Integrating VERITAS Enterprise Vault Message Archival with NetApp Storage Solutions

VERITAS and Network Appliance | TR-3267

1. Introduction

Securities and Exchange Commission (SEC) regulations require financial broker-dealers to retain e-mails and messages for a specified period of time after their origination. In addition, internal policies are increasingly being established by companies across various industries requiring e-mails be retained for future reference and/or audit. As a result, retaining e-mail messages for longer periods of time and being able to quickly search and retrieve specific records are becoming critical for many businesses. According to the SEC, financial broker-dealers must also exclusively preserve key business records such as e-mail on nonrewritable, nonerasable WORM (write once, read many) media that is fully indexed and easily searchable for two years from origination. Given this demanding set of requirements, how can businesses easily and effectively ensure compliance with these regulations?

Even organizations that do not have compliance requirements are faced with the problem of ever-growing e-mail data stores. E-mail is a primary means of communication, and many users are increasing the amount of data kept in their mailbox or personal data stores (pst files). Many administrators are pressured to remove mailbox quotas in response to increased user activities and then faced with larger issues such as management, scalability, and disaster recovery.

VERITAS has a suite of products to assist businesses with managing data and maintaining compliance with e-mail and message archival regulations. NetApp storage solutions provide scalable high-performance SAN and NAS devices with full integration of VERITAS Enterprise Vault. Optional WORM software functionality called SnapLock^{TM}, available on magnetic disk drive–based storage through the NearStore® product line, introduces critical new technology to further assist businesses with achieving regulatory compliance. The combination of VERITAS Enterprise Vault with NetApp storage offers a simple, cost-effective, and best-of-breed solution to businesses required to archive e-mail and messages.

2. Purpose and Scope

This paper will provide a design overview and best practices when using VERITAS Enterprise Vault to archive Microsoft® Exchange e-mails and messages to NetApp storage systems. It will provide all steps required to implement the solution outlined in this paper. This paper will address relevant background information on required infrastructure and NetApp technology, including SnapLock WORM functionality for compliance.

The solution covered in this paper is limited to VERITAS Enterprise Vault retention of Microsoft Exchange e-mails and messages to NetApp storage systems. While VERITAS Enterprise Vault includes the ability to archive Windows® file servers and Microsoft Sharepoint portal servers, these features will be covered in additional technical reports. Links to further information about VERITAS and Network Appliance and their products will be provided at the paper's conclusion.

3. Infrastructure

The following section provides an overview of the network architecture required to support an Enterprise Vault and NetApp environment. These recommendations are based on tests conducted with VERITAS Enterprise Vault V5.0 and NetApp Data ONTAP™ 7G.

3.1. Network

3.1.1. Connectivity

Most institutions required to comply with message retention standards are large enough to warrant having private Gigabit network connections between the VERITAS Enterprise Vault server, the Exchange server, the active directories domain controller server, and the NetApp filer. Either setting up a separate switch or creating a VLAN on existing switches would equally suffice. Client connectivity to the Exchange server can continue over current network infrastructure (e.g., 100Base-T).

Isolating the e-mail archival network in the manner just described affords two important benefits. Potential latency and contention between systems used in this solution white paper are eliminated by minimizing the number of overall servers attached to the network. This proposed network implementation also improves security of the e-mail archival process. Having this archival process available on a shared network drastically increases the risk of unwanted or illegal data access.

Network Appliance™ filers and NearStore devices can be connected by several different protocols, depending on the company's requirements. CIFS or Windows file sharing is used for easy access to a NetApp storage device located anywhere on the network. Generally, data sent over CIFS is sharing the network with other devices. iSCSI and Fibre Channel are used for high performance and high availability. While iSCSI is connected over Ethernet, this should be a dedicated high-speed connection such as Gigabit network connections. A dedicated network will improve performance and provide security. Fibre Channel also offers a fast and reliable solution.

3.1.2. Existing Microsoft Environment

Microsoft Exchange servers and domain controllers should already exist on the network. Enterprise Vault works with all versions of Exchange and Windows and requires a functional mail environment and domain name resolution.

3.2. VERITAS Enterprise Vault

3.2.1. Hardware

The actual requirements for Enterprise Vault vary, depending on the number of Exchange servers, locations, amount of data being archived, type of users, bandwidth, and archive storage medium. Contact VERITAS Professional Services for specific requirements to fit your environment.

Typical environments start with a dual-processor system, 2GB of memory, and 100MB for binary files. Archive storage, indexes, and configuration database (stored in SQL) disk space usage varies and will require sizing.

3.2.2. Software

> Enterprise Vault works with all versions of Windows. For the purpose of this report, Enterprise Vault was tested with Windows Server 2003 Standard Edition with IIS and MSMQ enabled.
>
> SQL Server 2000 with Service Pack 3 is required either on the same server or available on the network.
>
> Outlook 2000 Service Pack 2 or higher (on Enterprise Vault Server).

Additional software such as Exchange System Manager, MSXML, MDAC, and Windows .NET Framework will also be required; see Enterprise Vault preinstallation and installation help for more information.

