Technical Report

Understanding SnapLock ComplianceClock

Mark Hayakawa, NetApp
Updates by Manish M Agarwal and Timothy Isaacs, NetApp
September 2009 | TR-3618

THE SECURE TIME MECHANISM IN DATA ONTAP

For the purposes of regulatory compliance, Data ONTAP® uses a secure time mechanism called ComplianceClock™, which operates independently of the regular real-time system clock of the storage system. This permits the FAS system to be synchronized with the time base of the facility for correct operation of CIFS and NFS, while providing a secure mechanism to enable regulatory compliance for retained records.

TABLE OF CONTENTS

INTRODUCTION

Many businesses rely on write once, read many (WORM) 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 to maintain the permanence of archived data and therefore often stipulate that only nonerasable, nonrewritable WORM storage be used for meeting their regulations.
- Businesses place a premium on protecting certain business records and critical data files from accidental or intentional alteration or deletion, and WORM functionality such as nonerasable, nonrewritable data storage can achieve long-term data permanence.

To address the issues faced by growing business requirements for WORM data storage and to alleviate the 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 of WORM data storage has progressed from paper and microfiche to optical and has now arrived at a new best-in-class solution: NetApp® NearStore and FAS systems configured with SnapLock Compliance and SnapLock Enterprise software for potentially high levels of data integrity and retention and low total cost of ownership (TCO).

1 COMPLIANCECLOCK: A SECURE TIME MECHANISM

ComplianceClock is a persistent software-based secure time base that, once set, is independent of the system clock. It’s important to make sure that the system clock is accurate when initializing ComplianceClock, because this can be done only once. This is so that no tampering with the system clock or with any one value can decrease the retention period of a locked file.

To initialize ComplianceClock, run the following command on Data ONTAP. You can use the current value of the system clock on Data ONTAP or specify another value.

```
netapp1> date -c initialize
```

The following warning appears, followed by a question:

```
*** WARNING: YOU ARE INITIALIZING THE SECURE COMPLIANCE CLOCK ***
You are about to initialize the secure Compliance Clock of this system to
the current value of the system clock. This procedure can be performed ONLY
ONCE on this system so you should ensure that the system time is set
correctly before proceeding.
The current local system time is: Mon Oct 13 23:21:36 GMT 2008
Is the current local system time correct? y
Are you REALLY sure you want initialize the Compliance Clock? y
Mon Oct 13 23:21:49 GMT [rc:info]: Compliance Clock initialized (via
"date") to Mon Oct 13 23:21:49 GMT 2008
Mon Oct 13 23:21:49 GMT [snaplock.clock.set:info]: The Compliance Clock
date and time have been set to 'Mon Oct 13 23:21:49 GMT 2008 '.
Compliance Clock: Mon Oct 13 23:21:49 GMT 2008
```

The current value of ComplianceClock can be found by using the command-line interface (`date -c`). The ComplianceClock time is stored in several areas in Data ONTAP. It is placed on disk in the header of all of the volumes (both SnapLock and non-SnapLock), on the NetApp storage system, and at an in-core location. Additionally, there is WORM information in the aggregate header and the RAID group headers associated with the SnapLock volume.

The movement of the disks that compose the SnapLock volume to another FAS system on which the system clock has been surreptitiously changed will not affect the release timing of the retention period of locked files on the moved SnapLock volume. The contents of disks composing the SnapLock volume cannot be destroyed by moving the disks to another FAS system, whether or not ComplianceClock has been initialized on the new system. If an entire aggregate is moved to another FAS system, then one of the following occurs:

- If the ComplianceClock time of the foreign aggregate is ahead of the ComplianceClock time of the system, the foreign aggregate's ComplianceClock time will be adjusted to match that of the system.
- If the ComplianceClock time of the foreign aggregate is behind the ComplianceClock time of the system, then the system ComplianceClock time is drifted back to the ComplianceClock time of the foreign aggregate once the foreign aggregate is brought online.

