display various information about the igroups. Beginning with 9.11.1, the connection status of the igroup is also displayed. Hover over status alerts to view details.

CLI

- List iSCSI initiators:

  ```
  iscsi initiator show -fields igroup,initiator-name,tpgroup
  ```

- List FC initiators:

  ```
  fcp initiator show -fields igroup,wwpn,lif
  ```

SnapMirror

Compatible ONTAP versions for SnapMirror relationships

The source and destination volumes must be running compatible ONTAP versions before creating a SnapMirror data protection relationship. Before you upgrade ONTAP, you should verify that your current ONTAP version is compatible with your target ONTAP version for SnapMirror relationships.

Unified replication relationships

For SnapMirror relationships of type "XDP", using on premises or Cloud Volumes ONTAP releases:

Beginning with ONTAP 9.9.0:

- ONTAP 9.x.0 releases are cloud-only releases and support Cloud Volumes ONTAP systems. The asterisk (*) after the release version indicates a cloud-only release.

  > ⓘ ONTAP 9.16.0 is an exception to the cloud-only rule because it provides support for ASA r2 systems. The plus sign (+) after the release version indicates both an ASA r2 and cloud supported release. ASA r2 systems support SnapMirror relationships only to other ASA r2 systems.

- ONTAP 9.x.1 releases are general releases and support both on-premises and Cloud Volumes ONTAP systems.

When [advanced capacity balancing](#) is enabled on volumes in clusters running ONTAP 9.16.1 or later, SnapMirror transfers are not supported to clusters running ONTAP versions earlier than ONTAP 9.16.1.

Interoperability is bidirectional.

Interoperability for ONTAP version 9.4 and later

ONTAP version…	Interoperates with these previous ONTAP versions…																					
	9.18.1	9.17.1	9.16.1	9.16.0+	9.15.1	9.15.0*	9.14.1	9.14.0*	9.13.1	9.13.0*	9.12.1	9.12.0*	9.11.1	9.11.0*	9.10.1	9.10.0*	9.9.1	9.9.0*	9.8	9.7	9.6	9.5
9.18.1	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	No	No	No	No	No	No	No	No	No	No	No	No
9.17.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No	No	No	No
9.16.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No	No
9.16.0+	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	No	No	No	No	No	No
9.15.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No
9.15.0*	No	Yes	Yes	No	Yes	Yes	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	No	No	No	No
9.14.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No
9.14.0*	No	Yes	Yes	No	Yes	No	Yes	Yes	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	No	No	No	No
9.13.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
9.13.0*	No	Yes	Yes	No	Yes	No	Yes	No	Yes	Yes	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	No	No
9.12.1	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No

9.12.0*	No	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	Yes	Yes	No	Yes	No	Yes	No	Yes	Yes	No	No
9.11.1	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
9.11.0*	No	No	No	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	No
9.10.1	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
9.10.0*	No	No	No	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
9.9.1	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
9.9.0*	No	No	No	No	No	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
9.8	No	No	No	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
9.7	No	No	No	No	No	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
9.6	No	No	No	No	No	No	No	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
9.5	No	No	No	No	No	No	No	No	No	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

SnapMirror synchronous relationships

ⓘ SnapMirror synchronous is not supported for ONTAP cloud instances.

ONTAP version…	Interoperates with these previous ONTAP versions…													
	9.18.1	9.17.1	9.16.1	9.15.1	9.14.1	9.13.1	9.12.1	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5
9.18.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No
9.17.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No
9.16.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No
9.15.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No
9.14.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
9.13.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9.12.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No

9.11.1	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No	No
9.10.1	No	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No
9.9.1	No	No	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No
9.8	No	No	No	No	**Yes**	**Yes**	**Yes**	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No
9.7	No	No	No	No	No	**Yes**	**Yes**	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
9.6	No	No	No	No	No	No	No	No	No	No	**Yes**	**Yes**	**Yes**	**Yes**
9.5	No	No	No	No	No	No	No	No	No	No	No	**Yes**	**Yes**	**Yes**

SnapMirror SVM disaster recovery relationships

ⓘ
- This matrix applies to the SVM data mobility migration feature beginning with ONTAP 9.10.1.
- You can use SVM DR to migrate an SVM that does not meet the restrictions indicated for SVM migration (SVM data mobility).
- In both cases, a maximum of 2 major **newer** ONTAP versions can separate the source and destination clusters, with the requirement that the destination be same version or newer than source ONTAP version.

