Volume backup using SnapVault

System Manager Classic

NetApp
June 22, 2024

Table of Contents

Volume backup using SnapVault

Volume backup using SnapVault overview

You can quickly configure SnapVault backup relationships between volumes that are located in different clusters. The SnapVault backup contains a set of read-only backup copies, which are located on a destination volume that you can use for restoring data when data is corrupted or lost.

Use this procedure if you want to create SnapVault backup relationships for volumes in the following way:

- You are working with clusters running ONTAP 9.
- You are a cluster administrator.
- You have configured the cluster peer relationship and the SVM peer relationship.

  Cluster and SVM peering configuration
- You must have enabled either the SnapMirror or SnapVault license, after all of the nodes in the cluster have been upgraded to the same version of ONTAP 9.
- You want to use default protection policies and schedules, and not create custom policies.
- You do not want to back up data for a single file or LUN restore.
- You want to use best practices, not explore every available option.
- You do not want to read a lot of conceptual background.
- You want to use System Manager, not the ONTAP command-line interface or an automated scripting tool.
- You want to use the System Manager classic interface for ONTAP 9.7 and earlier releases, not the ONTAP System Manager UI for ONTAP 9.7 and later.

If these assumptions are not correct for your situation, or if you want more conceptual background information, you should see the following resource:

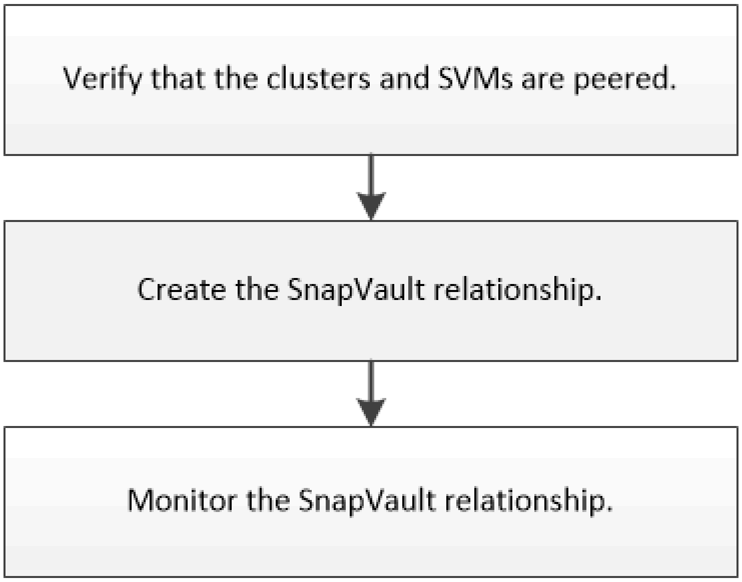
NetApp Technical Report 4183: SnapVault Best Practices

Other ways to do this in ONTAP

To perform these tasks with…	See this content…
The redesigned System Manager (available with ONTAP 9.7 and later)	Configure mirrors and vaults
The ONTAP command line interface	Create a replication relationship

SnapVault backup configuration workflow

Configuring a SnapVault backup relationship includes verifying the cluster peer relationship, creating the SnapVault relationship between the source and the destination volumes, and monitoring the SnapVault relationship.


Verify that the clusters and SVMs are peered.
Create the SnapVault relationship.
Monitor the SnapVault relationship.

Additional documentation is available to help you restore data from a destination volume to test the backed-up data or when the source volume is lost.

- Volume restore management using SnapVault

  Describes how to quickly restore a volume from a SnapVault backup in ONTAP

Verify cluster peer relationship and SVM peer relationship

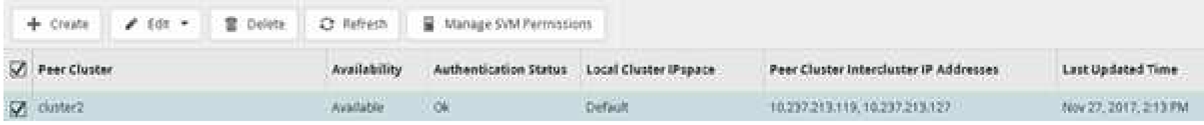
Before you set up a volume for data protection by using SnapVault technology, you must verify that the source cluster and destination cluster are peered and are communicating with each other through the peer relationship. You must also verify that the source SVM and destination SVM are peered and are communicating with each other through the peer relationship.