3.3. Network Appliance Filers and NearStore

3.3.1. System Requirements

Enterprise Vault for Exchange works with all versions of Data ONTAP. Support for SnapLock WORM volumes is provided in Data ONTAP 6.4.1 and above. Support for file deletion on expired items in a WORM volume is provided in Data ONTAP 7G.

More information on SnapLock Enterprise and SnapLock Compliance can be found later in this document in section 6. For a detailed report on using SnapLock Enterprise and SnapLock Compliance with Data ONTAP 7G, see NetApp Technical Report 3342 at *www.netapp.com/tech_library/ftp/3342.pdf*.

3.3.2. Licensing Requirements

Depending on the technology used on the filer or NearStore system, there may be some components that must be licensed before implementing. This includes (but is not limited to) SnapLock, CIFS, ISCSI, and FCP.

4. Deployment Overview

There are many possible scenarios when designing a VERITAS Enterprise Vault architecture with NetApp storage. The final design can change depending on the needs of the organization, the physical layout of the organization, or the amount of data to be archived. This paper will address an optimal design and best practices for deploying Enterprise Vault with NetApp NearStore, with NetApp filers, and with both NearStore and filers. Contact VERITAS Professional Services or NetApp to design a solution that is best for your environment.

4.1. Enterprise Vault with NetApp NearStore

The NetApp NearStore R200 system is a disk-based nearline storage system that combines the benefits of the Data ONTAP operating system with inexpensive ATA disk drives. This enables NearStore to provide near-primary storage performance at near-tape storage costs. NearStore further enhances data protection and management by consolidating nearline workload data from both NetApp systems and other storage devices. NearStore systems are commonly used in disaster recovery and archival solutions. The NearStore R200 system scales from 8TB to 96TB.

NearStore systems are ideal for storing large amounts of data that are accessed less frequently but are still available on the network, such as archived e-mails. NearStore features such as WORM (write once, read many) volumes and support for retention periods help ensure companies can archive data to a location that will meet their compliance requirements.

A NearStore system can be used as an archival destination for Enterprise Vault archives and for storing index files. Enterprise Vault vault store partitions can be placed on a single NearStore volume or on separate volumes. Depending on compliance requirements, vault stores can be divided among SnapLock WORM volumes or volumes not based on SnapLock. Data archived to a SnapLock volume will apply the retention period configured in Enterprise Vault. More information on choosing a SnapLock volume as an archival destination can be found later in the document.

Technical Note: Archives are collected together in vault stores, which contain vault store partitions. You must create a vault store and a vault store partition before enabling mailboxes for archiving. Each vault store can have multiple partitions, on different storage media, if required, but only one partition is active at a time.

The last component that can be stored on a NearStore system is the SQL Server database, as long as there is an iSCSI or Fibre Channel connection to the NearStore system. SQL Server databases should not be stored over CIFS or file shares to the NearStore system.

Components that are not ideal for storing on NearStore include the Microsoft Exchange databases.

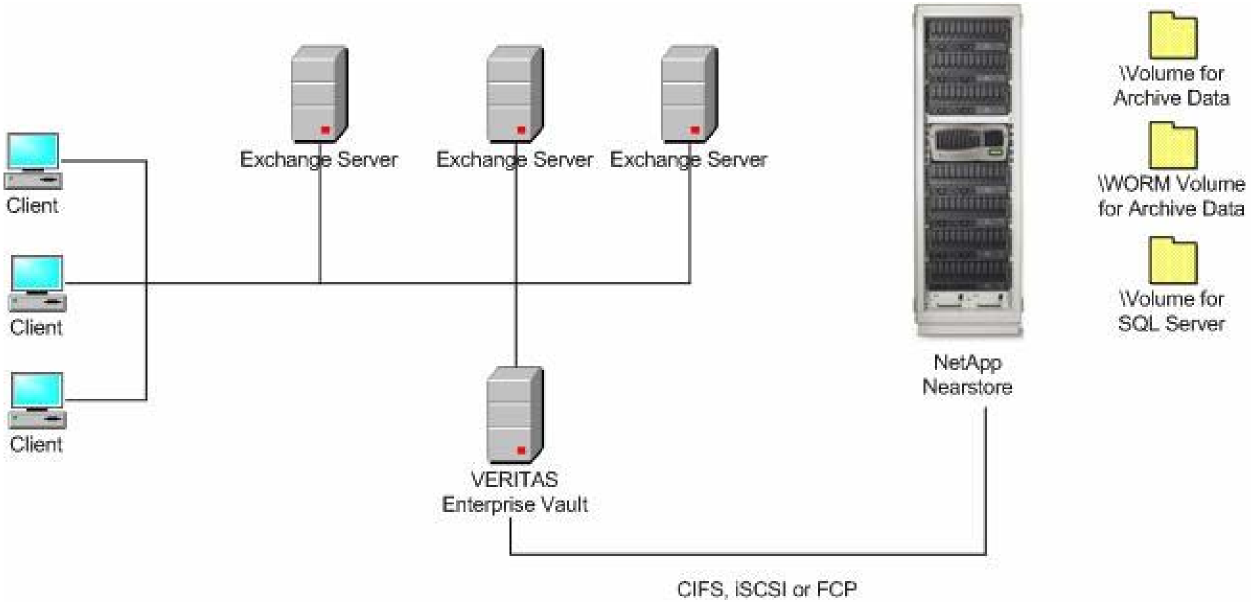


Figure 1) Enterprise Vault with NetApp NearStore.

