Snapshots User Guide

Introduction

In any storage system, the feature that is of paramount importance to the user is data protection. Snapshots are an industry-wide standard for protecting data at a very fine granularity. Either according to a schedule or under the direction of an administrator, the storage system takes point-in-time snapshots of the contents of a volume in a storage system. Each snapshot is similar to an incremental backup of the data within the system; what distinguishes various snapshots is the way the data is backed up, improving both space utilization as well as performance. AMI's StorTrends iTX storage has industry-leading support for snapshots, offering an exhaustive array of innovative features, with an implementation that optimizes performance and storage capacity utilization.

In the case of multiple storage devices, there needs to be some application and host aware agent on the application server that communicates with the storage server in order to create application-aware consistent snapshots. This host agent must be able to quiesce the application and trigger the snapshots on all the application-specific volumes. AMI Storage Server and Host Attach Kit (HAK), with its Microsoft VSS Hardware Provider and Application-specific agents such as MS Exchange and Oracle snapshot agents, with the solution.

Overview of Snapshots

Data protection is changing; it used to be backing up data onto tape which could be as often as once an hour, once a day, once a week or even once a month. Times have changed. With increasing regulatory plus the glut of stored data, which doubles every 18 months or so, traditional data protection methodologies can no longer

adequately protect the data. This problem has led to the development of a plethora of next generation data protection (NGDP) technologies, such as snapshots.

A storage snapshot is a set of reference markers or pointers, to data stored on a disk drive, a tape, or in a storage area network (SAN). A snapshot is like a detailed table of contents, but the computer treats it as a complete data backup. Snapshots streamline access to stored data and can speed up the process of data recovery. There are two main types of storage snapshot, called the 'copy-on-write' (or low-capacity) snapshot and the 'split-mirror' snapshot.

A copy-on-write snapshot utility creates a snapshot of changes to stored data every time new data is entered or existing data is updated. This allows rapid recovery of data in case of a disk write error, corrupted file, or program malfunction. However, all previous snapshots must be available if a complete archiving or recovery of all the data on a network or storage medium is needed.

A split-mirror-snapshot utility references all the data on a set of mirrored drives. Every time the utility is run, a snapshot is created of the entire volume, not only of the new or updated data. This makes it possible to access data offline, and simplifies the process of recovering, duplicating, or archiving all the data on a drive. However, this is a slower process, and it requires more storage space for each snapshot.

Configuring Snapshots using ManageTrends

Creating Snapshots

Ensure that the iSCSI target is connected and mounted to the Windows machine before proceeding to create snapshots.

Creating a SAN Volume Snapshot:

1. After the SAN and NAS volumes are created, click on the expander ('+') to reveal the 'Snapshots' directory in the Management tree in the left panel.
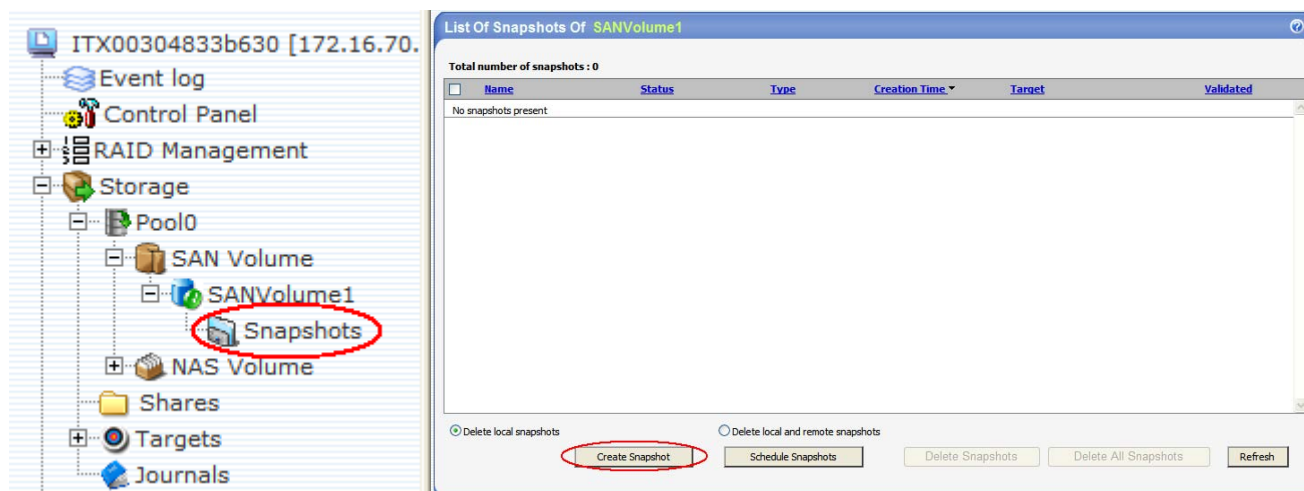

Figure 1: Snapshot Management Window

2. Click on 'Create Snapshot' in the List of Snapshots screen shown above. The 'Create Snapshot' window opens as shown in Figure 2 below.
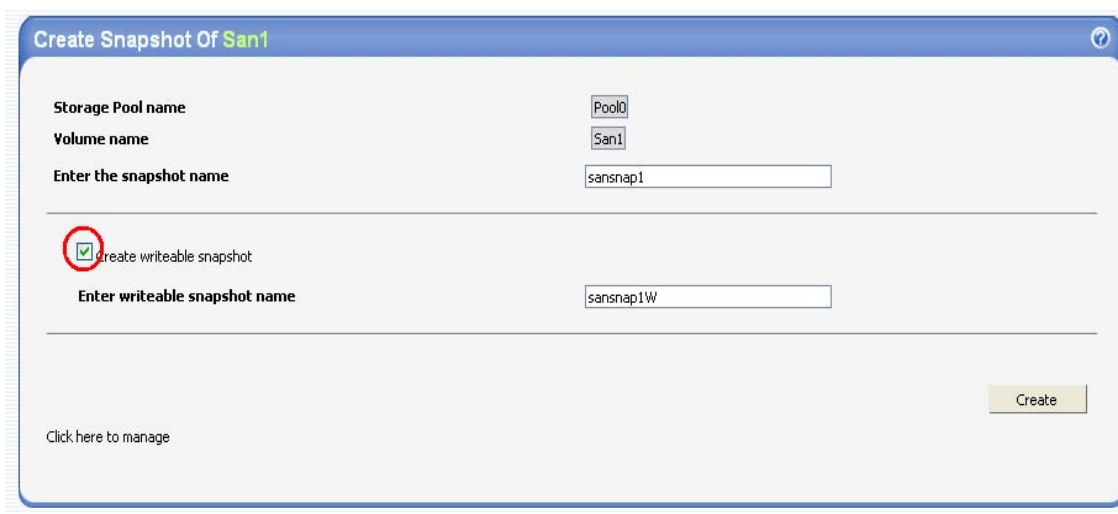
Figure 2: Creating a Snapshot