The ComplianceClock time 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 time, and all of the ComplianceClock times are updated in the same manner as the system clock while the volumes are online. This is so that any tampering with the system clock, ComplianceClock time, or volumes moved from any other NetApp storage system is not propagated to the ComplianceClock on another NetApp storage system.

To mitigate some of the drift in the ComplianceClock time, Data ONTAP advances the ComplianceClock time toward the system clock at a rate of one week a year. This is to allow for a reasonable amount of system maintenance during the year.

ComplianceClock time is not updated on offline volumes. When an offline volume (say, vol1) is brought online, it has the effect of pulling back the ComplianceClock time of the system to match the value of ComplianceClock time stored in the header of the offline volume (vol1). If the ComplianceClock time in vol1's header is ahead of the ComplianceClock time on the system, vol1's ComplianceClock time is set back to match the time on the other volumes in the system. The same happens if a system goes down and comes back up after a while or if its volumes are taken over by the cluster pair. The ComplianceClock time on all the volumes is set to the match the ComplianceClock time that is lowest (furthest back in the past).

Note: If your ComplianceClock time does drift backward, you are not, potentially, out of compliance with regulations that require data to be retained for the initial retention period. The storage system simply retains the file for a bit longer than expected. To make sure of expected behavior of the system, the implications of any downtime should be carefully considered.

2 SNAPLOCK ENTERPRISE AND COMPLIANCECLOCK

SnapLock Enterprise is a variant of SnapLock for more flexible customer environments. It operates under a "trusted storage administrator" model in which Data ONTAP permits all administrative actions while still enforcing WORM protection for all file protocols. However, even those with administrative access to the storage system are not permitted to violate the WORM protection at an individual file level on a SnapLock Enterprise volume. However, other operations (for example, “SnapRestore” and “vol destroy”), are permitted unconditionally by an administrator.

ComplianceClock is required for the implementation of SnapLock Compliance volumes. However, it is highly recommended in production systems where the deletion of SnapLock Enterprise volumes needs to be monitored and assured. ComplianceClock provides a reliable base for setting the initial retention date of the WORM file. It also provides a mechanism for the proper deletion of WORM files. If the ComplianceClock time is not set, individual WORM files could be deleted prior to their expiration date. If the compliance officer doesn't set the ComplianceClock time before creating WORM data, that officer is allowing some other administrator to set the ComplianceClock time to an arbitrary date in the future and then delete individual WORM files (assuming they weren't infinitely retained). As a consequence, a system could be considered out of compliance if SnapLock Enterprise volumes are used without the ComplianceClock time set.

Features such as privileged delete (available in Data ONTAP 7.3.1 and later) require a SnapLock Compliance volume to be designated for the compliance log of privileged delete operations. SnapLock Compliance aggregates and volumes cannot be created unless ComplianceClock is initialized. Because the privileged delete feature for SnapLock Enterprise volumes depends on the presence of a SnapLock Compliance volume, those features cannot be used without first establishing the ComplianceClock time.

3 DATA PROTECTION AND COMPLIANCECLOCK

ComplianceClock has a unique set of behaviors when the SnapLock volume data is moving between two systems, as is the case when data protection techniques are applied to the WORM data. For details about setting this up, see the *Archive and Compliance Management Guide* and *Data Protection Online Backup and Recovery Guide.*

3.1 VOLUME SNAPMIRROR

When the destination is a SnapLock Compliance volume, the ComplianceClock time on the destination must be initialized before the SnapMirror relationship is initiated. Because Volume SnapMirror works at a block level, the ComplianceClock time from the source copy of the volume automatically gets transferred to the destination. When the mirroring relationship is broken and the destination copy is brought online, the ComplianceClock time on the destination system is adjusted back if the ComplianceClock time in the copy is behind the ComplianceClock time on the destination system.

