



Special considerations

ONTAP 9

NetApp
April 06, 2024

Table of Contents

- Special considerations 1
 - Special considerations prior to an ONTAP upgrade. 1
 - Mixed version ONTAP clusters. 1
 - ONTAP upgrade requirements for MetroCluster configurations. 3
 - Verify SAN host configuration before an ONTAP upgrade. 4
 - SnapMirror 5
 - Delete existing external key management server connections before upgrading ONTAP 15
 - Verify netgroup file is present on all nodes before an ONTAP upgrade. 16
 - Configure LDAP clients to use TLS for highest security 17
 - Considerations for session-oriented protocols 18
 - Verify SSH host key algorithm support before ONTAP upgrade 19

Special considerations

Special considerations prior to an ONTAP 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 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
Do I have LDAP clients using SSLv3?	Configure LDAP clients to use TLS
Am I using session-oriented protocols?	Review considerations for 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

Mixed version ONTAP clusters

A mixed version ONTAP cluster consists of nodes running two different major ONTAP releases for a limited time. For example, if a cluster currently consists of nodes running ONTAP 9.8 and 9.12.1, the cluster is a mixed version cluster. Similarly, a cluster in which nodes are running ONTAP 9.9.1 and 9.13.1 would be a mixed version cluster. 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
- ONTAP software upgrades required when you plan to add new nodes to a cluster

The information applies to ONTAP versions that support NetApp platforms systems, such as AFF A-Series and C-Series, ASA, and FAS, and C-series systems. The information does not apply to ONTAP cloud releases (9.x.0) such as 9.12.0.

Requirements for mixed version ONTAP clusters

If your cluster needs to enter a mixed ONTAP version state, you need to be aware of important requirements and restrictions.

- There cannot be more than two different major ONTAP versions in a cluster at any given time. For example, ONTAP 9.9.1 and 9.13.1 is supported but ONTAP 9.9.1, 9.12.1, and 9.13.1 is not. Clusters that have nodes running with different P or D patch levels of the same ONTAP release, such as ONTAP 9.9.1P1 and 9.9.1P5, are not considered mixed version ONTAP clusters.
- 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.
- 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 can remain 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 higher	90 days
ONTAP 9.7 or lower	7 days

- Beginning with ONTAP 9.8, the version difference between the original nodes and the new nodes cannot be greater than four. For example, a mixed version ONTAP cluster could have nodes running ONTAP 9.8 and 9.12.1, or it could have nodes running ONTAP 9.9.1 and 9.13.1. However, a mixed version ONTAP cluster with nodes running ONTAP 9.8 and 9.13.1 would not be supported.

For a complete list of supported mixed version clusters, see [supported upgrade paths](#). All *direct* upgrade paths are supported for mixed version clusters.

Updating the ONTAP version of a large cluster

One scenario for entering a mixed version cluster state involves upgrading the ONTAP version of a cluster with multiple nodes to take advantage of the features available in later versions of ONTAP 9. When you need to upgrade the ONTAP version of a larger cluster, you will enter a mixed version cluster state for a period of time as you upgrade each node in your cluster.

Adding new nodes to an ONTAP cluster

Another scenario for entering a mixed version cluster state involves adding new nodes to your 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 to enable the migration of your data from existing controllers to the new nodes in your new system.

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. If you have nodes that do not support the minimum ONTAP version required by your new controllers, you should do the following:

1. [Upgrade](#) the nodes that do not support the minimum ONTAP version required by your new controllers to the maximum ONTAP version that they do 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 maximum 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 remaining nodes in your cluster to the same version as the new nodes.

Optionally, upgrade the entire cluster (including your new nodes) to the [latest recommended patch release](#) of the ONTAP version running on the new nodes.

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](#)

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.

- 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.

For...	Enter...
iSCSI	<pre>iscsi initiator show -fields igroup,initiator-name,tpgroup</pre>

For...	Enter...
FC	<pre>fcv initiator show -fields igroup,wwpn,lif</pre>

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



Interoperability is bidirectional.