3. Enter a name for the snapshot and click on 'Create'. The list of snapshots created will now appear.

Note: If the snapshot needs to be mounted on a Windows platform, then a writeable snapshot needs to be created. The writeable snapshot can be created at any point of time from the corresponding read-only snapshot. For illustrative purpose, we create a writeable snapshot along with the read-only snapshot.
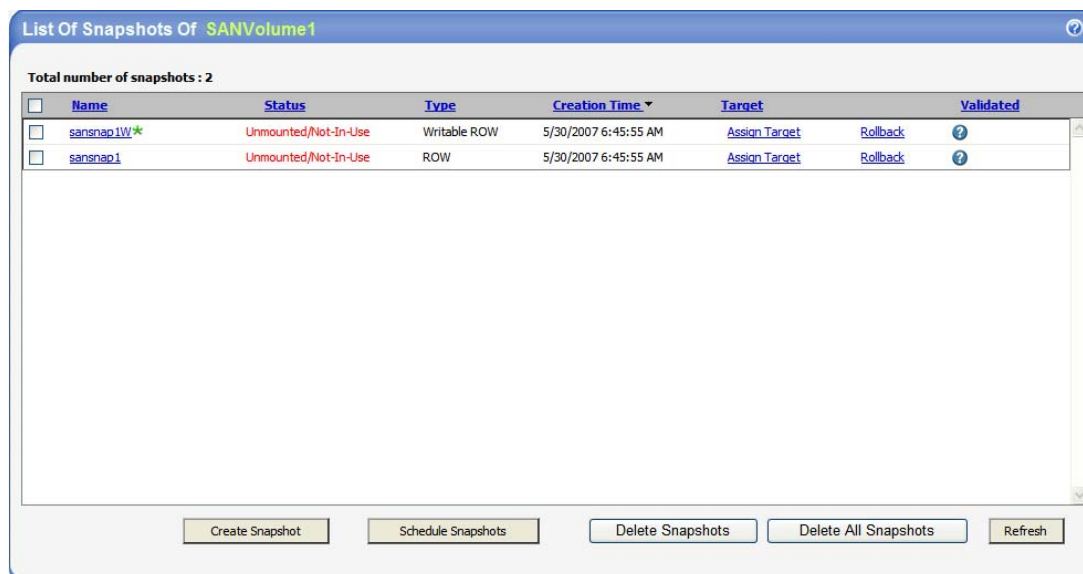
Figure 3: List of snapshots

4. To activate and mount a snapshot, click on 'Assign Target' (Figure 3) of a Writeable ROW and create a new target. Ensure that the target is enabled.

Figure 4: Creating a target for the snapshot

Note: A 'Read-Only' Snapshot (ROW) **cannot** be mounted on a Windows platform.

Refresh the iSCSI initiator to log on to the new target.
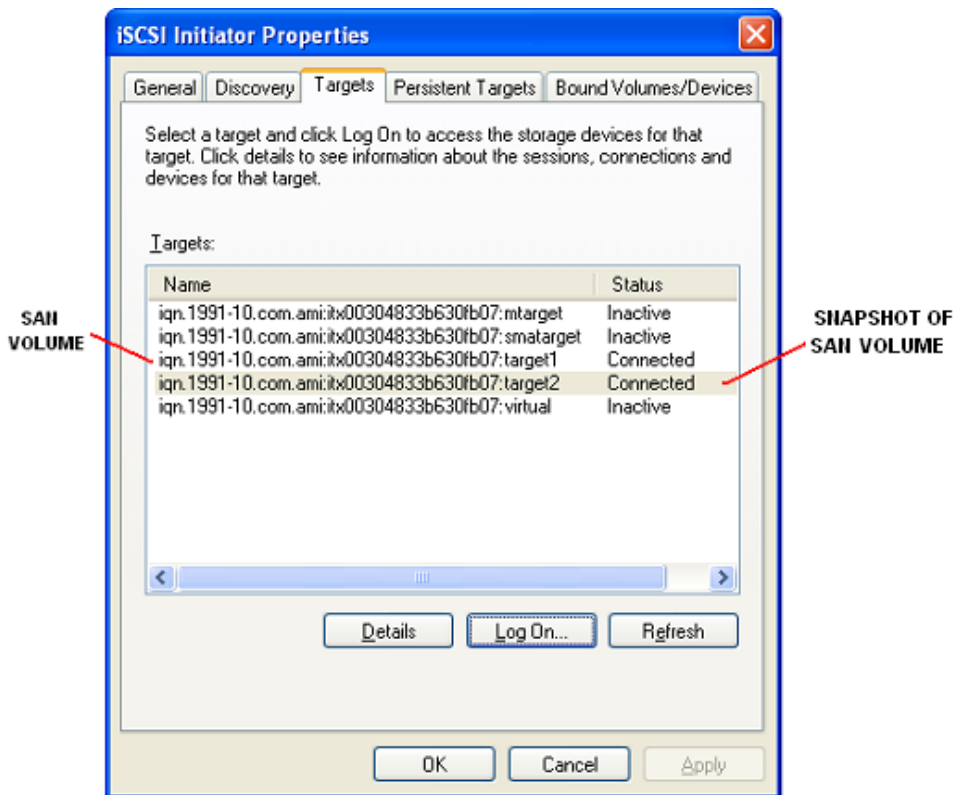
Figure 5: Mounting the snapshot target on the iSCSI Initiator

