Snapshot Technology for GuardianOS™

Snapshots and How to Use Them With The GuardianOS Platform

Introduction

In the digital age, an ever-increasing percentage of a company's critical business data is stored electronically. With prohibitively high costs of network and data downtime, high availability of this critical asset is a necessity for any network infrastructure. This data must be well protected to enable easy and rapid recovery in the event of a file loss, data corruption, or user error. Snap Server™ by Adaptec, built on GuardianOS by Adaptec provides storage solutions designed to protect a company's data assets with its integrated proprietary snapshot technology.

Overview

GuardianOS Provides Powerful, Flexible Snapshot Technology

The snapshot implementation of GuardianOS enables users to take instant, disk-based point-in-time images of any volume on a GuardianOS-powered Snap Server. Key features of a snapshot include:

Key Features

- **Instant virtual volume** — The snapshot instantly captures a copy of the live volume.
- **Point-in-time image** — The snapshot is a virtual image of the live volume as it appeared at the point-in-time when the snapshot was captured. It creates a nearly instant map of pointers to the actual blocks of data found in the live volume.
- **Disk-based storage** — The snapshot images are stored entirely on disk. Blocks of data that have not changed since the completion of the snapshot remain in the live volume, while the original contents of data blocks that have changed are stored in designated "snapshot" spaces.
- **Sustained client access to the live volume** — With the exception of a momentary pause as the live volume is frozen and captured in the snapshot image, network clients maintain read/write access.
- **Read-only access to the snapshot volume** — Users have read-only access to the individual snapshot volumes. Since these snapshot images are true point-in-time copies of live volumes, users cannot manually modify them, protecting the snapshot from inadvertent user error.
- **Performance maintained during concurrent snapshots** — The GuardianOS server can accommodate multiple concurrent snapshots per unit while continuing to maintain optimal performance.

How It Works

Creation of Point-in-Time Images

The snapshot technology utilizes an optimized copy-on-write implementation to create point-in-time images of the live volume. When a snapshot is initiated:

1. The snapshot technology momentarily "quiesces" or freezes the live volume.
2. The virtual copy of the live volume is near-instantly created, as a database of pointers to the actual blocks of data (which presently exist in the live volume) is created.

3. When client-initiated write requests are made, the snapshot technology intercepts these requests, reads the data in the soon to-be-overwritten blocks, and saves the "original data" in the snapshot volume (Figure 1).
4. After a copy of the original data is made, the client-initiated write requests are completed (Figure 1).

   Please note that for simplicity's sake, Figure 1 shows only one snapshot volume, implying that only one snapshot is created. In the event that multiple snapshots are created and maintained concurrently, a separate snapshot volume exists for each individual snapshot image.

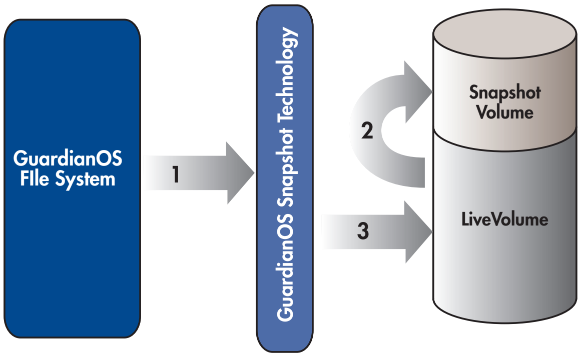


Figure 1. *GuardianOS Snapshot Copy-on-Write Operation*
1. Client-initiated write request
2. Original content of the soon-to-be overwritten blocks are saved to the snapshot volume
3. Write request is committed to live volume

5. Further write requests to the live volume trigger steps 3 and 4, as a copy of the original data is made when new write requests are initiated.

   Please note that if the volume receives further requests to overwrite blocks of data which have already been overwritten and the original contents have already been captured in a snapshot volume, those requests will be ignored by the snapshot subsystem. Instead, only the very first overwrite of a set of data blocks will trigger the copy-on-write operation described above.
6. Upon receiving client requests to read the contents of individual snapshots, the snapshot technology simply substitutes the original data blocks for the changed data blocks (Figure 2).

