Symantec® Enterprise Vault™ Data Protection with Network Appliance™ Storage Systems

Gangoor Sridhara, Network Appliance, Inc.

TR-3635

Executive Summary or Abstract

Enterprise Vault (EV) Server has several dataset components to manage the messaging data. Enterprise Vault deployment is complex and often requires high level of planning and analysis work to be done. Enterprise Vault configuration has several inter-related dataset components that need to be consistent at all time, especially during the backup and recovery period. Access to emails is critical to businesses and hence, there is a need to offer a solution reducing or eliminating the downtime while maintaining the data consistency. This paper discusses Enterprise Vault backup and recovery solutions exploiting the unique NetApp advantages of NetApp cascading Snapshot procedure. This paper discusses the storage considerations for backup and recovery of Enterprise Vault using cascading Snapshots of backup copy of various components of Enterprise Vault datasets.

TABLE OF CONTENTS

1. Purpose and Scope

The purpose of this technical paper is to educate the reader about NetApp storage solutions for backup and restore of Symantec e-mail archival application Enterprise Vault server data set components. This paper is not a substitute for any product documentation and release notes provided with Symantec Enterprise Vault and the NetApp storage system and additional NetApp software solutions such as SnapLock®.

For detailed procedures on how to install and configure these products, please refer to the appropriate product documentation supplied with your release of software and hardware. This applies as well to the SQL Server™ and Microsoft® Exchange Server(s) required for a complete demo or production environment.

This paper describes the steps required to deploy Symantec Enterprise Vault in combination with NetApp storage systems within the context of an exchange messaging and NTFS file system environment.

Note: Enterprise Vault also supports several other messaging applications, including IBM Domino and Microsoft SharePoint® portal. Additional information regarding Enterprise Vault support for these applications can be found on the Symantec Enterprise Vault Web site. These topics are not covered in this document.

2. Introduction

Enterprise Vault has several data components. Enterprise Vault architecture involves SQL Server data set, Enterprise Vault Archive files, Enterprise Vault Index services and file locations, Enterprise Vault Storage service and file locations, and optional Enterprise Vault FSA file system data and SharePoint portal data set. It is critical to maintain data consistency among these data sets at all times. It is important to manage the several components of Enterprise Vault during the backup and recovery process. This leads to understanding the various data sets involved with Enterprise Vault configuration. Backup and recovery of data within Enterprise Vault need to be evaluated carefully while designing a backup and recovery architecture. Today's solution to backing up an Enterprise Vault data set involves a complex procedure and may involve the offline mode to maintain data consistency. This paper will provide a solution to put Enterprise Vault into a consistent state and create a consistent state of backup. This paper explains the procedure to using cascading Snapshot copies of various Enterprise Vault component data. By using cascading Snapshot copies, Enterprise Vault data can be backed up quickly, maintaining data consistency. Various components of Enterprise Vault are listed below:

- Enterprise Vault Directory database
- Vault Store database(s)
- Enterprise Vault Monitor database
- FSA Reporting database (if FSA configured)

Note the location of the following data sets:

- Enterprise Vault Index Services and files
- Enterprise Vault Shopping service
- Enterprise Vault store files

2.1. Cascading Snapshot Copy Approach

This paper uses the cascading Snapshot copies capability to achieve a consistent state of data backup of different components of Enterprise Vault data set. Enterprise Vault consists of several underlying data sets such as SQL Server database(s), Enterprise Vault Index service and locations, Shopping service, Archival

items, File system archival data set, SharePoint portal, and public folder data sets. It is critical to maintain the consistency across various components of Enterprise Vault data sets, enabling the quick recovery of data when needed. Using cascading Snapshot copies, this paper describes the procedure involved with Enterprise Vault backup and recovery. Figure 1 provides a brief overview of the cascading Snapshot copy process used with backup and restore.

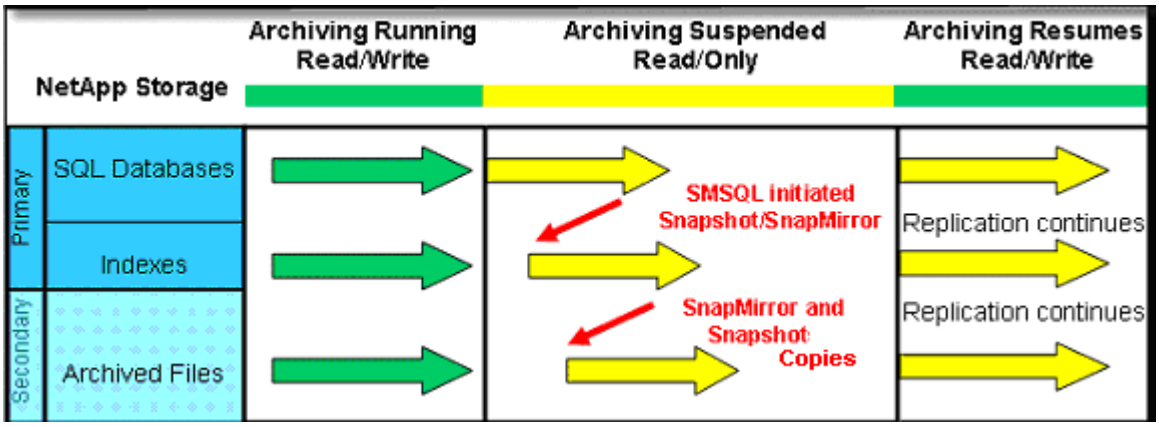

Figure 1: Cascading Snapshot Copy

This document covers the Enterprise Vault server configurations, techniques for backing up Enterprise Vault data, as well as the ability to restore it while providing data consistency and a reduced backup/recovery window. This paper describes the procedure based on a NetApp disk-based backup and recovery solution. The paper also discusses the data management tools involved with the process, such as SnapDrive® for Windows®, SnapManager® for SQL Server, Snapshot, and SnapRestore® technologies.

This paper does not provide a disaster recovery solution and is not a replacement to any Enterprise Vault product manuals. This paper is not applicable for designing an Enterprise Vault implementation architecture. If data components are stored on third-party storage systems, explained procedures may not work.

Note that the backup procedure to maintain data consistency without the cascading Snapshot copies involves a complex and time consuming alternative process. By using the cascading Snapshot copy approach, an Enterprise Vault administrator can configure an elegant solution for backup and recovery requirements.

After reading this paper, the reader will be to understand the Enterprise Vault backup and recovery methodology. Readers will be able to leverage the advantages of NetApp storage system solution offerings particular to Enterprise Vault and Exchange environments.

Specifically, this report covers the procedure to back up and restore Enterprise Vault data sets using cascading Snapshot copies, SnapManager for SQL Server, SnapMirror, and optionally SnapManager for Exchange server.

2.2. Assumptions

This paper makes the following assumptions while explaining the backup and restore procedure in an Enterprise Vault environment.

The reader has good Windows administration skills. Reader is assumed to have the necessary user authentication and administrative access to the Enterprise Vault and SQL Servers.

The reader has the necessary administrative skills to manage Network Appliance storage systems.

The reader has the necessary database administration skills or has access to SQL Server Administrator.

NetApp storage systems have the necessary product licenses enabled.

Both NetApp storage system(s) and Enterprise Vault server configurations are complete.

3. Additional Information

This section provides information required to understand the Enterprise Vault backup and restore environment such as requirements, background information, and the test infrastructure details.

3.1. Requirements

Successful backup and restoring of Enterprise Vault require a good plan and a well-laid-out configuration of SQL Server, databases, Enterprise Vault Server, and data setup. It is required to make the above assumptions to ensure the information provided in this paper is useful.