Once the target is connected, the 'List of Snapshots' window will show the snapshot drive as 'Mounted/ In use' (Figure 6).
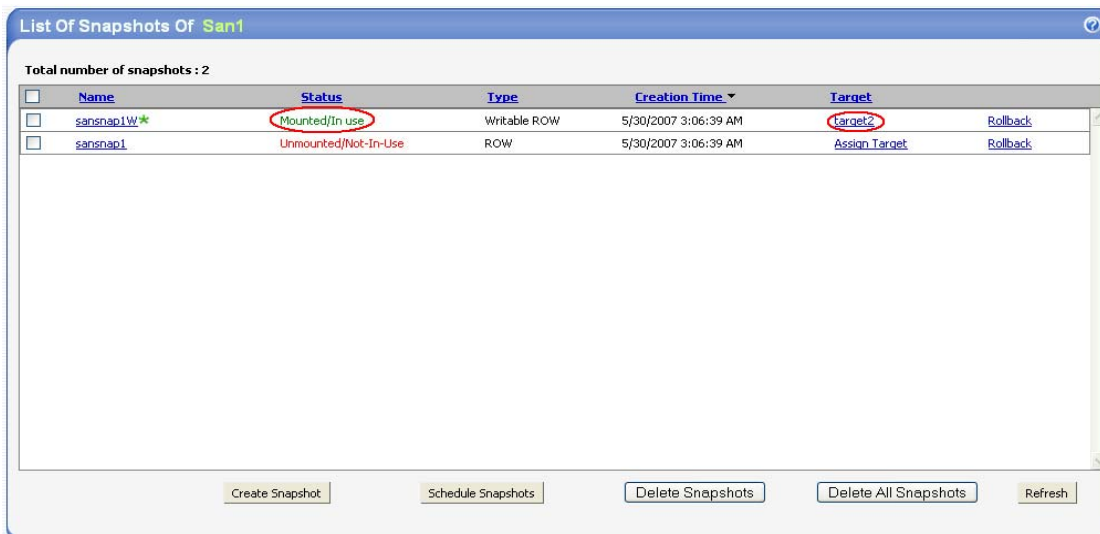
The snapshot volume is now mounted and the data present on the original SAN volume is also present in this volume. The SAN volume can be used as a normal hard drive and the snapshot volume can be updated with the data according to schedule.

The 'Disk Management' utility in the Computer Management Tool can be used to verify that the volumes have been partitioned correctly and data in the snapshot is consistent with that of the parent SAN volume. The SAN volume and its snapshot will show up as identical drives
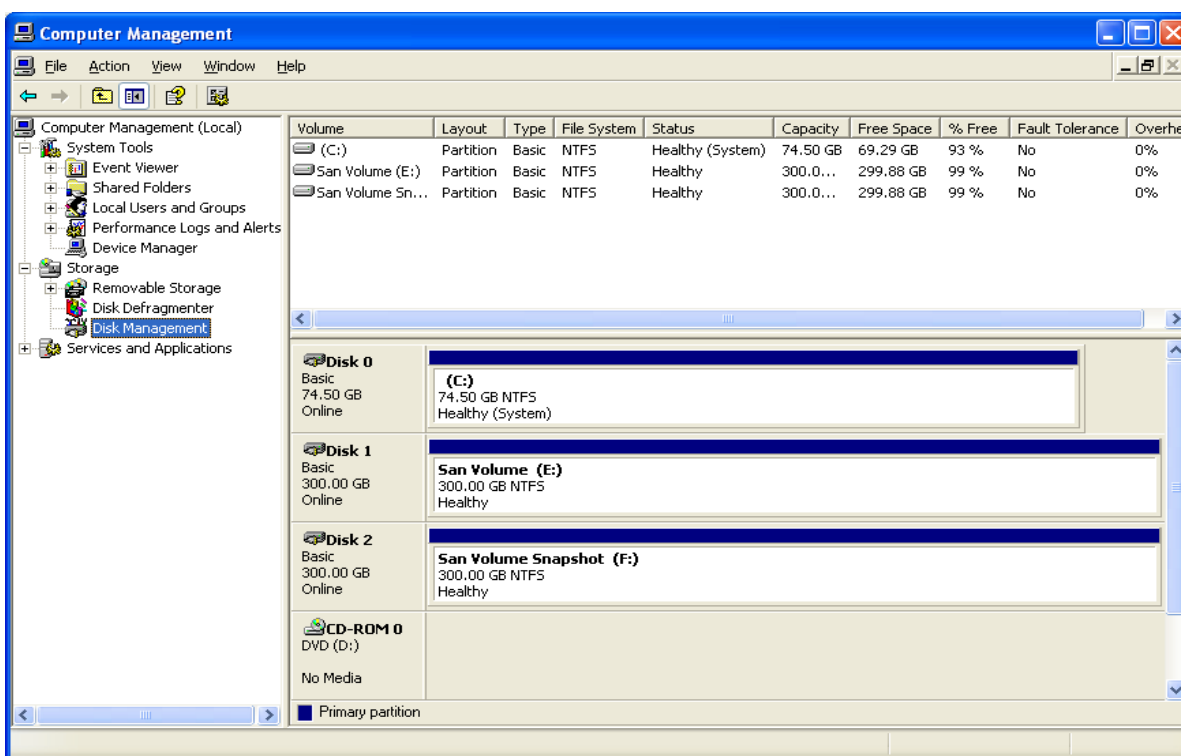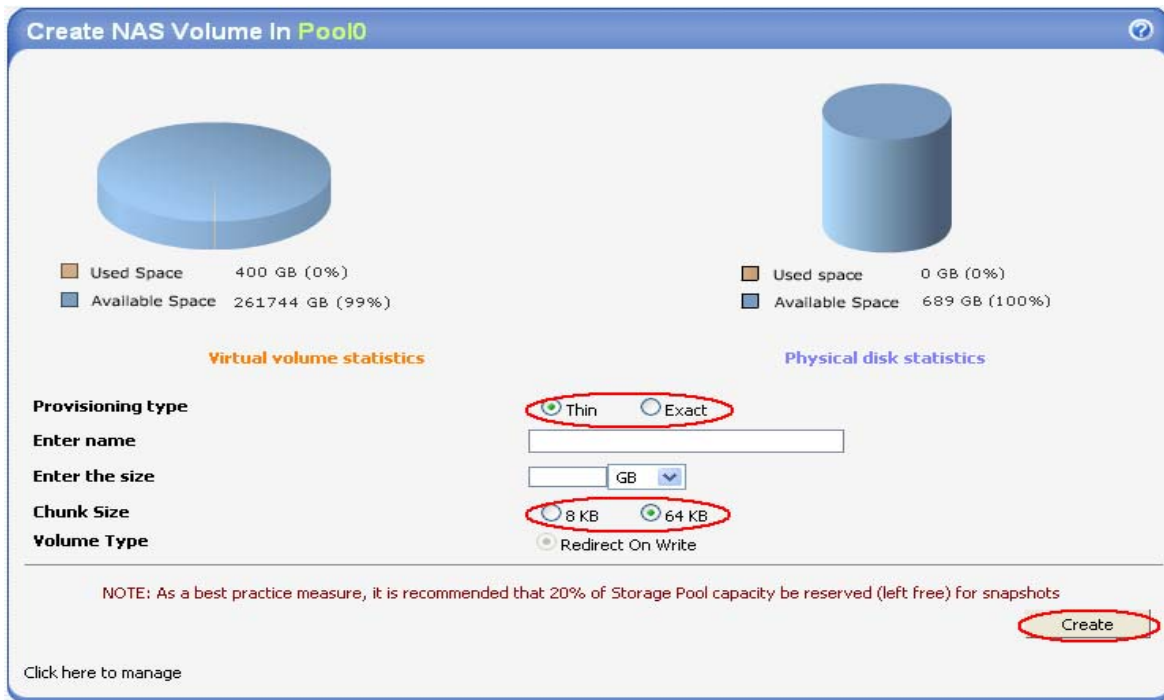
Figure 7: SAN Volume and its Snapshot mounted on Windows platform