For SVM disaster recovery data and SVM protection:

SVM disaster recovery is supported only between clusters running the same version of ONTAP. **Version-independence is not supported for SVM replication**.

For SVM disaster recovery for SVM migration:
- Replication is supported in a single direction from an earlier version of ONTAP on the source to the same or later version of ONTAP on the destination.
- The ONTAP version on the target cluster must be no more than two major on-premises versions newer or two major cloud versions newer (beginning with ONTAP 9.9.0), as shown in the table below.
  - Replication is not supported for long-term data protection use cases.

The asterisk (*) after the release version indicates a cloud-only release.

To determine support, locate the source version in the left table column, and then locate the destination version on the top row (DR/Migration for like versions and Migration only for newer versions).

ⓘ If you are using ONTAP 9.10.1 or later, you can use the SVM data mobility feature instead of SVM DR to migrate SVMs from one cluster to another.

Source	Destination																					
	9.5	9.6	9.7	9.8	9.9.0*	9.9.1	9.10.0*	9.10.1	9.11.0*	9.11.1	9.12.0*	9.12.1	9.13.0*	9.13.1	9.14.0*	9.14.1	9.15.0*	9.15.1	9.16.0	9.16.1	9.17.1	9.18.1

Version																	
9.5	DR/Migration	Migration	Migration														
9.6		DR/Migration	Migration	Migration													
9.7			DR/Migration	Migration	Migration												
9.8				DR/Migration	Migration	Migration		Migration									
9.9.0*					DR/Migration	Migration	Migration	Migration	Migration	Migration							
9.9.1						DR/Migration	Migration	Migration	Migration	Migration							
9.10.0*							DR/Migration	Migration	Migration	Migration	Migration						
9.10.1								DR/Migration	Migration	Migration	Migration	Migration					
9.11.0*									DR/Migration	Migration	Migration	Migration	Migration	Migration			
9.11.1										DR/Migration	Migration	Migration	Migration	Migration			
9.12.0*											DR/Migration	Migration	Migration	Migration	Migration	Migration	

9.12.1											DR/Migration	Migration	Migration	Migration	Migration						
9.13.0*												DR/Migration	Migration	Migration	Migration	Migration	Migration				
9.13.1													DR/Migration	Migration	Migration	Migration	Migration					
9.14.0*														DR/Migration	Migration	Migration	Migration	Migration	Migration			
9.14.1															DR/Migration	Migration	Migration	Migration	Migration			
9.15.0*																DR/Migration	Migration	Migration	Migration	Migration		
9.15.1																	DR/Migration	Migration	Migration	Migration		
9.16.0																		DR/Migration	Migration	Migration	Migration	
9.16.1																			DR/Migration	Migration	Migration	
9.17.1																				DR/Migration	Migration	
9.18.1																					DR/Migration	

SnapMirror disaster recovery relationships

For SnapMirror relationships of type "DP" and policy type "async-mirror":

> ⓘ   DP-type mirrors cannot be initialized beginning with ONTAP 9.11.1 and are completely
>   deprecated in ONTAP 9.12.1. For more information, see Deprecation of data protection
>   SnapMirror relationships.

> ⓘ   In the following table, the column on the left indicates the ONTAP version on the source volume,
>   and the top row indicates the ONTAP versions you can have on your destination volume.