About this task

You must perform this task from the **source** cluster.

Procedure

- If you are running ONTAP 9.3 or later, perform the following steps to verify the cluster peer relationship and SVM peer relationship:
  a. Click **Configuration** > **Cluster Peers**.
  b. Verify that the peered cluster is authenticated and is available.



☑	Peer Cluster	Availability	Authentication Status	Local Cluster IPspace	Peer Cluster Intercluster IP Addresses	Last Updated Time
☑	cluster2	Available	Ok	Default	10.237.213.119, 10.237.213.127	Nov 27, 2017, 2:13 PM

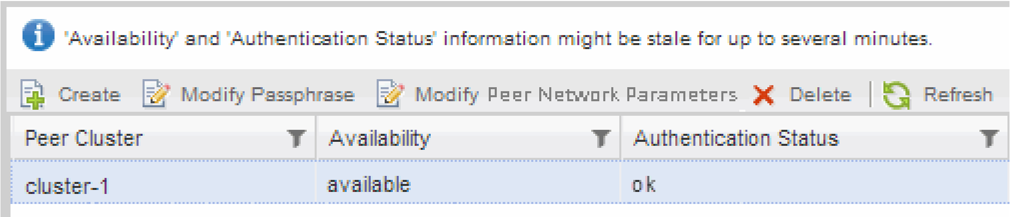
  c. Click **Configuration** > **SVM Peers**.
  d. Verify that the destination SVM is peered with the source SVM.

- If you are running ONTAP 9.2 or earlier, perform the following steps to verify the cluster peer relationship and SVM peer relationship:

a. Click the **Configurations** tab.

b. In the **Cluster Details** pane, click **Cluster Peers**.

c. Verify that the peered cluster is authenticated and available.



'Availability' and 'Authentication Status' information might be stale for up to several minutes.

Peer Cluster	Availability	Authentication Status
cluster-1	available	ok

d. Click the **SVMs** tab and select the source SVM.

e. In the **Peer Storage Virtual Machines** area, verify the destination SVM is peered with the source SVM.

If you do not see any peered SVM in this area, you can create the SVM peer relationship when creating the SnapVault relationship.

Creating the SnapVault relationship (ONTAP 9.2 or earlier)

Create a SnapVault relationship (Beginning with ONTAP 9.3)

You must create a SnapVault relationship between the source volume on one cluster and the destination volume on the peered cluster to create a SnapVault backup.

Before you begin

- You must have the cluster administrator user name and password for the destination cluster.
- The destination aggregate must have available space.

About this task

You must perform this task from the **source** cluster.

Steps

1. Click **Storage** > **Volumes**.
2. Select the volume that you want to back up, and then click **Actions** > **Protect**.

   You can also select multiple source volumes, and then create SnapVault relationships with a single destination volume.

3. In the **Volumes: Protect Volumes** page, provide the following information:

   a. Select **Vault** from the **Relationship Type** drop-down list.

   b. Select the destination cluster, destination SVM, and the suffix for the destination volume.

   Only peered SVMs and permitted SVMs are listed under destination SVMs.

   The destination volume is automatically created. The name of the destination volume is the source volume name appended with the suffix.

   c. Click .

d. In the **Advanced Options** dialog box, verify that the **Protection Policy** is set as `XDPDefault`.

