NETAPP TECHNICAL REPORT

# Solutions Blueprint for Symantec Enterprise Vault Mailbox Archiving on NetApp Storage Systems

NetApp Technical Marketing

Rick Krieger, Symantec

TR-3717

## 5,000 Seat Environment

This document is a blueprint for architecting and deploying Symantec Enterprise Vault in a 5,000 seat customer environment. This Enterprise Vault on NetApp deployment guide describes server sizing and storage requirements for mailbox archiving environments. As always, please refer to the latest technical publications on the NOW (NetApp on the Web) site for updates on processes, Data ONTAP command syntax, and the latest requirements, issues, and limitations. This document is intended for field personnel who require assistance in deploying and architecting an Enterprise Vault on a NetApp solution.

## TABLE OF CONTENTS

# 1 INTRODUCTION

## 1.1 PURPOSE

This Solutions Blueprint is a guide for field engineers to use when implementing Enterprise Vault for mailbox archiving on NetApp storage systems. It describes the architectural requirements for Symantec Enterprise Vault Mailbox Archiving running on NetApp FAS3000 series storage and protected by NetApp solutions.

## 1.2 TARGET AUDIENCE

This document is intended for information technology professionals and storage professionals who are responsible for corporate messaging infrastructure management. It assumes the reader has some technical experience installing, configuring, and administering the following technologies

- Symantec Enterprise Vault
- Data ONTAP
- Snap Manager for SQL
- SnapDrive
- Microsoft SQL Server
- Microsoft Exchange

## 1.3 SCOPE

This document only discusses architectural requirements for Mailbox Archiving with Symantec Enterprise Vault for Microsoft Exchange 2007, NetApp FAS3000 series storage, Data ONTAP 7.2, NetApp Snapshot technology, SnapMirror, and Snap Manager for SQL Server. For installation processes, refer to the references section of this document for the Enterprise Vault Installing and Configuring Guide, the Data Protection Online Backup and Recovery Guide, and the Data ONTAP Software Setup Guide.

Symantec Enterprise Vault also supports archiving from several other platforms. For more information, see the Symantec Enterprise Vault micro site at http://edm.symantec.com/enterprisevault.

# 2 NETAPP SOLUTIONS FOR SYMANTEC ENTERPRISE VAULT

## 2.1 ENTERPRISE STORAGE

Enterprise Vault stores and manages large volumes of data. Selecting and properly architecting the underlying storage system for an Enterprise Vault solution offers superior performance.  The three main data types Enterprise Vault works with are vault store data, indexes and vault store databases.

### 2.1.1 Disk Types

There are several data sets that can reside on different storage based on IOPS requirements. Enterprise Vault data can reside on many different types of disks. The two discussed here are Fibre Channel (FC) and Serial ATA (SATA) disks.

#### FIBRE CHANNEL

Fibre Channel disk drives have been on the market for a very long time. They are a proven and reliable storage device, with high read/write speeds, and they can handle high I/O loads. FC disks are ideally suited to handle Enterprise Vault I/O requirements.

#### SERIAL ATA

Lower-cost NetApp SATA storage solutions provide customers with an excellent opportunity to reduce storage costs or stretch their IT budget without incurring a noticeable application performance impact. SATA storage solutions can be leveraged in some environments for storing and managing Enterprise Vault indexes and vault store data. Although SATA disks are not intended to replace higher-performance FC disk drives, knowing candidate applications that could perform satisfactorily  on SATA disks helps achieve the best value and use of a given storage purchase.

SATA disk drives are becoming increasingly popular as a storage medium. SATA disks are a low-cost, high-capacity storage solution. Based on performance testing, SATA drives are suitable to host vault store data in several instances as well as indexes for customers that have up to 5,000 users.

### 2.1.2 RAID DP

RAID-DP is a double parity implementation of RAID 6 that prevents data loss when two drives fail. RAID-DP offers businesses the most compelling total cost of ownership storage option without putting their data at increased risk.[1]

## 2.2 DATA PROTECTION

Enterprise Vault has several data components that require proper planning for data protection. It is critical to maintain data consistency among these data sets at all times. NetApp's solution to backing up an Enterprise Vault data set involves a series of procedures and may use the read-only mode of Enterprise Vault to maintain data consistency among Enterprise Vault data components. The NetApp technologies described in this section can be used to back up Enterprise Vault data sets.

Many existing Enterprise Vault-NetApp customers have implemented one or more of the following technologies in their environment and are enjoying the benefits that they offer.

### 2.2.1 Snap Manager for Microsoft SQL Server

NetApp SnapManager for Microsoft SQL Server (SMSQL) is an integral part of the complete NetApp solution for protection of Enterprise Vault data.

#### SMSQL BENEFITS

Near-instantaneous backup and fast restore of entire SQL Server databases and full text indexes (SQL Server 2005) using NetApp Snapshot technology

- Easy migration wizards to move databases to SAN and IP SAN environments
- Easy-to-use, intuitive graphical user interface
- Rich backup scheduling and reporting
- Integration with SnapMirror for wide area data replication

### 2.2.2 Snapshot Copies

NetApp strongly recommends using Snapshot copies and SnapRestore for Enterprise Vault vault store and index backup and restore operations. Snapshot provides a point-in-time copy of the entire vault store data and index in seconds without incurring any performance penalty, and SnapRestore can instantly restore an entire database to a point in time in the past.