Source	Destination								
	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5	9.4	9.3
9.11.1	Yes	No	No	No	No	No	No	No	No
9.10.1	Yes	Yes	No	No	No	No	No	No	No
9.9.1	Yes	Yes	Yes	No	No	No	No	No	No
9.8	No	Yes	Yes	Yes	No	No	No	No	No
9.7	No	No	Yes	Yes	Yes	No	No	No	No
9.6	No	No	No	Yes	Yes	Yes	No	No	No
9.5	No	No	No	No	Yes	Yes	Yes	No	No
9.4	No	No	No	No	No	Yes	Yes	Yes	No
9.3	No	No	No	No	No	No	Yes	Yes	Yes

> ⓘ   Interoperability is not bidirectional.

Convert an existing ONTAP SnapMirror DP-type relationship to XDP

If you are upgrading to ONTAP 9.12.1 or later, you must convert DP-type relationships to
XDP before upgrading. ONTAP 9.12.1 and later does not support DP-type relationships.
You can easily convert an existing DP-type relationship to XDP to take advantage of
version-flexible SnapMirror.

Before upgrading to ONTAP 9.12.1, you must convert existing DP-type relationships to XDP before you can
upgrade to ONTAP 9.12.1 and later releases.

About this task

- SnapMirror does not automatically convert existing DP-type relationships to XDP. To convert the
  relationship, you need to break and delete the existing relationship, create a new XDP relationship, and
  resync the relationship.

- When planning your conversion, you should be aware that background preparation and the data
  warehousing phase of an XDP SnapMirror relationship can take a long time. It is not uncommon to see the
  SnapMirror relationship reporting the status "preparing" for an extended time period.

(i)	After you convert a SnapMirror relationship type from DP to XDP, space-related settings, such as autosize and space guarantee are no longer replicated to the destination.

Steps

1. From the destination cluster, ensure that the SnapMirror relationship is type DP, that the mirror state is SnapMirrored, the relationship status is Idle, and the relationship is healthy:

```
snapmirror show -destination-path <SVM:volume>
```

The following example shows the output from the `snapmirror show` command:

```
cluster_dst::>snapmirror show -destination-path svm_backup:volA_dst

Source Path: svm1:volA
Destination Path: svm_backup:volA_dst
Relationship Type: DP
SnapMirror Schedule: -
Tries Limit: -
Throttle (KB/sec): unlimited
Mirror State: Snapmirrored
Relationship Status: Idle
Transfer Snapshot: -
Snapshot Progress: -
Total Progress: -
Snapshot Checkpoint: -
Newest Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Newest Snapshot Timestamp: 06/27 10:00:55
Exported Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Exported Snapshot Timestamp: 06/27 10:00:55
Healthy: true
```

(i)	You might find it helpful to retain a copy of the `snapmirror show` command output to keep track existing of the relationship settings. Learn more about `snapmirror show` in the ONTAP command reference.

2. From the source and the destination volumes, ensure that both volumes have a common snapshot:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

The following example shows the `volume snapshot show` output for the source and the destination volumes:

```
cluster_src:> volume snapshot show -vserver vsm1 -volume volA
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm1 volA
weekly.2014-06-09_0736 valid 76KB 0% 28%
weekly.2014-06-16_1305 valid 80KB 0% 29%
daily.2014-06-26_0842 valid 76KB 0% 28%
hourly.2014-06-26_1205 valid 72KB 0% 27%
hourly.2014-06-26_1305 valid 72KB 0% 27%
hourly.2014-06-26_1405 valid 76KB 0% 28%
hourly.2014-06-26_1505 valid 72KB 0% 27%
hourly.2014-06-26_1605 valid 72KB 0% 27%
daily.2014-06-27_0921 valid 60KB 0% 24%
hourly.2014-06-27_0921 valid 76KB 0% 28%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
valid 44KB 0% 19%
11 entries were displayed.


cluster_dest:> volume snapshot show -vserver svm_backup -volume volA_dst
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm_backup volA_dst
weekly.2014-06-09_0736 valid 76KB 0% 30%
weekly.2014-06-16_1305 valid 80KB 0% 31%
daily.2014-06-26_0842 valid 76KB 0% 30%
hourly.2014-06-26_1205 valid 72KB 0% 29%
hourly.2014-06-26_1305 valid 72KB 0% 29%
hourly.2014-06-26_1405 valid 76KB 0% 30%
hourly.2014-06-26_1505 valid 72KB 0% 29%
hourly.2014-06-26_1605 valid 72KB 0% 29%
daily.2014-06-27_0921 valid 60KB 0% 25%
hourly.2014-06-27_0921 valid 76KB 0% 30%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
```