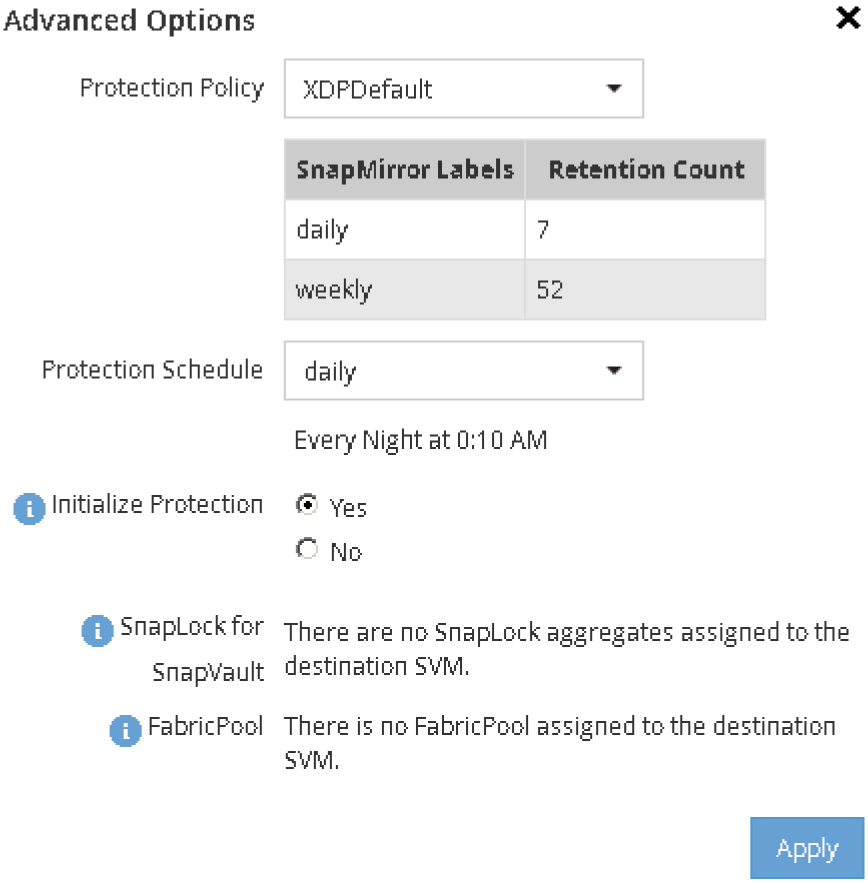
e. Select the **Protection Schedule**.

By default, the `daily` schedule is selected.

f. Verify that **Yes** is selected for initializing the SnapVault relationship.

All data protection relationships are initialized by default.

g. Click **Apply** to save the changes.



Advanced Options

Protection Policy: XDPDefault

SnapMirror Labels	Retention Count
daily	7
weekly	52

Protection Schedule: daily

Every Night at 0:10 AM

Initialize Protection: ● Yes ○ No

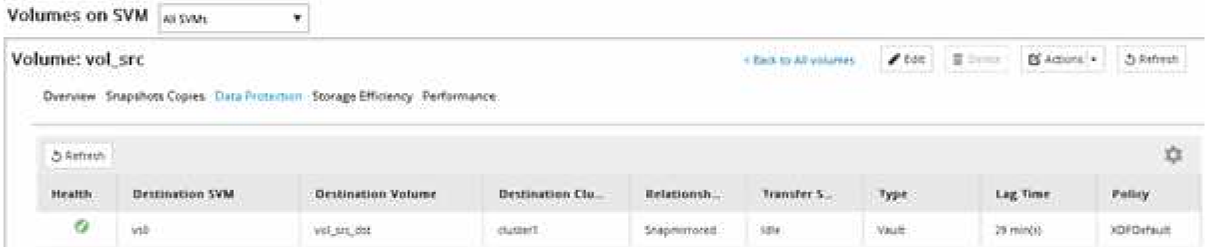
SnapLock for SnapVault: There are no SnapLock aggregates assigned to the destination SVM.

FabricPool: There is no FabricPool assigned to the destination SVM.

4. In the **Volumes: Protect Volumes** page, click **Validate** to verify whether the volumes have matching SnapMirror labels.
5. Click **Save** to create the SnapVault relationship.
6. Verify that the status of the SnapVault relationship is in the `Snapmirrored` state.

    a. Navigate to the **Volumes** window, and then select the volume that is backed up.

    b. Expand the volume and click **PROTECTION** to view the data protection status of the volume.