For Snapshot copies to be effectively used with Enterprise Vault, they must be coordinated with the Enterprise Vault trigger file mechanism, which tells Enterprise Vault that the copy has been completed and that it is OK to remove safety copies. For this reason, NetApp recommends that automatic Snapshot copies be turned off on volumes that are storing data files for an Enterprise Vault vault store data and indexes. For details about the cascading Snapshot methodology, see TR 3635:Symantec Enterprise Vault Data Protection with Network Appliance Storage System for additional details on the cascading snapshot methodology. For more information about the trigger file mechanism, see the Enterprise Vault Administrator's Guide.

[1] WP-7005-1006: NETAPP RAID-DP™: DUAL-PARITY RAID 6 PROTECTION WITHOUT COMPROMISE

### 2.2.3 SnapMirror

There are several approaches to increasing data availability in the face of hardware, software, and even site failures. Backups provide a way to recover lost data from an archival medium (tape or disk). Redundant hardware technologies also help mitigate the damage caused by hardware issues or failures. Mirroring provides a third mechanism to enhance data availability and minimize downtime. NetApp SnapMirror provides a fast and flexible enterprise solution for mirroring or replicating data over local area, wide area, and Fibre Channel (FC) networks. SnapMirror can be a key component in implementing enterprise data protection and disaster recovery (DR) strategies. If a disaster occurs at a source site, businesses can access mission-critical data from a mirror on a remote NetApp system for uninterrupted operation.

BENEFITS OF SNAPMIRROR

- Block-level updates reduce bandwidth and time requirements.
- Data consistency can be maintained at a DR site.
- A DR plan can be tested without affecting production.
- Synchronization between source and destination sites is complete.
- Mission-critical data can be mirrored.
- A DR location can keep many Snapshot copies at once; data can be restored to a point in time before data corruption occurred.
- Data can be replicated between dissimilar NetApp storage systems.
- A standard IP or FC network can be used for replication.
- SnapMirror supports one-to-one, one-to-many, many-to-one, and many-to-many replication, referred to as *cascading* and *multihop.*

**Note:** To achieve a true disaster recovery plan, NetApp recommends that SnapMirror either be in a different facility or backed up to tape.

# 3 SCENARIO: MAILBOX ARCHIVING 5,000 MAILBOXES

## 3.1 CONFIGURATION

To design a mailbox archiving solution, the following environment was assumed.

**Table 1) Environment configuration.**

| Quantity | Item | Version |
|---|---|---|
| One | Active Directory domain | 2003 |
| One | Enterprise Vault | 2007 |
| One | Microsoft Exchange | 2007 |
| One | Microsoft SQL Server | 2005 |
| One | FAS3000 Series – Data ONTAP | 7.2 |
| 5,000 Users | | |

### 3.1.1 Software Used

The following software was used in developing this solution blueprint:

- Single Active Directory forest
- Single Active Directory domain

- NetApp FAS3000 Series with Data ONTAP 7.2
- Symantec Enterprise Vault for Microsoft Exchange 2007
- Microsoft Exchange 2007 on Windows 2003
- Microsoft SQL 2005 on Windows 2003
- Windows 2003 Client Machines
- NetApp SnapDrive
- NetApp SnapManager for Microsoft SQL Server

# 4 SOLUTION BLUEPRINT

## 4.1 HIGH-LEVEL ARCHITECTURE

This section describes the detailed solution blueprint, including in-depth information about the Enterprise Vault architecture and the proposed storage configuration. It describes the way that Enterprise Vault should be configured to meet the customer business requirements and technical requirements discussed earlier in this document.

## 4.2 ENTERPRISE VAULT

### 4.2.1 Recommended Allocation of Enterprise Vault Site Servers

The following information is complete and is fully scalable to support a multisite failover.

**Table 2) Enterprise Vault environment server allocation.**

| Server | Quantity | Server Specification (see below) |
|---|---|---|
| Mailbox Archiving (EVMBA01) | 1 | Type 1 |
| SQL Server (32bit)(EVSQL01) | 1 | Type 1 |