It is required to have a NetApp storage system configuration with Enterprise Vault deployment to complete the procedures discussed in this paper.

3.2. Background

Enterprise Vault deployments require a well-designed architecture to address data availability, performance, and reliability. Enterprise Vault has several moving parts in reference to its underlying data sets. Enterprise Vault application needs to coordinate with SQL Server and various client services. It is a challenging task to back up the various components of Enterprise Vault data sets while maintaining data consistency. Each component of an Enterprise Vault data set plays an important role. It is a common practice to rebuild the Enterprise Vault Index in case of corruption of that Index data. Rebuilding the Index could take days, affecting not only the data availability, but also the performance of Enterprise Vault server. This might result in lost productivity. This paper provides a solution to address such issues by creating the backup with cascading Snapshot copies. Creating Snapshot copies happens almost instantly. By employing this strategy, Enterprise Vault server will be in read-only for a very brief period. This paper explains the procedure to back up Enterprise Vault data sets by creating a Snapshot copy of data by cascading each data set. By using this paper, an effective disaster recovery solution may be developed by using NetApp storage management solutions. These solutions include SnapManager for SQL Server, Snapshot, SnapRestore, and SnapMirror® technologies.

Understanding the infrastructure requirement to back up and restore Enterprise Vault data plays a critical role. In an enterprise customer environment, the configuration involves multiple Enterprise Vault computers, multiple Exchange Servers, in addition to several NetApp storage systems. In addition to the server information, note down the database layout information, including the names and locations of the database data and log files. With best practices in mind, this paper assumes that SQL Server system databases reside on a separate LUN from Enterprise Vault databases. Enterprise Vault Directory database resides on another LUN and Enterprise Vault store databases reside on a separate LUN to provide the ability to restore a specific vault store database without affecting the directory database or Enterprise Vault environment. Note that SnapManager for SQL Server (version 2.1R1 or later) supports the ability to back up or restore a single database maintaining data consistency. Analyze the infrastructure of servers and storage systems in an Enterprise Vault environment.

3.3. Test Infrastructure

The test setup in this paper used the following infrastructure:

- Microsoft Exchange Server on Windows 2003 Server
- Microsoft SQL Server 2005 on Windows 2003 Server
- Enterprise Vault Server 2007 on Windows 2003 Server
- NetApp FAS3050 Storage System
- Windows 2003 Client Machines
- NetApp SnapDrive 5.x Software
- NetApp SnapManager for SQL Server Version 2.1R1
- Enterprise Vault Directory Database on a separate LUN
- Microsoft SQL Server system database on separate LUN from user databases
- Vault Store databases on separate LUN
- Enterprise Vault index and shopping service files shared on LUNs
- Enterprise Vault store archive files on compliance volume using SnapLock feature

3.4. Key Benefits of SnapManager for SQL Server

SnapManager for SQL Server offers several advantages in a Symantec Enterprise Vault environment to back up and restore SQL database components. Following are some of the key benefits:

- Ability to restore clustered databases without taking the virtual server offline
- Option to skip transaction log backup prior to a database restore operation
- Ability to store multiple databases on a LUN with the transaction logs for the databases on another LUN
- Multiple management groups for designating various levels of backup retention: Standard, Daily, and Weekly
- Restore of individual databases when multiple databases share the same LUN
- Post-backup command execution (typically used for archiving purposes, including archiving through SnapVault® software)
- Backup naming conventions: generic naming and unique naming
- Increased control of SnapMirror replication
- Command line interface for backup and verification operations
- Unattended installation of SnapManager application
- Near-instantaneous hot backups and near-online restores, which reduce backup and recovery time from hours or days to minutes
- Automation of administrative tasks within an easy-to-use user interface (UI)
- Support for both iSCSI and Fibre Channel environments
- Support for storage of multiple LUNs belonging to same or different SQL Servers or partitioned servers on a single storage system volume, provided by SnapDrive software

- Support for Microsoft Cluster Server (MSCS)
- Support for e-mail alerts sent to administrators warning of critical potential problems
- Support for storage system SysLog and AutoSupport services to convey information about errors and other events pertaining to virtual disks

4. Setup

It is important to understand the storage configuration environment in creating a good backup and recovery plan for Enterprise Vault setup. Enterprise Vault requires NTFS file systems. Data could be archived onto a network share.

In our test setup, we installed SQL Server on a virtual local disk configured by SnapDrive software. SnapDrive supports both iSCSI and FCP protocol LUNs. Local disks configured by SnapDrive were used to install applications and store data, and the details are provided below.

- Microsoft Exchange Server 2003 installation on a separate Windows server
- Enterprise Vault application installation on another Windows server
- Microsoft SQL Server installation on a separate Windows server or on Enterprise Vault Server
- For storing the SQL Server database data file(s)
- For storing the SQL Server transaction log(s)
- For storing Enterprise Vault Index Services and files
- For storing Enterprise Vault Storage Service and files
- SQL databases include the following databases in Enterprise Vault environment
    - Enterprise Vault Directory database
    - Enterprise Vault store database(s) for each Vault Store
    - Enterprise Vault Monitoring database

In addition to the above data sets, Enterprise Vault setup requires a storage configuration for archiving the vault store files. Configure the network share with a SnapLock volume to enable the compliance write-once read-many (WORM) feature. SnapLock enables maintaining the retention period set by the application. On our test setup, we used the compliance edition of SnapLock while configuring the Vault store partition to archive the vault store files.

Create a SnapManager data configuration plan using the information provided in the SnapManager for SQL Server administration guide. SnapManager does not support backups of databases stored on third-party storage devices.

4.1. Procedure to Use SnapManager for SQL Server

- Install SnapManager for SQL Server if not already installed.
- After Installation use Configuration wizard to move databases to LUN(s).
- Use SnapManager Backup to create backup data.
- Use SnapManager Restore (when required to restore backup).
- Use SnapManager backup facility to initiate SnapMirror through SnapDrive.

Figure 2 provides a storage management architecture while using SnapManager for SQL Server on a NetApp storage system setup.

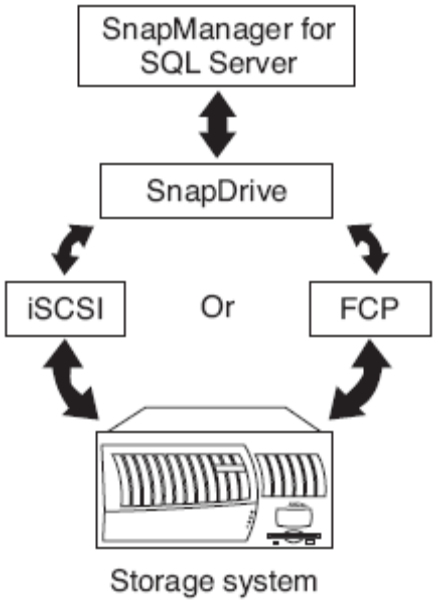

Figure 2: Storage Management Architecture on NetApp Storage System

In order to effectively back up or restore an Enterprise Vault data set, it is important to understand the storage system configuration. This includes the configuration of local drives and network share. On our test setup, we configured the local drives to store Enterprise Vault databases such as Vault Directory database, vault store databases, and SQL system databases on separate LUNs. Figure 3 shows the SnapDrive created local drives on the Enterprise Vault Server.