Technical Tip: Turn oplocks (opportunistic locks off for any volumes containing index files. Oplocks enable a CIFS client in certain file-sharing scenarios to perform client-side caching of read-ahead, write-behind, and lock information. A client can then read from or write to a file without regularly reminding the server that it needs access to the file in question. This improves performance by reducing network traffic. Under some circumstances, if a process has an exclusive oplock on a file and a second process attempts to open the file, the first process must relinquish the oplock and access to the file. An application with write-cached data can lose that data if it has an exclusive oplock on the file or it is told to break that oplock or close the file.

To disable oplocks on a filer or NearStore system (it is enabled by default when CIFS is licensed):

```
filer> options cifs.oplocks.enable off
```

4.2. Enterprise Vault with NetApp Filers

NetApp filers are primary storage devices that enable you to unify your infrastructure by consolidating storage across many servers and applications over any storage fabric. NetApp fabric-attached storage (FAS) systems integrate easily into enterprise environments and simultaneously support Fibre Channel SAN, IP SAN (iSCSI), and NAS. These high performance systems have a proven ability to continuously serve data at higher than 99.99% availability and can scale from 50GB to many terabytes.

Filers can be used with Enterprise Vault, providing the same benefits as NearStore. Filers can act as an archival destination and can be configured with WORM volumes for compliance. Enterprise Vault components can be stored on a filer, such as the index files and the SQL Server database.

Note: Exchange 2000 or 2003 databases must be accessed using iSCSI or Fibre Channel. Ideally, the SQL Server databases and index files are also stored over these protocols.

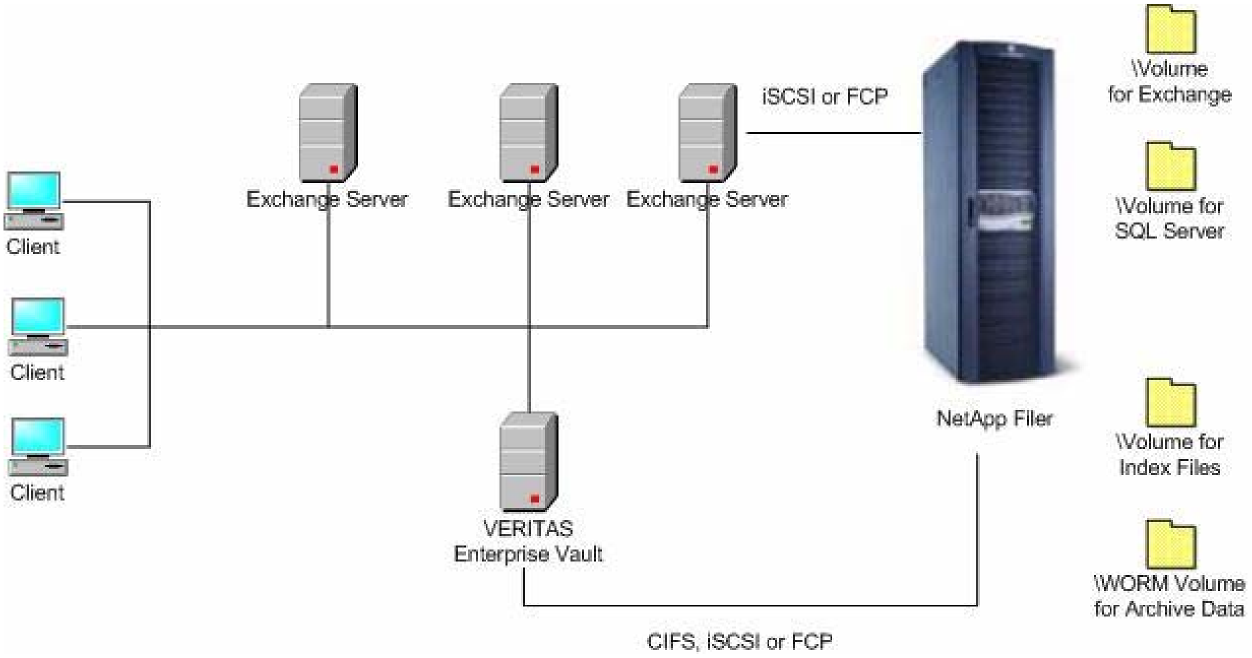


Figure 2) Enterprise Vault with NetApp filers.

A complete design solution when using filers with Enterprise Vault might include the following:

Exchange databases consolidated and migrated to the filer using either iSCSI or Fibre Channel. NetApp SnapManager® for Exchange (SME) data management software works with Enterprise Vault for automated VSS Snapshot™ copies of the Exchange databases.