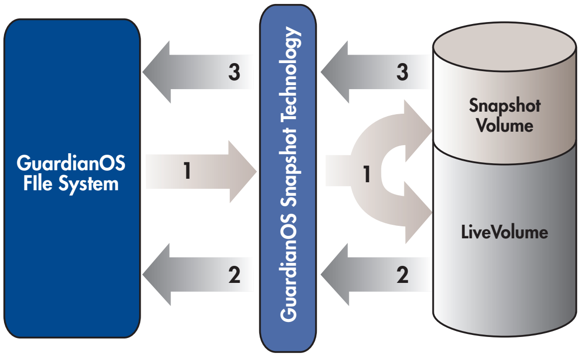


Figure 2. *GuardianOS Snapshot Copy-on-Write Operation*
1. Client-initiated request to read data from a snapshot image
2. Data blocks that have not changed are read from the live volume
3. For data blocks that have changed, the original contents of the blocks are retrieved from the snapshot volume

Applications

High-Performance/High-Availability Storage Solutions for Demanding Environments

When deployed in any given application or environment, the GuardianOS storage solution's optimized snapshot implementation provides:

Online backup. Each snapshot is a consistent image or virtual copy of the live data volume at a given point in time. The GuardianOS snapshot technology enables users to maintain multiple concurrent snapshot images as online disk-based archives. Furthermore, each of these snapshot images may be shared for user access, and subsequently backed up to tape or alternate media for archival purposes.

An elegant means of side-stepping the backup window. In traditional network environments, the network administrator performs regular backups of critical server data to tape for both backup and archival purposes. Typically, this includes any combination of daily incremental backups and weekly/monthly full backups. To minimize business impact, the daily backup operations are usually performed, with the servers taken offline, during non-business hours, or the so-called "backup window."

In today's global marketplace, information systems infrastructure and digital business assets must be made available 24x7. The cost of downtime can be prohibitive, particularly in the e-commerce, financial, and banking industries. When network storage is deployed in such transaction- and/or I/O-intensive applications, the protection of digital business assets and valuable data is more crucial than ever before.

The GuardianOS snapshot implementation provides the means to elegantly sidestep the backup window by allowing network administrators to more quickly and easily perform daily incremental backups and weekly/monthly full backups to tape. The snapshot images of the volume can be backed up throughout the course of the day as needed. Because snapshots are chained, system performance is maintained whether a volume contains one snapshot or many. In addition, all of the snapshot backup and archival operations are transparent to users.

Instant recovery of user data. The GuardianOS snapshot technology enables the storage and maintenance of multiple snapshot images. Each of these snapshot images remains available online as a disk-based archive. Furthermore, the network administrator can configure each snapshot image to be shared over the network. This enables individual users read-only access to the snapshot images from which they can copy any inadvertently modified, deleted, and/or corrupted user data and files back into the live volume.

Offline volume for reporting and revision testing. The snapshot volume contains the collection of all completed and active snapshots. Third-party or SRM-provided reporting of storage trends by volumes, file types, and applications may be run on individual snapshot images. This enables the administrator to proactively monitor storage utilization and plan for data growth, while removing the access contention and performance overhead associated with running reports on a publicly accessed live volume. The ability to maintain a collection of snapshot images, corresponding to multiple points-in-time, makes the snapshot technology ideal for revision management and testing. Multiple copies of software code or documentation can be easily tracked, maintained, accessed, and audited for testing purposes.

Benefits

Reducing Costs While Enhancing Data Availability

Regardless of the application and the environment in which the GuardianOS-based solution is deployed, it is easy to see that snapshot technology provides many real benefits to administrators and end users. These benefits include:

- **Increased availability of both storage resources and user/system data.** The use of multiple snapshots as online backups provides maintenance of multiple, consistent copies of data at various points-in-time.
- **Enhanced protection of critical data.** The use of both snapshots as disk-based "virtual volumes" and regular incremental backups of daily snapshots to tape provides multiple levels of protection for critical business data.
- **Instant recoverability of user and system data from disk.** This capability provides time-to-data advantages over traditional data retrievals from tape. Users and network administrators can recover specific data from disk-based snapshots almost instantly.
- **Lower total cost of ownership (TCO); higher return on investment (ROI).** The increased uptime, availability of critical business assets and user access to data translates into higher user productivity. The easy administration and use of snapshots for a myriad of applications further contribute to lower TCO and increased ROI.