Volumes on SVM: All SVMs

Volume: vol_src

Health	Destination SVM	Destination Volume	Destination Clu...	Relationsh...	Transfer S...	Type	Lag Time	Policy
✓	vs0	vol_src_dst	cluster1	Snapmirrored	Idle	Vault	29 min(s)	XDPDefault

Create the SnapVault relationship (ONTAP 9.2 or earlier)

You must create a SnapVault relationship between the source volume on one cluster and the destination volume on the peered cluster to create a SnapVault backup.

Before you begin

- You must have the cluster administrator user name and password for the destination cluster.
- The destination aggregate must have available space.

About this task

You must perform this task from the **source** cluster.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. Click the **Volumes** tab.
4. Select the volume that you want to back up, and then click **Protect**.
5. In the **Create Protection Relationship** dialog box, select **Vault** from the **Relationship Type** drop-down list.
6. In the **Destination Volume** section, select the peered cluster.
7. Specify the SVM for the destination volume:

If the SVM is…	Then…
Peered	Select the peered SVM from the list.
Not peered	a. Select the SVM. b. Click **Authenticate**. c. Enter the cluster administrator’s credentials of the peered cluster, and then click **Create**.

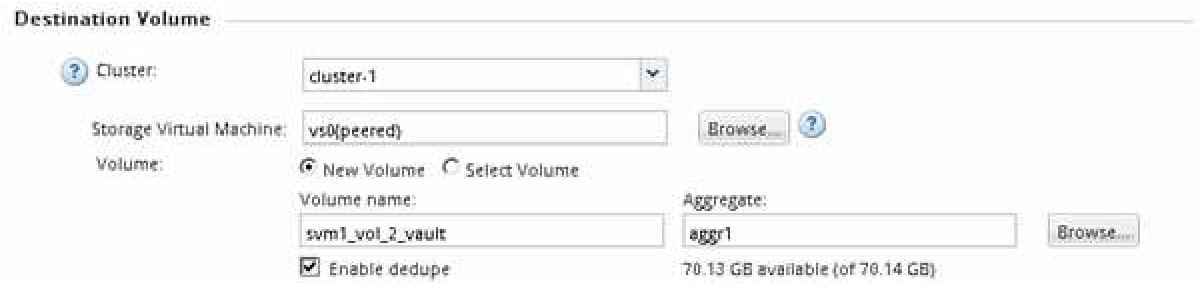
8. Create a new destination volume:

   a. Select the **New Volume** option.

   b. Use the default volume name or enter a new volume name.

   c. Select the destination aggregate.

   d. Ensure that the **Enable dedupe** check box is selected.



Destination Volume

Cluster: cluster-1

Storage Virtual Machine: vs0(peered)

Volume: ● New Volume ○ Select Volume

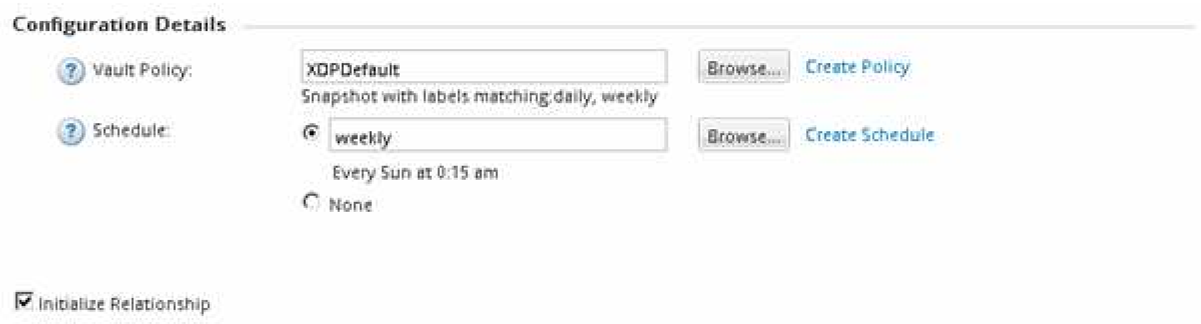
Volume name: svm1_vol_2_vault

Aggregate: aggr1

☑ Enable dedupe

70.13 GB available (of 70.14 GB)

9. In the **Configuration Details** section, select `XDPDefault` as the protection policy.
10. Select a protection schedule from the list of schedules.
11. Ensure that the **Initialize Relationship** check box is selected to transfer the base Snapshot copy, and then click **Create**