3.2 QTREE SNAPMIRROR AND SNAPVAULT

ComplianceClock time is transferred from the source qtree to the destination when the destination qtree resides on a SnapLock Compliance or a SnapLock Enterprise volume. (It is possible to set up a qtree SnapMirror® relationship between a SnapLock Compliance or a SnapLock Enterprise qtree to a regular, non SnapLock qtree.) However, the ComplianceClock time on the destination system is not adjusted until the SnapMirror relationship is broken. When the mirroring relationship is broken, the ComplianceClock time on the destination system is adjusted to match the ComplianceClock time in the qtree if the qtree ComplianceClock value is behind.

Even though SnapVault® uses qtree SnapMirror under the covers, ComplianceClock does not behave the same way. In qtree SnapMirror, in order to do clock adjustments at “snapmirror break” time, the source ComplianceClock time is stored as metadata on the destination qtree. In SnapVault the source ComplianceClock time is *not* stored as metadata on the destination qtree, making ComplianceClock time drifts impossible. This effectively means that when using SnapVault, if the source ComplianceClock time is behind the current ComplianceClock time on the destination, there will be no drift in the destination ComplianceClock time.

3.3 VOLUME COPY, AGGREGATE COPY, AND VOLUME SNAPMIRROR

When copying to a SnapLock Compliance destination, the ComplianceClock time on the destination must be initialized before the volume or aggregate copy is initiated. The copy causes the ComplianceClock time on the source to be transferred to the destination copy. All of these require the destination object to be in restricted state. Once the copy is complete, the object (aggregate or volume) can be brought online. Bringing the copy online causes the ComplianceClock time on the destination system to be adjusted back if the ComplianceClock time in the copy is behind the ComplianceClock time on the destination system.

4 COMPLIANCECLOCK BEHAVIOR WITH BACKUP RELATIONSHIPS

4.1 VOLUME SNAPMIRROR

Volume SnapMirror is block-for-block replication; it transfers the file system verbatim. The ComplianceClock time is transferred over from the source to the destination volume. If the source ComplianceClock time is behind the current ComplianceClock time at the destination system, then the destination system ComplianceClock time is drifted back to match the most recently transferred ComplianceClock time.

Typically, a volume SnapMirror relationship involves the following workflow:

- **Initialize**: Initializing the SnapMirror relationship between the source and destination volume. This causes the first data transfer from the source to the destination volume. The destination should have the source file system at the end of the operation.
- **Update**: Periodic SnapMirror updates between the source and destination volumes. This causes the file system changes to be propagated from the source to the destination volume.
- **Break**: Breaks the SnapMirror relationship between the source and destination volumes.
- **Resync**: Resynchronizes a broken-off destination to its former source.

ComplianceClock behavior during these operations:

1. Initialize

For a SnapMirror initialize to take place, the destination volume needs to be in the restricted state. Restricted volumes have the effect of pulling back the system's current ComplianceClock time when they are brought online because on completion of the Initialize step the current ComplianceClock time on the destination system is to be drifted back to match the ComplianceClock time of the now online destination volume. This drift is approximately equal to the time taken for the initialize step.

	Actual System Clock (Source and Destination)	ComplianceClock Time on Source System	ComplianceClock Time on Destination System
Snapmirror initialize issued	01:00	01:00	01:00
Snapmirror initialize completes	01:15	01:15	01:00

In the preceding table, notice that the `snapmirror initialize` took 15 minutes to complete. This had the effect of drifting the ComplianceClock time on the destination system back by 15 minutes.

We know that during the initialize step, the ComplianceClock time from the source is copied over to the destination volume. If this copied-over ComplianceClock time is behind the current ComplianceClock time on the destination system, then the ComplianceClock time on the destination system is drifted back to match the copied-over ComplianceClock time.

	Actual System Clock (Source and Destination)	ComplianceClock Time on Source System	ComplianceClock Time on Destination System
Snapmirror initialize issued	02:00	01:00	02:00
Snapmirror initialize completes	02:15	01:15	01:00

In the preceding table the ComplianceClock time copied over was 01:00; therefore, when `snapmirror initialize` completed, the destination ComplianceClock time was drifted back to match 01:00.

