IBM Tivoli Storage Manager and SnapLock™ Integration for Regulatory Compliance

Network Appliance | TR 3378

TECHNICAL REPORT

Network Appliance, a pioneer and industry leader in data storage technology, helps organizations understand and meet complex technical challenges with advanced storage solutions and global data management strategies.

Network Appliance Inc.

Table of Contents

List of Figures

1. INTRODUCTION

Industry regulations have increasingly introduced significant financial penalties for failing to comply with retention, indexing, auditing, privacy, and reporting requirements. These regulations are mandatory by law for all U.S. public companies and are expected to spread rapidly into other parts of the world such as Europe and Asia. Nearly every major corporation will put a regulatory compliance solution in place within the next five years or face the risk of being exposed to litigation and fines.

IBM Tivoli Storage Manager (TSM) fully supports disk-based archive/backup of servers, storage devices, and clients in combination with NetApp NearStore® disk storage systems. The NearStore system is managed by TSM as a magnetic sequential file device with the benefits of faster data access for data protection and disaster recovery compared with traditional sequential storage devices such as tape libraries. TSM is used by more than 80 of the Fortune 100 companies that are subject to strict record retention regulations such as SEC Rule 17a-4 and Sarbanes-Oxley.

NetApp SnapLock is the perfect solution to customers' requirements for data permanence. It offers write once, read many (WORM) protection without the need to buy dedicated WORM hardware. It also allows WORM and non-WORM storage to reside on the same system (resulting in a significant cost savings) if the customer so desires. SnapLock also offers a simple, elegant solution for the data destruction problem by allowing customers to delete and destroy expired data according to company retention policies. The expiration date can be specified for any file in a SnapLock environment. In summary, SnapLock gives customers the power to protect their data for regulatory compliance (data permanence) while maintaining the flexibility of deleting that data at the end of its lifecycle (data destruction) when necessary. The reclamation of free space thus greatly reduces the customers' TCO of their storage infrastructure.

Recent collaboration between IBM and NetApp has led to the integration of SnapLock and TSM; the purpose of this document is to describe the configuration and usage of this integration.

2. INTEGRATION OVERVIEW

Although TSM supports both backup and archive functionalities, only the archive functionality is integrated with NetApp for regulatory compliance. Figure 1 shows a typical TSM archive/retrieve environment with NearStore as the underlying storage infrastructure. The archive clients are split into two domains—server and workstation domains. Each domain has a separate policy set maintained by a management class; the management class contains a copy group, where archive expiration policies are defined. TSM orchestrates the archival/retrieval of data with two important pieces of databases—metadata and log. The NearStore system is used as the primary storage for archival. SnapLock volumes are enabled to provide WORM capability for data that needs to meet retention requirements of various compliance regulations. The data in the primary storage can be dumped to a tape copy pool utilizing NDMP for off-site data protection. Secondary storage, or copy pools, can reside on NearStore for data recovery from media in the event of a disaster. Alternatively, the copy pool–enabled SnapLock can be subsequently copied using SnapMirror® or SnapVault® to a DR site for business or regulatory compliance requirements.

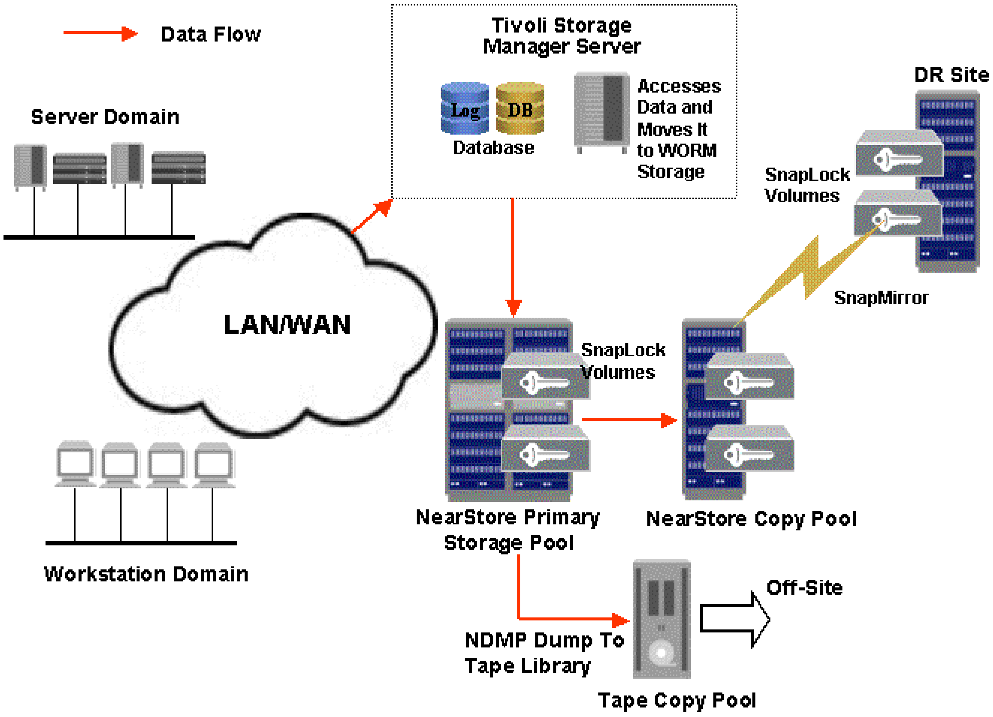

Figure 1) Deployment architecture of integration.