Configuration Details

Vault Policy: XDPDefault

Snapshot with labels matching:daily, weekly

Schedule: ● weekly

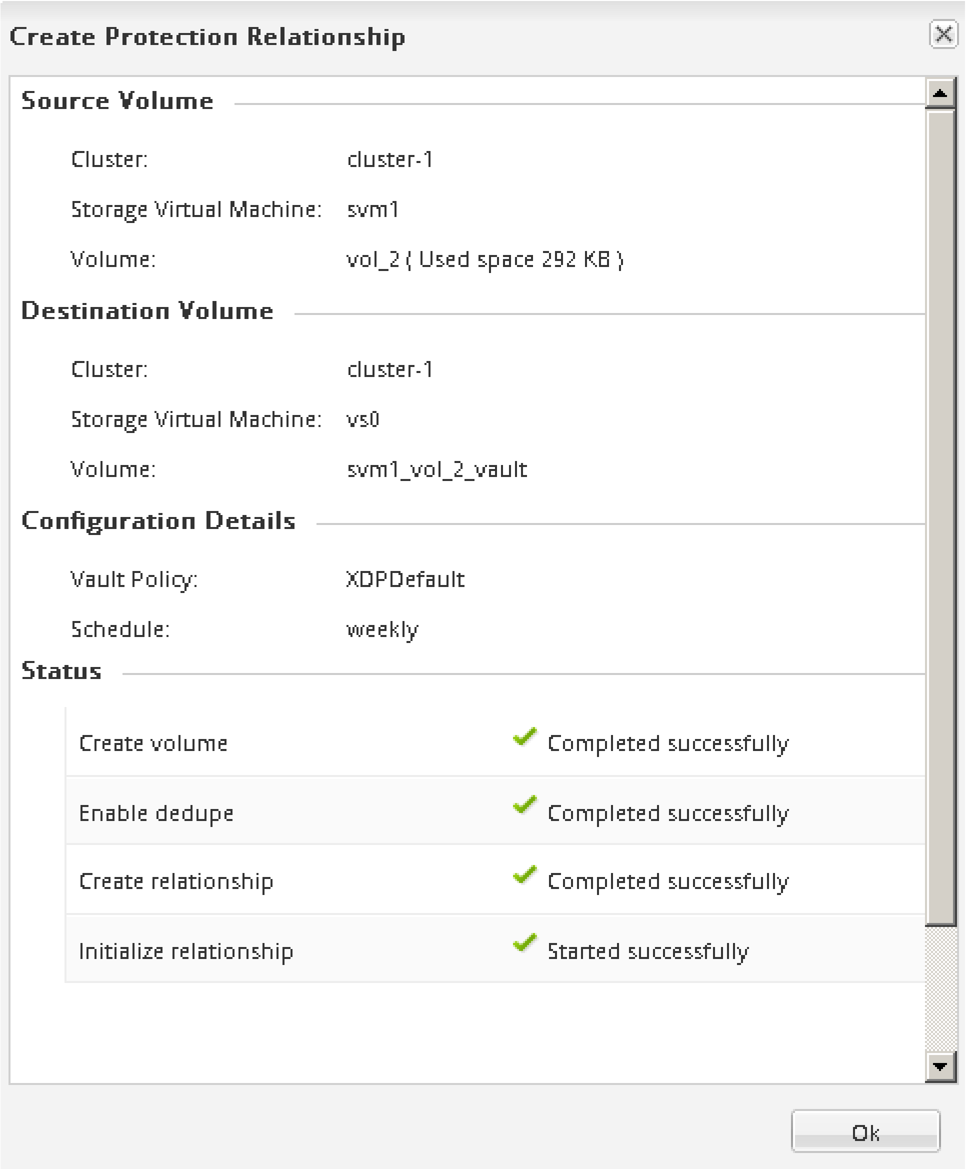
Every Sun at 0:15 am

○ None

☑ Initialize Relationship

The wizard creates the relationship with the specified vault policy and schedule. The relationship is initialized by starting a baseline transfer of data from the source volume to the destination volume.