Creating a NAS Volume Snapshot:

A NAS snapshot can be created in a similar manner as the SAN except that a writeable snapshot need not be created to mount the volume.

1. Click on the 'NAS Volume' directory in the Management tree on the left panel to go to the 'Create NAS Volume' page. Enter the name and size of the NAS

volume. The chunk size and provisioning type can also be chosen. Click on 'Create'.
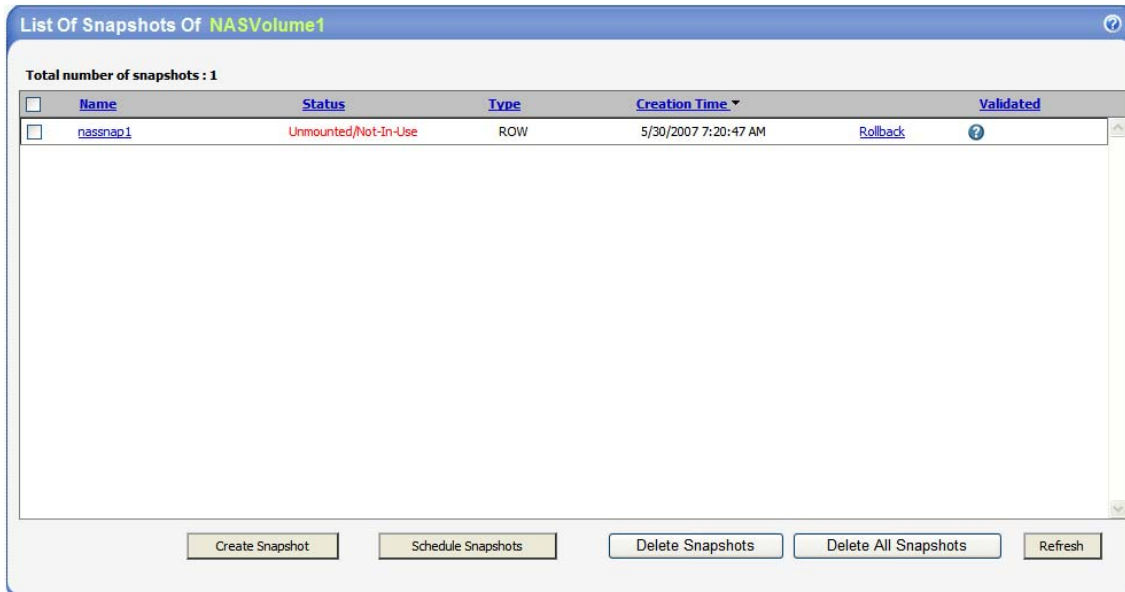
Figure 8: Creating a NAS Volume

The snapshot appears in the list as shown in Figure 9.

Figure 9: List of NAS Volumes created

2. To activate and mount a snapshot, click on the name of the NAS snapshot created
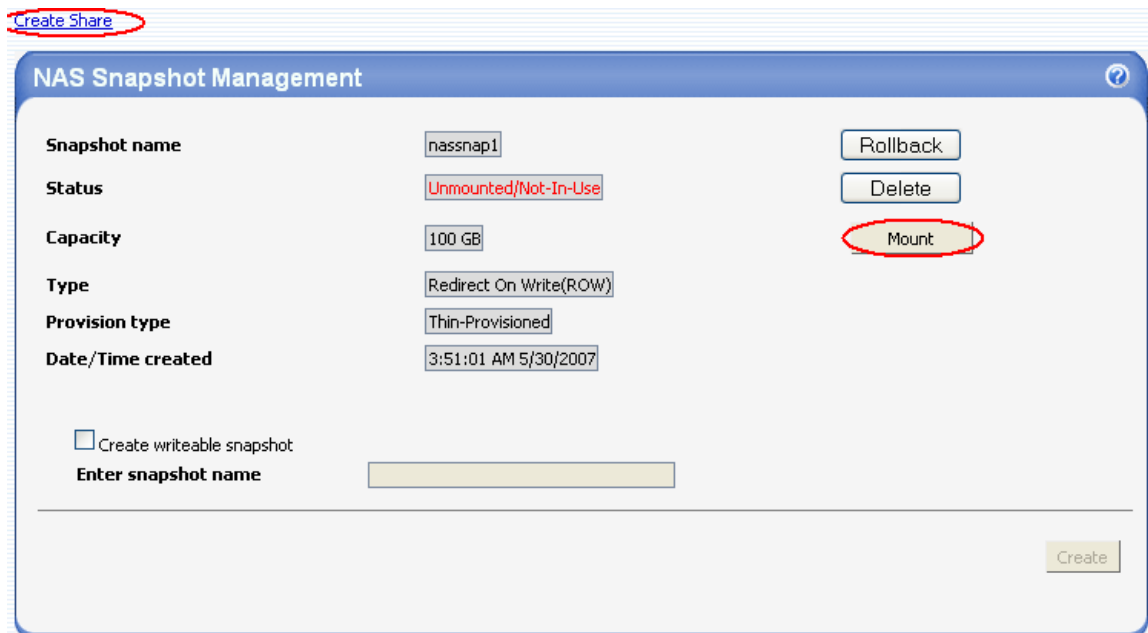(Figure 9) and then click on 'Mount' (Figure 10).

