WORM Storage on Magnetic Disks Using SnapLock® Compliance and SnapLock Enterprise

TR-3263 | Updated July 2007

Mark Hayakawa, Sr. Product Partner Engineer - Network Appliance

TABLE OF CONTENTS

Abstract

Many businesses rely on some usage of WORM (write once, read many) data storage to meet regulatory compliance or simply to add another layer to their data protection roadmap. This document will discuss the integration of Network Appliance™ storage systems into environments that require WORM data storage.

1. Introduction

Many businesses rely on some usage of WORM (write once, read many) data storage to meet regulatory compliance or simply to add another layer to their data protection roadmap. Why have so many companies implemented WORM data storage given the myriad of data storage options available? There are two primary reasons:

- Regulatory agencies recognize the ability of WORM data storage in ensuring the permanence of archived data and therefore often stipulate only non-erasable, non-rewritable WORM storage be used for meeting their regulations.
- Businesses place a premium on protecting certain business records or critical data files from accidental or intentional alteration or deletion, and WORM functionality such as non-erasable and non-rewritable data storage can ensure long-term data permanence.

Other existing WORM implementations are based on older media technology with limited storage capacity, slow data throughput, and substantial management overhead. Existing WORM storage options are optical WORM platters, which each hold about 30GB of data, and WORM tape, with each cartridge able to store 50GB of data (best case storage numbers based on latest technology). Traditional WORM storage vendors have gotten around capacity limitations of individual media by implementing expensive, complex media library and jukebox solutions that house numerous pieces of media. Although this solution addresses capacity limitations, it creates a problem of ever-increasing management overhead for the volumes of full media removed from the library or jukebox, and not to mention data loss when tapes are misplaced or lost.

To address issues faced by growing business requirements for WORM data storage and alleviate issues inherent with traditional WORM storage solutions, NetApp introduced SnapLock on its NearStore® and Fabric Attached Storage (FAS) systems SnapLock allows companies to implement the data permanence functionality of traditional WORM storage in an easier to manage, faster access, low-cost magnetic disk-based solution. As technology has improved, the lineage for WORM data storage started with paper and microfiche, progressed to optical, and has now arrived at a new best-of-breed solution: NetApp NearStore and FAS systems configured with SnapLock Compliance and SnapLock Enterprise software for high levels of data integrity and retention and low TCO (total cost of ownership).

2. SnapLock Overview

2.1. What Are SnapLock Compliance and SnapLock Enterprise?

Both SnapLock software products provide non-erasable, non-rewritable WORM data permanence functionality utilizing high-throughput magnetic disk drives in a cost-efficient, highly available RAID configuration. From a data protection perspective, the process of committing data to WORM status on either SnapLock product can be thought of in the same manner as storing data on an optical platter. Like an optical platter "burned" with data, both SnapLock software products protect data committed to WORM status from any possible alteration or deletion until their retention period has expired.

Although SnapLock Compliance and SnapLock Enterprise data permanence is analogous to traditional optical WORM media, comparisons end there. SnapLock offers performance and reliability improvements over traditional WORM storage while reducing both maintenance overhead and TCO. SnapLock Compliance and SnapLock Enterprise are implemented as add-on licenses to Data ONTAP®. Both SnapLock software products run on the NetApp NearStore near-line storage solution, which features lower cost ATA-based drives, and on higher performance FAS system, featuring fiber-attached disk drives. This flexibility allows customers to buy the amount of storage that fits their business needs for SnapLock WORM storage, whether it be a few hundred gigabytes or hundreds of terabytes of data. In addition, and to highlight this flexibility further, SnapLock Compliance or SnapLock Enterprise can be combined on the same appliance with traditional NetApp read-write volumes.

SnapLock Compliance was designed to assist organizations in implementing a comprehensive archival solution for meeting SEC regulations for data retention. Records and files committed to WORM storage on a SnapLock Compliance volume cannot be altered or deleted before the expiration of their retention period. Moreover, a SnapLock Compliance volume cannot be deleted until all data stored on it has passed its retention period.

SnapLock Enterprise is geared toward assisting organizations with meeting self-regulated and best practice guidelines for protecting digital assets with WORM-type data storage. Data stored as WORM on a SnapLock Enterprise volume is protected from alteration or modification with one main difference from SnapLock Compliance. As the data being stored is not for regulatory compliance, a SnapLock Enterprise volume can be deleted, including the data it contains, by an administrator with root privileges on the FAS system containing the SnapLock Enterprise volume.

2.2. SnapLock Implementation

2.2.1. Data ONTAP

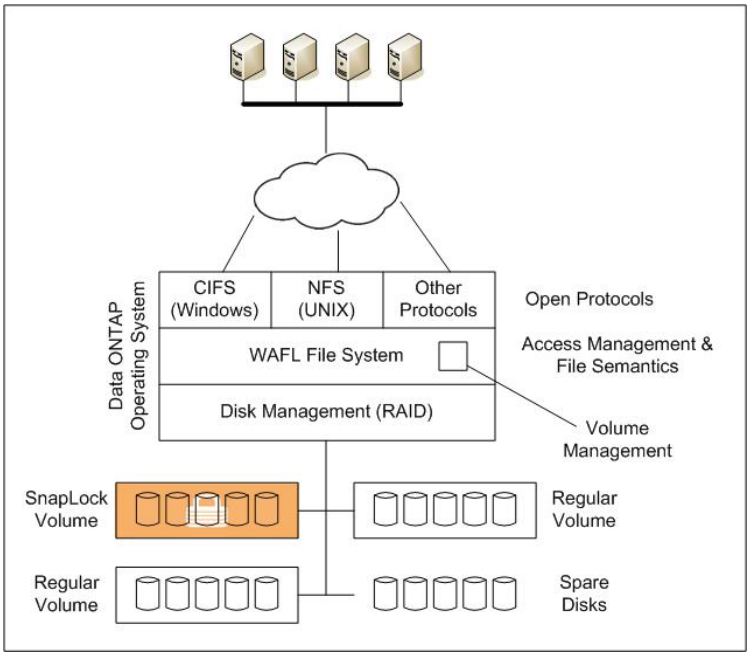


Figure 1 - Data ONTAP

SnapLock Compliance and SnapLock Enterprise are extensions to the NetApp Data ONTAP operating system. Data ONTAP provides a complete infrastructure for storage, including RAID

protection for data, a suite of tools and products to promote high data availability, and open protocol connectivity for data access. The same hallmarks of Data ONTAP, such as ease of deployment, ease of management, and ease of administration, also apply to both SnapLock software products. To learn more about Data ONTAP, please read information at www.netapp.com/products/filer/ontap.html.