Interoperability for ONTAP version 9.3 and later

ONTAP version ...	Interoperates with these previous ONTAP versions...																	
	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	9.4	9.3
9.14.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No
9.14.0*	Yes	Yes	Yes	No	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	No	No	No	No	No
9.13.0*	Yes	No	Yes	Yes	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	No	No	No	No

9.12.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No
9.12.0*	Yes	No	Yes	No	Yes	Yes	Yes	No	Yes	No	Yes	No	Yes	Yes	No	No	No	No
9.11.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
9.11.0*	Yes	No	Yes	No	Yes	No	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	No	No	No
9.10.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9.10.0*	Yes	No	Yes	No	Yes	No	Yes	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No
9.9.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9.9.0*	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9.8	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
9.7	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
9.6	No	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
9.5	No	No	No	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
9.4	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	Yes	Yes	Yes
9.3	No	No	No	No	No	No	No	No	No	No	No	No	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...									
	9.14.1	9.13.1	9.12.1	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5
9.14.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
9.13.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9.12.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9.11.1	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No
9.10.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
9.9.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
9.8	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No
9.7	No	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes

9.6	No	No	No	No	No	No	Yes	Yes	Yes	Yes
9.5	No	No	No	No	No	No	No	Yes	Yes	Yes

SnapMirror SVM disaster recovery relationships

- 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, 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).

Source	Destination																	
	9.3	9.4	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
9.3	DR/Migration	Migration	Migration	Migration	Migration													
9.4		DR/Migration	Migration	Migration	Migration	Migration												
9.5			DR/Migration	Migration	Migration	Migration	Migration											
9.6				DR/Migration	Migration	Migration	Migration	Migration										
9.7					DR/Migration	Migration	Migration	Migration	Migration									

9.8						DR/ Migratio n	Migratio n	Migratio n	Migratio n	Migratio n							
9.9. 0*							DR/ Migratio n	Migratio n	Migratio n	Migratio n	Migratio n						
9.9. 1								DR/ Migratio n	Migratio n	Migratio n	Migratio n	Migratio n					
9.10 .0*									DR/ Migratio n	Migratio n	Migratio n	Migratio n	Migratio n				
9.10 .1										DR/ Migratio n	Migratio n	Migratio n	Migratio n	Migratio n			
9.11 .0*											DR/ Migratio n	Migratio n	Migratio n	Migratio n	Migratio n		
9.11 .1												DR/ Migratio n	Migratio n	Migratio n	Migratio n	Migratio n	
9.12 .0*													DR/ Migratio n	Migratio n	Migratio n	Migratio n	Migratio n
9.12 .1														DR/ Migratio n	Migratio n	Migratio n	Migratio n
9.13 .0*															DR/ Migratio n	Migratio n	Migratio n
9.13 .1																DR/ Migratio n	Migratio n

9.14.0*																	DR/Migration	Migration
9.14.1																		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	9.2	9.1	9
9.11.1	Yes	No	No	No	No	No	No	No	No	No	No	No
9.10.1	Yes	Yes	No	No	No	No	No	No	No	No	No	No
9.9.1	Yes	Yes	Yes	No	No	No	No	No	No	No	No	No
9.8	No	Yes	Yes	Yes	No	No	No	No	No	No	No	No
9.7	No	No	Yes	Yes	Yes	No	No	No	No	No	No	No
9.6	No	No	No	Yes	Yes	Yes	No	No	No	No	No	No
9.5	No	No	No	No	Yes	Yes	Yes	No	No	No	No	No
9.4	No	No	No	No	No	Yes	Yes	Yes	No	No	No	No
9.3	No	No	No	No	No	No	Yes	Yes	Yes	No	No	No
9.2	No	No	No	No	No	No	No	Yes	Yes	Yes	No	No
9.1	No	No	No	No	No	No	No	No	Yes	Yes	Yes	No
9	No	No	No	No	No	No	No	No	No	Yes	Yes	Yes



Interoperability is not bidirectional.

Convert an existing 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.

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. For background information, see [XDP replaces DP as the SnapMirror default](#).
- 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.



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
```



You might find it helpful to retain a copy of the `snapmirror show` command output to keep track existing of the relationship settings.

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

```
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 vsml -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>
```

For complete command syntax, see the [man page](#).



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
```

4. Break the existing DP-type relationship:

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

For complete command syntax, see the [man page](#).



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
```

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

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

The following example disables Snapshot copy 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>
```

For complete command syntax, see the [man page](#).



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
```

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. For complete command syntax, see the man page.



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. For complete command syntax, see the man page: [SnapMirror resync command](#).



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
```

10. If you disabled automatic deletion of Snapshot copies, 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.
2. Once the SnapMirror XDP destination volume begins updating Snapshot copies 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.

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 *
```

2. Enter the advanced privilege mode:

```
set -privilege advanced
```

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 *
```

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

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

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

```
storage encryption disk show
```

6. View the configured KMIP servers:

```
security key-manager show
```

7. Delete the configured KMIP servers:

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

8. Delete the external key manager configuration:

```
security key-manager delete-kmip-config
```



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](#)

Configure LDAP clients to use TLS for highest security

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](#)

Considerations for session-oriented protocols

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.



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](#).

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.