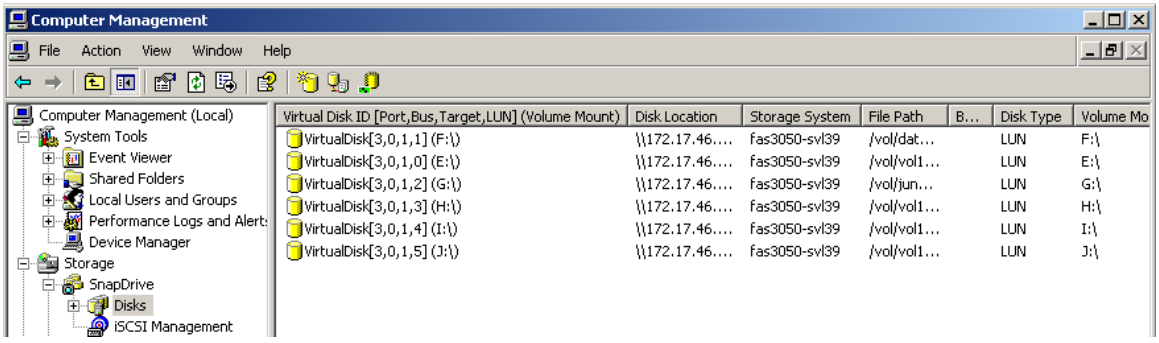

Figure 3: List of Available LUNs on Enterprise Vault Server

Figure 4 clearly explains the architecture of SnapManager for Windows platform. SnapManager for SQL Server is able to interact with SnapDrive as well as SQL Server using VDI API and SQL-DMO layers.

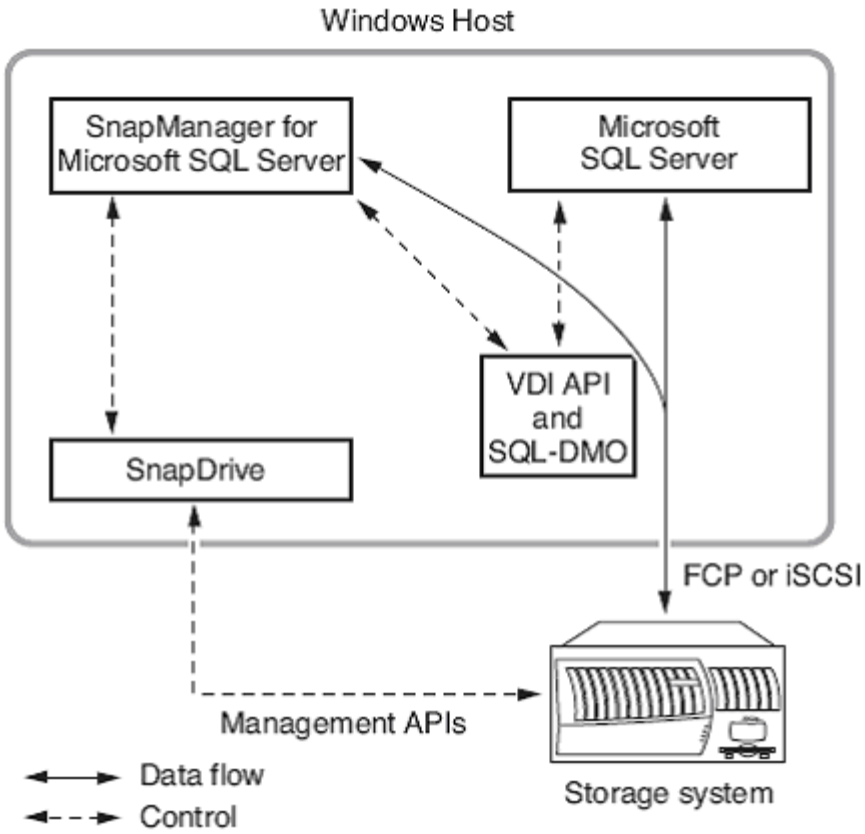

Figure 4: SnapManager for Windows Architecture

It is recommended to use SnapManager for SQL Server technology as a complement to conventional backup processes. SnapManager backup data resides on primary disk, and this paper strongly suggests moving your backed up data to alternative media locations such as a NearStore® storage system or to another NetApp storage system. This provides an additional level of backup data availability in case of loss of backup data on the primary location. NDMP or the '*dump*' (storage system) command efficiently transfers the backup data to other media locations.

When SnapManager for SQL Server is used to back up databases, do not perform backup of transaction logs using any other applications. Some backup applications are known to truncate the transaction logs after the backup is done.

Use NTBackup or another tool to archive SnapManager for SQL Server backups to a file instead of tape. This file set can be stored on a storage system.

SnapManager Preinstallation Tasks

Verify Windows host system requirements.

Verify Storage system requirements.

Prepare Windows host system for installing SnapManager.

Make sure to create three or more dedicated LUNs to hold SQL Server data and log files and the SnapManager SnapInfo directory. SnapInfo directory and the transaction log files cannot be housed on the same LUN.

Best practice is to place System databases and User databases on separate LUNs.

4.2. Required Storage Infrastructure

According to the Unified Storage methodology, Fibre Channel (FC) or iSCSI protocol devices should be used for the Microsoft Exchange Information Store and SQL Server database. Additionally, the Enterprise Vault indexes should be put on this same type of storage. Note that Enterprise Vault supports Enterprise Vault Indexes on network share as well as LUN storage. If compliance is required for Enterprise Vault Index storage, this paper recommends configuring the network share and using SnapLock enabled volumes. Storing Enterprise Vault Index on network share may provide easier data management. Network share configuration may provide a quicker way to recover compared to data stored on a LUN. Putting Enterprise Vault Index on LUN may offer improved performance compared to network connectivity.

4.3. Required Infrastructure Used in Test Setup

The environment documented in this report is composed of the following components:

- Exchange Server: Windows 2003 Service Pack 1 Enterprise Edition
- SQL Server 2005 and Enterprise Vault Server: Windows 2003 Service Pack 2 Enterprise Edition
- E-mail archival and file system archival: NetApp FAS3050C storage system running Data ONTAP® 7G
- E-mail archival and FSA data migrating service: NetApp R200 storage system running Data ONTAP 7.x or later releases
- Storage management software such as NetApp SnapDrive and SnapManager for SQL Server
- Enterprise Vault Server 2007 with necessary license enabled

For complete compatibility and support matrix, refer to the NOW™ (NetApp on the Web) site. (This link requires NOW access.)

4.4. Enterprise Vault Configuration

By installing the Enterprise Vault server application on a NetApp storage system, system administrators can quickly restore the system from the backup of a previous Snapshot copy.

Review the Enterprise Vault configuration to make sure it includes the server information for SQL Server, Exchange Server, Enterprise Vault Installation path, Databases, and the storage configuration. Understanding the Enterprise Vault deployment architecture provides critical information to develop backup and recovery plans. SnapManager for SQL Server provides the ability to back up or restore individual or all databases residing on the same LUN.

The following figure illustrates a configuration of Enterprise Vault system with relevant Enterprise Vault components.