2.2.2. Network Appliance Storage Appliances

The NetApp family of storage systems allows enterprises to pick configurations that fit business needs, including capacity, performance, and fault tolerance. Providing coverage on the storage product line and configuration options is outside the scope of this paper. To learn more about NetApp products and solutions geared for enterprise storage needs and business continuance, please contact your existing NetApp sales representative or use the contact information resources at www.netapp.com/company/contact.html.

Additional information about the NetApp storage systems and software products can be obtained at the NetApp Website for product information: www.netapp.com/products.

2.2.3. Network Appliance SnapLock

SnapLock provides the capability to ensure that when data is committed to WORM state it cannot be altered or deleted. SnapLock is implemented at the volume level, and a single NetApp storage appliance can support combinations of traditional and either SnapLock Compliance or SnapLock Enterprise volumes. Companies can leverage this flexibility to allocate WORM and non-WORM storage on a storage appliance to fit their unique business requirements. The data permanence capabilities built into both SnapLock products, while innovative and simple to administer, do necessitate some best-practices guidelines for initial and ongoing testing, volume creation, and ongoing volume maintenance and support. These best-practice guidelines will be covered later in this paper. Both SnapLock software products utilize CIFS and NFS open protocols to store and access archived data. One of the core NetApp value propositions is that of open connectivity to data without requiring use of a closed, proprietary API. This methodology provides easier access to data and simpler integration between application vendors and storage vendors. The open protocol aspect of SnapLock provides a natural and flexible way to manage, store, and retrieve data via regular CIFS and NFS clients.

2.2.4. SnapLock Feature Availability

The SnapLock product was initially implemented as a license-based feature available starting in Data ONTAP version 6.4.1. Newer features of SnapLock have been added to subsequent releases of Data ONTAP. The following table describes the new features that have been added by release.

Data ONTAP Release	Feature	Comment
7.0	Secure ComplianceClock™	The ComplianceClock feature is implemented as a software clock to eliminate the possibility of prematurely expiring a retention period by maliciously adjusting the system clock.
7.0	Files can be deleted with expired retention periods	ComplianceClock must be initialized Cannot revert to a prior Data ONTAP release if ComplianceClock is initialized and a SnapLock Compliance volume present.

Data ONTAP Release	Feature	Comment
7.0	Minimum, maximum, and default retention periods on traditional or flexible volumes	Volume-enforced retention period limits established as well as default retention period. This is to ensure that an application cannot set a retention period outside of a specified range, and Data ONTAP will set the retention period to the default if no retention period is specified.
7.0	Destroy SnapLock Compliance volumes	If all of the files on the SnapLock Compliance volume have expired, then the SnapLock Compliance volume can be destroyed. Previously a SnapLock Compliance volume could not be destroyed.
7.0	For FlexVol®, the SnapLock type is a property of the aggregate	An aggregate can be SnapLock Compliance or SnapLock Enterprise. A FlexVol will inherit the SnapLock attribute of the underlying aggregate.
7.1	LockVault™	Integration between SnapVault® and SnapLock. LockVault is implemented with a secure compliance log to track LockVault activity.
7.1	Appendable WORM files	Blocks are locked as they are written to specially defined appendable WORM files. Additional blocks can be appended to file after initial writing.
7.1	QSM resync no longer a hidden feature	QSM resync was a hidden feature in the previous release.
7.1	SnapLock Compliance and SnapLock Enterprise supported on the same appliance	SnapLock Compliance and SnapLock Enterprise volumes can now coexist on the same appliance for greater flexibility.
7.1	Support for infinite retention dates and retention dates beyond 2038	Retention periods can be calculated with an additional wraparound capability that will allow retention periods to 2071.
7.2	New option to autocommit files to SnapLock	The new option snaplock.autocommit_period enables a storage system to automatically commit files to WORM status after they have not been changed for a specified period of time. The time can be specified as (none|time[h|d|m|y]). Note that this option is enabled for all SnapLock volumes present on the FAS system.

3. Using SnapLock

SnapLock Compliance is available starting with Data ONTAP 6.4.1 and SnapLock Enterprise with Data ONTAP 6.5. If your storage appliance has an older version of Data ONTAP, please follow your company guidelines for obtaining an upgrade (normally handled through the Network Appliance NOW™ site at http://now.netapp.com). Included at the NOW site are detailed instructions for downloading and installing the Data ONTAP upgrade on your NearStore appliance.

3.1. Licensing SnapLock

Licensing SnapLock Compliance or SnapLock Enterprise can be added through the GUI-based FilerView® software, a console session, or a telnet session to NearStore. From FilerView, first select the Filer tab, select Manage Licenses, scroll down to the appropriate SnapLock option, and enter your license. From the console or telnet session, enter the command

Filer> license add license_code

SnapLock Compliance and SnapLock Enterprise are different licenses. Prior releases would only allow one of the two to be active on a storage appliance at any one time. As of Data ONTAP 7.1 the appliance can have both types of SnapLock volumes enabled at the same time. A SnapLock volume forever maintains the rules and policies of the particular SnapLock license that was indicated when the volume was created. In other words, a SnapLock volume created with an active SnapLock Compliance license will always retain the rules associated with SnapLock Compliance. This protection holds even when a SnapLock volume is created with an active SnapLock Compliance license and then a SnapLock Enterprise license is made active on the appliance or the SnapLock license is removed.

3.2. SnapLock Volume Creation

After a storage appliance has been licensed with SnapLock Compliance and/or SnapLock Enterprise, the steps below show various aspects of a SnapLock volume, including creation and attempted destruction, operations such as WORM commits, attempted deletion or modification, and overall ease of use. Some thought and planning are required to optimize reliability and performance on your NearStore appliance, and this information is contained in the Best Practice guidelines section later in this document.

Creating a SnapLock volume can be done either through the FilerView GUI or by command line method below. After a session is established, use the following command:

filer> vol create snap_vol -L -r 6 6

Using the -L switch in the above command creates a SnapLock volume called **snap_vol** with a RAID group size of six drives and initial volume of six drives. RAID groups and volume size will be covered further in the Best Practices section.

Next, ensure the SnapLock volume is available and online.

filer> vol status

Volume	***State***	***Status***	***Options***
vol2	***online***	***normal***	***raidsize=6***
vol1	***online***	***normal***	***raidsize=6***
snap_vol	***online***	***normal***	***snaplock***
vol0	***online***	***normal***	***root***

If the status returned for the new SnapLock volume is "growing," then the FAS system is still in the process of creating it. To monitor the progress of the volume creation on a percentage-completed basis, use the ***vol status -d snap_vol*** command.

3.3. SnapLock Volume Usage

NetApp SnapLock WORM protection works at the individual file level. Committing a file to WORM on a SnapLock volume for both Microsoft® and UNIX® environments requires a two-step sequence:

1. Through a CIFS share or NFS mount, copy or create a file with write permission on a SnapLock volume.
2. Change permission on the file to read-only.