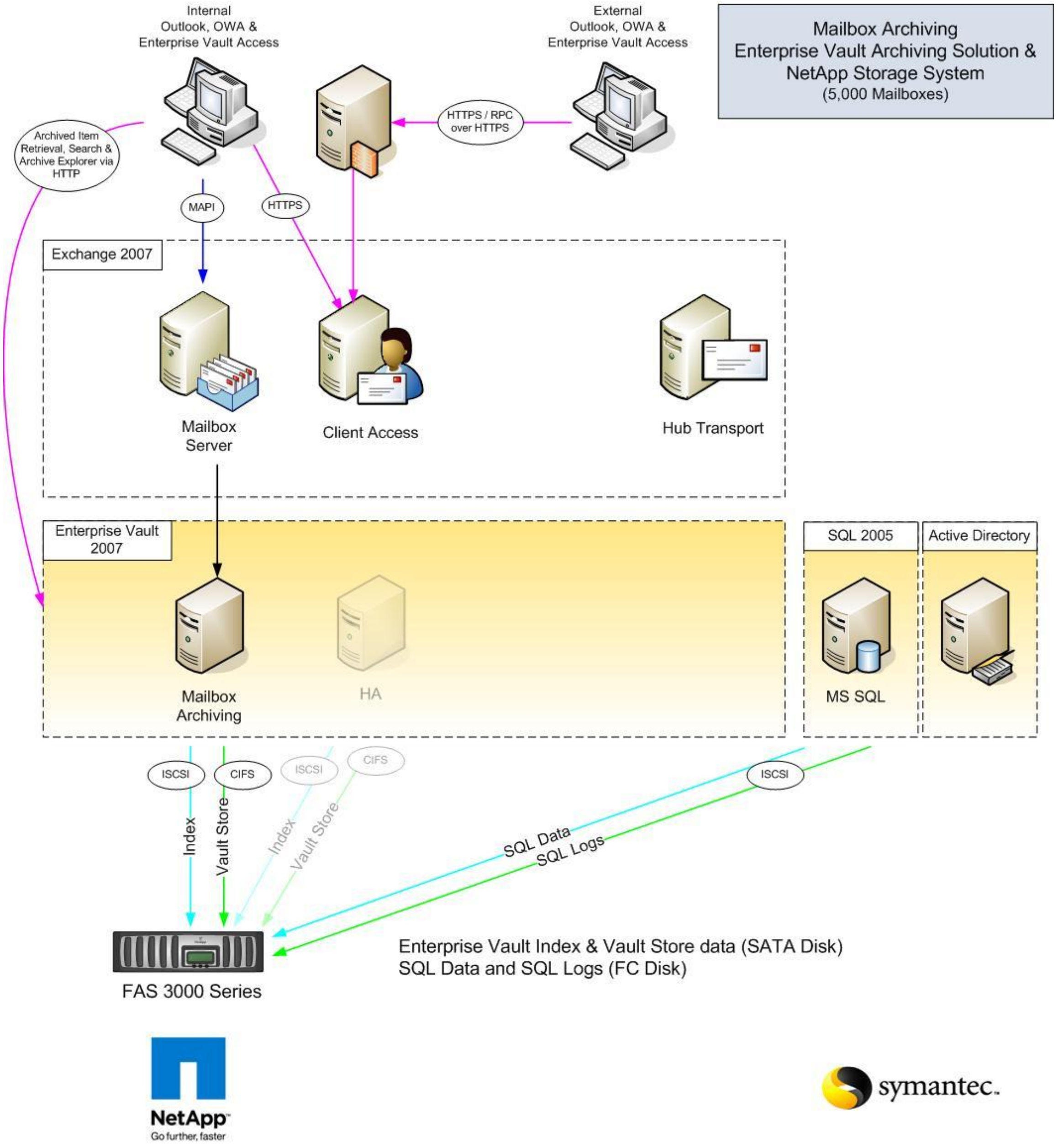

**Figure 1) Enterprise Vault recommended architecture.**

## SERVER SPECIFICATIONS: TYPE 1

| | |
|---|---|
| Processor: | Dual 3.2+ GHz, dual core |
| OS: | Windows 2003 Server Enterprise (32 bit) |
| Memory: | 4+ GB |
| HDD: | 20+ GB (system/boot), 20+ GB (application) |
| Recommended: | For fault tolerance, include mirrored system partitions |
| Public Network: | Two Gigabit Ethernet NICs (teamed and configured for “fail on fault”) for public access and public cluster heartbeat, connected to different switches |
| Storage Network: | Two iSCSI Hardware Initiators |

## 4.3 STORAGE REQUIREMENTS

Enterprise Vault requires space to store archived items and metadata that describes those items, as well as space to be used for steady state processing. The following list outlines the main items to consider when sizing an Enterprise Vault environment.

- SQL databases
- Index locations
- Index level (brief, medium, full)
- Vault store partitions
- Shopping locations
- MSMQ storage locations
- PST Holding temp folder
- PST Migration temp folder

The one-year storage projections that follow in this section focus on the following items:

- SQL databases
- Index locations
- Vault store partitions

These items grow as content is archived; they represent the majority of the storage requirements for an Enterprise Vault environment. The system shown in table 3 meets the requirements for the Enterprise Vault site.

**Table 3) FAS3000 series storage system.**

| Feature | |
|---|---|
| Controller | FAS 3000 Series |
| Raw Capacity | 10TB SATA<br>1.1TB FC |
| Disk Shelves | 2 |
| SATA Drives | 20 * 500GB 7.2 K RPM |
| FC Drive | 8 * 144 10K RPM Disks |
| ECC Memory | 4GB |
| iSCSI Hardware Initiator | |

This section describes the projected storage required to support the deployment of Enterprise Vault for one year of archived data. These numbers do not include backlog numbers, which can vary greatly from site to site. The projections are based on the assumptions shown in table 4.