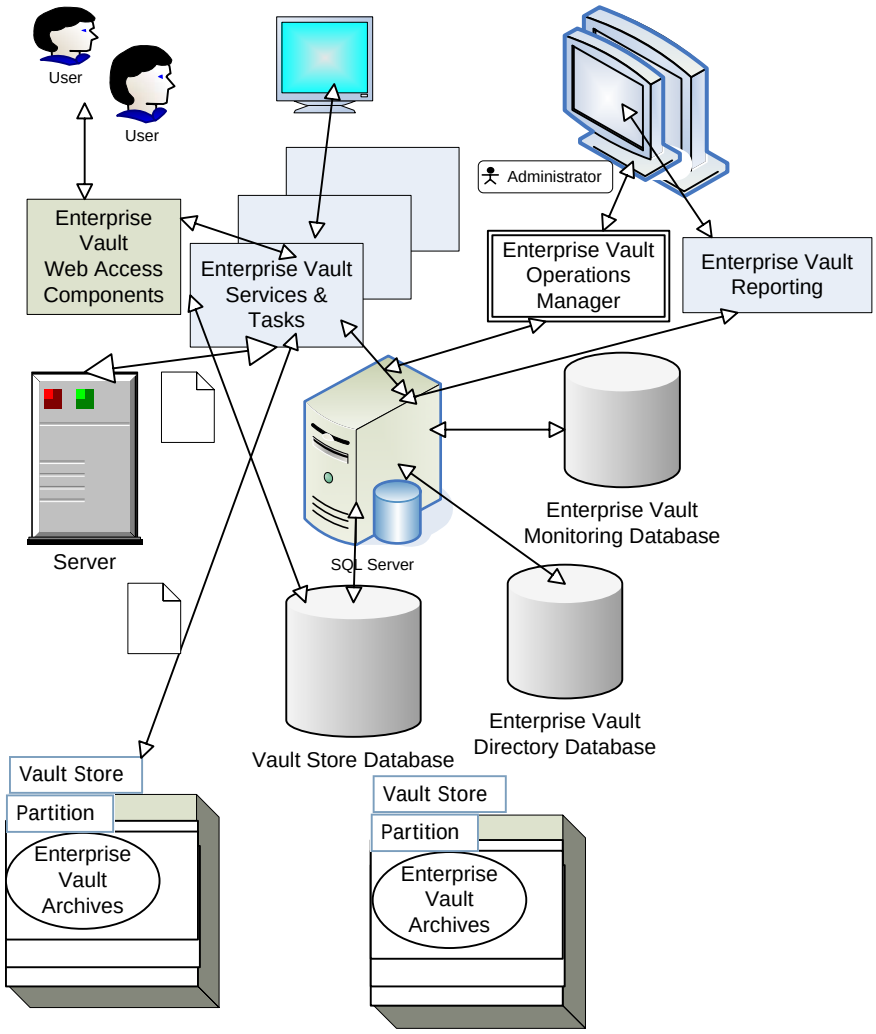

Figure 5: Enterprise Vault Server Configuration

Storage solutions from NetApp address the Enterprise Vault backup and recovery issues by maintaining the databases in consistent state. They also reduce the backup and recovery window as well as improve data availability by reducing the time required to put Enterprise Vault server in read-only mode during the backup.

4.5. Directory Database Location

Enterprise Vault Directory database is a critical component in Enterprise Vault configuration. For successful backup and recovery of Enterprise Vault, it is important to maintain a backup copy of this database. As a prebackup task, note the Enterprise Vault Directory database and its location. Best practice is to place this database in a separate LUN, separating the SQL Server system databases.

4.6. Vault Store Database(s)

Enterprise Vault Directory database may contain more than one Vault Store. Each Vault Store requires a Vault store database. As a best practice, this paper suggests placing the databases and corresponding transaction logs on a different LUN created by SnapDrive. SnapManager for SQL Server is able to restore the data of a particular database. Hence, it may not be required to store databases and logs on separate

volumes. This configuration allows administrators to restore just the Vault store database(s) without having to restore the Directory database.

4.7. Enterprise Vault Monitoring Database

When the Enterprise Vault Operations Manager component is installed, this database is created. This contains data collected by monitoring agents to be used by Operations Manager and reporting services.

The database created is called “EnterpriseVaultMonitoring.”

4.8. File System Archival Reporting Database (FSA Reporting Database)

If FSA Reporting is configured, it is necessary to back up the database called “EnterpriseVaultFSAReporting.”

4.9. Vault Store Files and Locations

When Enterprise Vault archives the items from Exchange server, it archives onto a specified storage destination. In our case, Vault store files are archived onto NetApp SnapLock volumes. While configuring Enterprise Vault, this paper recommends using a Windows Schedule task to map the required NetApp storage volumes automatically during the system startup process. This setup ensures the storage accessibility to Enterprise Vault to write to the target storage location.

When Vault store files are stored on a SnapLock volume to meet compliance requirements, the data has to be replicated by using qtree level SnapMirror configuration. This configuration requires the resync of the data with the original data set each time a backup is created.

Once the Exchange Server is installed and configured, update with Service Pack 2. On our test setup, the Microsoft Exchange Wizard displayed a message about successful installation status of the software product.

4.10. Microsoft SQL Server

Enterprise Vault requires Microsoft SQL Server 2005 or SQL Server 2000 SP3 Server. A large Enterprise Vault environment may need a dedicated SQL Server on Windows Server. SnapManager for SQL Server allows the database backup and recovery to occur easily. In a production environment, several scenarios cause the Enterprise Vault index to be corrupted. In case of Enterprise Vault index corruption, the administrator has to restore the data from the backup. Using SnapManager for SQL Server and SnapDrive, a consistent backup and restore of the data is required. It helps to bring the system into production. If the SQL Server is already installed, skip this section.

During the test setup, this paper used SQL Server 2005 and created data and log devices on SnapDrive configured virtual disks. During a test setup, the SQL Server installation utility checks the system configuration as shown below.

Figure 6: SQL Server Used in Enterprise Vault Environment

4.11. Installation

This paper will not discuss the installation procedure for Enterprise Vault. It is recommended to refer the appropriate product manuals to understand the application installation process. TR3500 describes the procedure for deploying Enterprise Vault using NetApp storage system(s). As a prerequisite, understand the current deployment configuration of Enterprise Vault. Note down the details of the Enterprise Vault data set such as names, storage location, and so on.

4.12. Policy Scheduling

It is possible to set a policy to back up Enterprise Vault data. Policy scheduling involves Enterprise Vault and NetApp storage system configuration. Enterprise Vault configuration allows setting a policy regarding data archival and other settings. It is possible to configure the data backup using storage management tools such as SnapManager for SQL Server and SnapMirror technology to back up the data, then replicate to a second location.

5. Possible Scenarios for Breakdown of Enterprise Vault Processes

There are several reasons for the loss of data in an Enterprise Vault environment, causing Enterprise Vault server accessibility problems to users. In this section, a few possible reasons are listed.

5.1. Accessibility to Directory Database

Enterprise Vault configuration information is stored in this database. Access to this database is always required to continue running Enterprise Vault. If the access to this database is lost, Enterprise Vault stops working. The Enterprise Vault server could be configured in a LAN cluster and replicate the database to provide a higher data availability for Directory database access. Restoring Directory database from a previous Snapshot copy is possible and quicker.

5.2. Enterprise Vault Index Corruptions

Due to several operational reasons, the Enterprise Vault Indexes can become corrupted. If the Enterprise Vault Index gets corrupted, it has to be rebuilt. When the Enterprise Vault Index gets corrupted, data loss on Enterprise Vault server happens. This could be addressed in a NetApp storage environment with Snapshot, as it is simple to back up and easy to restore the Enterprise Vault Index from the previously known Snapshot data. Again, replicating the Enterprise Vault Index is another alternative while developing the backup option.