3. To ensure scheduled updates will not run during the conversion, quiesce the existing DP-type relationship:

```
snapmirror quiesce -source-path <SVM:volume> -destination-path
<SVM:volume>
```

> ℹ️ You must run this command from the destination SVM or the destination cluster.

The following example quiesces the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
```

Learn more about `snapmirror quiesce` in the ONTAP command reference.

4. Break the existing DP-type relationship:

```
snapmirror break -destination-path <SVM:volume>
```

> ℹ️ You must run this command from the destination SVM or the destination cluster.

The following example breaks the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror break -destination-path svm_backup:volA_dst
```

Learn more about `snapmirror break` in the ONTAP command reference.

5. If automatic deletion of snapshots is enabled on the destination volume, disable it:

```
volume snapshot autodelete modify -vserver _SVM_ -volume _volume_
-enabled false
```

The following example disables snapshot autodelete on the destination volume `volA_dst`:

```
cluster_dst::> volume snapshot autodelete modify -vserver svm_backup
-volume volA_dst -enabled false
```

6. Delete the existing DP-type relationship:

```
snapmirror delete -destination-path <SVM:volume>
```

Learn more about `snapmirror-delete` in the ONTAP command reference.

> ℹ️ You must run this command from the destination SVM or the destination cluster.

The following example deletes the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror delete -destination-path svm_backup:volA_dst
```

7. Release the origin SVM disaster recovery relationship on the source:

```
snapmirror release -destination-path <SVM:volume> -relationship-info
-only true
```

The following example releases the SVM disaster recovery relationship:

```
cluster_src::> snapmirror release -destination-path svm_backup:volA_dst
-relationship-info-only true
```

Learn more about `snapmirror release` in the ONTAP command reference.

8. You can use the output you retained from the `snapmirror show` command to create the new XDP-type relationship:

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume>  -type XDP -schedule <schedule> -policy <policy>
```

The new relationship must use the same source and destination volume. Learn more about the commands described in this procedure in the ONTAP command reference.

> ℹ️ You must run this command from the destination SVM or the destination cluster.

The following example creates a SnapMirror disaster recovery relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup` using the default `MirrorAllSnapshots` policy:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst
-type XDP -schedule my_daily -policy MirrorAllSnapshots
```

9. Resync the source and destination volumes:

```
snapmirror resync -source-path <SVM:volume> -destination-path
<SVM:volume>
```

To improve resync time, you can use the `-quick-resync` option, but you should be aware that storage efficiency savings can be lost.

(i) You must run this command from the destination SVM or the destination cluster. Although resync does not require a baseline transfer, it can be time-consuming. You might want to run the resync in off-peak hours.

The following example resyncs the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Learn more about `snapmirror resync` in the [ONTAP command reference](#).

10. If you disabled automatic deletion of snapshots, reenable it:

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume>
-enabled true
```

After you finish

1. Use the `snapmirror show` command to verify that the SnapMirror relationship was created.

   Learn more about `snapmirror show` in the [ONTAP command reference](#).

2. Once the SnapMirror XDP destination volume begins updating snapshots as defined by the SnapMirror policy, use the output of `snapmirror list-destinations` command from the source cluster to display the new SnapMirror XDP relationship.