2. Update

SnapMirror update propagates the file system changes between source and destination volumes, which includes the ComplianceClock time. If this value is behind the current ComplianceClock time on the destination system and the relationship is subsequently broken, then the ComplianceClock time on the destination system is drifted back to match the propagated ComplianceClock time.

3. Break

If the last propagated ComplianceClock time is behind the current ComplianceClock time on the destination system, then breaking the SnapMirror relationship causes the ComplianceClock time on the destination system to drift back to match the last propagated ComplianceClock time from the source.

	Actual System Clock (Source and Destination)	ComplianceClock Time on Source System	ComplianceClock Time on Destination System
Snapmirror initialize issued	02:00	01:00	02:00
Snapmirror initialize completes	02:05	01:05	01:00
Snapmirror update issued	03:05	01:05 (assume ComplianceClock time not updated for some reason such as a volume being offline)	02:00
Snapmirror update completes	03:06	01:05	02:01
Snapmirror break issued	03:30	01:05	01:05

In the preceding table we assume that the ComplianceClock time on the source system does not get updated starting at step 2. Notice that the last propagated ComplianceClock time to the destination system is 01:05 (step 3); therefore, when the SnapMirror break is issued, the ComplianceClock time on the destination system is drifted back to match 01:05.

4. Resync

A SnapMirror resync involves transmitting data from source to destination to reestablish the SnapMirror relationship. This includes the ComplianceClock time; thus, if the ComplianceClock time transferred over is behind the current ComplianceClock time on the destination system and the relationship is subsequently broken, then the ComplianceClock time on the destination will be drifted back to match the transferred-over ComplianceClock time.

	Actual System Clock (Source and Destination)	ComplianceClock Time on Source System	ComplianceClock Time on Destination System

Snapmirror resync issued	02:00	01:00	02:00
Snapmirror resync completes	02:05	01:05	02:05
Snapmirror break issued	02:30	01:30	01:00

In the preceding example the latest ComplianceClock time transmitted from source to destination is 01:00. The ComplianceClock time on the destination drifts from 02:30 to 01:00 when the SnapMirror break is issued.

CAVEAT

Prior to Data ONTAP 7.0.1, all volume combinations “non-SnapLock to non-SnapLock,” “SnapLock to non-SnapLock,” and “non- SnapLock to SnapLock” could result in a ComplianceClock skew on the destination systems, if the source ComplianceClock time was behind the current ComplianceClock time on the destination system. The ComplianceClock skews caused by the combination of “non-SnapLock to ‘non-SnapLock” and “SnapLock to ‘non-SnapLock” had no compliance reason and hence were fixed (to not cause a skew) in Data ONTAP 7.0.1. Note that the combination of non-SnapLock to SnapLock Enterprise will cause a ComplianceClock skew (source ComplianceClock time behind destination ComplianceClock time) and that Non-SnapLock to SnapLock Compliance is not a supported configuration.

4.2 QTREE SNAPMIRROR

SnapMirror qtree replication is logical replication; all of the files and directories in the source file system are created on the destination file system. The destination qtree is read-only, but the volume on which it is located must be online and writable.

Unlike volume SnapMirror, in qtree SnapMirror the ComplianceClock time is not replicated automatically. Explicit changes are made in the code to send the ComplianceClock time from source to destination at the time of the SnapMirror break. The ComplianceClock time is sent from the source to destination only if the replication is from a SnapLock volume to a SnapLock volume. When the source ComplianceClock time is behind the destination, unlike volume SnapMirror, which drifts the destination ComplianceClock value to match the last propagated source ComplianceClock time, qtree SnapMirror aims to drift the destination ComplianceClock time to match the current ComplianceClock time on the source system.