2.1. Storage Reclamation

TSM has a process called reclamation that monitors the utilization of storage pools in its inventory. When the age of the retained data reaches a customer-defined retention period, TSM automatically frees up the SnapLock volume and moves the remaining data to another eligible SnapLock volume. This archive-only function of the TSM for Data Retention Server is integrated with NetApp SnapLock to help address customers' requirements for regulatory compliance. The remaining data in a SnapLock volume that is due for reclamation will be moved to another SnapLock volume. Data stored on a SnapLock volume has "double protection" by both TSM for Data Retention and SnapLock. If a TSM administrator tried to delete the data, TSM for Data Retention would fail the command. If someone tried to delete the data on the R200, SnapLock would prevent this from happening.

2.2. Benefits

Applications such as Lotus Domino, Exchange, and SAP have data that is subject to regulatory compliance. TSM for Data Retention sets a retention policy for the application data and commits it to a SnapLock WORM state through an API client.[1] Data stored with a TSM retention policy cannot be deleted from the integrated TSM and SnapLock system until the retention policy criteria have been satisfied. The integration enables NetApp to provide the most comprehensive, secure, highly scalable, easy-to-manage, and low-TCO storage solutions for customers who have the requirement for regulatory compliance.

3. SOLUTION CONFIGURATION

3.1. Prerequisites

Tivoli Storage Manager

Tivoli Storage Manager (TSM)—Extended Edition and Tivoli Storage Manager for Data Retention V5.3 are required for the integration. The TSM server has to be a new one; no objects should be stored before using TSM. The license for data retention is also required.

NetApp NearStore

Either a SnapLock Enterprise or SnapLock Compliance license is required to handle data retention. It is important to note that a SnapLock Compliance volume cannot be destroyed until such time as all retained files and Snapshot™ copies on the volume have expired, whereas an administrator can destroy a SnapLock Enterprise volume at any time. SnapLock Compliance is the version required for the strictest retention requirements, such as those of SEC 17a-4. SnapLock Enterprise is recommended for regulatory requirements where the administrator is a trusted entity or to comply with corporate best practices retention policies. A compliance version of the Data ONTAP™ build is required for this integration. This functionality will be generally available in the Data ONTAP 7.1 release.

3.2. NearStore Configuration

The following steps prepare NetApp NearStore for TSM and SnapLock integration. The volume and qtree names used in the examples are in italic font and are arbitrary.

1. Enable the SnapLock license**:**
license add <SnapLock license code>

2. Initialize ComplianceClock™:
date –c initialize

ComplianceClock can be initialized only once for the system, so extreme care should be exercised at install time to ensure that the clock time is set correctly. Make sure that the system time and time zone are correctly set, and everything should go smoothly, as ComplianceClock can only be set from the system time to prevent any data input errors. Once ComplianceClock has been initialized, it can be displayed with the “**date -c**” command.

3. Create a SnapLock volume:

[1] SnapLock can only be used by TSM server with data retention protection enabled for archiving purposes. Therefore, a TSM API client instead of a TSM backup/archive client is required.

```
vol create <volume name> -L
```

For example:

```
vol create slvol –L Enterprise 8
```

A SnapLock volume named “slvol” containing eight disks is created:

```
vol status slvol
  Volume    State     Status         Options
     slvol     online    raid4          no_atime_update=on,
                                          snaplock_enterprise
```

4. Set up appropriate maximum, minimum, and default retention periods:

   The maximum retention period specifies the maximum allowable retention period for any file or Snapshot copy committed to WORM state on the SnapLock volume. This option is useful in regulatory environments to ensure that applications or users do not intentionally or unintentionally assign excessive retention periods to retained records. Any file or Snapshot copy committed to WORM state with a retention period greater than this maximum will automatically have this maximum retention period assigned. The maximum retention period takes precedence over the default retention period. We do not recommend exceeding a maximum retention period of 30 years for TSM and SnapLock deployments.