Additional information about DP-type relationships

Beginning with ONTAP 9.3, XDP mode is the default, and any invocations of DP mode on the command line or in new or existing scripts are automatically converted to XDP mode.

Existing relationships are not affected. If a relationship is already of type DP, it will continue to be of type DP. Beginning with ONTAP 9.5, MirrorAndVault is the default policy when no data protection mode is specified or when XDP mode is specified as the relationship type. The table below shows the expected behavior.

If you specify…	The type is…	The default policy (if you do not specify a policy) is…
DP	XDP	MirrorAllSnapshots (SnapMirror DR)

| Nothing | XDP | MirrorAndVault (unified replication) |
| XDP | XDP | MirrorAndVault (unified replication) |

As the table shows, the default policies assigned to XDP in different circumstances ensure that the conversion maintains the functional equivalence of the previous types. Of course, you can use different policies as needed, including policies for unified replication:

If you specify…	And the policy is…	The result is…
DP	MirrorAllSnapshots	SnapMirror DR
	XDPDefault	SnapVault
	MirrorAndVault	Unified replication
XDP	MirrorAllSnapshots	SnapMirror DR
	XDPDefault	SnapVault
	MirrorAndVault	Unified replication

The only exceptions to conversion are as follows:

- SVM data protection relationships continue to default to DP mode in ONTAP 9.3 and earlier.

  Beginning with ONTAP 9.4, SVM data protection relationships default to XDP mode.

- Root volume load-sharing data protection relationships continue to default to DP mode.
- SnapLock data protection relationships continue to default to DP mode in ONTAP 9.4 and earlier.

  Beginning with ONTAP 9.5, SnapLock data protection relationships default to XDP mode.

- Explicit invocations of DP continue to default to DP mode if you set the following cluster-wide option:

```
options replication.create_data_protection_rels.enable on
```

  This option is ignored if you do not explicitly invoke DP.

Related information

- snapmirror create
- snapmirror delete
- snapmirror quiesce
- snapmirror release
- snapmirror resync

Disable long-term retention snapshots before ONTAP upgrade

In a relationship of cascaded volumes, long-term retention snapshots are supported only on the final SnapMirror destination volume of the cascade in all versions of ONTAP 9. Enabling long-term retention snapshots on any middle volume in the cascade results in missed backups and snapshots.

Learn more about long-term retention snapshots.

If you have an unsupported configuration in which long-term retention snapshots have been enabled on any middle volume of a cascade, contact technical support and reference the link:https://kb.netapp.com/on-prem/ontap/DP/SnapMirror/SnapMirror-KBs/Cascading_a_volume_with_Long-Term_Retention_(long-term retention)_snapshots_enabled_is_not_supported[NetApp Knowledge Base: Cascading a volume with Long-Term Retention (LTR) snapshots enabled is not supported^] for assistance.

The following ONTAP versions do not allow you to enable long-term retention snapshots on any volume in a cascade except the final SnapMirror destination volume.

- 9.15.1 and later
- 9.14.1P2 and P4 through P14
- 9.13.1P9 through P17
- 9.12.1 P12 through P19
- 9.11.1P15 through P20
- 9.10.1P18 through P20
- 9.9.1P20

Before upgrading from an ONTAP version that allows you to enable long-term retention snapshots on middle volumes of a cascade to an ONTAP version that blocks it, you need to disable long-term retention snapshots to avoid missed backups and snapshots.

You need to take action in the following scenarios:

- Long-Term Retention snapshots are configured on the "B" volume in an **A › B › C** SnapMirror cascade or on another middle SnapMirror destination volume in your larger cascade.
- long-term retention snapshots are defined by a schedule applied to a SnapMirror policy rule. This rule does not replicate snapshots from the source volume but creates them directly on the destination volume.

> ⓘ For more information on schedules and SnapMirror policies, see the NetApp Knowledge Base: How does the "schedule" parameter in an ONTAP 9 SnapMirror policy rule work?.