Following are the ComplianceClock behaviors during initialize, update, break, and resync, in the context of qtree SnapMirror:

1. Initialize

Unlike volume SnapMirror, in qtree SnapMirror the destination volume does not need to be in the restricted state. This means that lengthy SnapMirror initialize operations will not cause a ComplianceClock drift on the destination system.

However, if the ComplianceClock time in the source qtree is behind the current ComplianceClock time on the destination system, then the idea is to drift the ComplianceClock time on the destination system to match the current ComplianceClock time on the source system when the relationship is broken. Note that volume SnapMirror in such a situation drifts the ComplianceClock time on the destination system to match the ComplianceClock time that was transferred over; however, in qtree SnapMirror the idea is to match the current ComplianceClock time on the source system.

This drift does not reflect upon completion of the SnapMirror initialize operation but rather on breaking the SnapMirror relationship.

2. Update

SnapMirror update propagates the file system changes between source and destination qtrees, which includes the ComplianceClock time. If this value is behind the current ComplianceClock time on the destination system and the relationship is subsequently broken, then the ComplianceClock time on the destination system is drifted back to match the current ComplianceClock time on the source system.

3. Break

On breaking the SnapMirror relationship, the ComplianceClock time changes, if any, reflect on the destination system.

	Actual System Clock (Source and Destination)	ComplianceClock Time on Source System	ComplianceClock Time on Destination System
Snapmirror Initialize issued	02:00	01:00	02:00 (01:00 gets copied to destination)
Snapmirror initialize completes	02:05	01:05	02:05
Snapmirror update issued	02:30	01:30	02:30 (01:30 gets copied to destination)
Snapmirror update completes	02:31	01:31	02:31
Snapmirror break issued (quiesced first)	02:45	01:45	01:45

In the preceding example, during initialize the ComplianceClock time transferred over from the source was 01:00; 30 minutes later a SnapMirror update is issued; the previous value of 01:00 is overwritten by 01:30. 15 minutes later a SnapMirror break is issued; this period is added to the most recent ComplianceClock time from source (01:30), and then the destination ComplianceClock time is drifted back to match it (01:45).

	Actual System Clock (Source and Destination)	ComplianceClock Time on Source System	ComplianceClock Time on Destination System
Snapmirror Initialize issued	02:00	01:00	02:00
Snapmirror initialize completes	02:05	01:05	02:05
Snapmirror break issued (quiesced first)	02:30	01:30	01:30

The preceding example is similar to the previous one, only here no update is issued. The most recent and only ComplianceClock time from source is 01:00, and the total wait period before the SnapMirror break is 30 minutes, setting the destination ComplianceClock time to 01:30.

4. Resync

The underlying idea is the same. If the ComplianceClock time transferred over from the source is behind the current ComplianceClock time on the destination (and the relationship is subsequently broken), then the ComplianceClock time on the destination system is drifted back to match the current ComplianceClock time on the source system.

	Actual System Clock (Source and Destination)	ComplianceClock Time on Source System	ComplianceClock Time on Destination System
Snapmirror resync issued	02:00	01:00	02:00
Snapmirror resync completes	02:05	01:05	02:05
Snapmirror break issued (quiesced first)	02:30	01:30	01:30

Destination ComplianceClock Time Not in Sync with Source ComplianceClock Time

It's possible that the destination system ComplianceClock time will *not* be in sync with the source at the time of the break, as demonstrated in the following example.

	Actual System Clock (Source and Destination)	ComplianceClock Time on Source System	ComplianceClock Time on Destination System
Snapmirror initialize issued	02:00	01:00	02:00
Snapmirror initialize completes	02:05	01:05	02:05
Snapmirror update issued	02:30	01:30	02:30 (01:30 gets copied to destination)
Snapmirror update completes	02:31	01:31	02:31
ComplianceClock time on the source drifts back to 00:00 after 15 minutes of the update being issued, due to some reason.			
Snapmirror break issued	03:00	00:15	02:00 (01:30 [copied during last update] + 30 minutes)

When the update is issued, the ComplianceClock time transferred over from the source to the destination is 01:30. The relationship is broken 30 minutes later; therefore, the destination gets a ComplianceClock time of 02:00 (01:30 + 30). The source, in contrast, drifted back to 00:00 due to some reason (say, a volume previously offline coming online) 15 minutes after the update was issued. Therefore, at 02:45 (actual time) the ComplianceClock time on the source drifted back to 00:00. The relationship was broken 15 minutes after the drift took place (03:00 actual time); therefore, the ComplianceClock time on the source advanced 15 minutes to 00:15.