The Enterprise Vault configuration information is contained in a SQL Server database. This database can be stored on the filer using either iSCSI or Fibre Channel. NetApp SnapManager for SQL Server (SMSQL) data management software is compatible with Enterprise Vault, thus enabling application-aware Snapshot for data recovery.

A volume dedicated to the Enterprise Vault content index. Additional disks will improve performance when building searches. The index files can be accessed over CIFS, iSCSI, or Fibre Channel.

One or more volume(s) for vault stores and vault store partitions containing the archived data. Enterprise Vault vault archives can be separated onto different volumes for compliance requirements to ensure data is contained on a WORM volume. Vault store partitions can be configured to use a Windows share (using CIFS on the filer) or SnapLock volume in the Enterprise Vault configuration wizard.

Technical Tip: Some filers use qtrees, which are a special subdirectory of the root directory of a volume. Qtrees are used to group files that have similar characteristics for easier and faster management, including tasks such as backing up and restoring data and mirroring qtree data for disaster recovery. Vault partitions work with qtrees and can be completed by following these steps:

1. Create the appropriate volumes and qtrees within the volumes (using NTFS security style) on the NetApp filer.

2. Create a CIFS share on the filer for each of the qtrees.

3. Create a folder on the qtree for the new vault partition. **Important:** This directory is necessary, as Enterprise Vault will not create a vault partition unless there is at least one directory below the share point.

4. Within Enterprise Vault, create a new vault store partition within an existing vault store (or when creating a new vault store). Choose to create the vault store partition on a network share when prompted and enter the share location created in step 2. Vault store partitions should never be placed on more than one qtree.

5. **Caution:** When creating a vault store partition marked as open, the existing open vault store partition will be closed. KVS Enterprise Vault can only archive data to one vault store partition at a time.

This configuration is helpful for environments with many vault store partitions—for example, companies that are interested in grouping archived items by dates such as month or year or grouping data by size. An example of this includes using a dedicated qtree and vault store partition to contain all items archived over the course of a year. At the end of the year, the existing vault store partition is closed and a new vault store partition is created on a new qtree. Closed vault store partitions will remain accessible for searching and retrieving items from the vault.

4.3. Enterprise Vault with NetApp NearStore and Filers

Combining NetApp filers and NearStore in an Enterprise Vault deployment offers flexibility and optimal design. Archived data can be stored on near-online systems using cheaper ATA disks, while components such as index files and Exchange data can be moved to a high-performance filer. Both filers and NearStore offer scalable storage, support for Snapshot, and the ability to add additional disks to an existing volume without any disruption in service.

When designing a deployment using filers and NearStore, the Exchange and SQL Server data should be stored on the filer and accessed over iSCSI or FCP. SnapManager for Exchange and SQL can be used for Snapshot backups and restores of the production mail system and databases. Ideally, the index files should be stored on the filer; however, they could be stored on a NearStore system, assuming it is not located across a WAN.

Vault store partitions containing the archived data should be stored on the NearStore system using either CIFS or SnapLock volumes. Enterprise Vault archives can be stored on a single volume or across several volumes for scalability or compliant storage (WORM).

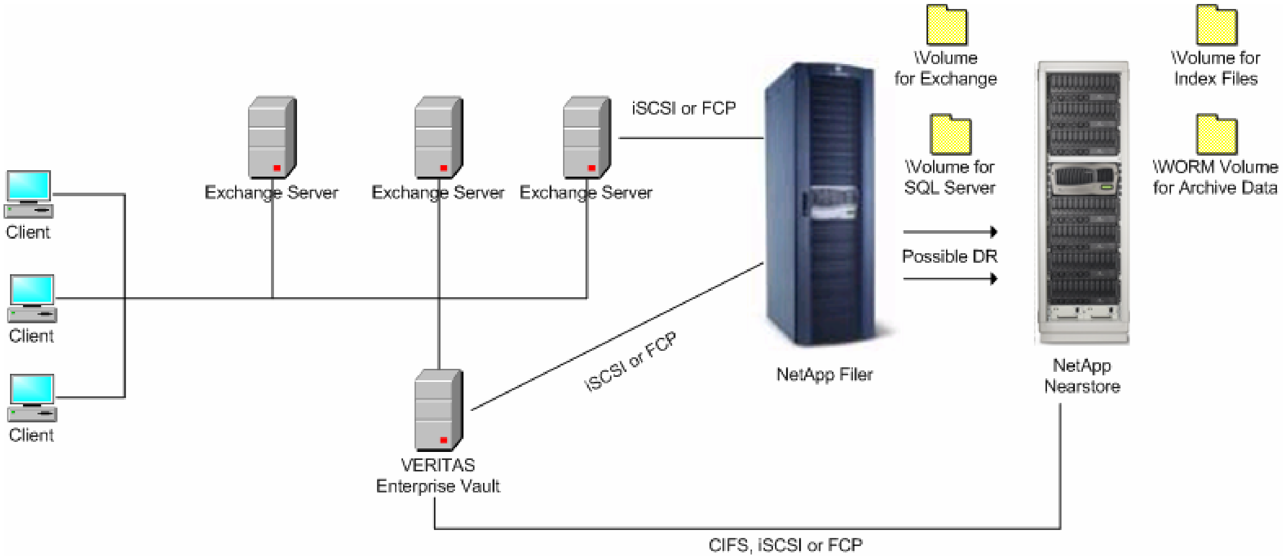


Figure 3) Enterprise Vault with NetApp filers and NearStore.