Steps

1. Remove the long-term retention rule from the SnapMirror policy on the middle volume of the cascade:

```
Secondary::> snapmirror policy remove-rule -vserver <> -policy <>
-snapmirror-label <>
```

Learn more about `snapmirror policy remove-rule` in the ONTAP command reference.

2. Add the rule again for the SnapMirror label without the long-term retention schedule:

```
Secondary::> snapmirror policy add-rule -vserver <> -policy <>
-snapmirror-label <> -keep <>
```

> ⓘ Removing long-term retention snapshots from the SnapMirror policy rules means SnapMirror will pull the snapshots with the given label from the source volume. You might also need to add or modify a schedule on the source volume's snapshot policy to create properly labeled snapshots.

Learn more about `snapmirror policy add-rule` in the ONTAP command reference.

3. If necessary, modify (or create) a schedule on the source volume snapshot policy to allow snapshots to be created with a SnapMirror label:

```
Primary::> volume snapshot policy modify-schedule -vserver <> -policy <>
-schedule <> -snapmirror-label <>
```

```
Primary::> volume snapshot policy add-schedule -vserver <> -policy <>
-schedule <> -snapmirror-label <> -count <>
```

> ⓘ long-term retention snapshots can still be enabled on the final SnapMirror destination volume within a SnapMirror cascade configuration.

Verify ONTAP licensing for SnapMirror S3 configurations

Before you upgrade ONTAP, if you are using SnapMirror S3, and you are upgrading to ONTAP 9.12.1 or later, you should verify that you have the proper SnapMirror licenses.

After upgrading ONTAP, licensing changes that occurred between ONTAP 9.11.1 and earlier and ONTAP 9.12.1 and later might cause SnapMirror S3 relationships to fail.

ONTAP 9.11.1 and earlier

- When replicating to a NetApp-hosted destination bucket (ONTAP S3 or StorageGRID), SnapMirror S3 checks for the SnapMirror synchronous license, included in the Data Protection Bundle prior to the introduction of the ONTAP One software suite.
- When replicating to a non-NetApp destination bucket, SnapMirror S3 checks for the SnapMirror cloud license, included in the Hybrid Cloud Bundle which was available prior to the introduction of the ONTAP One software suite.

ONTAP 9.12.1 and later

- When replicating to a NetApp-hosted destination bucket (ONTAP S3 or StorageGRID), SnapMirror S3 checks for the SnapMirror S3 license, included in the Data Protection bundle which was available prior to

the introduction of the ONTAP One software suite.

- When replicating to a non-NetApp destination bucket, SnapMirror S3 checks for the SnapMirror S3 External license, included in the Hybrid Cloud Bundle which was available prior to the introduction of ONTAP One software suite and the ONTAP One Compatibility bundle.

Existing SnapMirror S3 relationships

Existing SnapMirror S3 relationships should continue to work after an upgrade from ONTAP 9.11.1 or earlier to ONTAP 9.12.1 or later, even if the cluster does not have the new licensing.

Creation of new SnapMirror S3 relationships will fail if the cluster does not have the proper license installed.

Delete existing external key management server connections before upgrading ONTAP

Before you upgrade ONTAP, if you are running ONTAP 9.2 or earlier with NetApp Storage Encryption (NSE) and upgrading to ONTAP 9.3 or later, you must use the command line interface (CLI) to delete any existing external key management (KMIP) server connections.

Steps

1. Verify that the NSE drives are unlocked, open, and set to the default manufacture secure ID 0x0:

   ```
   storage encryption disk show -disk *
   ```

   Learn more about `storage encryption disk show` in the ONTAP command reference.

2. Enter the advanced privilege mode:

   ```
   set -privilege advanced
   ```

   Learn more about `set` in the ONTAP command reference.

3. Use the default manufacture secure ID 0x0 to assign the FIPS key to the self-encrypting disks (SEDs):

   ```
   storage encryption disk modify -fips-key-id 0x0 -disk *
   ```

   Learn more about `storage encryption disk modify` in the ONTAP command reference.