CAVEAT

To allow a qtree SnapMirror resync between the SnapLock Compliance qtrees after upgrading Data ONTAP, we need to make at least one update from the qtree source to the destination volume before attempting the resync.

In qtree SnapMirror the ComplianceClock time is sent from the source to destination only if the replication is from a SnapLock volume to a SnapLock volume. Therefore, a volume combination of non-SnapLock to SnapLock will *not* cause a ComplianceClock skew (if source ComplianceClock time is behind destination ComplianceClock time), which is unlike volume SnapMirror behavior (see volume SnapMirror caveat).

5 USING THE NETAPP STORAGE SYSTEM SIMULATOR

Because of the strict protection that SnapLock Compliance volumes offer, the preferred method of testing or evaluating SnapLock Compliance processes is to use the Data ONTAP simulator. Without the use of a simulator, it is possible to indefinitely lock disks into SnapLock compliance volumes when the system is used naively. Simulators for several current releases are available on the NOW™ (NetApp on the Web) site 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 time can be set, and SnapLock Compliance volumes can be created for testing purposes. When the testing is complete, 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, see the documentation for the simulator.

The simulator's root aggregate, aggr0, is not a SnapLock aggregate. To use the simulator, additional "simdisks" should be created to house the SnapLock aggregate. Additionally, the appropriate SnapLock simulator license is needed to enable SnapLock functionality. Contact your NetApp account representative or system engineer to obtain this license key.

Note: This key does not work on real FAS and NearStore systems.

6 SUMMARY

SnapLock Compliance and SnapLock Enterprise are designed to be critical pieces of a comprehensive data archiving solution for businesses that require higher performance and lower TCO alternatives for WORM storage functionality. SnapLock benefits over traditional WORM storage include potential improvements to performance, capacity, and reliability, along with reduced management overhead. These benefits layer nicely for businesses that need WORM data storage for regulatory compliance or to protect critical enterprise content beyond the capabilities of normal data storage.

The powerful data permanence and data integrity features of SnapLock combine with the potential 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 can provide a superior solution in the WORM data storage space. For more information on solutions-based products from NetApp, go to www.netapp.com/products.

7 REFERENCES

1. Archive and Compliance Management Guide
2. Data Protection Online Backup and Recovery Guide
3. TR-3263: WORM Storage on Magnetic Disks Using SnapLock Compliance and SnapLock Enterprise
4. TR-3738: SnapLock Record Retention Date and Implementation Strategy
5. TR-3446: SnapMirror Async Overview and Best Practices Guide

REVISION HISTORY

[09/2007] Author: Mark Hayakawa

- Original TR

[05/2008] Author: Mark Hayakawa

- Included section “ComplianceClock and SnapMirror”
- Minor edits

[02/2009] Author: Manish Agarwal

- Updated section “ComplianceClock and SnapMirror” to “Data Protection and SnapMirror”
- Minor edits

[09/2009] Author: Timothy Isaacs

- Included section “Compliance Clock Behavior with Backup Relationships”
- Minor edits

NetApp provides no representations or warranties regarding the accuracy, reliability or serviceability of any information or recommendations provided in this publication, or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS, and the use of this information or the implementation of any recommendations or techniques herein is a customer’s responsibility and depends on the customer’s ability to evaluate and integrate them into the customer’s operational environment. This document and the information contained herein must be used solely in connection with the NetApp products discussed in this document.

www.netapp.com