5.3. Loss of Digital Vault Saveset (DVS) Files

Enterprise Vault archives the items and saves them in digital vault saveset (DVS) files. It is important to back up all Vault store files. These Vault store files are stored in several directories depending upon the Enterprise Vault archival setup. If these files are stored in a volume location other than SnapLock, Snapshot is the best way to back up the data as it could be accomplished almost instantly without any performance impact on applications. Other ways to back up are to replicate using SnapMirror and migrating to tape or secondary storage systems or by clustering configuration and replicating to another site. If the Vault store archive files are stored in a SnapLock volume, you must use qtree level SnapMirror to maintain the data backup. By using qtree level SnapMirror, data on the target system can be resynced with the source at the next backup process. This approach will help to maintain the compliance properties of the source archive files.

5.4. Loss of Vault Store Database(s)

Each Vault store created generates a new Vault store database. These databases are prone to corruption due to various reasons. The most common reasons for data corruption are dropping communication midway through a file check-in and running out of disk space. Other reasons could include physical overwriting of the database file or deleting the file. In this scenario, the Enterprise Vault Administrator needs to restore Vault store databases from a previously known good backup copy. Using SnapDrive, Vault store database(s) could be restored from an available Snapshot copy. This paper recommends using SnapManager for Exchange to back up or restore Exchange data in an Enterprise Vault environment.

5.5. Exchange Server Database Corruption

Similar to Enterprise Vault SQL database(s) corruption, Exchange server databases could get corrupted due to several reasons. If the Exchange database gets corrupted, there is loss of connectivity to the Enterprise Vault archival process. The Exchange database could be backed up using SnapDrive or using SnapManager for Exchange server. SnapManager for Exchange allows easier storage management of Exchange server data. Again, a NetApp storage solution such SnapDrive for Windows and/or SnapManager for Exchange Server can help to bring Exchange online quickly.

5.6. Loss of Enterprise Vault Server

If the Enterprise Vault Server becomes offline or has any server related issues such as network connectivity, loss of connectivity occurs. When the system is recovered, restore the data on the Enterprise Vault Server and bring online the Enterprise Vault Server application.

5.7. Loss of Shopping Service Files

Due to the reasons explained earlier, data related a specific Enterprise Vault component might be lost or corrupted. When the Shopping services files are lost, the shopping service may have disruptions. Using the Snapshot copy created by SnapDrive, these files and locations could be restored. These files are automatically restored if the data is shared with Index data on the same LUN.

6. Ongoing Operation or Workflow

The Enterprise Vault environment supports a full system or the application data backup types. In addition to this, it is necessary to back up Enterprise Vault registry keys on all Enterprise Vault computers where the

Vault Service Account (VSA) user logged into a system. This paper recommends developing a good backup strategy to prevent data loss in an Enterprise Vault environment. Understand completely the configuration of Enterprise Vault server, SQL Server, e-mail servers such as Microsoft Exchange Server, Domino server, as well as network connectivity. Enterprise Vault configurations involve multiple Windows servers and data spread across various servers. Having NetApp storage systems, a single, or multiple storage systems may be deployed to achieve storage and performance efficiency. Unique advantage of NetApp for Enterprise Vault in such configurations is the ability to support multiple hosts (Windows server in this case) to have storage setup. There are two types of backup configurations available in protecting the Enterprise Vault data. Another option is to back up the systems, services, and tasks that are treated as application backup in addition to full system backup.

6.1. Full System Backup

First, one is data backup, in which all the data needed to restore a complete system is backed up. This backup type allows restoring an entire system because of system data loss or data corruption. Recovery of Enterprise Vault depends on the type of backup involved. Cases of backing up only data require installing Enterprise Vault server, meeting all its prerequisite tasks.

6.2. Application Data Backup

Another option is to back up the systems, services, and tasks that are treated as application backup. Application data backup provides a quicker way of recovering the Enterprise Vault server environment.

6.3. Backing Up Enterprise Vault Registry Keys

It is important to back up the Enterprise Vault registry keys on all Enterprise Vault servers. Enterprise Vault creates or uses the registry keys to perform certain tasks. It is necessary to back up the registry keys to restore Enterprise Vault in case of data loss or during the rebuilding of the system.

6.4. Backup Procedure Tasks

This section provides the detailed procedure to back up Enterprise Vault data. It specifically discusses offline backup and online backup modes.

6.5. Offline Backup

Requires Enterprise Vault Services to be stopped and use SQL Server to back up database(s). When third-party configuration is used, a significant amount of time may be required to complete the backup. When stored on a NetApp storage system, a quick and efficient backup copy of the SQL Servers can be created using Snapshot technology. Advantages of offline backup procedure are that it is easy and data is always consistent. However, the major disadvantage is nonavailability of applications such as Enterprise Vault Server and SQL Server. Using a NetApp disk-based backup solution eliminates the requirement of longer time to finish the data backup. It is possible to create backup online and complete it quickly using NetApp storage solutions.

6.6. Online Backup

In enterprise environments, it is recommended to use separate servers for running SQL Server and Enterprise Vault servers. It is a requirement to run e-mail server applications such as Exchange server and Notes Server on dedicated servers.

6.7. SnapManager for SQL Server and Its Advantages

SnapManager for SQL Server provides an enhanced backup solution compared to SnapDrive capabilities. SnapManager for SQL Server provides a normal SQL Server backup capability. Hence, it is strongly recommended to implement SnapManager for SQL Server in an Enterprise Vault environment. SnapManager for SQL Server manages SQL Server to databases.

Use SnapManager for SQL Server to manage SQL Server. SnapManager for SQL Server provides database management in a consistent and easier way to back up and restore database data. SnapManager is a storage management utility managing NetApp storage systems on the operating servers. SnapManager for SQL Server provides a transparent approach to back up database data. SnapManager for Windows allows backup of the storage system's data. This data may include Enterprise Vault installation path, Index service, and Shopping service and file locations.

In the absence of SnapManager for SQL Server configuration, use the SnapDrive for Windows utility to back up the SQL databases. However, care must be taken if the databases reside across multiple NetApp storage system volumes.

To make it easier to understand the backup process, this paper assumes that the Enterprise Vault system has a clustered configuration not based on Enterprise Vault. Backing up data from a clustered environment is different, and it will be discussed later.

6.8. Backing Up Data

Normally it is required to stop all Enterprise Vault services prior to backing up the data. Stopping Enterprise Vault Services allows you to maintain data consistency among various Enterprise Vault data components such as Enterprise Vault databases, vault store databases, indexes, shopping service, and archival process. This paper provides a procedure to perform backup of data while Enterprise Vault server is online. This procedure helps to improve data availability compared to offline backup processes. No new data must be added to Enterprise Vault to maintain data consistency.

Determine the type of backup such as full system or application backup (whether to back up just the data or the application data).

Application Backup of Enterprise Vault Server Using NetApp Storage System Solution

It is important to have a backup of the complete system and files. This means the backup data must include the registry values while Enterprise Vault server is in operation.

Backup of Enterprise Vault Application Data Using NetApp Storage Solution

The data backed up using this procedure requires installing Enterprise Vault server along with its prerequisite software prior to recovering the Enterprise Vault server configuration. In this section, we provide the procedure to back up Enterprise Vault data using the SnapDrive for Windows utility and database backup with SnapManager for SQL Server tool. SnapDrive uses the underlying Snapshot technology to back up the data while maintaining data consistency. By default, it is recommended to back up at least once a week and truncate the transaction logs after the backup is done. 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 may be used to back up the Enterprise Vault data such as Enterprise Vault Indexing data, Shopping data, and vault store files. Use the SnapDrive snap-in tool in the Computer management console on the host server to back up the Enterprise Vault data.

It is important to understand the different stages involved in the backup process. Main events for the Enterprise Vault backup are listed below.