The Status section shows the status of each job.



Create Protection Relationship

Source Volume

Cluster: cluster-1

Storage Virtual Machine: svm1

Volume: vol_2 (Used space 292 KB)

Destination Volume

Cluster: cluster-1

Storage Virtual Machine: vs0

Volume: svm1_vol_2_vault

Configuration Details

Vault Policy: XDPDefault

Schedule: weekly

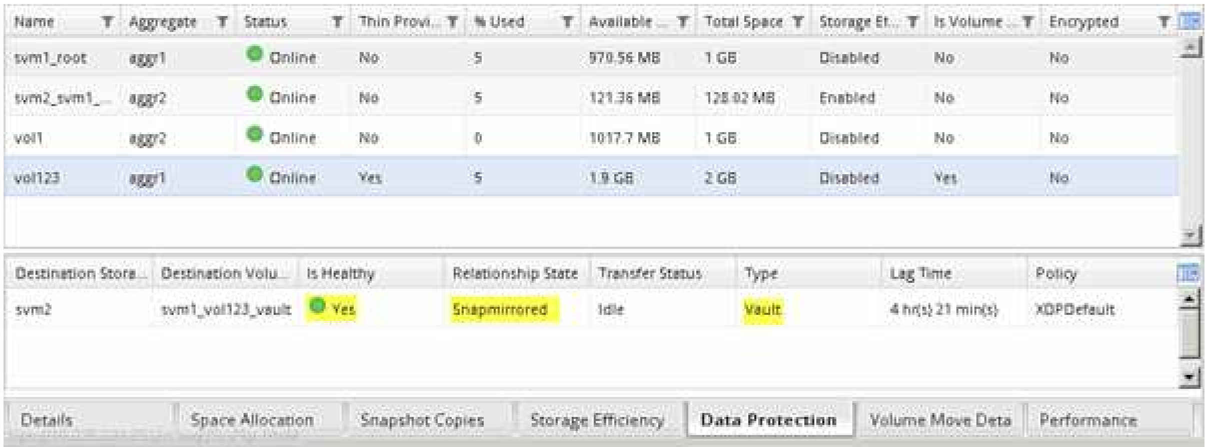
Status

Create volume	✓ Completed successfully
Enable dedupe	✓ Completed successfully
Create relationship	✓ Completed successfully
Initialize relationship	✓ Started successfully

12. Verify that the relationship status of the SnapVault relationship is in the `Snapmirrored` state.

    a. Select the volume from the Volumes list, and then click **Data Protection**.

    b. In the **Data Protection** bottom tab, verify that the SnapMirror relationship you created is listed and the relationship state is `Snapmirrored` and type is `Vault`.



Name	Aggregate	Status	Thin Provi...	% Used	Available ...	Total Space	Storage Ef...	Is Volume ...	Encrypted
svm1_root	aggr1	● Online	No	5	970.56 MB	1 GB	Disabled	No	No
svm2_svm1_...	aggr2	● Online	No	5	121.36 MB	128.02 MB	Enabled	No	No
vol1	aggr2	● Online	No	0	1017.7 MB	1 GB	Disabled	No	No
vol123	aggr1	● Online	Yes	5	1.9 GB	2 GB	Disabled	Yes	No

Destination Stora...	Destination Volu...	Is Healthy	Relationship State	Transfer Status	Type	Lag Time	Policy
svm2	svm1_vol123_vault	● Yes	Snapmirrored	Idle	Vault	4 hr(s) 21 min(s)	XDPDefault

Monitor the SnapVault relationship

You should periodically monitor the status of the SnapVault relationships to ensure that the data is backed up on the destination volume per the specified schedule.

About this task

You must perform this task from the **destination** cluster.

Steps

1. Depending on the System Manager version that you are running, perform one of the following steps:
   - ONTAP 9.4 or earlier: Click **Protection** > **Relationships**.
   - Beginning with ONTAP 9.5: Click **Protection** > **Volume Relationships**.
2. Select the SnapVault relationship between the source and the destination volumes, and then verify the status in the **Details** bottom tab.

