Special considerations

ONTAP 9

NetApp
August 15, 2023

Table of Contents

Special considerations

Pre-upgrade checks

Depending on your environment, you need to consider certain factors before you start your upgrade. 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 mixed version cluster?	Check mixed version requirements
Do I have a SAN configuration?	Verify the SAN configuration
Do I have a MetroCluster configuration?	• Review specific upgrade requirements for MetroCluster configurations • Verify networking and storage status
Are nodes on my cluster using root-data partitioning and root-data-data-partitioning?	Examine upgrade considerations for root-data and root-data-data partitioning
Do I have deduplicated volumes and aggregates?	Verify you have enough free space for your deduplicated volumes and aggregates
Is my cluster running SnapMirror?	• Review upgrade requirements for SnapMirror • Prepare your SnapMirror relationships for upgrade
Am I upgrading from ONTAP 8.3 and have load-sharing mirrors?	Prepare all load-sharing mirrors for upgrade
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?	Review requirements for SSH public keys
Am I upgrading to ONTAP 9.12.1 or later and have DP-type relationships?	Convert existing DP-type relationships to XDP

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 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. 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 destruction 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, a mixed version ONTAP cluster can span a maximum of 5 major releases. 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. A mixed version ONTAP cluster with nodes running ONTAP 9.8 and 9.13.1 would not be supported, because that mixed version cluster spans 6 major releases.

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 your 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 FAS8000 running ONTAP 9.5 and you are adding a new C-Series platform running ONTAP 9.12.1, you should upgrade your FAS8000 to ONTAP 9.8 (which is the maximum ONTAP version it supports).

2. Add the new nodes to your cluster.

   Use the ONTAP command cluster `add-node -allow-mixed-version-join` at the advanced privilege level to join the new nodes.

3. Migrate the data from any nodes that cannot be upgraded to a node running the higher ONTAP version.
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

Verifying the SAN configuration

Upgrading in a SAN environment changes which paths are direct. Therefore, before performing an upgrade, 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.

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	`iscsi initiator show -fields igroup,initiator-name,tpgroup`
FC	`fcp initiator show -fields igroup,wwpn,lif`

MetroCluster configurations

Upgrade requirements for MetroCluster configurations

If you have to upgrade a MetroCluster configuration, you should be aware of some important requirements.

Required methods for performing major and minor upgrades of MetroCluster configurations

Patch upgrades to MetroCluster configurations can be performed with automatic non-disruptive upgrade (NDU) procedure.

Beginning with ONTAP 9.3, major upgrades to MetroCluster configurations can be performed with automatic non-disruptive upgrade (NDU) procedure. On systems running ONTAP 9.2 or earlier, major upgrades to MetroCluster configurations must be performed with the NDU procedure that is specific to MetroCluster configurations.

General requirements

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

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

- The MetroCluster configuration must be in either normal or switchover mode.

  Upgrade in switchover mode is only supported in minor patch upgrades.

- 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 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 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 networking and storage status for MetroCluster configurations

Before performing an upgrade in a MetroCluster configuration, you should verify the status of the LIFs, aggregates, and volumes for each cluster.

1. Verify the LIF status: `network interface show`

   In normal operation, LIFs for source SVMs must have an admin status of up and be located on their home nodes. LIFs for destination SVMs are not required to be up or located on their home nodes. In switchover, all LIFs have an admin status of up, but they do not need to be located on their home nodes.

```
cluster1::> network interface show
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            cluster1-a1_clus1
                         up/up    192.0.2.1/24       cluster1-01
                                                                  e2a
true
            cluster1-a1_clus2
                         up/up    192.0.2.2/24       cluster1-01
                                                                  e2b
true


cluster1-01
            clus_mgmt    up/up    198.51.100.1/24    cluster1-01
                                                                  e3a
true
            cluster1-a1_inet4_intercluster1
                         up/up    198.51.100.2/24    cluster1-01
                                                                  e3c
true
            ...

27 entries were displayed.
```

2. Verify the state of the aggregates: `storage aggregate show -state !online`

   This command displays any aggregates that are *not* online. In normal operation, all aggregates located at the local site must be online. However, if the MetroCluster configuration is in switchover, root aggregates at the disaster recovery site are permitted to be offline.

   This example shows a cluster in normal operation:

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

   This example shows a cluster in switchover, in which the root aggregates at the disaster recovery site are offline:

```
cluster1::> storage aggregate show -state !online
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_b1
                0B        0B    0% offline      0 cluster2-01
raid_dp,

mirror

degraded
aggr0_b2
                0B        0B    0% offline      0 cluster2-02
raid_dp,

mirror

degraded
2 entries were displayed.
```

3. Verify the state of the volumes: `volume show -state !online`

   This command displays any volumes that are *not* online.