The optimal design when using both filers and NearStore includes:

Filer Configuration

Exchange databases consolidated and migrated to the filer using either iSCSI or Fibre Channel. NetApp SnapManager for Exchange (SME) data management software works with Enterprise Vault for automated VSS Snapshot copies of the Exchange databases.

The enterprise configuration information is contained in a SQL Server database. This database can be stored on the filer using either iSCSI or Fibre Channel. NetApp SnapManager for SQL Server (SMSQL) data management software is compatible with Enterprise Vault, enabling application-aware Snapshot for data recovery.

A volume dedicated to the Enterprise Vault index. Additional disks will improve performance when building searches. The index files can be accessed over CIFS, iSCSI, or Fibre Channel.

NearStore Configuration

One or more volume(s) for vault stores and vault store partitions containing the archived data. Enterprise Vault vault archives can be separated onto different volumes for compliance requirements to ensure data is contained on a WORM volume. Vault store partitions can be configured to use a Windows share (using CIFS on the filer) or SnapLock volume in the Enterprise Vault configuration wizard.

Optionally, NearStore can be used in a disaster recovery situation by:

- Mirroring the Exchange, SQL Server, and index files to locations on NearStore
- Using SnapVault® to mirror the Snapshot copies stored on the filer to NearStore

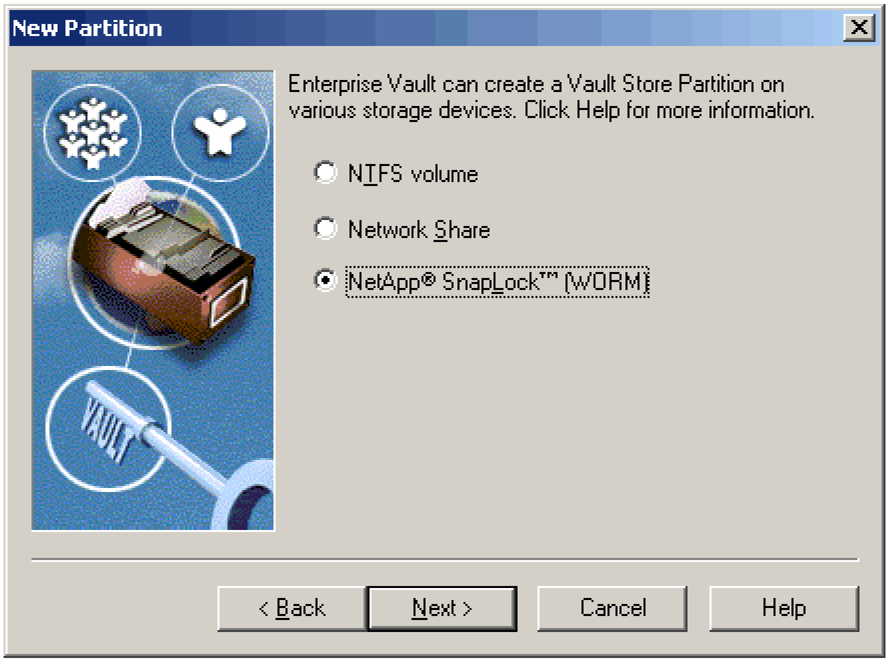
5. VERITAS Enterprise Vault Configuration

VERITAS stores archived messages in Enterprise Vault archives. Archives are collected together in vault stores. Vault stores use a storage partitioning scheme for scalability. A vault store partition resides on a Windows NT® file system (NTFS) volume, CIFS volume (network share), or NetApp SnapLock volume. When you set up Enterprise Vault, you specify on which device each vault store partition is created.

A single vault store can be divided into a number of vault store partitions. As Enterprise Vault grows, you can add vault stores and vault store partitions to extend the space available. A vault store can have only one active vault store partition, which is the vault store partition into which all new items are archived. You can change which vault store partition is active at any time. As you enable each mailbox archive, you specify the assigned vault stores.

Once a drive or pathway has been created and the vault service account has been given proper access rights to it, start the New Vault Store wizard from the administration console. To do this from the administration console (MMC snap in), right-click Vault Store container, point to New, and click Vault Store. Alternatively, click the Add New Vault Store icon on the toolbar.

Once the vault store is named and the SQL databases are selected, you will be prompted to create a partition.



New Partition

Enterprise Vault can create a Vault Store Partition on various storage devices. Click Help for more information.