Figure 10: Mounting a NAS Volume

3. To share the NAS snapshot, click on 'Create Share' (Figure 10) on the top left
corner of the window. Type a name and select a client for sharing the volume
(Figure 11). More than one client can also be selected.

Figure 11: Sharing a NAS Volume

Once the NAS volume is shared, the folder appears in the 'Shares' directory in the management tree on the left pane.

Scheduling SAN & NAS Snapshots:

Before proceeding to schedule automatic snapshots ensure that the Host Attach Kit (HAK), which is provided along with the StorTrends iTX package, has been installed on the Initiator machine. We will elaborate the procedure to be followed to schedule snapshots of a SAN Volume. Scheduling snapshots of NAS Volumes is the same.

1. There are 2 ways to schedule snapshots. One from the 'List of Snapshots' window (Figure 12) and the other from the 'Volume Management' window (Figure 13). Click on 'Schedule Snapshots' to configure the scheduling process.
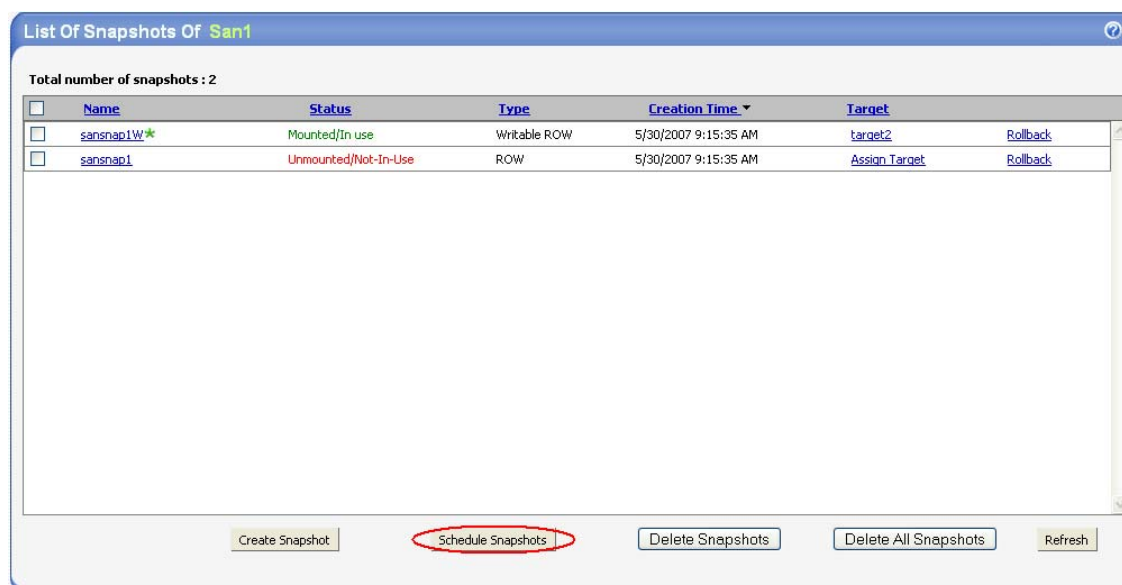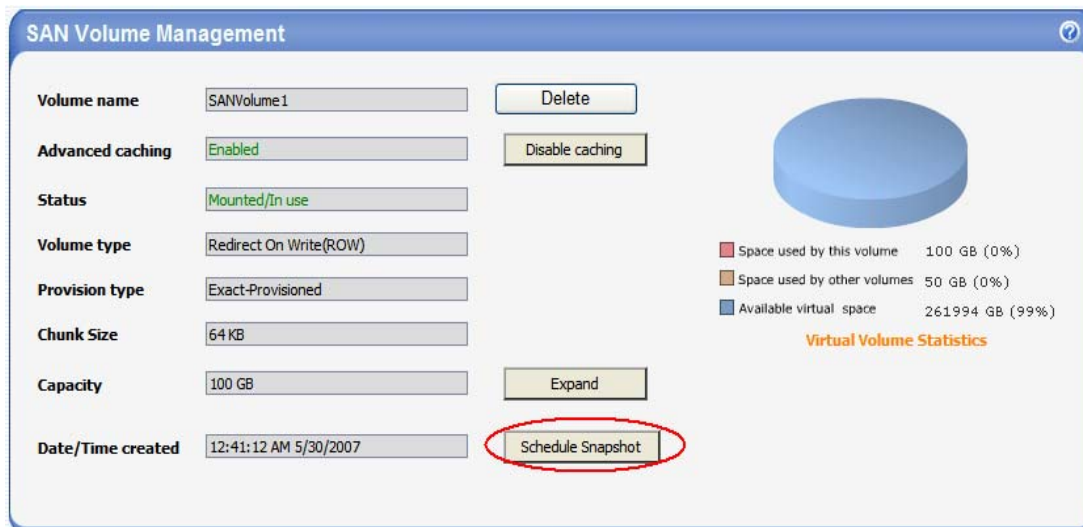