4. Verify that assigning the FIPS key to all disks is complete:

   ```
   storage encryption disk show-status
   ```

   Learn more about `storage encryption disk show-status` in the ONTAP command reference.

5. Verify that the **mode** for all disks is set to data

```
storage encryption disk show
```

Learn more about `storage encryption disk show` in the [ONTAP command reference](#).

6. View the configured KMIP servers:

```
security key-manager keystore show
```

Learn more about `security key-manager keystore show` in the [ONTAP command reference](#).

7. Delete the configured KMIP servers:

```
security key-manager delete -address <kmip_ip_address>
```

Learn more about `security key-manager delete` in the [ONTAP command reference](#).

8. Delete the external key manager configuration:

```
security key-manager external disable
```

Learn more about `security key-manager external disable` in the [ONTAP command reference](#).

> ⓘ This step does not remove the NSE certificates.

What's next

After the upgrade is complete, you must [reconfigure the KMIP server connections](#).

Verify netgroup file is present on all nodes before an ONTAP upgrade

Before you upgrade ONTAP, if you have loaded netgroups into storage virtual machines (SVMs), you must verify that the netgroup file is present on each node. A missing netgroup file on a node can cause an upgrade to fail.

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Display the netgroup status for each SVM:

```
vserver services netgroup status
```

3. Verify that for each SVM, each node shows the same netgroup file hash value:

```
vserver services name-service netgroup status
```

If this is the case, you can skip the next step and proceed with the upgrade or revert. Otherwise, proceed to the next step.

4. On any one node of the cluster, manually load the netgroup file:

```
vserver services netgroup load -vserver vserver_name -source uri
```

This command downloads the netgroup file on all nodes. If a netgroup file already exists on a node, it is overwritten.

Related information

Working with Netgroups

Assign an explicit value to the v4.2-xattrs option before an ONTAP upgrade

If you have an NFSv4.2 client, before you upgrade from certain releases and patches of ONTAP 9.12.1 and later you need to give an explicit value for the NFSv4.2 extended attributes option to prevent NFS response errors after upgrade.

If the `v4.2-xattrs` option is never explicitly assigned a value before the ONTAP upgrade to affected versions, NFSv4.2 clients are not informed that the server's extended attributes option has changed. This causes NFS response errors to specific `xattrs` calls due to a client and server mismatch.

Before you begin

You need to assign an explicit value for the NFSv4.2 extended attributes option if the following is true:

- You are using NFSv4.2 with an SVM created using ONTAP 9.11.1 or earlier
- You are upgrading ONTAP from any of these affected releases and patches:
  - 9.12.1RC1 to 9.12.1P11
  - 9.13.1RC1 to 9.13.1P8
  - 9.14.1RC1 to 9.14.1P1

About this task

You must be running ONTAP 9.12.1 or later to set the value using the command described in this procedure.

If `v4.2-xattrs` is already set to `enabled`, it should still be explicitly set to `enabled` to avoid future disruption. If you set `v4.2-xattrs` to disabled, NFSv4.2 clients can receive "invalid argument" responses

until they are remounted or the `v4.2-xattrs` option is set to `enabled`.

Steps

- Assign an explicit value to the `v4.2-xattrs` option:

```
nfs modify -v4.2-xattrs <enabled/disabled> -vserver <vserver_name>
```

Related information

NFS v4.2-xattrs field getting flipped after upgrades

Configure LDAP clients to use TLS before an ONTAP upgrade

Before you upgrade ONTAP, you must configure LDAP clients using SSLv3 for secure communications with LDAP servers to use TLS. SSL will not be available after the upgrade.

By default, LDAP communications between client and server applications are not encrypted. You must disallow the use of SSL and enforce the use of TLS.

Steps

1. Verify that the LDAP servers in your environment support TLS.

   If they do not, do not proceed. You should upgrade your LDAP servers to a version that supports TLS.