○ NTFS volume

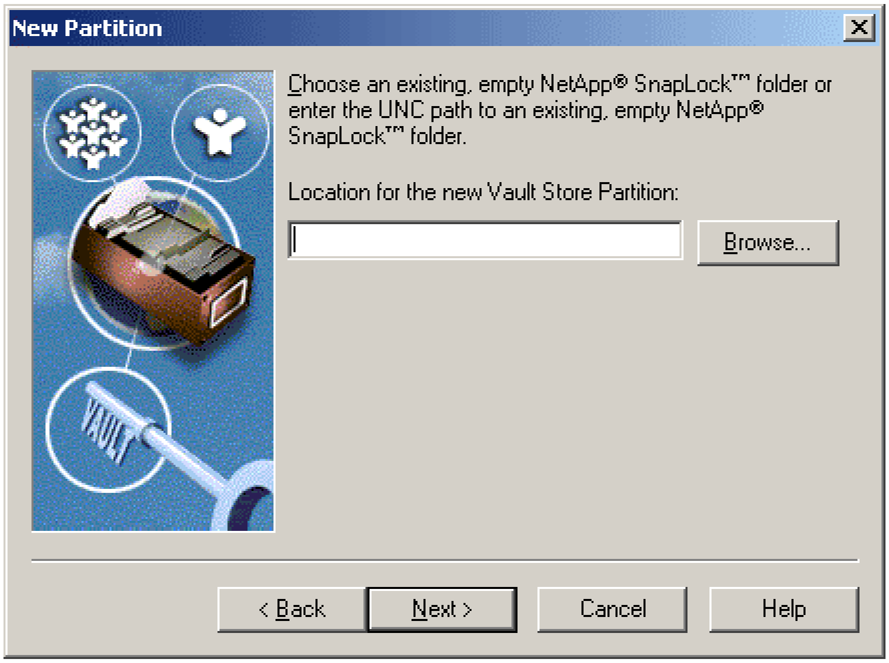
○ Network Share

● NetApp® SnapLock™ (WORM)

Figure 4) Selecting a vault store partition location.

Here, you will be asked for the type of storage solution. When connecting to a filer or to NearStore using iSCSI or Fibre Channel, the first option, NTFS volume, will be used. When connecting to a filer or to NearStore using CIFS or Windows file sharing, the second option, Network Share, is selected. For SnapLock WORM storage, the option highlighted in Figure 4 is used.

Either choice leads the administrator to a wizard page that asks the administrator to select a folder. Again, ensure that the service account for Enterprise Vault has been given read/write permissions to this folder location.



New Partition

Choose an existing, empty NetApp® SnapLock™ folder or enter the UNC path to an existing, empty NetApp® SnapLock™ folder.

Location for the new Vault Store Partition:

Figure 5) Choosing the SnapLock folder for a new partition.

Share archived items: Enterprise Vault optimizes the storage of shared items by archiving an item only one time, rather than archiving multiple copies. For example, if a message that has been sent to a large distribution list is archived, the message is stored on disk just once, rather than once for each recipient.

Technical Tip: On a SnapLock share, you must uncheck this option to prevent Enterprise Vault from attempting to update files, since they are already stored uniquely and cannot be modified once committed to WORM. There is a performance cost to provide share archived items.

6. NetApp SnapLock Configuration

Both SnapLock software products (SnapLock Enterprise and SnapLock Compliance) provide nonerasable, nonrewritable WORM functionality utilizing 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. As does an optical platter "burned" with data, both SnapLock software products protect data committed to WORM status from any possible alteration or deletion until its retention period has expired.

SnapLock Compliance and SnapLock Enterprise are implemented as add-on licenses to Data ONTAP. Both SnapLock software products run on a full range of NetApp storage platforms—from the NearStore nearline storage solution, which features lower-cost ATA-based drives, to the higher-performance filers, featuring fiber-attached disk drives. This flexibility allows customers to exactly match their storage choice to their business needs for SnapLock WORM storage, whether it is a few hundred gigabytes or hundreds of terabytes of data.

SnapLock Compliance was designed to assist organizations in implementing a comprehensive archival solution for meeting strict regulatory requirements for data retention (such as SEC 17a-4). Records and files committed to WORM storage on a SnapLock Compliance volume cannot ever be altered or modified but can be deleted after the expiration of their retention periods. Moreover, a SnapLock Compliance volume cannot be deleted until all data stored on it has passed its retention period and been deleted by the archival application or some other process.

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 permanently protected from alteration or modification but can be deleted after the expiration date. Functionality-wise, SnapLock Enterprise matches SnapLock Compliance exactly, with only one main difference: as the data being stored is not for the strictest regulatory applications, an administrator is trusted with the ability to delete a SnapLock Enterprise volume, including the data it contains.

VERITAS integrates with a NetApp storage device whether its volumes were created as traditional non-WORM, as SnapLock (WORM), or as a combination of both. The flexibility in VERITAS and NetApp environments provides businesses with configuration options to meet various needs while maximizing their investment in your archive framework.