Figure 12: Scheduling a snapshot

The schedule window looks as shown in Figure 13. Fill in the Maximum Copies and the Frequency at which the snapshots need to be taken and click on 'Add Schedule'. For example, a frequency of 10 minutes and maximum copies of 10 implies that a snapshot will be taken every 10 minutes and 10 such snapshots will be maintained. So after 100 minutes, the oldest snapshot will be replaced by the latest. Eight levels of schedule can be added to a single volume.
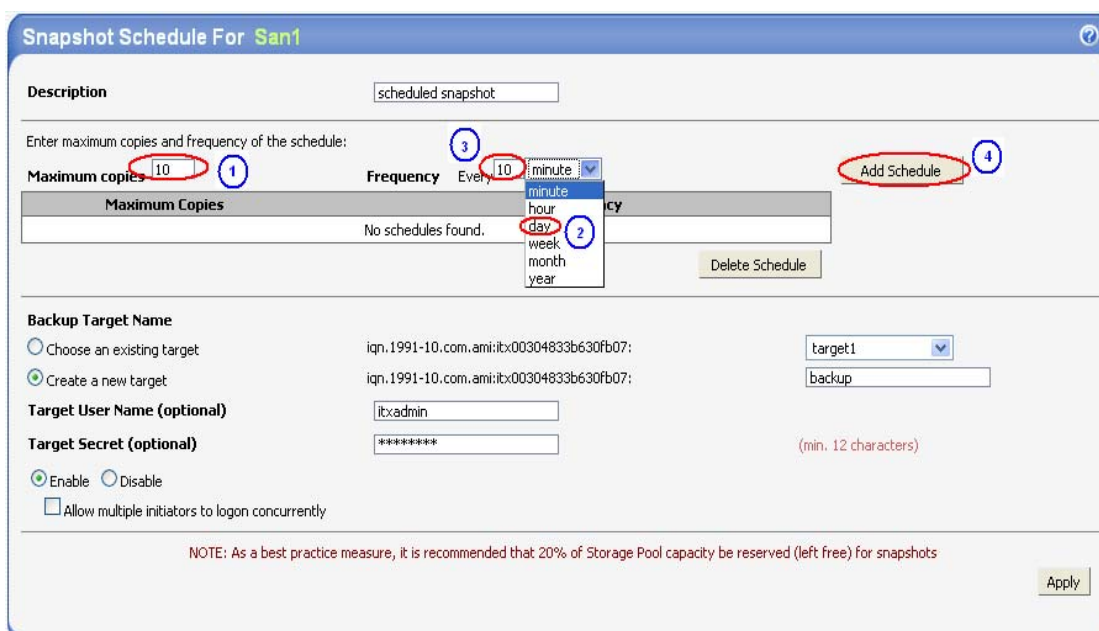
Figure 13: Scheduling a snapshot

Figure 14: Configuring a Schedule

Click the 'Apply' button to update the schedule information.

Rollback

Rolling back a snapshot is the process of bringing back the volume to a previous state. To rollback both SAN and NAS Volumes, the following procedure is followed.

1. Go to the list of snapshots, select a snapshot to which the system is to be restored and click on 'Rollback'. Once 'Rollback' is initiated, all snapshots taken after that time will be lost.
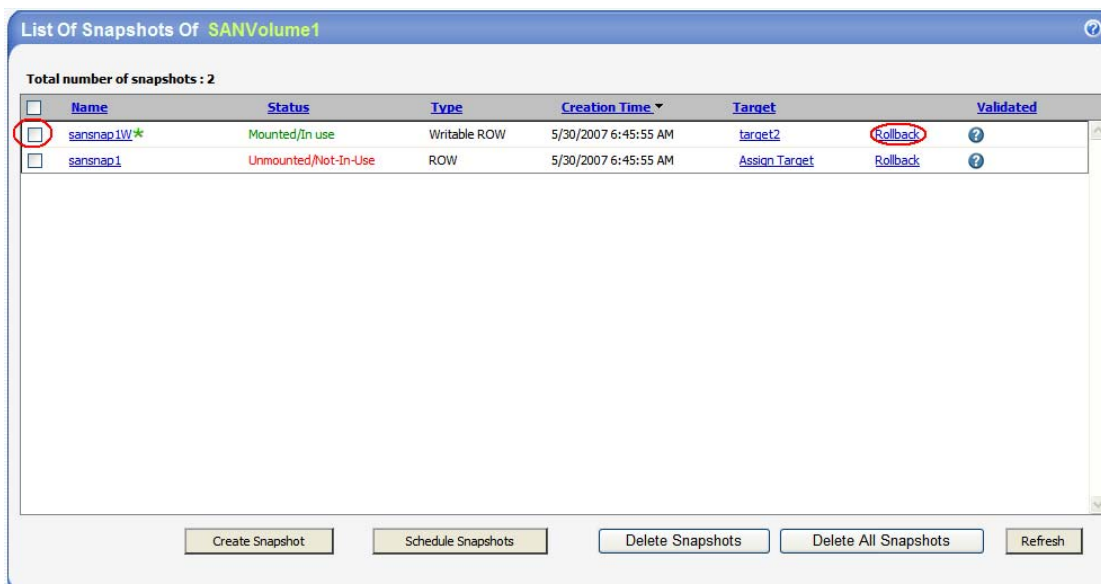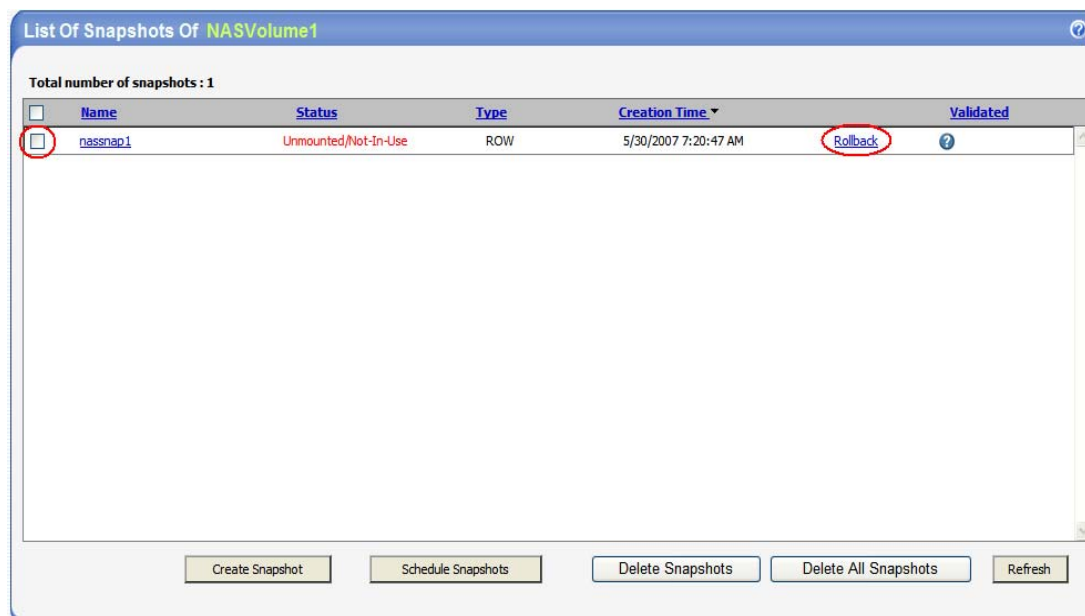