Archiving Exchange or Domino Mailbox Archiving

This requirement will be met with the setup of Exchange or Domino Server and enabling the mailbox archiving.

Enterprise Vault Archives E-Mail Items

Enabling the mailboxes for archiving is done in the Enterprise Vault Admin Console. Once the mailbox is enabled for archiving, the Enterprise Vault server archives the items.

Put Enterprise Vault into Read-Only Mode

This is to ensure data consistency between different sets of data within the Enterprise Vault environment. It is accomplished by changing the registry key values. During this mode, users will still able to access e-mails without having the ability to restore items from the archive.

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 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.

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 Enterprise Vault Index is stored on a SnapDrive managed LUN, this snap-in tool makes it an easy to manage the storage system, including the ability to back up and restore data.

Use CLI based commands to back up Enterprise Vault Archived items (Snapshot copies of network share). However, note that SnapLock volumes do not allow the data restoration from a Snapshot copy. Replicate the Enterprise Vault archived items to another NetApp storage system using SnapMirror to back up the data.

Enterprise Vault Archived items are stored on a network share. Use a CLI based command to create a Snapshot copy of the archived items. Note that if the archived items are stored on SnapLock volume, archived item data has to be replicated to a different NetApp storage system using the compliance SnapMirror feature.

Release Enterprise Vault from Read-Only Mode

It is important to release Enterprise Vault server into read-write mode. During read-only mode, items get queued up quickly. Releasing it enables it to address that by restating the archival process.

Removing the safety copy depends on the settings.

After backing up all Enterprise Vault related data, purge the archived items from the Exchange server.

6.9. Online Backup Procedure

- Verify Exchange and/or Domino mailbox setting is complete.
    - It is accomplished with the setting of Exchange or Domino server mailbox enablement.
- Put Enterprise Vault into read-only mode by following these steps.
- For a consistent data backup of Enterprise Vault server, put Enterprise Vault server in read-only mode. By changing the registry setting while Enterprise Vault services are stopped and then starting the services, Enterprise Vault server is configured to be in read-only mode. To put Enterprise Vault into read-only mode, use the following commands.
- EVservice stop “Enterprise Vault Task Controller Service”
- EVservice stop “Enterprise Vault Storage Service”
- EVService stop “Enterprise Vault Shopping Service”

- EVService stop “Enterprise Vault Shopping Service”

Wait for the services to be stopped and make the registry changes to the following keys under HKEY_LOCAL_MACHINE\SOFTWARE\KVS\Enterprise Vault\Storage. Create a file called BackupModeKeysReadOnly.reg to set the registry keys with the following registry value.

"*EnableArchive"=dword:00000000*

"EnableCrawler"=dword:00000000

"EnableExpiry"=dword:00000000

"EnableFileWatch"=dword:00000000

"EnablePSTMigrations"=dword:00000000

"EnableReplayIndex"=dword:00000000

“EnableRestore”=dword:00000000

a. Use regedit command to change the registry key entries.

b. Start Enterprise Vault Services by using the following commands:

c. EVService start IBMX336-SVL21 “Enterprise Vault Storage Service”

d. EVService start IBMX336-SVL21 “Enterprise Vault Index Service”

e. EVService start IBMX336-SVL21 “Enterprise Vault Shopping Service”

f. Verify that the Services are started.

g. Use SnapManager for SQL Server to back up Databases.

h. Start the SnapManager for SQL Server Backup and Restore configuration wizard.

i. We can use the SnapManager for SQL Server wizard to back up the data. In this section, we will discuss the procedure using the SnapManager for SQL Server wizard as well as command line syntax.

j. Select the databases to be backed up.

k. Select the Snap-Info directory location.

l. Start the backup.

m. Verify the backup status.

If SnapManager for SQL Server is not configured on the Windows server, complete it by running the configuration wizard before proceeding with the backup and restore feature. Start the SnapManager for SQL Server backup and restore wizard and complete the initial configuration of SQL Server as shown below.

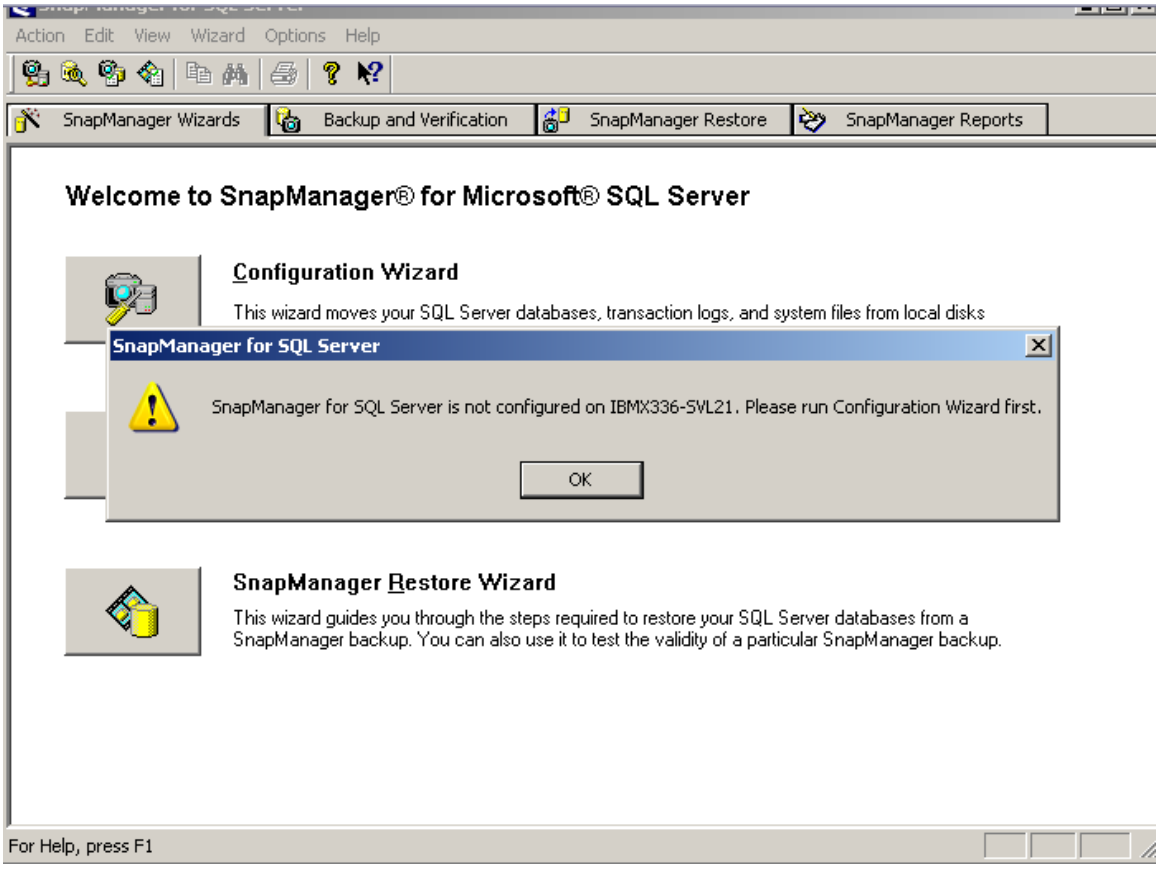

Figure 7: SnapManager for Microsoft SQL Server

SnapManager for SQL allows online backup of databases by creating a Snapshot copy of the data on the LUN by leveraging the Microsoft backup application programming interfaces (API) for Microsoft SQL Server. SnapManager for SQL Server works exactly as a third party SQL Server backup and recovery application. Once SnapManager is configured on the Windows server, select the database backup wizard to select the databases for the backup. The tool provides the details of the database selected such as database name, NetApp storage system where the LUN is configured, and volume name. Note that SnapManager for SQL Server 2.1R1 or later releases supports the capability to back up or restore a single database. On our system, we selected all the databases to be backed up, as shown in the following figure.