Table 4) Projected storage assumptions.

| Assumption | |
|---|---|
| Total number of mailboxes | 5,000 |
| Number of mailboxes to be archived | 5,000 |
| Number of working days in the year | 260 |
| Average message size (KB) | 130 |
| Average messages sent/received per user per day | 45 |
| Percentage of deleted mail per user per year (%) | 45 |
| Indexing (Full, Medium, Brief) | Full |
| Single instance storage ratio | 1.1 |
| Compression percent of original size (%) | 60 |

Table 4) Year-one storage requirements.

| Year One Storage Estimate | Archiving from Users' Mailboxes after One Year |
|---|---|
| | |
| Number of mailboxes | 5,000 |
| Average message size | 130 |
| Total number of items archived | 35,100,000 |
| **Total Amount Archived in Year (GB)** | 4,352 |
| | |
| Vault store NTFS (GB) | 2,654 |
| Indexes (GB) | 522 |
| Vault store DB (GB) | 8 |
| **Total (GB)** | **3,184** |

**Note**: The storage numbers in table 4 do not include e-mail backlog or ingestion of PST files.

## 4.4 STORAGE LAYOUT

### 4.4.1 Disk Utilization Estimation

This section estimates disk utilization for the underlying storage subsystem for Enterprise Vault indexes, vault stores, and SQL databases. These data are expressed in IOPS and are based on the estimated maximum disk utilization during an archiving window. Table 5 shows the assumptions behind these estimates.

Table 5) Disk utilization estimate assumptions.

| Assumptions | | |
|---|---|---|
| Archiving rate | 35,000 | Items per hour |
| Average message size | 130 | KB |
| Single instance ratio | 1.1 | |
| Compression percent | 60 | % |
| Indexing level | Full | |
| Disk array standard block size | 4 | KB |

Table 6) Disk IOPS estimates during archiving.

| | Archiving Rate (GB per hour) | Disk Usage (IOPS) | Data Profile |
|---|---|---|---|
| Vault store | 1.46 | 106 | Sequential writes |
| Indexes | 0.40 | 29 | Random reads and writes |
| SQL DB and logs | 0.76 | 56 | Random reads and writes |

Table 7) Disk IOPS estimates during basic index search.

| | Concurrent Searches | Disk Usage (IOPS) | Data Profile |
|---|---|---|---|
| Indexes | 30 | 3.5 | Random reads and writes |

### 4.4.2 Aggregate Sizing and Layout

Table 8) Storage layout for year one.

| Server | Aggregate Name | Raid Group Size | Disk Capacity/Type | Total Disks | RAW Aggregate (right sized) | Usable Aggregate |
|---|---|---|---|---|---|---|
| EV | EV_Data | 12+2 | 500 GB 7.2K rpm SATA | 14 | 5.3TB | 4.6TB |
| SQL | EV_SQL | 6+1 | 144 GB 10K rpm FC | 7 | 864GB | 800GB |

### 4.4.3 Volume Sizing and Layout *

Table 9) Volume layout.

| Server | Volume Name | Containing Aggregate | Volume Size |
|---|---|---|---|
| EV | EV_MSMQ | EV_Data | 50GB |
| EV | EVIndex1 | EV_Data | 500GB |
| EV | EVIndex2 | EV_Data | 500GB |
| EV | EVData1 | EV_Data | 1.75TB |
| EV | EVData2 | EV_Data | 1.75TB |

| | | | |
|---|---|---|---|
| SQL | SQL_DATA | EV_SQL | 100GB |
| SQL | SQL_LOGS | EV_SQL | 100GB |

[*] Includes the directory database and vault store database.

**Note:** The sizing shown in table 9 includes estimates for Snapshot reserves.

### 4.4.4 Drive Mapping

**Table 10) Storage layout, Enterprise Vault server.**

| Drive Letter | Description | Disk Label |
|---|---|---|
| C:\ | Operating system | |
| D:\ | Application install directory | |
| E:\ | MSMQ | |
| F:\ | | |
| G:\ | | |
| H:\ | Index data (connected via iSCSI) | |
| I:\ | Index Data (connected via iSCSI) | |
| UNC | Vault store data (connected via CIFS) | |
| UNC | Vault store data (connected via CIFS) | |

**Note:** If required by the customer, mount points are supported. See Microsoft KB - http://support.microsoft.com/default.aspx?scid=kb;en-us;205524.