   ```
   vol options slvol snaplock_maximum_period 30y
   ```

   The minimum retention period specifies the minimum allowable retention period for any file or Snapshot copy committed to WORM state on the SnapLock volume. This option is useful in regulatory environments to ensure that applications or users do not intentionally or unintentionally assign noncompliant retention periods to retained records. Any file or Snapshot copy committed to WORM state with a retention period less than this minimum will automatically have this minimum retention period assigned. The minimum retention period takes precedence over the default retention period. Set the higher value: either 30 days or the minimum number of days specified by **RETMIN** (see section 3.3) in any copy group.

   ```
   vol options slvol snaplock_minimum_period 30d
   ```

   The default retention period specifies the retention period that will be assigned to any file or Snapshot copy committed to WORM state on the SnapLock volume without an explicitly assigned retention period. The following command sets a default retention period of 30 days, recommended by TSM:

   ```
   vol options slvol snaplock_default_period 30d
   ```

5. Create a qtree in the SnapLock volume:

   ```
   qtree create /vol/slvol/accounting
   ```

   This command creates a qtree named “***accounting***” in the newly created SnapLock volume “***slvol.***”

6. Share the newly created SnapLock volume through CIFS:

```
cifs shares –add accounting  /vol/slvol/accounting
```

This command generates a CIFS share named ***accounting*** based on qtree **/vol/*slvol/accounting***.

3.3. Tivoli Storage Manager Configuration

The following commands are the steps required to configure TSM in order for it to access the SnapLock volumes appropriately. The names used in italic font are arbitrary; users can pick any names they prefer.

1. Turn on the archive retention protection feature in TSM:

   ```
   SET ARCHIVERETENTIONPROTECTION ON
   ```

2. Create a WORM device class based on device type "**FILE**":

   ```
   DEFINE DEVCLASS WORMDEV DEVTYPE=FILE \
   DIRECTORY=\\FILER\ACCOUNTING
   ```

3. Create a WORM storage pool:

   ```
   DEFINE STGPOOL WORM_POOL WORMDEV
   RECLAMATIONTYPE=SNAPLOCK \
   MAXSCRATCH=10000
   ```

   The value of **MAXSCRATCH** specifies the maximum number of storage volumes allowed in the SnapLock storage pool. It is recommended that this value be set to a large one to allow efficient use of the space on the SnapLock volume on the filer. This value should also be set based on the size of the SnapLock volume and the **MAXCAP** value of the **FILE** device class.

4. Create a domain:

   ```
   DEFINE DOMAIN DOMAIN_WORM
   ```

   This command creates a domain called "***DOMAIN_WORM***."

5. Create a policy set:

   ```
   DEFINE POLICYSET DOMAIN_WORM POLICY_WORM
   ```

   This creates a policy set called "***POLICY_WORM***" in domain "***DOMAIN_WORM.***"

6. Create a management class:

   ```
   DEFINE MGMTCLASS DOMAIN_WORM POLICY_WORM MGMTCLS_WORM
   ```

   This command creates a management class set in domain "***DOMAIN_WORM***" and policy set "***POLICY_WORM***" called "***MGMTCLS_WORM.***"

7. Assign a default management class:

```
ASSIGN DEFMGMTCLASS DOMAIN_WORM POLICY_WORM MGMTCLS_WORM
```

8. Define a copy group:

   ```
   DEFINE COPYGROUP DOMAIN_WORM POLICY_WORM MGMTCLS_WORM \
   DESTINATION=WORM_POOL TYPE=ARCHIVE RETINIT=CREATION
   RETVER=120 RETMIN=90
   ```

   RETINIT=CREATION indicates that the application-initiated retention policy is initiated at the time the object is created. The value of **RETVER** specifies the number of days to keep an archive copy after the event has occurred. The value of **RETMIN** specifies the minimum number of days to keep an archive copy after it has been archived. Adjust the values of **RETVER** and **RETMIN** to your requirements for protecting the data in WORM storage.

   There are two types of copy groups—backup and archive. The archive copy group is required for using SnapLock integration.

9. Activate the policy set:

   ```
   ACTIVATE POLICYSET DOMAIN_WORM POLICY_WORM
   ```

4. SUMMARY

This document provides information on integrated solutions for regulatory compliance offered by IBM Tivoli Storage Manager and NetApp SnapLock. The benefits of the joint solution are discussed. The configurations of the solutions are also described in detail.

In addition to this document, these other useful links provide more information:

Using SnapLock Compliance and SnapLock Enterprise with Data ONTAP 7G
WORM Storage on Magnetic Disks Using SnapLock Compliance and SnapLock Enterprise
Using IBM Tivoli Storage Manager with Network Appliance™ NearStore
NetApp SnapLock Enterprise Software
IBM Tivoli Storage Manager for Data Retention
Tivoli Storage Manager Administrator's Guide
Tivoli Storage Manager Administrator's Reference

NetApp®

Network Appliance, Inc.
495 East Java Drive
Sunnyvale, CA 94089
www.netapp.com