6.1. Creation of a SnapLock Volume

Creating a SnapLock volume must be done from either the console or a telnet session to the filer or to NearStore and not through the FilerView® GUI. After a session is established, use the following command:

```
filer> vol create slcvol -L 14
```

Using the -L switch in the above command creates a SnapLock volume called slcvol with a default RAID-DP™ group and RAID size depending on the appliance.

Next, issue the following command to share the new volume to be accessed by Windows clients:

```
filer> cifs shares -add slcvol /vol/slcvol
```

Once the above steps are completed, verify the SnapLock volume and CIFS share status by using the commands `vol status` and `cifs shares`, respectively.

Files on a SnapLock volume get their SnapLock state flag set when their status is changed to read-only. Once this trigger event has occurred, attempts to modify or delete the file will fail. This is true no matter which user triggered the transaction to SnapLock state and which user is trying to modify or delete the file (i.e., administrator). Deletion of directories is allowed provided no SnapLock state files exist within their hierarchy.

Technical Tip: Create SnapLock volumes with care! They are meant to be hard to delete, so if there is a desire to create a "test" volume, be careful about setting parameters so that the space can be reclaimed easily—see the next section regarding retention dates.

Beginning in Data ONTAP 7G, files that have expired retention dates can be deleted from a SnapLock volume. Prior versions of Data ONTAP that are currently using SnapLock volumes with retention dates can upgrade to Data ONTAP 7G and enable the deletion feature, although it is not possible to revert from Data ONTAP 7G back to an earlier version. For more information, see NetApp Technical Report 3342, *Using SnapLock Compliance and SnapLock Enterprise with Data ONTAP 7G,* at http://www.netapp.com/tech_library/ftp/3342.pdf.

6.2. NetApp ComplianceClock™ and Retention Options

Secure Time Mechanism

For the purposes of regulatory compliance, Data ONTAP will utilize the ComplianceClock secure time mechanism, which will operate independently from the regular real-time clock of the storage system. This will permit the storage 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. It is important to ensure your filer or NearStore system is operating with the proper date and time before implementing ComplianceClock. To start ComplianceClock on a filer, issue the follow command:

```
filer> date –c initialize
```

Note: You will be asked to confirm that you want to initialize ComplianceClock and to verify the current date and time before implementing.

For regulatory purposes, the setting of the clock needs to be done in a compliant manner, including a review of the process by those advising the customer on compliance. The setting of the clock must also be included in compliance procedures in the event of an audit.

Steps for Successfully Configuring Retention Settings

It is critical that the SnapLock volume, ComplianceClock, and Enterprise Vault with retention dates are all set up properly to meet the requirements for compliance. These steps are as follows:

1. Create the SnapLock volume on the NetApp filer or NearStore system using the –L option, as demonstrated in section 6.1 of this document.
2. Ensure the filer or NearStore date and time are set properly by issuing the date command. Once the date and time are set properly, use the date –c command, as demonstrated in section 6.2 of this document, to set ComplianceClock.
3. Create or modify an Enterprise Vault vault partition and set the partition to archive to the newly created SnapLock volume, as demonstrated in section 5 of this document.
4. Create an Enterprise Vault retention category and assign it to the vault partition specified in step 3 above.

NetApp Volume Retention Parameters

SnapLock volumes provide options for configuring basic retention policies for both WORM files and Snapshot copies. These options include a default, minimum, and retention periods for the volume. A fast procedure to check the option setting of a volume is as follows.

```
filer> vol options wormvol
```

A sample output is as follows:

```
nosnap=off, nosnapdir=off, minra=off, no_atime_update=on,
raidtype=raid4, raidsize=8, nvfail=off, snapmirrored=off,
resyncsnaptime=60, create_ucode=off, convert_ucode=off,
maxdirsize=2621, fs_size_fixed=off, create_reserved=off,
snaplock_compliance, snaplock_default_period=max,
snaplock_minimum_period=0y, snaplock_maximum_period=30y
```

These retention parameters should be set prior to bringing a SnapLock volume into service to ensure that the desired retention policy is correctly reflected. The default values are not what most customers would choose to deploy when meeting regulatory requirements.

Minimum and Maximum Retention Periods

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.

The procedure for setting the minimum retention period is as follows (example: six-month period):

```
filer> vol options wormvol snaplock_minimum_period 6m
```

If not explicitly configured, the minimum retention period is 0.

The maximum retention period specifies the maximum allowable retention period for any file or Snapshot copy committed to WORM state on the SnapLock volume. The maximum retention period takes precedence over the default retention period.

The procedure for setting the maximum retention period is as follows (example: three-year period):

```
filer> vol options wormvol snaplock_maximum_period 3y
```

If not explicitly configured, the maximum retention period is 30 years.

Default Retention Period

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 procedure for setting the default retention period is as follows (example: one-year period):

```
filer> vol options wormvol snaplock_maximum_period 1y
```

The default retention period also accepts the values "min" and "max," which instruct the storage system to use the current minimum or maximum retention periods, respectively, as the default retention date. These can be specified as follows:

```
filer> vol options wormvol snaplock_default_period min

filer> vol options wormvol snaplock_default_period max
```

Technical Tip: It is important to take note of the default value of this parameter when not explicitly configured. For SnapLock Compliance volumes this parameter defaults to "max," which is by default and SEC mandate 30 years. For SnapLock Enterprise volumes this parameter defaults to "min," which is, by default, zero.

