Technical Brief

Introduction to SANWatch – Snapshot

Abstract

This document introduces the basic technology and features of SANWatch – Snapshot, how it addresses the problems about traditional way of data copying and recovery and its main uses.

Infortrend® Technology, Inc.

Networked Storage Solution Provider

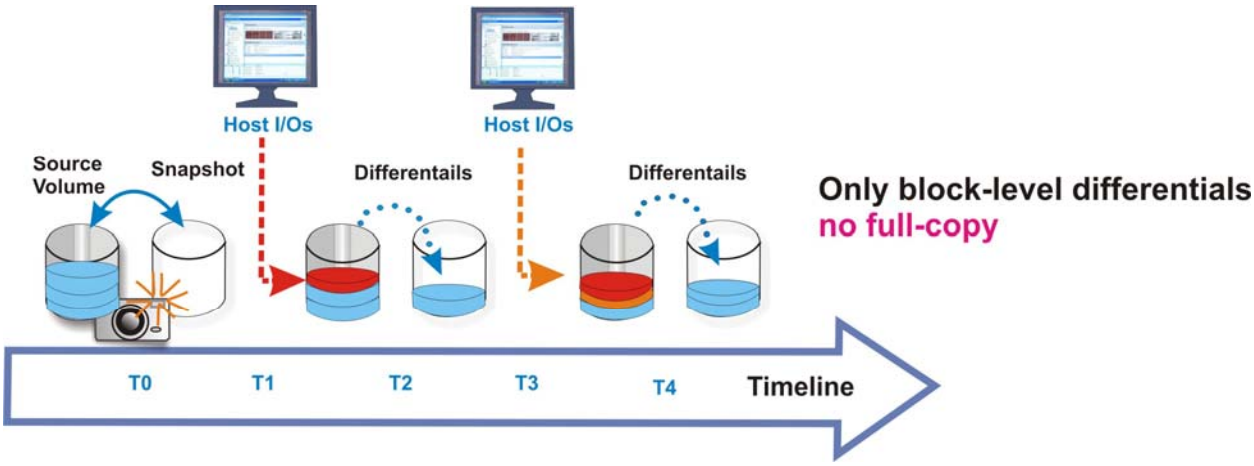
Revision 1.0

Aug, 2008

SANWatch-Snapshot Basics

Companies often need data copies for backup, testing, sharing, or analysis, which makes data copying a necessary and repetitive IT operation. Traditionally, to ensure data integrity and avoid degrading system performance, data copying is done when the application is shut down. In today's IT environments demanding 24x7, year-round uptime, suffering prolonged service interruption for full data copies is no longer an acceptable choice. Moreover, when the data copies are used for recovery, the copying operation has to be frequently done to set multiple recovery points. Culminating data replicas can rapidly consume company's storage capacity, further burdening the storage costs already made high by exponentially growing application data. The recovery time is also long. Extended application downtime, exhausted disk space, limited points of recovery and long recovery time – snapshot technology perfectly resolves these main problems of traditional data copying and recovery.

Snapshot is a point-in-time (PIT) copy of data. Instead of a full copy, it is a "picture" of what the data looks like. When a snapshot is initially created, no data is really copied so the snapshot-taking job can be done almost instantaneously. To ensure data integrity, the host data cache has to be flushed and the online application has to be temporarily suspended for the few seconds when the snapshot image is taken. This is a great improvement to the old data copying scenario where the application has to be brought off-line for hours, days or even weeks. Moreover, since SANWatch-Snapshot is storage-based, host CPUs don't have to contribute any computing power to creating and updating snapshot images. After the snapshot image is created, the snapshot software will use the copy-on-write (COW) technology to copy the changed data blocks of the source volume (the data protected by snapshot) before the write happens and store them in the snapshot container (the reserved space for snapshot image storage). Since only data block differentials are stored, snapshots consume much less capacity than full copies.



Management Features

Through SANWatch's user-friendly GUI, leveraging snapshot benefits is as simple as point-and-click. To free IT managers from the trouble of repeatedly taking snapshots by hand for routine backup operation, SANWatch-Snapshot also provides scheduling functionality. The centrally-managed scheduler allows users to flexibly set the interval at which they want snapshots to be automatically taken in a specified duration. The intervals can be set by hours, days, weeks and months. When the schedule is functioning, users can still manually take snapshots for specific source volumes anytime they want.

Complemented by the Prune action, the scheduler of SANWatch-Snapshot automates not only snapshot-taking but also snapshot-removing. By configuring the Prune policy of a snapshot schedule, users can control when the snapshot images taken by this schedule should be removed. Prune policy can be based on the maximum snapshot image count or snapshot lifespan. For example, if users set the maximum image count as 20 and there have already been 20 snapshots, when the 21th snapshot is created according to the schedule, the oldest snapshot will be automatically erased so that the maximum threshold count won't be exceeded. If the snapshot lifespan is set as 5, all the snapshots taken more than 5 days ago will be automatically removed.

Besides timing, ensuring there is enough space for the taken snapshots is another important concern. Using up snapshot container capacity can lead to snapshot failure. SANWatch-Snapshot provides a space management feature - Purge - for users to monitor and control the capacity of snapshot containers. The Purge action is triggered by a capacity threshold value on a specific snapshot container. Users can choose issuing alerts, removing the highest purge priority snapshot images or failing the following snapshot-creating operation as the purge control action. The system will automatically take the action when the designated capacity threshold is violated. Purge

priority is determined by the Purge policy parameters users set. Purge policy can be configured as either the minimum number of snapshot images or the life span of individual snapshot images. For example, if the capacity threshold is set as 80% and the Purge policy is configured as the one-week life span of snapshot images, when the taken snapshot images consume over 80% of the snapshot container space, all the snapshots created more than an week ago will be removed. If the capacity threshold is set as 80% and the Purge policy is configured as the minimum number of snapshot images as 20, when the taken snapshot images consume more than 80% of the snapshot container space, the snapshots will be removed until there are only 20 images left in the snapshot container. The older a snapshot is, the higher its purge priority is.

Uses of SANWatch-Snapshot

The two main uses of SANWatch-Snapshot are the enhancement of full backup (whether local or remote) and timely recovery. In the traditional backup scenario, the production volume is severely impacted because it is the direct source reference for the copying operation. When snapshot technology is introduced into the backup process, the point-in-time copies can replace the production volume's role as the direct source reference, thus minimizing the performance degradation applications suffer for backup. Moreover, the duration of service disruption is greatly reduced from hours, days or weeks to seconds.

Compared with full data copies, snapshot images as differential copies are much more space-efficient. They can be frequently created to serve as multiple points of recovery without much burdening the storage capacity. There are two levels of recovery: file-level and block-level. File-level recovery mainly helps restore the files maliciously modified or accidentally deleted because of human errors. The restoring process is as simple as mapping the snapshot image to the host as a "virtual volume", copying the original of the deleted or modified file in the "virtual volume," and then pasting it to the source volume. However, in the case of system/application malfunction and virus attacks, file-level recovery may not be able to bring the system back to its normal state. In such cases, users need the help of block-level rollback. If a user takes a snapshot image at 8:00 and some system/application errors occur in 8:15, he/she can choose to make the whole system rollback to the state it was at the time when the snapshot was created – 8:00. During the rollback operation, the up-to-date volume remains accessible. Snapshot enables instantaneous data protection at fine granularity.