**Table 11) Storage layout, Microsoft SQL Server.**

| Drive Letter | Description | Disk Label |
|---|---|---|
| C:\ | Operating system | |
| D:\ | Application install directory | |
| E:\ | | |
| F:\ | | |
| G:\ | | |
| H:\ | | |
| I:\ | SQL data | |
| J:\ | SQL logs | |

## 4.5 CASCADING SNAPSHOT METHODOLOGY

This section, describes the procedure to back up Enterprise Vault data by using the SnapDrive for Windows utility and database backup with the SnapManager for SQL Server tool. This process creates cascading Snapshots copies. SnapDrive uses the underlying Snapshot technology to back up the data while maintaining data consistency. By default, NetApp recommends backing up nightly all Enterprise Vault data sets and truncating the Microsoft SQL transaction logs after the backup is complete. When SnapManager for SQL Server is installed to manage SQL Server databases, and the databases reside on one or several NetApp storage volumes, the database consistency is maintained by SnapManager for SQL Server. SnapDrive can be used to back up the Enterprise Vault data such as Enterprise Vault indexing data, shopping data, and vault store files. The rest of this section describes the main events for the Enterprise Vault backup.

### 4.5.1 Put Enterprise Vault into Read-Only Mode

This is to maintain data consistency between different sets of data in the Enterprise Vault environment. It is accomplished by changing the registry key values. In this mode, users are still able to access e-mail, but they cannot restore items from the archive.

### 4.5.2 Use SnapManager for SQL Server Backup/Restore Wizard or CLI-Based Commands to Back Up SQL Server and Enterprise Vault Related Databases

Maintaining the database in a consistent state is critical in an Enterprise Vault environment. SnapManager for SQL Server provides the tool to back up SQL Server databases. SnapManager for SQL Server allows CLI-based commands to back up SQL Server databases.

### 4.5.3 Use SnapDrive Snap-In tool or CLI-Based commands to Back Up Enterprise Vault Index and Storage Service File Locations (Stored on LUNs)

For performance reasons, Index and storage services and file locations use LUNs. If an Enterprise Vault Index is stored on a SnapDrive managed LUN, this snap-in tool makes it easy to manage the storage system, including the ability to back up and restore data.

### 4.5.4 Release Enterprise Vault from Read-Only Mode

It is important to release Enterprise Vault server into read-write mode. In read-only mode, items get queued up quickly. Releasing Enterprise Vault enables it to address that problem by restarting the archival process. Removing the safety copy depends on the settings. After backing up all Enterprise Vault related data, you should purge the archived items from the Exchange server.

### 4.5.5 Schedule

The Snapshot scheduler is not used with Enterprise Vault data sets. Because of the requirement to put Enterprise Vault into a quiesced state, a scheduled script is used to perform the task.

The backup script used to automate this process is shown in Appendix 8.2.

## 4.6 HIGH AVAILABILITY

To provide mission-critical and high-availability solutions to customers, Symantec offers a planned strategy in case of system down time. High-availability server configurations for Enterprise Vault use clustering or Enterprise Vault Update Service Location (USL)/building blocks configuration. With these technologies, Enterprise Vault can be configured in active-active or active-passive (N+1) mode.

With the USL active-active mode, Enterprise Vault services can run on both servers simultaneously (via USL only). If one server fails, the second server takes over the additional services.

With the USL clustered active-passive mode, all Enterprise Vault services run on one server. The passive server simply waits in standby until the production server fails.

Here are several possible Enterprise Vault high-availability solutions that are used in customer sites:

- SAN or NAS boot
- Enterprise Vault Update Service Location (USL)
- Active-passive pair
- Enterprise Vault Warm Standby (N+1)
- Clustering with Veritas Cluster Server (VCS / SFW-HA)
- Clustering with Microsoft Server clusters – MSCS

This blueprint uses USL as the high-availability strategy for Enterprise Vault.

NetApp recommends using volume management software to handle movement of SAN disk resources on the Enterprise Vault servers. This facilitates faster and easier failover with USL. For example, SnapDrive can be used to accomplish this.

### 4.6.1 Update Service Location

To use the Update Service Location function, Enterprise Vault must be installed with DNS aliases for all the physical computers. This abstraction layer creates a virtualization of Enterprise Vault computers and the services that run on them. When a failure takes place, the computer DNS alias can be directed to either another server running Enterprise Vault (active-active) or a hot spare (N+1). The USL command is run and Enterprise Vault checks which services should be configured on the server to which the alias is pointing. If new services are needed, they are created automatically; if there are more services than required, they are removed. As long as the underlying Enterprise Vault data is still available, user downtime can be calculated by the length of time it takes to update a DNS alias and run the EV Update Service Location command.  If Enterprise Vault is to be configured in an active-active solution, you must calculate the workload for two servers and make sure that a single server can handle the extra requests. When running in a failed state, Enterprise Vault should be configured to run in Read Only mode.

Figure 2 illustrates a failure of the server that is using USL.