Figure 15: SAN Volume Rollback

Figure 16: NAS Volume Rollback

Snapshots in Synchronous Replication

There are two ways to take snapshots in the Synchronous Replication (SR) mode – Manual and Automatic Scheduling. Snapshots can be taken manually on both the local and remote machines independently. The machines maybe *in-sync* or *out-of-sync*. But if scheduled, the snapshots will be taken only if both the machines are *in-sync*, i.e. only if their connection is established. If they are *out-of-sync*, then no snapshot will be taken on either machine. Also, it is important to configure the same scheduling pattern on both the local and remote machines to maintain consistency. This has to be done individually on both machines, as ManageTrends does not support automatic remote scheduling.

Manual Snapshots on Remote Machine

Before creating Snapshots on the remote machine, ensure that both the local and remote machines are *in-sync*.

1. If the local machine is connected to a remote replica, then the Snapshot Management Window will look as in Figure 23.
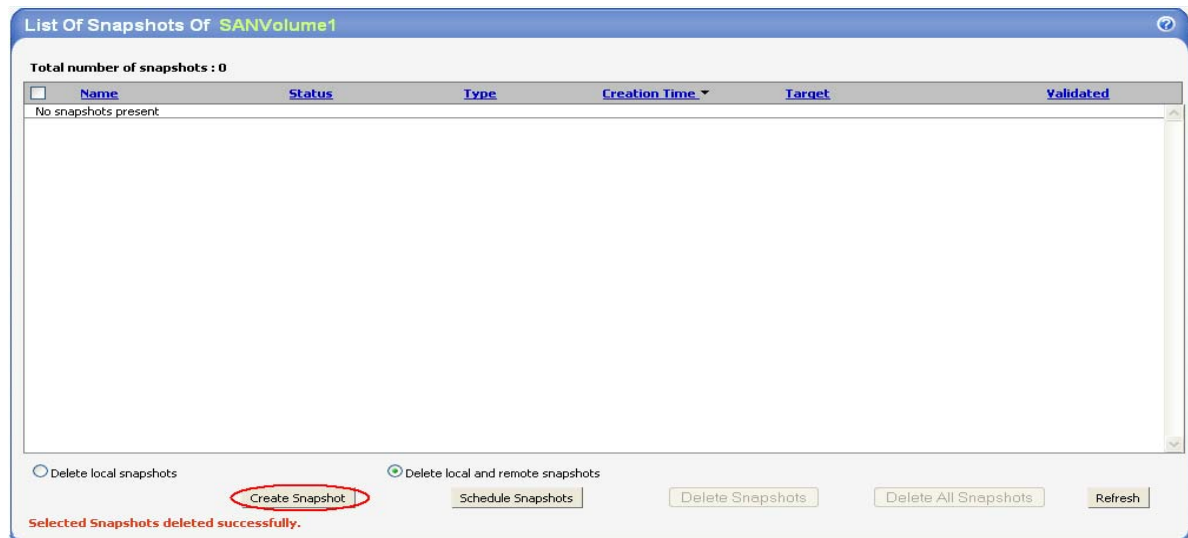

Figure 17: Snapshot Management Window

2. To create a snapshot on a remote machine, choose 'Create local and remote snapshot' option in the Create Snapshot window.
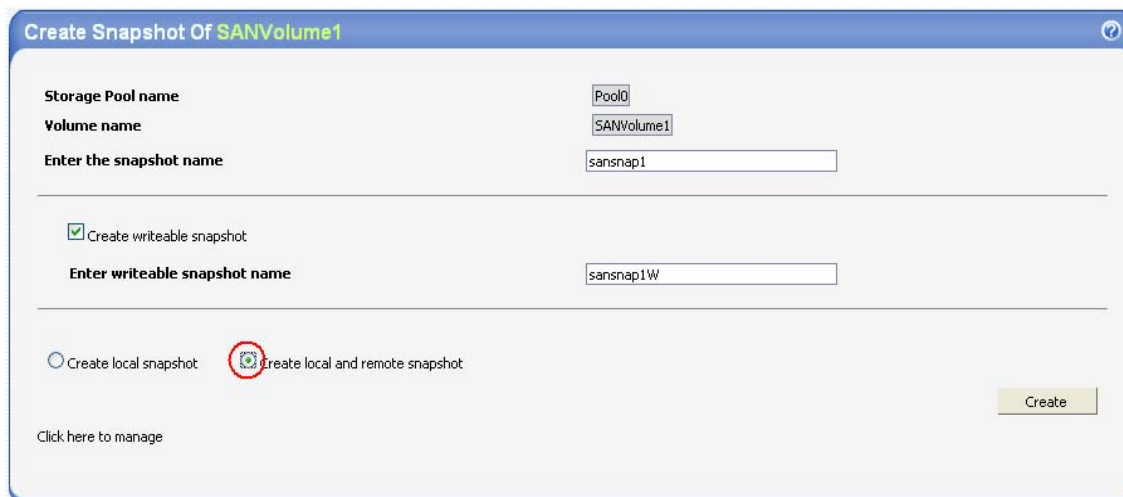

Figure 18: Creating Remote Snapshots

Verify that the snapshots are created on both the local primary and the remote secondary machine.