The two-step process for triggering a WORM commit can be manual for testing purposes or scripted for an in-house archival application development. In most enterprises, applications will drive the archival process and perform the WORM commit process. The SnapLock commit action occurs after a transition from a writable to a read-only state no matter who owns the file or which user carried out the SnapLock trigger operation. Once the commit of a file to SnapLock state occurs, any modification or deletion attempt will fail, even from traditional superuser accounts, until the file's retention period has expired. Even after a file's retention period has expired, it still cannot be modified, only deleted or have its retention date extended. Conversely, files created on or copied to a SnapLock volume, but not having the WORM commit steps, can be modified or deleted in accordance with permissions set on the file.

Please note that creating a file or copying a read-only file to a SnapLock volume does not trigger the WORM commit operation required for SnapLock data protection unless the SnapLock autocommit option is enabled. If the autocommit option is enabled, a time period is specified as the amount of time before a file is automatically committed to WORM using the volume default retention period.

An important consideration for SnapLock storage is how directories are treated. Directories, once created on a SnapLock volume, cannot be renamed regardless of their access permissions. This is an important consideration when using the Microsoft Explorer tool to create a new folder. The first step Explorer takes is creating a directory called New Folder, then attempts afterward to rename this to something more useful, which is not possible on a SnapLock volume. Manually creating directories on SnapLock volumes in either the Microsoft or the UNIX environment is better handled using ***mkdir*** in a command line interface. While directories cannot be renamed, they can be deleted as long as no files committed to WORM state are contained within their hierarchy.

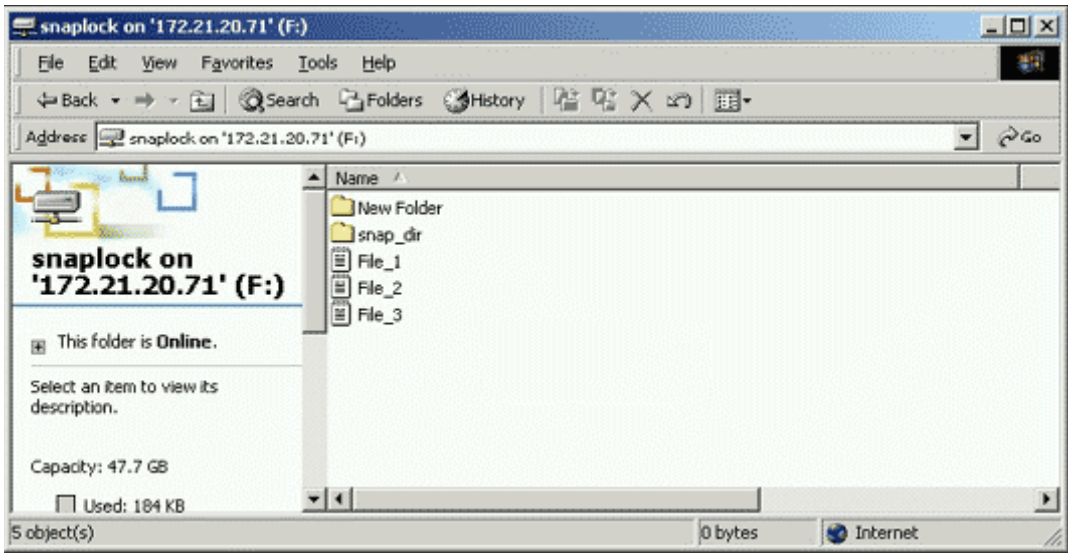
Applications certified to support SnapLock execute the required actions to create directories, archive files to the SnapLock volume, set the retention dates (retention dates are covered in the next section), and then execute the WORM commit. The above background is provided to assist with a conceptual understanding of the SnapLock process in an application-driven archival solution.

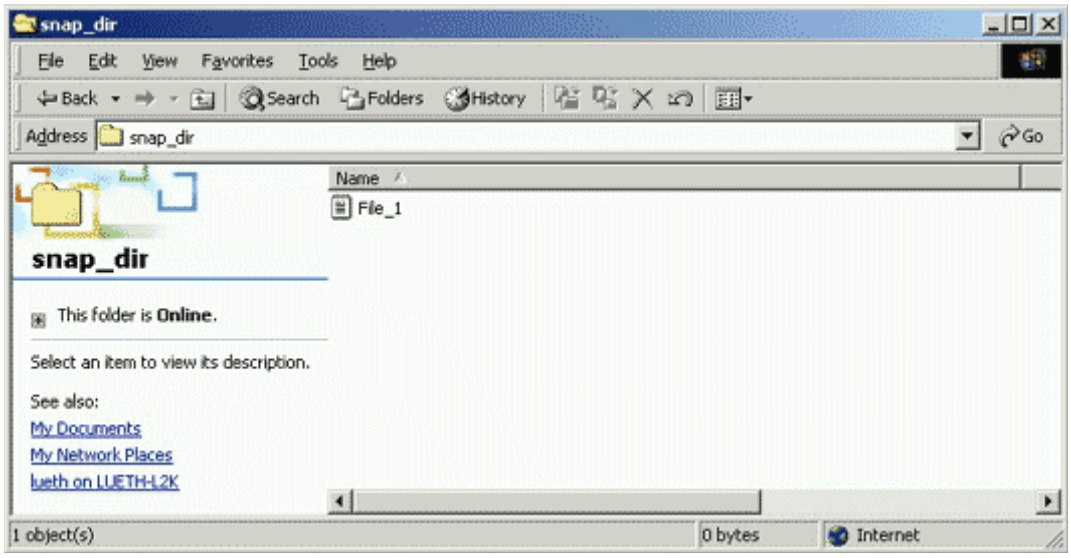
3.3.1. SnapLock Usage: CIFS and Microsoft Environment

In order to map a SnapLock volume on Microsoft software-based servers, first configure CIFS share information on the storage appliance (please note CIFS is a license-based option under Data ONTAP). From a telnet or console session run the command:

filer> cifs shares -add snap_vol /vol/snap_vol

Alternatively, this can also be performed through the GUI-based FilerView by going to ***CIFS-Shares-Add*** and sharing the SnapLock volume. Once the SnapLock volume has been shared, it can be mapped using Explorer. the following is an example of the results after the above steps have been performed:

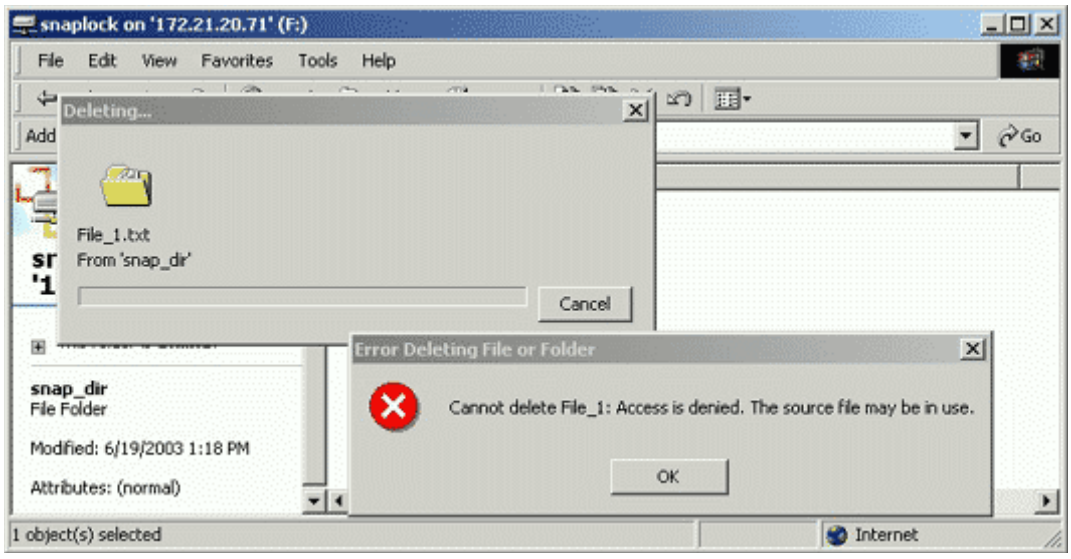




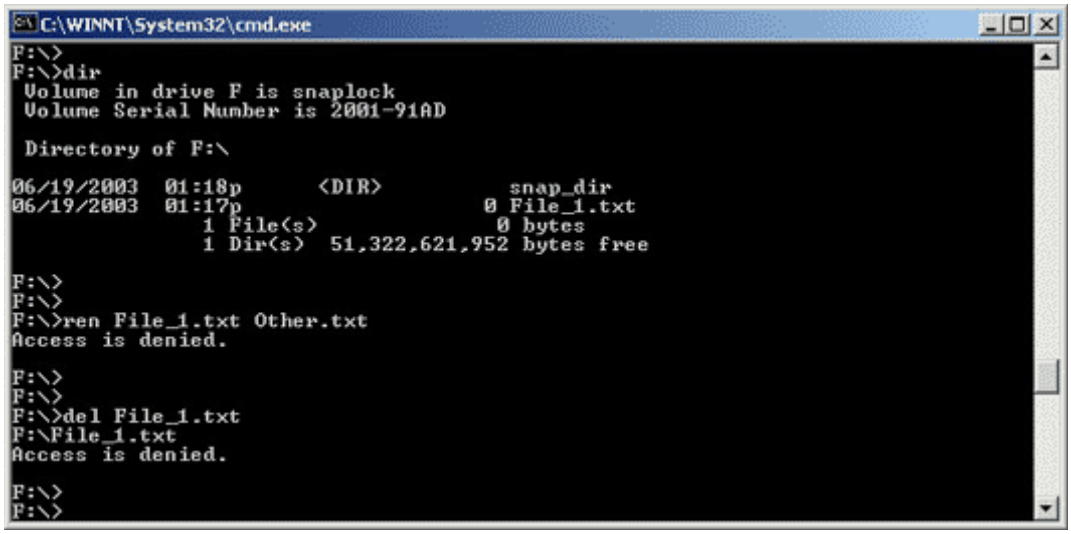
Here is a description of the directories and files in the above SnapLock volume.

1. New Folder has been manually created using Explorer to highlight an issue covered earlier. There are no additional files under its hierarchy.
2. **snap_dir** was manually created by command line interface using the ***mkdir*** command and contains one file under its hierarchy, named File 1.txt, that has been committed to WORM state (as seen in the second Windows® Explorer screen shot above).
3. File 1 was manually committed to WORM state by having its permissions manually changed to read-only after it was already copied to the SnapLock volume.
4. File 2 and File 3 were manually set to read-only before being copied to the SnapLock volume and thus have not been committed to SnapLock WORM storage.

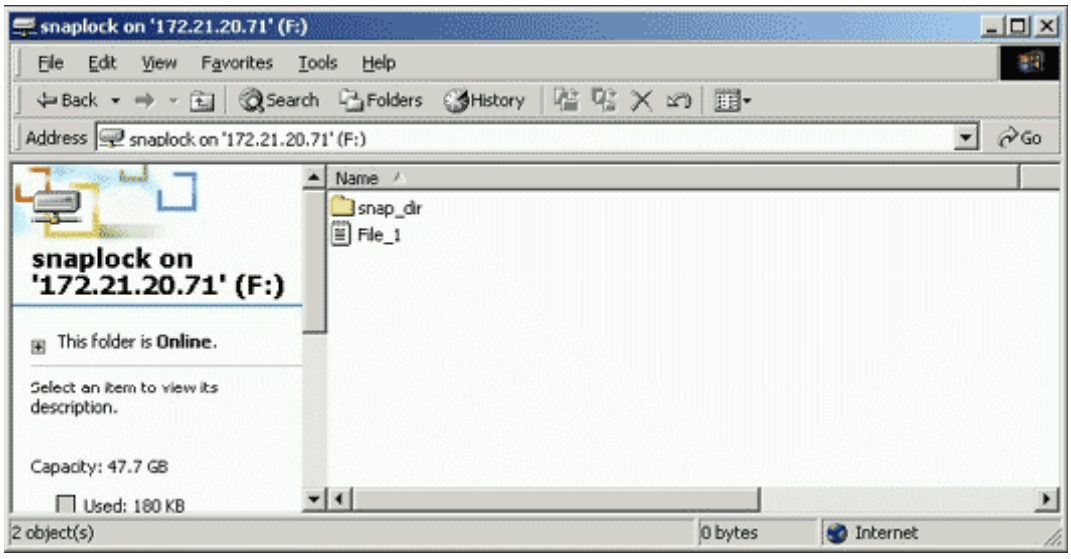
Next, deletion or modification will be attempted on all directories and files above with results displayed below. Based on file and directory conditions in 1 through 4 above, it will be helpful to try to predict what the outcomes of these actions will be. Attempting to delete the **snap_dir** directory that contained a file committed to SnapLock yielded this message:

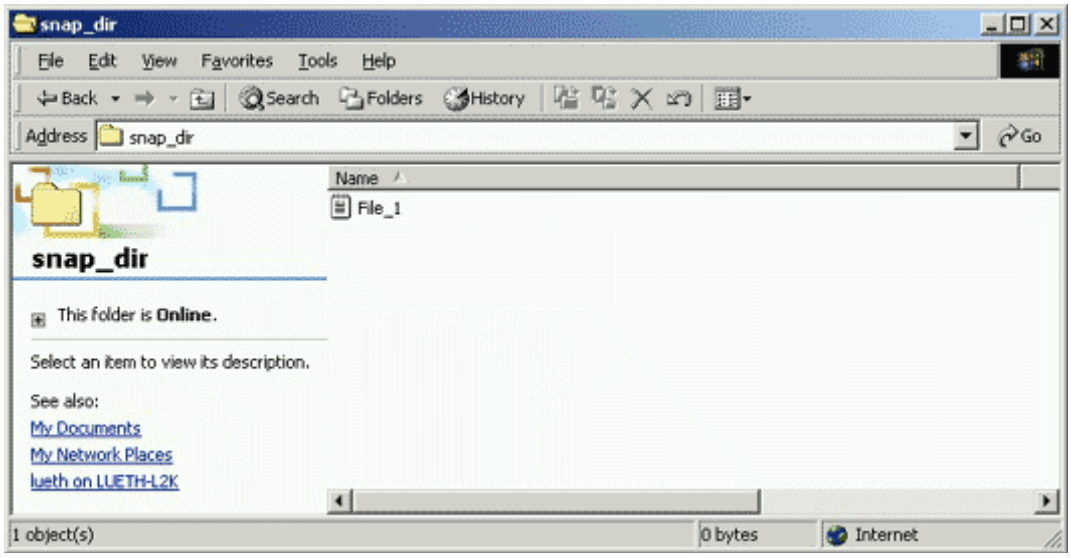


Attempting to delete or rename File 1.txt that was committed to WORM state yielded these error messages:



Final results on attempts to delete or modify files and directories on the SnapLock volume:



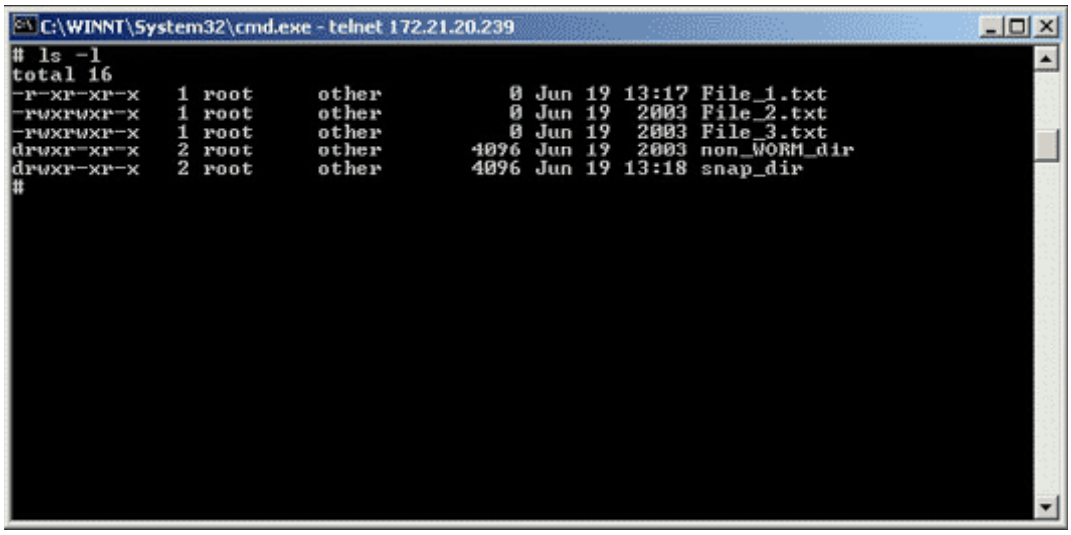


3.3.2. Sample SnapLock Usage: NFS and UNIX Environment

In order to mount a SnapLock volume on UNIX system-based servers, first configure NFS export information on the storage appliance (please note NFS is a license-based option under Data ONTAP). From a telnet or console session run the command:

filer> exportfs -i -o anon=0 /vol/snap_vol

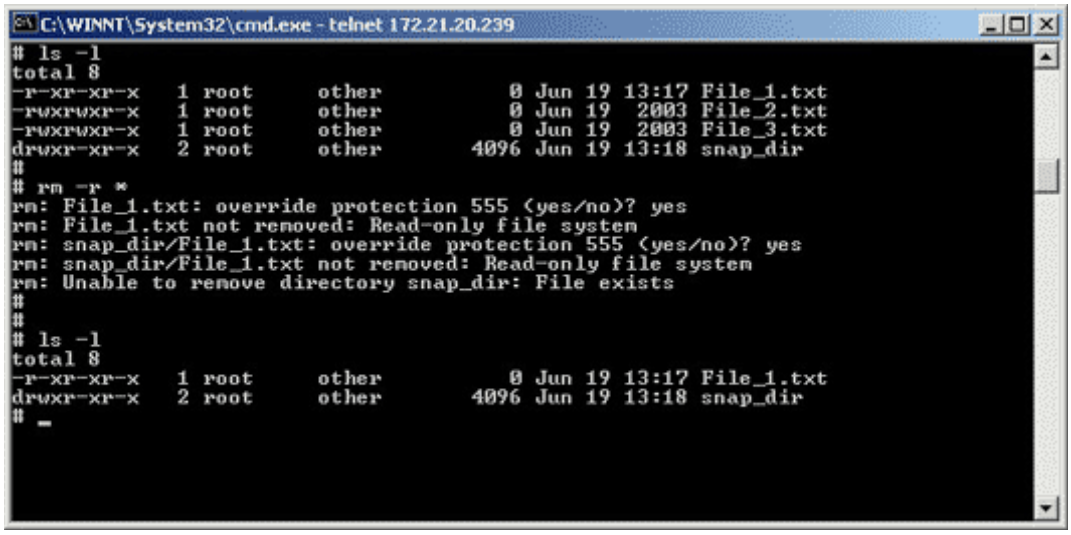
To make the export permanent, modify ***/etc/exports*** on the NearStore appliance or use the FilerView GUI. In FilerView, go to NFS => Manage Exports and enter information about the volume to be exported, and then select Apply and Export All. After the volume has been exported, it can be mounted by UNIX servers. Here is an example after the above steps have been performed:



Here is a description of the directories and files in the above SnapLock volume.

1. **non_WORM_dir** was manually created using ***mkdir*** and contains no additional files under its hierarchy.
2. **snap_dir** was manually created using ***mkdir*** and contains one file under its hierarchy, named **File 1.txt**, that has been committed to WORM state.
3. **File 1.txt** was manually committed to WORM state by having its permissions manually changed to read-only after it was already copied to the SnapLock volume.
4. **File_2.txt** and **File_3.txt** were manually set to read-only before being copied to the SnapLock volume and thus have not been committed to SnapLock WORM storage.