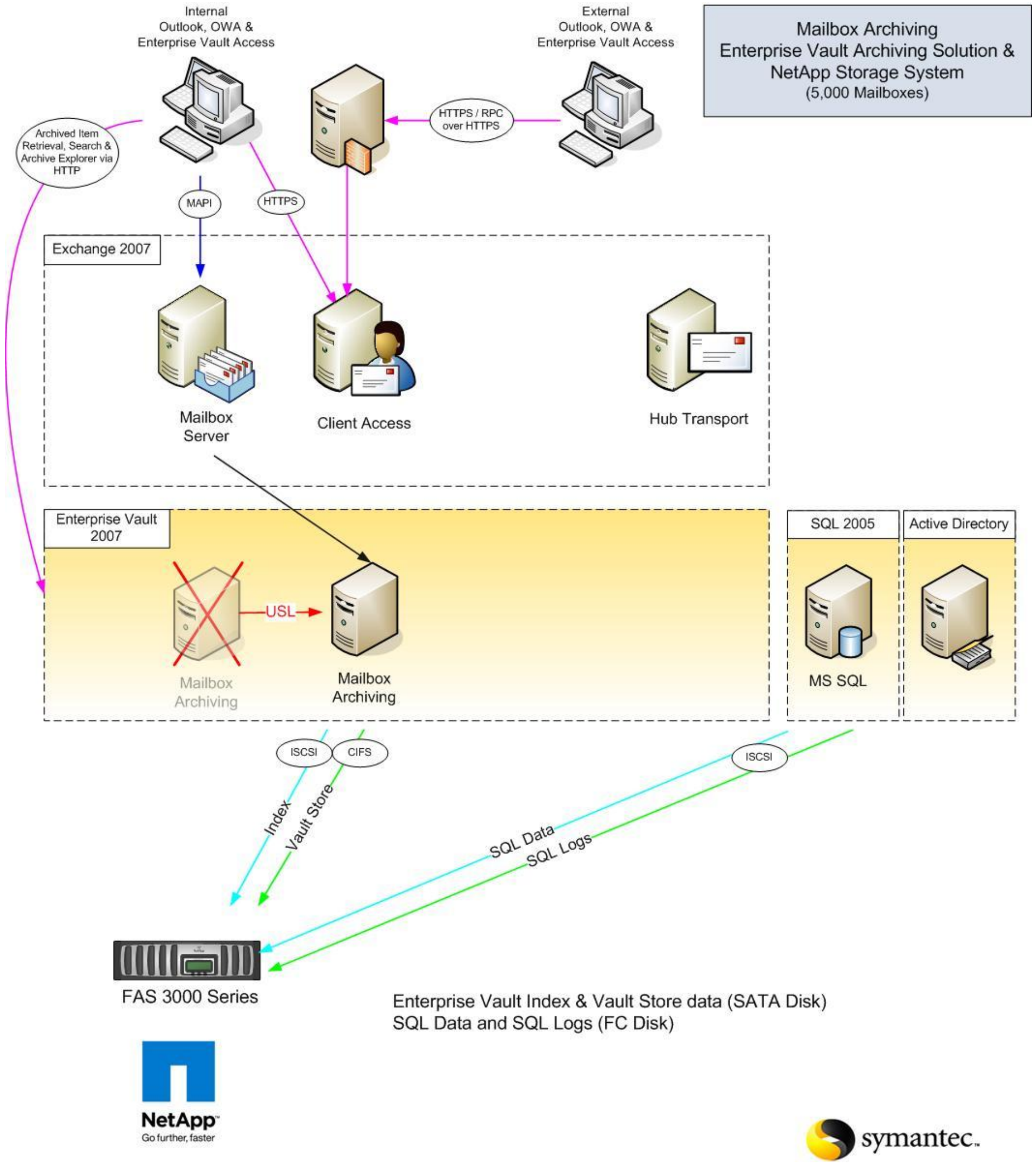

**Figure 2) Enterprise Vault recommended architecture for high availability.**

### 4.7 HIGH-LEVEL RESTORE SCENARIOS

Table 12) Disaster recovery options.

| Scenario | Impact | Restore action |
|---|---|---|
| A single Enterprise Vault server failure | All access is unavailable | Perform disaster recovery process, described in Chapter 23, Enterprise Vault Administrator's Guide. |
| Loss of SQL Server | All access is unavailable | Perform disaster recovery process, described in Chapter 23, Enterprise Vault Administrator's Guide. Restore Microsoft SQL Databases by using SnapManager for SQL. |
| Loss of a single storage head | All access is unavailable | Surviving head at the same site automatically takes the name of the failed controller and services all iSCSI disk requests from all local servers. |
| Loss or corruption of index data | User Web Search and Archive Explorer may be unavailable. | Recover corrupted or lost folder by using SnapRestore. Rebuilding the index is an alternative, although time-consuming, option. |
| Loss of directory SQL database | All archiving, retrieval, and search are unavailable | Stop all Enterprise Vault Services and restore Microsoft SQL Databases by using SnapManager for SQL. |
| Loss of vault store SQL database | Archiving and retrieval of the lost database are unavailable | Stop all Enterprise Vault Services and restore Microsoft SQL Databases by using SnapManager for SQL. |
| Loss of vault store data | Archiving to and retrieving from the lost Vault Store are unavailable | Recover lost folder by using SnapRestore. |
| Full disaster, such as loss of all servers | All access is unavailable | Perform disaster recovery process described in Chapter 23 of the Enterprise Vault Administrator's Guide. |

# 5 BEST PRACTICE RECOMMENDED CONFIGRUATIONS

### 5.1 ENTERPRISE VAULT APPLICATION REGISTRY SETTINGS

## 5.1.1 Indexing Schema Type

The default behavior of Enterprise Vault is to build indexes in a way that provides an index entry for attachments separately from their parent e-mail item. Setting this to a value of 1 enables the use of the optional schema when building new indexes and prevents this behavior, resulting in fewer index entries being made. (That is, the separate entry for attachments is not made.)