   The health status of the SnapVault relationship, any transfer errors, and the lag time are displayed:

   - The Is Healthy field must display `Yes`.

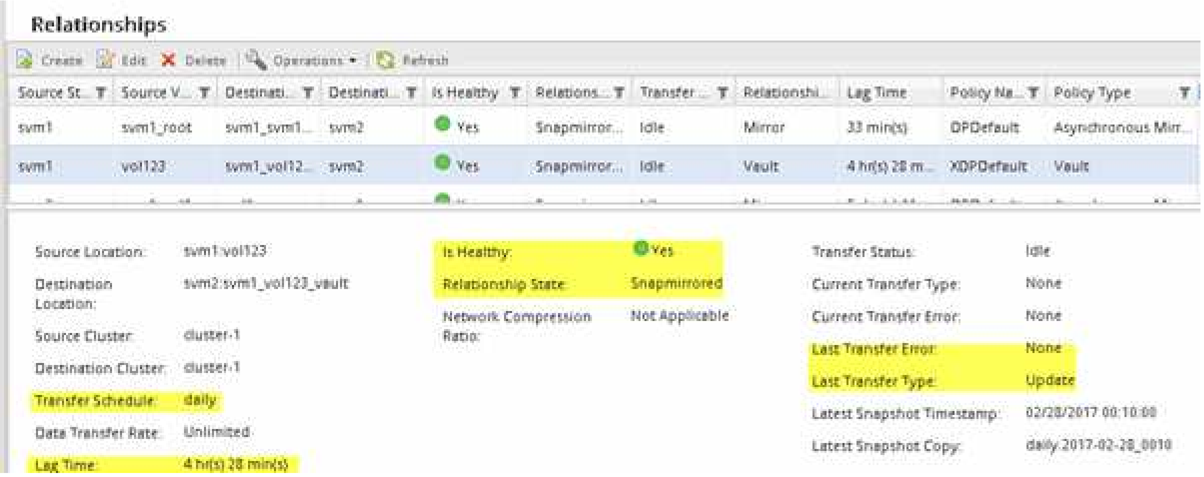
     For most data transfer failures, the field displays `No`. In some failure cases, however, the field continues to display `Yes`. You must check the transfer errors in the Details section to ensure that no data transfer failure occurred.

   - The Relationship State field must display `Snapmirrored`.
   - The Lag Time must be not more than the transfer schedule interval.

     For example, if the transfer schedule is daily, then the lag time must not be more than a day.

     You should troubleshoot any issues in the SnapVault relationships. The troubleshooting procedures for SnapMirror relationships are also applicable to SnapVault relationships.

     NetApp Technical Report 4015: SnapMirror Configuration and Best Practices for ONTAP 9.1, 9.2



Relationships

Source St...	Source V...	Destinati...	Destinati...	Is Healthy	Relations...	Transfer ...	Relationshi...	Lag Time	Policy Na...	Policy Type
svm1	svm1_root	svm1_svm1...	svm2	● Yes	Snapmirror...	Idle	Mirror	33 min(s)	DPDefault	Asynchronous Mirr...
svm1	vol123	svm1_vol12...	svm2	● Yes	Snapmirror...	Idle	Vault	4 hr(s) 28 m...	XDPDefault	Vault

Source Location:	svm1:vol123	Is Healthy:	● Yes	Transfer Status:	Idle
Destination Location:	svm2:svm1_vol123_vault	Relationship State:	Snapmirrored	Current Transfer Type:	None
Source Cluster:	cluster-1	Network Compression Ratio:	Not Applicable	Current Transfer Error:	None
Destination Cluster:	cluster-1			Last Transfer Error:	None
Transfer Schedule:	daily			Last Transfer Type:	Update
Data Transfer Rate:	Unlimited			Latest Snapshot Timestamp:	02/28/2017 00:10:00
Lag Time:	4 hr(s) 28 min(s)			Latest Snapshot Copy:	daily.2017-02-28_0010

Copyright information

Trademark information