First, **File_2.txt** will be committed to WORM state. Then deletion or modification will be attempted on all directories and files above with results displayed below. Again, based on file and directory conditions in 1 through 4 above, it will be helpful to try to predict what the outcomes will be. Here are results of attempts to alter or delete files or directories given the above conditions:



3.4. Using Retention Dates with SnapLock Compliance

A record retention date is the date after which Data ONTAP will permit the deletion of a WORM file on a SnapLock volume. SnapLock allows for association of a retention period for each record or file, and the retention period must be set before committing the file to SnapLock WORM storage. Using retention dates on SnapLock requires adding one more step to the steps covered earlier for the SnapLock WORM commit operation (additional step is step 2 below):

1. Copy a writable file to a SnapLock volume via CIFS or NFS.
2. Update the last access time field for the file using whatever programming language supports this activity. Typically C is used. Optionally, the field can be left blank, and the default retention period assigned to the SnapLock volume will be used.
3. Commit the file to SnapLock WORM storage by changing its permissions to read-only.

Once the retention period has been set and the SnapLock commit operation has occurred, Data ONTAP enforces retention of these records until the retention dates of the records have expired. After the retention period for a record or file has expired, the disposition of the records will automatically change to allow deletion, but not modification, of the records. Data ONTAP will never autonomously delete any records, including ones with expired retention dates. Instead, all deletions of files with expired retention dates must be handled by the application or some other process such as a script or batch job. SnapLock will also allow the extension of file retention dates further into the future to allow records to be retained beyond their original retention period. SnapLock will not allow record retention periods on files to be shortened.

3.4.1 Setting Record Retention Dates with SnapLock

In keeping with the SnapLock open protocol design, support for record retention periods was implemented without need for the use of proprietary APIs or protocols. Record retention dates can be set and queried programmatically through standard system call interfaces supplied by most operating systems or interactively via standard command line tools. As with SnapLock operations, operations for setting retention dates occur over standard network file system interfaces such as NFS and CIFS. This flexibility allows applications to utilize SnapLock from compiled code or scripts without the requirement for any libraries or software to be installed on the client systems.

The retention date for WORM records on a SnapLock volume is stored in the last access timestamp of the record file metadata. To set a retention date for a WORM record, the application must explicitly set the file last access time to the desired retention date before setting the file to read-only and engaging the WORM commit operation. Once committed to WORM state the access time of the file is immutable with the only exception being for extending the record retention period.

3.4.2. Record Disposition after Retention Period

Once the retention date of a WORM record has been reached, Data ONTAP will permit applications to change the record permissions back to writable from read-only, then allow the record to be deleted. Data ONTAP will not allow any alteration or modification on the SnapLock record when back in a writable state. The only action allowed at this point is to delete the record or set a new retention date and change the record to read-only to reengage SnapLock WORM protection.

3.4.3. Permanent SnapLock WORM State

Prior to release 7 of Data ONTAP, a record committed to WORM state on a SnapLock volume without having a retention date explicitly set in the last access time would, by default, receive an infinite retention period and would have been kept indefinitely by SnapLock. With version 7 of Data ONTAP, a file that is committed to WORM without a retention date set will use the snaplock_default_period value for the volume it is residing on. The snaplock_default_period for a

SnapLock Compliance volume is set to the snaplock_maximum_period, which is by default 30 years. The snaplock_default_period for an SnapLock Enterprise volume is set to the snaplock_minimum_period, which is by default 0 years. For this reason it is very important to carefully verify that the application is correctly setting the retention periods of records before committing them to WORM state.

3.4.4. Secure Time Mechanism: ComplianceClock

For the purposes of regulatory compliance, Data ONTAP utilizes the ComplianceClock secure time mechanism, which will operate independently from the regular real time clock of the storage system. This will permit the FAS system to be synchronized with the time base of the facility for correct operation of CIFS and NFS yet still provide a secure mechanism via which regulatory compliance can be assured for retained records.

ComplianceClock is a software-based clock that, once set, is independent of the system clock. The ComplianceClock value is set only once on the NetApp storage system, so be sure that the system clock is accurate. The ComplianceClock value is stored on all of the disks that compose the aggregates and volumes on the NetApp storage system; both SnapLock and non-SnapLock. This is to ensure that tampering with the system clock by resetting the clock value will not affect the release timing of the retention period of a locked file. The movement of the disks that compose the SnapLock volume to another FAS system that has the system clock surreptitiously changed will not affect the release timing of the retention period of locked files on the moved SnapLock volume. If the disks are moved to another FAS system that does not have the ComplianceClock value set, Data ONTAP will automatically start ComplianceClock and assign the value of the oldest ComplianceClock time on the disks introduced to the NetApp storage system.

The ComplianceClock value is updated on a regular basis for all volumes that are online, and all of the values are compared against one another. The value that is the furthest back in time is used as the current ComplianceClock value, and all of the ComplianceClock values are updated accordingly. This is to ensure that any tampering with the system clock, disks, or volumes is not propagated to the other ComplianceClock values on the NetApp storage system.

If a volume is taken offline for any reason, the ComplianceClock values on the disks that make up the volume are not updated, as they are only updated while the volume is online. When the volume is brought online or the disks are moved to another system, the ComplianceClock value that is loaded in memory will be adjusted based on the oldest ComplianceClock value on the disks brought online.

To mitigate some of the drift in the ComplianceClock value, WAFL® will catch up the ComplianceClock value to the system clock at a rate of one week a year. This is to allow for some volume downtime during the year.

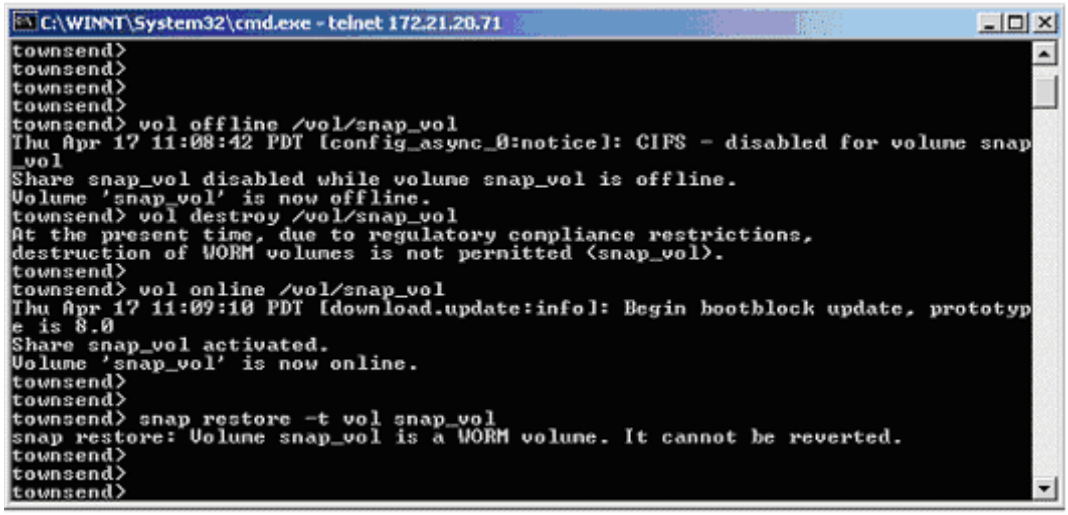
3.5. Differences between SnapLock Compliance and Non-SnapLock Volumes