2. Check which ONTAP LDAP client configurations have LDAP over SSL/TLS enabled:

```
vserver services name-service ldap client show
```

   If there are none, you can skip the remaining steps. However, you should consider using LDAP over TLS for better security.

3. For each LDAP client configuration, disallow SSL to enforce the use of TLS:

```
vserver services name-service ldap client modify -vserver <vserver_name>
-client-config <ldap_client_config_name> -allow-ssl false
```

4. Verify that the use of SSL is no longer allowed for any LDAP clients:

```
vserver services name-service ldap client show
```

Related information

NFS management

Learn about adverse effects of session-oriented protocols during ONTAP upgrades

Clusters and session-oriented protocols might cause adverse effects on clients and applications in certain areas such as I/O service during upgrades.

If you are using session-oriented protocols, consider the following:

- SMB

  If you serve continuously available (CA) shares with SMBv3, you can use the automated nondisruptive upgrade method (with System Manager or the CLI), and no disruption is experienced by the client.

  If you are serving shares with SMBv1 or SMBv2, or non-CA shares with SMBv3, client sessions are disrupted during upgrade takeover and reboot operations. You should direct users to end their sessions before you upgrade.

  Hyper-V and SQL Server over SMB support nondisruptive operations (NDOs). If you configured a Hyper-V or SQL Server over SMB solution, the application servers and the contained virtual machines or databases remain online and provide continuous availability during the ONTAP upgrade.

- NFSv4.x

  NFSv4.x clients will automatically recover from connection losses experienced during the upgrade using normal NFSv4.x recovery procedures. Applications might experience a temporary I/O delay during this process.

- NDMP

  State is lost and the client user must retry the operation.

- Backups and restores

  State is lost and the client user must retry the operation.

  > (i) Do not initiate a backup or restore during or immediately before an upgrade. Doing so might result in data loss.

- Applications (for example, Oracle or Exchange)

  Effects depend on the applications. For timeout-based applications, you might be able to change the timeout setting to longer than the ONTAP reboot time to minimize adverse effects.

Verify SSH host key algorithm support before ONTAP upgrade

Before you upgrade ONTAP, if SSL FIPS mode is enabled on a cluster where administrator accounts authenticate with an SSH public key, you must ensure that the host key algorithm is supported on the target ONTAP release.

The following table indicates host key type algorithms that are supported for ONTAP SSH connections. These

key types do not apply to configuring SSH public authentication.

ONTAP release	Key types supported in FIPS mode	Key types supported in non-FIPS mode
9.11.1 and later	ecdsa-sha2-nistp256	ecdsa-sha2-nistp256 rsa-sha2-512 rsa-sha2-256 ssh-ed25519 ssh-dss ssh-rsa
9.10.1 and earlier	ecdsa-sha2-nistp256 ssh-ed25519	ecdsa-sha2-nistp256 ssh-ed25519 ssh-dss ssh-rsa

ⓘ   Support for the ssh-ed25519 host key algorithm is removed beginning with ONTAP 9.11.1.

For more information, see Configure network security using FIPS.

Existing SSH public key accounts without the supported key algorithms must be reconfigured with a supported key type before upgrading or administrator authentication will fail.

Learn more about enabling SSH public key accounts.

Resolve activity warnings in Autonomous Ransomware Protection (ARP) before an ONTAP upgrade

Before you upgrade to ONTAP 9.16.1 or later, you should respond to any abnormal activity warnings reported by Autonomous Ransomware Protection (ARP). In ONTAP 9.16.1, ARP changed to a machine learning/artificial intelligence (AI)-based model. Because of this change, any unresolved active warnings from the existing ARP in ONTAP 9.15.1 or earlier will be lost after upgrade.

Steps

1. Respond to any abnormal activity warnings reported by ARP and resolve any potential issues.

2. Confirm the resolution of these issues before upgrading by selecting **Update and Clear Suspect File Types** to record your decision and resume normal ARP monitoring.