This is an index server-level flag that affects *all* new and rebuilt indexes on the server. Existing indexes are not affected by this flag.

**Key:** HKEY_LOCAL_MACHINE\SOFTWARE\KVS\Enterprise Vault\Indexing\

**Value name:** SchemaType

**Base:** DWORD

**Value data:** 1

### 5.1.2 Convert File Types to Text

Enterprise Vault by default tries to convert items into HTML. For certain documents this can be time consuming. NetApp recommends converting these items to text to improve the performance of the archiving process.

**Key:** HKEY_LOCAL-MACHINE\SOFTWARE\KVS\ENTERPRISE VAULT

**Value name:** TextConversionFileTypes

**Base:** String

**Value data:** DOC .XLS .PPT .RTF .POT .PPS .ZIP .PDF

## 5.2 STORAGE BEST PRACTICES

### 5.2.1 Storage Layout Best Practices

NetApp recommends putting the MSMQ storage area on a separate volume or separate spindles if possible to enhance performance because Enterprise Vault uses MSMQ extensively.

If necessary, shopping locations can be located on the same volume as the index or vault store data.

NetApp recommends a minimum of 8 Index locations per indexing service. They can be placed in separate LUNS, placed in folders inside one larger LUN, or in mount points underneath an empty folder. The LUN and folder sizes should be designed to accommodate efficient and regular backups.

Based on the data collected from the Exchange environment and the 1:2 allocation of Enterprise Vault servers to Exchange servers and on the data rates observed on these servers, the utilization of space for index and vault store location may vary slightly between Enterprise Vault servers, as shown in Table 9.

SQL Transaction Log partition size determined by taking multiplying the expected daily transaction log volume (2.3GB per day) by 10 to provide a buffer in case the database maintenance plan is not truncating the log as expected.

### 5.2.2 I/O Requirements and Disk Selection

It is important to strike a balance between storage capacity and I/O throughput. Larger drives such as 1TB SATA drives provide tremendous storage capacity and value, but with these larger drives the amount of I/O that can be handled per given storage amount goes down. This may not be a problem for some applications, or even Enterprise Vault, but care should be taken to understand the amount of I/O that a given disk subsystem or volume can provide.

If indexes are to be placed on SATA disks in an environment of this size, then the volumes used by the Enterprise Vault indexes should be sized to provide 2,000 I/Os for adequate end- user search, discovery search, archiving, and reindexing performance.

### 5.2.3 Disable Opportunistic Locking

The CIFS protocol allows a client to request the ability to cache locally the contents and attributes of an open file. This usually results in a dramatic performance gain. However NetApp recommends disabling opportunistic locking (oplock) for Enterprise Vault indexes because the indexes usually contain extremely important data in large files, so if oplock is enabled, a lot of important data being cached on the client could get lost if the network or the power failure.

Oplock can be disabled on the NetApp storage by using the command options cifs.oplocks.enable off or by using FilerView.

### 5.2.4 Disable Opportunistic Locking on Enterprise Vault Archiving Server

It is a best practice to disable opportunistic locking on the Enterprise Vault server as well,. so that opportunistic locking is not used even if it is enabled on the NetApp storage solution. This can be done by configuring the OpslocksDisabled registry key on the Enterprise Vault server.

For more information, see the following technote: http://seer.entsupport.symantec.com/docs/280922.htm

### 5.2.5 Hardware Initiator for iSCSI Configurations

There is some evidence that a software iSCSI initiator can affect CPU performance. Therefore NetApp recommends attaching the server to the storage by using a hardware initiator card for iSCSI.

A hardware initiator uses dedicated hardware, typically in combination with software (firmware) running on that hardware, to implement iSCSI. A hardware initiator mitigates the overhead of iSCSI and TCP processing and Ethernet interrupts, and therefore may improve the performance of servers that use iSCSI.

Also see the Symantec Enterprise Vault Indexing Best Practice Guide.

# 6 CONCLUSION

This technical report highlights the importance of the message that a joint solution of Symantec Enterprise Vault and NetApp storage is the right solution to exploit the benefits of both architectures. The NetApp storage solution complements the Enterprise Vault capabilities in the simplified storage architecture, backup, and restores areas.

The procedures described in this paper give an overview of the Enterprise Vault architecture. This paper serves as a starting guide for designing and deploying an Enterprise Vault on NetApp solution. During the design phase, it’s important to involve Microsoft Exchange and SQL Server specialists along with Enterprise Vault experts and to discuss the deployment plans and requirements with the Symantec and NetApp professional services teams. For details, refer to the product manuals.