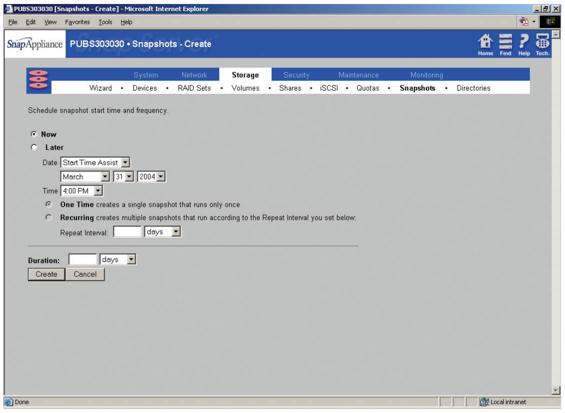
How To Create Snapshots

Simple, Flexible Implementation

Set up snapshots for on-demand or scheduled execution (Figure 3). The administrator has control over the following options:

- **Name** of the snapshot.
- **Source Volume to Snapshot.** The administrator can specify any available volume.
- **Start Date and Time** to the nearest half hour.
- **Repeat Intervals** to schedule recurrence and frequency. Multiple concurrent snapshots can be maintained, enabling an administrator to keep up to approximately two weeks' worth of daily and weekly snapshots.
- **Duration** of the individual snapshots. The administrator sets a snapshot's lifetime or duration, at the end of which the individual snapshot is automatically deleted to conserve storage capacity. This is typically used to dispose of older snapshots that have been properly backed up to tape.
- **Create Recovery File** to capture volume attributes and settings. This enables the administrator to capture volume settings and extended attributes such as ACLs and quotas.

Note that optimal performance and the number of stored snapshots depends on size of the snapshot storage pool the administrator has created and the amount of data being backed up. That said, many administrators have found the optimal balance between data protection and storage space to be roughly 15-20 concurrent snapshots.


PUBS303030 [Snapshots - Create] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
SnapAppliance
PUBS303030 • Snapshots - Create
Home
Find
Help
Tech.
System
Network
Storage
Security
Maintenance
Monitoring
Wizard • Devices • RAID Sets • Volumes • Shares • iSCSI • Quotas • Snapshots • Directories
Create
Cancel
Done
Local intranet

Schedule snapshot start time and frequency.

● Now

○ Later

Date: Start Time Assist; March 31 2004

Time: 4:00 PM

● **One Time** creates a single snapshot that runs only once

○ **Recurring** creates multiple snapshots that run according to the Repeat Interval you set below:

Repeat Interval: days

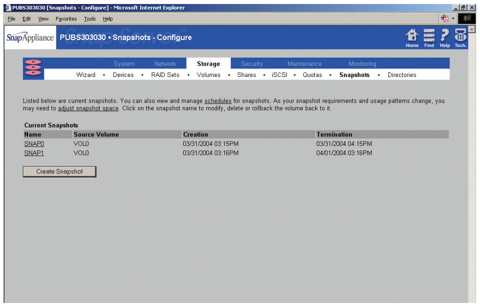
Duration: days

Figure 3. *GuardianOS Snapshot Scheduling*

Restoring Data From Snapshots

Accessing Snapshots/Instant Data Recovery

Once completed, snapshots are listed in order of creation, with a display of pertinent information (Figure 4). Completed snapshots can be accessed by the network administrator and any clients with appropriate security. The network administrator first needs to create a network share, named SS_Share1 by default, of the snapshot volume, corresponding to the network share, Share1, of the live volume. When viewed from Windows Explorer, the contents of the share SS_Share1 appear as shown in Figure 5. Should administrators or end users experience data loss from data corruption or user error, they can simply copy the needed data from the last available snapshot back into the live volume.


PUBS303030 [Snapshots - Configure] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
SnapAppliance
PUBS303030 • Snapshots - Configure
Home Find Help Tech.
System Network Storage Security Maintenance Monitoring
Wizard • Devices • RAID Sets • Volumes • Shares • iSCSI • Quotas • Snapshots • Directories
Create Snapshot

Listed below are current snapshots. You can also view and manage schedules for snapshots. As your snapshot requirements and usage patterns change, you may need to adjust snapshot space. Click on the snapshot name to modify, delete or rollback the volume back to it.