Scheduling Remote Snapshots

Snapshots have to be scheduled individually on both the local and remote machines. The procedure is similar to that elaborated in the earlier section.

Snap Validation

After Snapshots are created, Snap validation must be enabled manually to start validating the snapshots. Remember that the NAS volumes' snapshots can be validated locally, but SAN volumes can only be validated with a remote connection either with Synchronous Replication or Snap-Assisted Replication.

1. For NAS Snapshots, the validation can be enabled from the 'NAS Volume Management' window. Click on 'Enable Snap Validation'. The validation can be paused at anytime using the 'Pause' button.
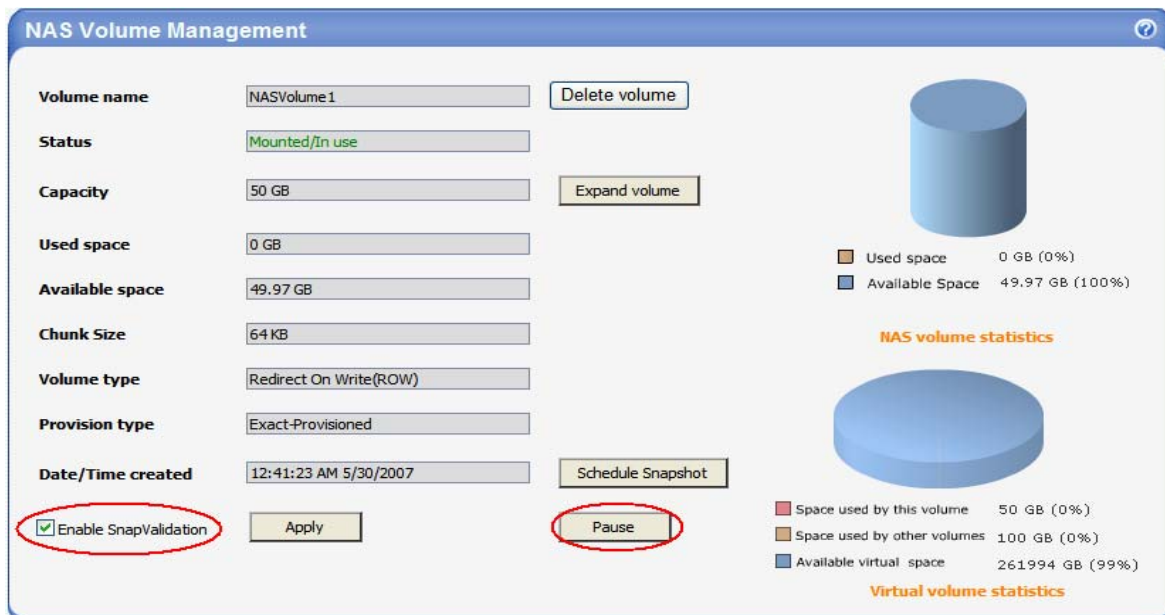
Figure 25: Enabling Snapshot Validation for NAS Volumes

For SAN Volumes, snap validation is enabled from the Replication Management Window. Figure 26 shows an example of a Synchronous Replication Management Window.
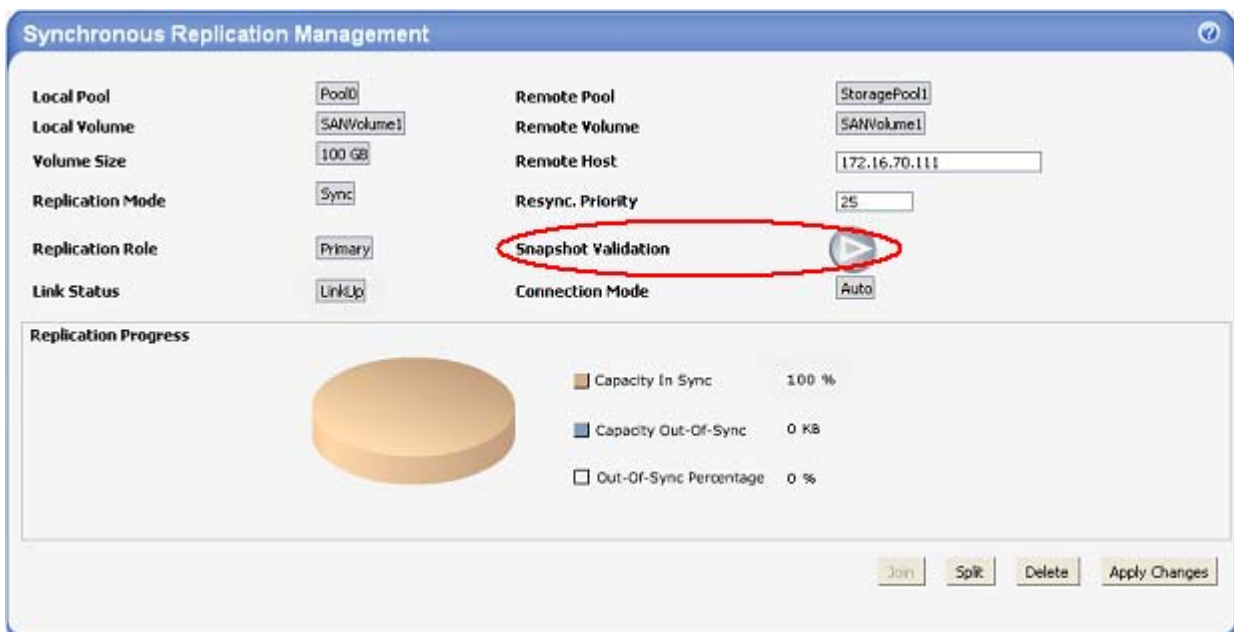

Figure 26: Enabling Snapshot Validation for SAN Volumes