Three minor differences exist between Data ONTAP commands used for configuration and administration of NetApp SnapLock Compliance volumes versus non-SnapLock volumes. One difference, adding the -L switch to the ***vol create*** command, was covered earlier when a new SnapLock volume was created. Provided the active SnapLock license is SnapLock Compliance, the command used to create SnapLock Compliance volume was:

filer> vol create snap_vol -L -r 6 6

Two other commands, ***vol destroy*** and ***SnapRestore***, are modified from carrying out their normal actions on SnapLock Compliance volumes. The reason for modifying the ***vol destroy*** command is straightforward, since allowing SnapLock Compliance volume destruction by a command violates the concept of WORM storage, especially in the regulated data archived space. The ***vol destroy*** command will only succeed on a SnapLock Compliance volume if all data with retention periods has expired and been removed from the volume. If any file exists on the SnapLock volume and its retention period has not expired, then a SnapLock volume cannot be destroyed.

The reason for modifying SnapRestore® commands on SnapLock Compliance is probably less straightforward but becomes apparent if the outcome of reverting to a previous Snapshot™ copy were allowed to successfully complete. SnapRestore operations are extremely valuable for file and data recovery or reverting to a previous known good state. In the case of SnapLock Compliance volumes, allowing a SnapRestore recovery to a previous state incurs a loss of all data written since the Snapshot copy was created. While this scenario is not as dramatic as the results of a ***vol destroy*** operation, the net result of an unacceptable loss of WORM data is the same. Here are results of attempts to destroy or perform a SnapRestore command on a SnapLock Compliance volume:



3.6. Differences between SnapLock Enterprise and Non-SnapLock Volumes

There is only one difference between Data ONTAP commands used for configuration and administration of NetApp SnapLock Enterprise volumes versus non-SnapLock volumes. As covered in the previous section, provided the SnapLock license active is the SnapLock Enterprise version, the command used to create a SnapLock Enterprise volume is:

filer> vol create snap_vol -L –r 6 6

Two other commands covered in the previous section about SnapLock Compliance, the ***vol destroy*** and SnapRestore commands, work the same on SnapLock Enterprise as they do on traditional NetApp volumes. An administrator can either restore a SnapLock Enterprise volume back to a previous state contained in a Snapshot copy or delete the volume.

4. Best Practices for SnapLock

4.1. Be Mindful of the ComplianceClock

The ComplianceClock is an independent clock from the system clock that is software based and updated by Data ONTAP. Make sure that all volumes, both SnapLock and non-SnapLock, on a FAS system with ComplianceClock enabled are taken offline for only brief periods. When a volume is offline, the ComplianceClock values on the disks that comprise the volume are not updated. When the volume is brought back online, the ComplianceClock value is adjusted accordingly and will be reset based on the length of time that the volume was offline. Additionally, disks from NetApp storage systems that have had their ComplianceClock enabled should not be reused on other NetApp NearStore or FAS systems to ensure that an invalid ComplianceClock is not propagated.

4.2. SnapLock Compliance Testing

IT organizations implementing new, comprehensive archival solutions that include application software and storage on a SnapLock Compliance volume often require testing from the proof-of-concept stage through final acceptance. Even after the acceptance milestone has been reached, future testing may arise as a natural part of upgrade efforts to any piece of the archival infrastructure. Testing an application that will use SnapLock Compliance volumes can have potential hazards. The SnapLock Compliance volume by nature cannot be destroyed until the retention period of all the files residing on the volume have expired. If the retention period is set for a long period by mistake, the disks that make up the SnapLock Compliance volume will not be available for reuse until the all of the retention periods have expired. There are ways to mitigate this.

4.2.1. Using Physical Volumes

For both initial and ongoing testing, storage administrators can establish a permanent dedicated test volume consisting of two drives. There is a slight performance hit to having a small volume of this size. However, testing and certifying interoperability between various components of the archival solution will not be impacted. When testing archival on a SnapLock Compliance volume, be sure that retention dates are set for each file or record. Files committed to SnapLock without having a retention date set are by default to a 30-year retention period and can not be removed before then. The SnapLock default retention period for the volume should be set to some value other than the default assigned when the volume was created. Once files archived during testing are deleted, the space used is available again, or, once all files have expired their retention dates and been deleted, the testing SnapLock Compliance volume can be deleted.

4.2.2. Using the NetApp Filer Simulator

Another method of testing SnapLock Compliance processes is to use the Data ONTAP simulator that is available on the NetApp NOW site. Simulators for several current releases can be found at http://now.netapp.com/NOW/cgi-bin/simulator. The simulator runs on a Linux® system and has all of the functionality of Data ONTAP found on FAS systems. ComplianceClock can be set, and SnapLock Compliance volumes can be created for testing purposes. Once the testing has completed, the simulator can be deleted, and the disk space that simulates the SnapLock Compliance volumes is returned to Linux. For more information on the use of the Data ONTAP simulator, please reference the accompanying documentation.

4.3. Creating and Growing Production SnapLock Volumes

NetApp recommends keeping SnapLock volumes small, then growing them as additional storage is required. Provided spare disks are available on the storage appliance, SnapLock volume sizes can easily and dynamically increased at any time. Following this recommendation will prevent an

inadvertent process from potentially filling up remaining space in a very large SnapLock volume with meaningless data having an infinite retention period. When growing production volumes, disks should be added to match the RAID group size rather than adding a single disk at a time.

4.4. Data Protection

Data ONTAP has numerous capabilities built in or available as add-on options to promote data protection and high data availability. However, attaining the levels of data protection mandated by regulatory agencies requires a more comprehensive enterprise storage strategy than using a single NearStore or FAS system. At a minimum, the following data protection strategies are recommended for consideration in a robust archival solution. Certainly, other options are available, and Network Appliance will work with customers to identify the best data protection strategy for their particular environment and needs.