Current Snapshots

Name	Source Volume	Creation	Termination
SNAP0	VOL0	03/31/2004 03:15PM	03/31/2004 04:15PM
SNAP1	VOL0	03/31/2004 03:16PM	04/01/2004 03:16PM

Figure 4. *View of Current GuardianOS Snapshot*

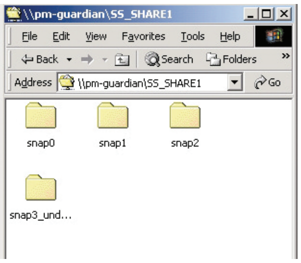

\\pm-guardian\SS_SHARE1
File Edit View Favorites Tools Help
Back Search Folders
Address \\pm-guardian\SS_SHARE1 Go
snap0
snap1
snap2
snap3_und...

Figure 5. *GuardianOS Snapshots Viewed in Windows Explorer*

Snapshot Backup Strategies

Easy Integration With Your Existing Data Protection Plan

Backing Up a Snapshot. An integral part of a company-wide data protection plan, the snapshot technology lends itself readily to providing both online backups and subsequent backups to tape. Using the network backup software (BakBone NetVault [included with OS], VERITAS NetBackup/Backup Exec, Legato NetWorker, or CA ARCserve) and a tape product of choice, the administrator may continue to do weekly and/or monthly full backups to tape on the weekends. On all other days of the week, they can perform daily incremental backups of the snapshot volume to tape.

In the example on the previous page, the network administrator can do weekly full backups to tape every Saturday at 12:00 a.m. Assuming that the weekly full backup requires up to 48 hours to complete, they can create daily snapshots of the live volume: snapshots snap0, snap1…through snap5, which are captured at precisely 12:00 a.m. on Monday, Tuesday…through Friday.

Since the snapshot process can take as little as a fraction of a second to complete, the administrator can safely initiate daily incremental backups of the snapshot volume any time after 12:00 a.m. on each of those days. Once configured for daily recurrence, the incremental backup job will automatically backup individual snapshots: snap0 on Monday, snap1 on Tuesday, etc. Consequently, the daily backups can take up to 24 hours to complete, enabling the administrator to sidestep the "backup window."

Restoring Data from Tape. To restore data from tape, administrators can simply use the backup software to select individual or groups of folders/files for restoration to the live volume. They can do so by using the latest backup job to find the required data for restoration. It may be necessary for the administrator to set the target for the redirection of the data restoration; by default, most backup software restores data to the original location. Since administrators (and end users) have read-only access to the snapshot volume, they must restore the data to the live volume instead.

Using snapshots with NDMP. An NDMP backup operation automatically initiates a snapshot. If the snapshot pool does not have sufficient space to file the new snapshot, it will create space for it by removing the oldest snasphots.

Using snapshots with iSCSI. It is not recommended that snapshots be used to backup iSCSI volumes.

Conclusion

Speeding Data Recovery While Minimizing Costs and Complexity

Storage solutions powered by GuardianOS provide snapshot technology. This easy-to-use yet powerful feature enables the capture of point-in-time images of the live volume to provide the network administrator with a means for effectively eliminating or sidestepping the backup window and give all users instant recoverability of lost or corrupted data. This feature, along with hardware component redundancy, enhanced system security, high performance, fault tolerance, and ease-of-deployment and administration contributes to the overall system and data reliability, availability, and serviceability. As a result, companies can achieve low TCO and high ROI.

adaptec®

691 South Milpitas Boulevard
Milpitas, CA 95035

888.343.7627 Tel
408.262.2533 Fax

Information supplied by Adaptec, Inc., is believed to be accurate and reliable at the time of printing, but Adaptec, Inc., assumes no responsibility for any errors that may appear in this document. Adaptec, Inc., reserves the right, without notice, to make changes in product design or specifcations. Information is subject to change without notice.

P/N: 986650-013 Printed in U.S.A. 02/07 4657_4.9