   If the MetroCluster configuration is in normal operation (it is not in switchover state), the output should show all volumes owned by the cluster's secondary SVMs (those with the SVM name appended with "-mc").

   Those volumes come online only in the event of a switchover.

   This example shows a cluster in normal operation, in which the volumes at the disaster recovery site are not online.

```
cluster1::> volume show -state !online
  (volume show)
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vs2-mc    vol1         aggr1_b1     -          RW            -
-     -
vs2-mc    root_vs2     aggr0_b1     -          RW            -
-     -
vs2-mc    vol2         aggr1_b1     -          RW            -
-     -
vs2-mc    vol3         aggr1_b1     -          RW            -
-     -
vs2-mc    vol4         aggr1_b1     -          RW            -
-     -
5 entries were displayed.
```

4. Verify that there are no inconsistent volumes: `volume show -is-inconsistent true`

   If any inconsistent volumes are returned, you must contact NetApp Support before you precede with the upgrade.

Related information

Upgrade requirements for MetroCluster configurations

Upgrade considerations for root-data partitioning and root-data-data partitioning

Root-data partitioning and root-data-data-partitioning is supported for some platform models and configurations. This partitioning capability is enabled during system initialization; it cannot be applied to existing aggregates.

For information about migrating your data to a node that is configured for root-data partitioning or root-data-data partitioning, contact your account team or partner organization.

Related information

ONTAP concepts

Verify that deduplicated volumes and aggregates contain sufficient free space

Before upgrading ONTAP, you must verify that any deduplicated volumes and the aggregates that contain them have sufficient free space for the deduplication metadata. If there is insufficient free space, deduplication will be disabled when the ONTAP upgrade is

completed.

Each deduplicated volume must contain at least 4% free space. Each aggregate that contains a deduplicated volume must contain at least 3% free space.

1. Determine which volumes are deduplicated: `volume efficiency show`
2. Determine the free space available on each volume that you identified: `vol show -vserver Vserver_name -volume volume_name -fields volume, size, used, available, percent-used, junction-path`

   Each deduplicated volume must not contain more than 96% used capacity. If necessary, you can increase the sizes of any volumes that exceed this capacity.

   Logical storage management

   In this example, the percent-used field displays the percentage of used space on the deduplicated volume.:

   ```
   vserver    volume size    junction-path available used   percent-used
   ---------- ------ ------- -------------
   cluster1-01 vol0   22.99GB -             14.11GB      7.73GB 35%
   cluster1-02 vol0   22.99GB -             12.97GB      8.87GB    40%
   2 entries were displayed.
   ```

3. Identify the free space available on each aggregate that contains a deduplicated volume: `aggr show -aggregate aggregate_name -fields aggregate, size, usedsize, availsize, percent-used`

   Each aggregate must not contain more than 97% used capacity. If necessary, you can increase the sizes of any aggregates that exceed this capacity.

   Disk and aggregate management

   In this example, the percent-used field displays the percentage of used space on the aggregate containing the deduplicated volume (aggr_2):

   ```
   aggr show -aggregate aggregate_name -fields
   aggregate,size,usedsize,availsize,percent-used
   aggregate         availsize percent-used size    usedsize
   ----------------- --------- ------------    ------- --------
   aggr0_cluster1_01    1.11GB    95%          24.30GB 23.19GB
   aggr0_cluster1_02 1022MB    96%          24.30GB    23.30GB
   2 entries were displayed.
   ```

SnapMirror

Upgrade requirements for SnapMirror

You must perform certain tasks to successfully upgrade a cluster that is running SnapMirror.

- If you are upgrading clusters with DP SnapMirror relationships, you must upgrade the destination cluster/nodes before you upgrade the source cluster/nodes.
- Before upgrading a cluster that is running SnapMirror, SnapMirror operations must be quiesced for each node that contains destination volumes, and each peered SVM must have a unique name across the clusters.

  To prevent SnapMirror transfers from failing, you must suspend SnapMirror operations. Alternatively, you can suspend SnapMirror transfers on a particular destination volume and upgrade the owning destination node before upgrading source nodes so the SnapMirror transfers for all other destination volumes can continue. The following table describes the two options for suspending SnapMirror operations.

Option	Description	Upgrade destination nodes before source nodes?
Suspend SnapMirror operations for the duration of the NDU (nondisruptive upgrade).	The simplest method for upgrading in a SnapMirror environment is to suspend all SnapMirror operations, perform the upgrade, and then resume the SnapMirror operations. However, no SnapMirror transfers will occur during the entire NDU. You must use this method if your cluster contains nodes that are mirroring volumes to each other.	No, the nodes can be upgraded in any order.
Suspend SnapMirror operations one destination volume at a time.	You can suspend SnapMirror transfers for a particular destination volume, upgrade the node (or HA pair) that contains the destination volume, upgrade the node (or HA pair) that contains the source volume, and then resume the SnapMirror transfers for the destination volume. By using this method, SnapMirror transfers for all other destination volumes can continue while the nodes that contain the original destination and source volumes are upgraded.	Yes.