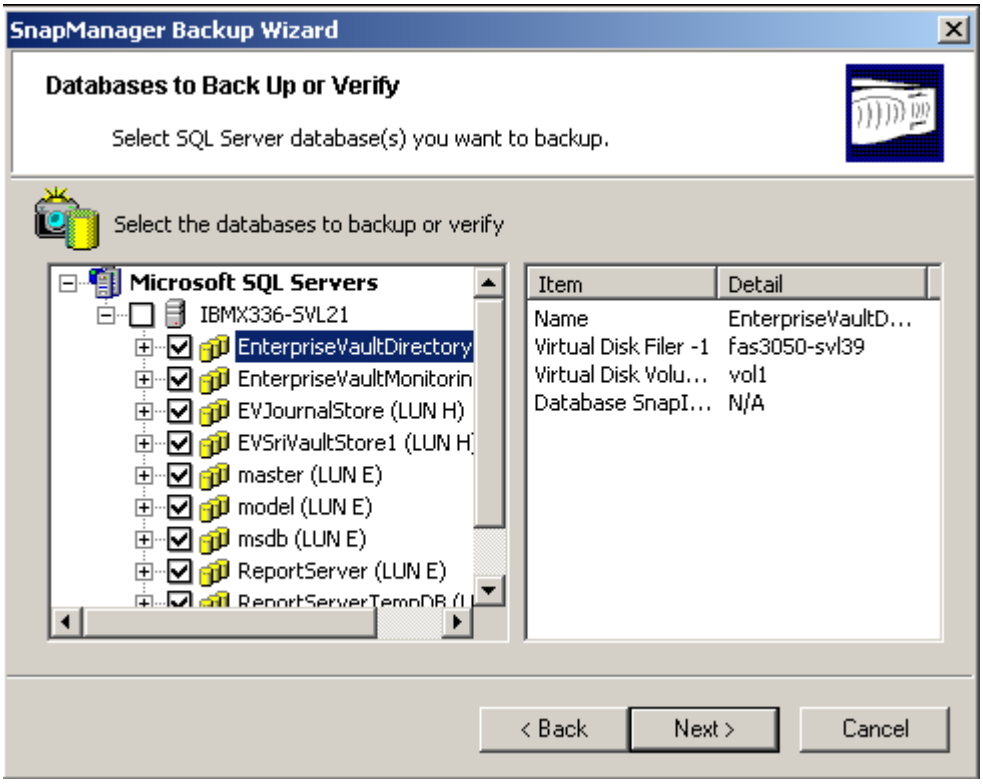

Figure 8: Databases to Back Up Using SnapManager for SQL Server

Select the databases that are to backed up on the verification server. The SnapManager for SQL Server backup wizard provides the option to select a full database backup, transaction log backup, and/or verify most recent unverified Snapshot backups by running the DBCC CHECKDB command. Using this wizard, configure the backup options such as the ability to retain a certain number of backup copies, retain up to the minute restore ability, and to verify the database after backup. On our test setup, we used the configuration as shown in the following figure.

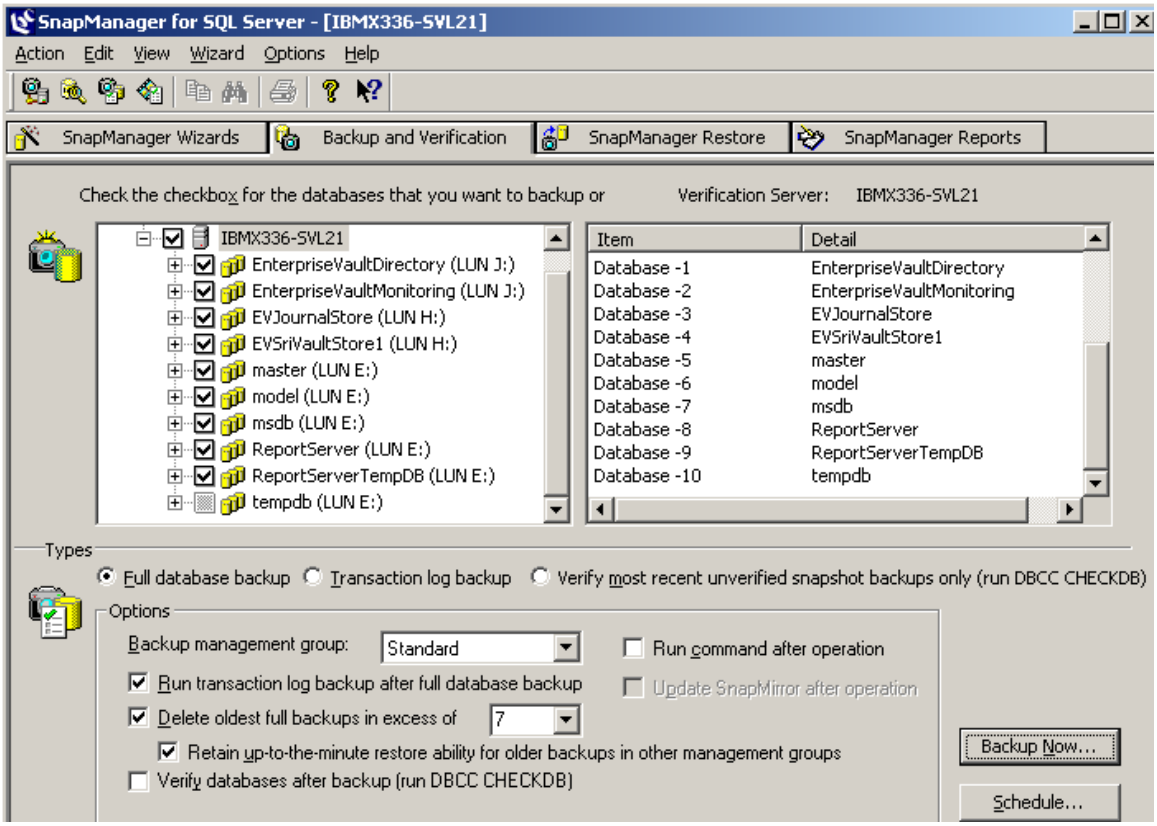

Figure 9: SnapManager for SQL Server Backup Configuration Wizard

Selecting a particular type of backup process depends on the available options. At this stage, choose to back up either the full database or just the transaction log, On our test setup, we selected to perform a full database backup as shown in the following figure.