7. Using Retention Dates with Enterprise Vault

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. This feature of SnapLock will allow for association of record retention periods at the granularity of individual records. Each and every record committed to WORM on a SnapLock volume can have an individual associated retention date.

Once the retention period and SnapLock operations have 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.

Retention dates are set by an application that integrates with Network Appliance SnapLock, such as VERITAS Enterprise Vault for Exchange. Once a file has been archived by VERITAS to a SnapLock Compliance volume, the file cannot be deleted until the retention date has passed. The deletion of files with expired retention dates must be handled by VERITAS Enterprise Vault. SnapLock will allow the extension of file retention dates to allow records to be retained beyond their original retention period for continued use of the files, but retention dates ***can never be shortened***.

Setting Retention Categories Using VERITAS Enterprise Vault

1. After licensing the SnapLock Compliance volume and creating a VERITAS vault store on the volume, use the Enterprise Vault administration console to expand the vault site hierarchy.
2. Select New Retention Category: right-click and select new Retention Category.
3. By assigning a retention category to items at the time they are archived, it is possible to categorize stored items. This categorization makes it easier to retrieve items because it is possible to search by category.
4. A retention category also specifies the minimum amount of time that an item must be retained by Enterprise Vault. This length of time is the retention period. For mail messages, the retention period is the time since the message was received. For documents, it is the time since the document was last modified.
5. Users can select retention categories for mailbox folders or items so that, when archiving occurs, items are stored with the appropriate retention category.

Enterprise Vault also has some default retention categories that you can use or modify. You can create as many extra retention categories as you need, and you can create or modify retention categories at any time.

Technical Tip: Any time an item is archived in Exchange, it can receive a custom retention date based on which Exchange folder the item is located in. In addition, Enterprise Vault filtering allows for custom retention based on categorically identifying the item during the archive process. Contact VERITAS Professional Services or Support for more information.

Deletion of Files during the Retention Period

An additional consideration is that a SnapLock Compliance volume containing files that have not reached their retention period expiration dates cannot be deleted, even by an administrator. For this reason it is very important to carefully verify that Enterprise Vault is correctly setting the retention periods and that proper planning is conducted before setting the retention period and committing files to WORM state.

Advantages when Using Retention Dates with VERITAS and NetApp

The combination of VERITAS Enterprise Vault for Exchange stored on a Network Appliance SnapLock Compliance volume provides organizations with a solution for SEC regulations related to data retention. The SnapLock Compliance volume ensures the data committed to WORM storage cannot be altered or deleted before the expiration of its retention period. VERITAS Enterprise Vault for Exchange provides administrators with an easy-to-use management console for creating and specifying retention periods for a company’s e-mail infrastructure. Together, these products create a simple and cost-effective solution to help businesses address SEC regulations.

8. Data Recovery

Snapshot is a fast and easy way to create point-in-time backups of your data on a NearStore system or filer. While Snapshot copies of Enterprise Vault store partitions are supported, a Snapshot copy does not set the archive bit on files like a full online backup does. VERITAS Enterprise Vault may not delete safety copies left in Exchange. This occurs when Enterprise Vault configuration is set to "Remove safety copies from mailboxes after backup." Only after the archive bit has been set to off on an archived item will these safety copies be removed. Therefore, a trigger file must be created to address removal of safety copies.

To configure the trigger file option, use the registry editor tool on the KVS server and browse to the following key (caution: the registry contains important information about Windows, so be sure to have a current backup before proceeding):

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
 \KVS
 \Enterprise Vault
 \Storage
```

Using regedit, create a DWORD value called FileWatchEnableIgnoreArchiveBit and give it a value of 1.

Next, a file called IgnoreArchiveBitTrigger.txt must be created and placed in the root folder of each partition located on a NetApp storage device. This file is renamed or deleted by the storage service when safety copies are successfully deleted.

If the trigger file does not exist or cannot be renamed or deleted, the storage service reverts to its normal behavior of checking each save set's archive file attribute to determine whether it has been backed up. If a file's archive file attribute is set, then, for safety, the storage service does not remove safety copies.

After creating a Snapshot copy of the vault store files, place the IgnoreArchiveBitTrigger.txt file in the root folder of each partition that has been backed up. The storage service performs a check when it starts and then every 12 hours, and the safety copies will be removed from the Exchange server.

9. Further Information

9.1. Network Appliance

www.netapp.com
www.netapp.com/products/NearStore
www.netapp.com/products/filers
www.netapp.com/tech_library/ftp/3342.pdf

9.2. VERITAS

www.VERITAS.com/kvs

10. Revision History

Date	Name	Description
1/9/2004	NetApp	Update
6/1/2003	Chris Lueth	Creation

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