SVM peering requires SVM names to be unique across clusters. It is best practice to name SVMs with a unique fully qualified domain name (FQDN), for example, “dataVerser.HQ” or “mirrorVserver.Offsite”. Using the FQDN naming style makes it much easier to make sure of uniqueness.

Related information

Prepare SnapMirror relationships for a nondisruptive upgrade

It is recommended that you quiesce your SnapMirror operations before performing a nondisruptive upgrade of ONTAP.

Steps

1. Use the `snapmirror show` command to determine the destination path for each SnapMirror relationship.
2. For each destination volume, suspend future SnapMirror transfers:

   `snapmirror quiesce -destination-path destination`

   If there are no active transfers for the SnapMirror relationship, this command sets its status to "Quiesced". If the relationship has active transfers, the status is set to "Quiescing" until the transfer is completed, and then the status becomes "Quiesced".

   This example quiesces transfers involving the destination volume "vol1" from "SVMvs0.example.com":

   ```
   cluster1::> snapmirror quiesce -destination-path vs0.example.com:vol1
   ```

3. Verify that all SnapMirror relationships are quiesced:

   `snapmirror show -status !Quiesced`

   This command displays any SnapMirror relationships that are *not* quiesced.

   This example shows that all SnapMirror relationships are quiesced:

   ```
   cluster1::> snapmirror show -status !Quiesced
   There are no entries matching your query.
   ```

4. If any SnapMirror relationships are currently being transferred, do one of the following options:

Option	Description
Wait for the transfers to finish before performing the ONTAP upgrade.	After each transfer finishes, the relationship changes to "Quiesced" status.
Stop the transfers: `snapmirror abort -destination-path destination -h` **Note:** You must use the `-foreground true` parameter if you are aborting load-sharing mirror transfers.	This command stops the SnapMirror transfer and restores the destination volume to the last Snapshot copy that was successfully transferred. The relationship is set to "Quiesced" status.

Related information

Upgrade requirements for SnapMirror

Prepare all load-sharing mirrors before upgrading from ONTAP 8.3

Before upgrading from ONTAP 8.3, you should move all of the load-sharing mirror source volumes to an aggregate on the node that you will upgrade last. This ensures that load-sharing mirror destination volumes are the same or later versions of ONTAP.

You only need to perform this procedure when upgrading from ONTAP 8.3.

1. Record the locations of all load-sharing mirror source volumes.

   Knowing where the load-sharing mirror source volumes came from helps facilitate returning them to their original locations after the major upgrade.

2. Determine the node and aggregate to which you will move the load-sharing mirror source volumes.
3. Move the load-sharing mirror source volumes to the node and aggregate by using the volume move start command.

Delete existing external key management server connections before upgrading

If you are using NetApp Storage Encryption (NSE) on ONTAP 9.2 or earlier 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 before performing the upgrade.

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.

After the upgrade is complete, you must reconfigure the KMIP server connections.

Related information

Reconfiguring KMIP server connections after upgrading to ONTAP 9.3 or later

Verifying that the netgroup file is present on all nodes

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

NFS management contains more information about netgroups and loading them from a URI.

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.

Configure LDAP clients to use TLS for highest security

Before upgrading to the target ONTAP release, 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.

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 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 upgrade

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 release before upgrading ONTAP.

Unresolved directive in upgrade/considerations-authenticate-ssh-public-key-fips-concept.adoc - include::_include/supported-ssh-key-types.adoc[]

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

Learn more about enabling SSH public key accounts.

Convert an existing DP-type relationship to XDP

You can easily convert an existing DP-type relationship to XDP to take advantage of version-flexible SnapMirror.

About this task

- 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.
- 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|cluster://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 souce 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|cluster://SVM/volume, …
-destination-path SVM:volume|cluster://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|cluster://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|cluster://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. 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|cluster://SVM/volume, … -destination -path SVM:volume|cluster://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 DR 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
```

8. Resync the source and destination volumes:

   `snapmirror resync -source-path SVM:volume|cluster://SVM/volume, … -destination -path SVM:volume|cluster://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
   ```

9. 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. For complete command syntax, see the man page.
2. Once the SnapMirror XDP destination volume begins updating Snapshot copies as defined by the SnapMirror policy, you can use the output of `snapmirror list-destinations` command from the source cluster to display the new SnapMirror XDP relationship.

Copyright information

Trademark information