4.4.1. Replication to Remote Site

For compliance with data retention rules, regulatory agencies may require a second copy of archived data be kept at a remote site. The most straightforward and natural way to comply with this requirement is to replicate data from a primary NearStore storage system or FAS system to a secondary NearStore storage system or FAS system in a separate location. There are two integrated NetApp solutions available to seamlessly perform data replication. The easiest and most robust solution is to use SnapMirror® in either synchronous or asynchronous mode to replicate data to a remote location. Asynchronous SnapMirror replicates SnapLock Compliance data to a remote NearStore or FAS system SnapLock volume while maintaining all aspects, such as date-time stamp and filename, including path, of the original WORM file. SnapMirror is an add-on license product available with SnapLock support. Synchronous SnapMirror is not supported with SnapLock Compliance volumes; however, for fully synchronous replication of SnapLock Compliance data, SyncMirror® can be used provided it is supported on the storage platform. The second solution, ndmpcopy, is a free utility and is already bundled with Data ONTAP. Like SnapMirror, ndmpcopy maintains WORM aspects of the original files in the replicated copy.

SnapMirror can replicate at either the volume or quota tree (also known as qtree) level. When replicating SnapLock Compliance data, NetApp recommends using SnapMirror with qtree replication rather than replicating at the volume level. The reason for using qtree replication is that it allows additional replication strategies, including the ability to resynchronize SnapLock Compliance volumes. Volume SnapMirror cannot restart the mirror because it would require that certain volume information be rewritten, violating the SnapLock Compliance model of not altering a locked volume. There may be special cases where this is acceptable; however, the risks must be carefully reviewed. Please contact your NetApp sales team to discuss SnapLock Compliance replication in further detail to determine which SnapMirror strategy best fits your business needs. Note that SnapMirror replication of SnapLock Enterprise volumes works the same as with traditional volumes.

4.4.2. Tape Backups

NearStore offers substantial performance improvement and storage capabilities for near-line data storage over optical or tape-based storage. Even so, tape backups or disk-to-disk VTL backups, including off-site tape rotation, are still a valuable part of an overall data protection strategy for enterprises. NetApp recommends that regulated data archived on a SnapLock volume also be backed up to another medium, whether it is tape or disk, using ndmpcopy to preserve the WORM aspects of the original files, if the SnapLock volume is not being mirrored with SnapMirror to another site. This is prudent to ensure that multiple copies of regulated data are available for redundant recovery scenarios. In most cases, a tape backup infrastructure including a backup application is already in place, and NearStore VTL can leverage the existing environment. To learn more about integrating tape backups with NearStore appliances, please review the following paper: www.netapp.com/tech_library/3149.html.

4.4.3. Physical Security

The level of protection afforded by each SnapLock product is such that only physical tampering can result in a loss of archived WORM data. In the same sense that an optical media platter can be physically destroyed, three or more drives in a RAID group used in a SnapLock volume can be removed from an appliance, then destroyed. In both cases, the storage media is only as resilient as the physical security of its location. NetApp storage appliances with SnapLock volumes should be housed in locked cabinets in a restricted area to minimize the risk of physical tampering.

4.4.4. Storage Resiliency

Other factors can help you make the SnapLock installation more resilient and productive. There is a paper that has many good suggestions about how to lay out the storage and provide for data resiliency in the NetApp document, Storage Best Practices and Resiliency Guide. It can be found at www.netapp.com/library/tr/3437.pdf.

4.5. SnapLock Volume Minimum, Maximum, and Default Retention Period Values

When a SnapLock volume is created, default values are set for the volume minimum, maximum, and default retention periods for files residing on the volume. The default values are as follows:

Option	SnapLock Enterprise Default	SnapLock Compliance Default
snaplock_minimum_period	0	0
snaplock_maximum_period	30 years	30 years
snaplock_default_period	Minimum period	Maximum period

These values are conservative values and will probably not reflect your company standards. It is recommended that these values be reviewed and reset to values that more closely reflect your company's retention policies. The commands to set these options are:

filer> vol options volume_name snaplock_minimum_period 2d
filer> vol options volume_name snaplock_maximum_period 2y
filer> vol options volume_name snaplock_default_period 30d

The snaplock_minimum_period value will not allow a retention period for a file residing on the volume to be set to a value less than the minimum period. If a file retention period is below the minimum value, the retention period will automatically be updated to the minimum. The snaplock_maximum_period value will not allow a retention period greater than the value set for the maximum period. If a file retention period is below the maximum value, the retention period will automatically be updated to the maximum. If there is no value specified in the retention period field, the default value is used.

4.6. Decru DataFort® and SnapLock

Customers most often want to encrypt data to comply with overlapping regulations, such as when regulatory compliance retention requirements conflict with privacy regulations. Customers may also want an additional layer of protection for expired and deleted compliant data.

Note that electronically shredding (either intentionally or accidentally) compliant data before its expiration may open a customer to litigation. A Decru® Lifetime Key Management™ server may be warranted in these installations.

Be aware that you cannot re-key data that has been committed to WORM state, due to the fact that it is immutable.

Also, no files named .decru should be copied to the root of the Cryptainer™ storage and committed to WORM state. The .decru file contains the Cryptainer key, and overwriting it and making the file immutable can interfere with the operation and recovery of the Cryptainer storage.

The .decru file does not contain the key itself. The key on the object being encrypted; it is an SHA512 signature that the Decru DataFort uses to locate the correct Cryptainer key, which is stored in the Decru DataFort and/or the Lifetime Key Management server.

4.7. Converting a SnapLock Enterprise Volume to a SnapLock Compliance Volume

The simplest way to accomplish this would be to use the volume copy command. The source volume is the SnapLock Enterprise volume and the destination volume must be an equivalently sized or larger Compliance volume. The volumes, other than the type of SnapLock volume (Enterprise or Compliance), should have the same attributes of min, max, and default retention periods specified. The volume copy command will retain the retention period attribute of the file in the Enterprise volume.

5. Summary

SnapLock Compliance and SnapLock Enterprise are designed to be critical pieces of a comprehensive data archival solution for businesses that require higher performance and lower TCO alternatives for WORM storage functionality. SnapLock benefits over traditional WORM storage include substantial improvements to performance, capacity, and reliability while significantly reducing management overhead. These benefits layer nicely for businesses needing WORM data storage for regulatory compliance or for protecting critical enterprise content beyond the capabilities of normal data storage.

The powerful data permanence and data integrity features of SnapLock combined with the low TCO driven by (1) leveraging existing NetApp Data ONTAP software and storage product line and (2) the use of open, industry-standard protocols for easier data access and application integration. Together these provide an unrivaled solution in the WORM data storage space. For more information on solutions-based products from Network Appliance, go to www.netapp.com/products.

6. Revisions

Status	Date	Author
New	December 2005	NetApp
Update	March 2007	Mark Hayakawa