# 7 REFERENCES

## 7.1 TECHNICAL REPORTS

TR 3525: Storage Performance Management

TR 3635:- Symantec Enterprise Vault Data Protection with Network Appliance Storage System

TR 3487: Snap Vault Best Practice

TR 3446: SnapMirror Best Practices

TR 3500: Installing EV with NetApp Storage Systems

## 7.2 BEST PRACTICES GUIDES

Symantec EV 2007 Performance Guide

Symantec Enterprise Vault Indexing Best Practice Guide

## 7.3 COMPATABILITY MATRIX

Symantec Enterprise Vault (tm) 6.0, 7.0 and 2007 Compatibility List

# 8 APPENDIX

## 8.1 BENCHMARK ENVIRONMENT

This section describes the environment used for the benchmark of the index performance.

The software components were distributed across several servers to isolate the components from shared resources that could potentially affect the benchmark.

| | |
|---|---|
| Active Directory<br>(Global Catalog) | 1 x Dell PowerEdge 2850 (2 x Intel Xeon 3GHz) 4GB RAM<br>(Hyper-threading Enabled)<br>2 x 33GB 15k disks in single logical RAID-1 volume<br>3 x 68GB 15k disk in single logical RAID-5 volume<br>Windows Server 2003 Enterprise Edition SP2, 32-bit<br>Active Directory Domain Controller with Global Catalog |
| Enterprise Vault | 1 x Dell PowerEdge 2950 (2 x Intel Xeon 3GHz Dual Core) 4GB RAM<br>(Hyper-threading Enabled)<br>Windows Server 2003 Enterprise Edition SP2, 32-bit<br>Microsoft ISCSI Initiator 2.04<br>Enterprise Vault 2007 SP2 Release Version. |
| User Simulator<br>(Python Host) | 1 x Dell PowerEdge 2950 (2 x Intel Xeon 3GHz Dual Core) 4GB RAM<br>(Hyper-threading Enabled)<br>1 x 136GB 15k SAS disks in single logical RAID-0 volume<br>4 x 136GB 15k SAS disks in single logical RAID-0 volume<br>Windows Server 2003 Enterprise Edition SP2, 32-bit<br>Python ActiveScript |
| Database | 1 x Dell PowerEdge 2850 (2 x Intel Xeon 3GHz Dual Core) 8GB RAM<br>2 x 36GB 15k disks in logical RAID-0 volume<br>1 x 146GB 15k disk in logical RAID-0 volume (log)<br>1 x 146GB 15k disks in logical RAID-0 volume (log)<br>1 x 146GB 15k disks in logical RAID-0 volume (log)<br>14 x 146GB 15k disks in three logical RAID-0 volumes (data)<br>Windows Server 2003 Enterprise x64 Edition, SP1<br>Microsoft SQL Server 2005 Enterprise x64 Edition |
| Vault Store | NetApp R200 |
| Index Storage<br>(System under test) | NetApp FAS3020—Data ONTAP 7.2.2 |

| | |
|---|---|
| Index Storage (Comparative) | NetApp FAS6030— Data ONTAP$^{TM}$ 7.2.1 |
| Index Storage (Comparative) | Local Disk 4 * 68 GB Raid 5 (3+1) – 15K Seagate |
| Network | -1000 Base-T TCP/IP Switched Network |

## 8.2 BACKUP SCRIPT

```
net stop /y "Enterprise Vault Task Controller Service"
net stop /y "Enterprise Vault Shopping Service"
net stop /y "Enterprise Vault Indexing Service"
net stop /y "Enterprise Vault Storage Service"

Echo Set EV to read only and restart services
Pause
regedit /s c:\temp\Backupmodekeysreadlonly.reg

net start "Enterprise Vault Storage Service"
net start "Enterprise Vault Indexing Service"
net start "Enterprise Vault Shopping Service"
net start "Enterprise Vault Task Controller Service"

rem Run this SQL Manager script
Echo Snapshot SQL with CLI
pause
rem cd\program files\netapp\snapmanager for SQl server
rem smsqlbi -H EVMAINSVR\EV -S EVMAINSVR\EV -C 0 -Recent -UM -R -N
Pause

Echo Snapshot indexes and data and replicate
Pause
rsh fas02 -l root:password snapmirror update -S fas01:evindex evindex2
rsh fas02 -l root:password snapmirror update -S fas01:evdata evdata2

Echo Stop EV Services
Pause
net stop /y "Enterprise Vault Task Controller Service"
net stop /y "Enterprise Vault Shopping Service"
net stop /y "Enterprise Vault Indexing Service"
net stop /y "Enterprise Vault Storage Service"

Echo Return EV to read write and restart services
regedit /s c:\temp\Backupmodekeysreadwrite.reg

net start "Enterprise Vault Storage Service"
net start "Enterprise Vault Indexing Service"
net start "Enterprise Vault Shopping Service"
net start "Enterprise Vault Task Controller Service"

Pause
Echo - remove safety copy
copy c:\temp\IgnoreArchiveBitTrigger.txt
J:\EVStores\EXCH_VS01\IgnoreArchiveBitTrigger.txt
net stop "Enterprise Vault Storage Service"
net start "Enterprise Vault Storage Service"
```