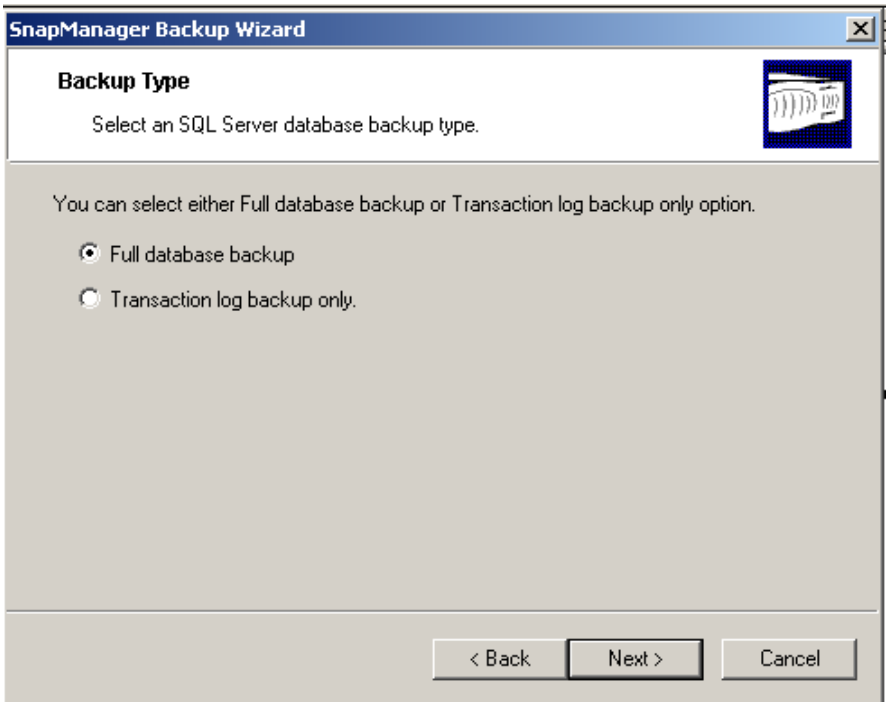

Figure 10: Select the Type of Database Backup

Start the database backup and monitor the backup task status as shown in the following figure. It is important to complete each task successfully. During this phase, it retains the specified number of older backups. Next figure shows the full database backup status along with the status of all backup tasks.

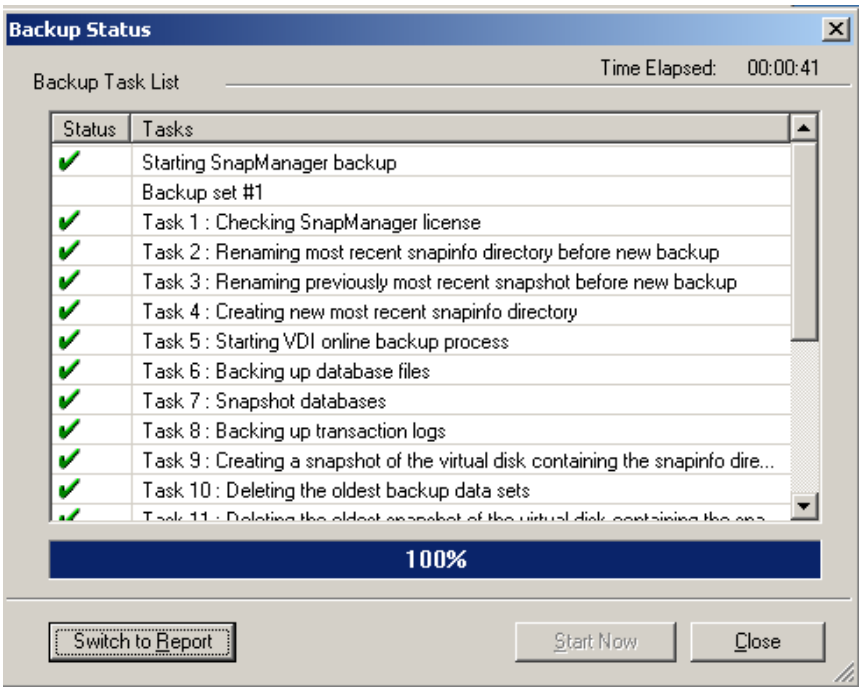

Figure 11: Monitor the Status of Backup Task Progress

On our test setup, we continued to monitor the status of backup tasks to ensure the successful backup of all databases using SnapManager for SQL Server. Once the databases were successfully backed up, the SnapManager for SQL Server tool displays the backup task status as shown in the following figure.

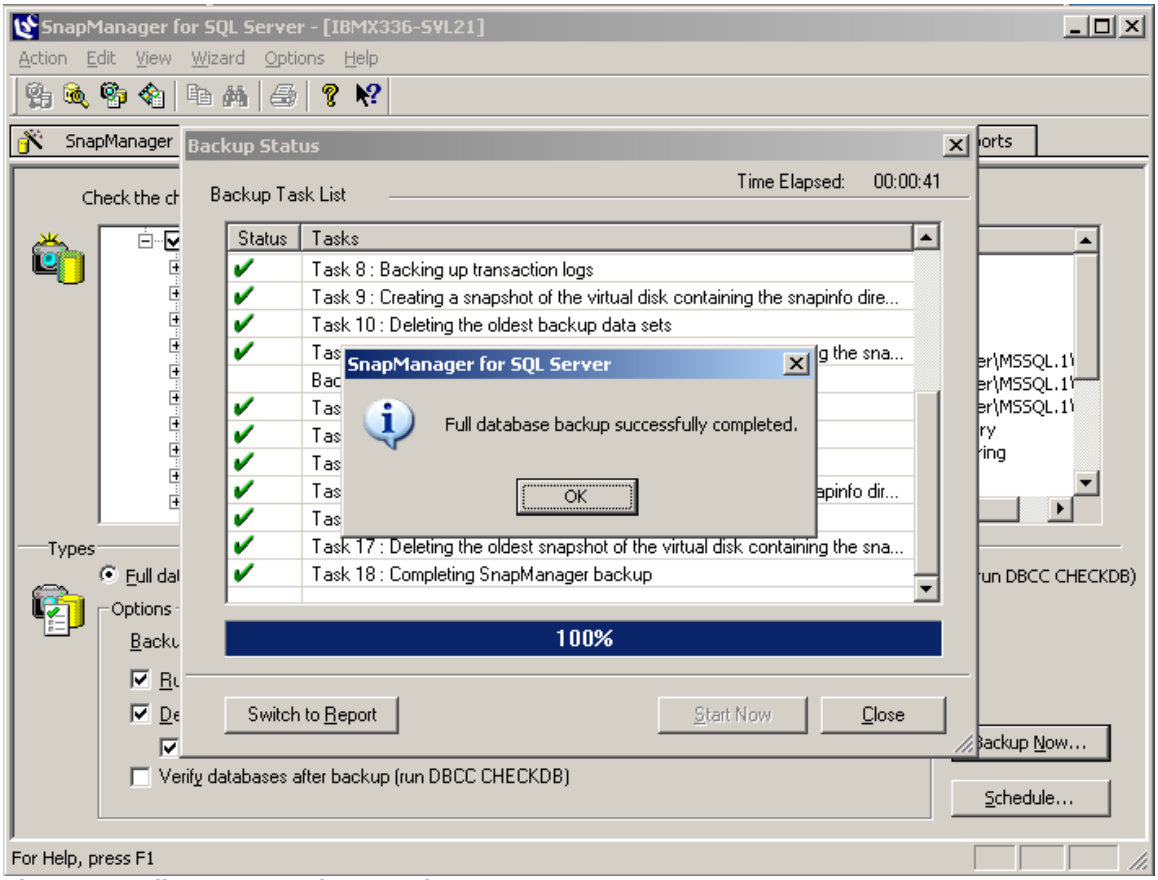

Figure 12: Full System Database Backup Status-

After demonstrating the procedure to back up SQL databases using the SnapManager for SQL Server backup and restore wizard, we will explain the procedure to back up SQL databases using a command-line interface (CLI). The *SmSqlBi* command allows users to back up and restore SQL databases using the SnapManager for SQL Server tool. This command provides capability to perform database backup with the same options as the GUI wizard. A sample SnapManager for SQL Server command with available options is listed below.

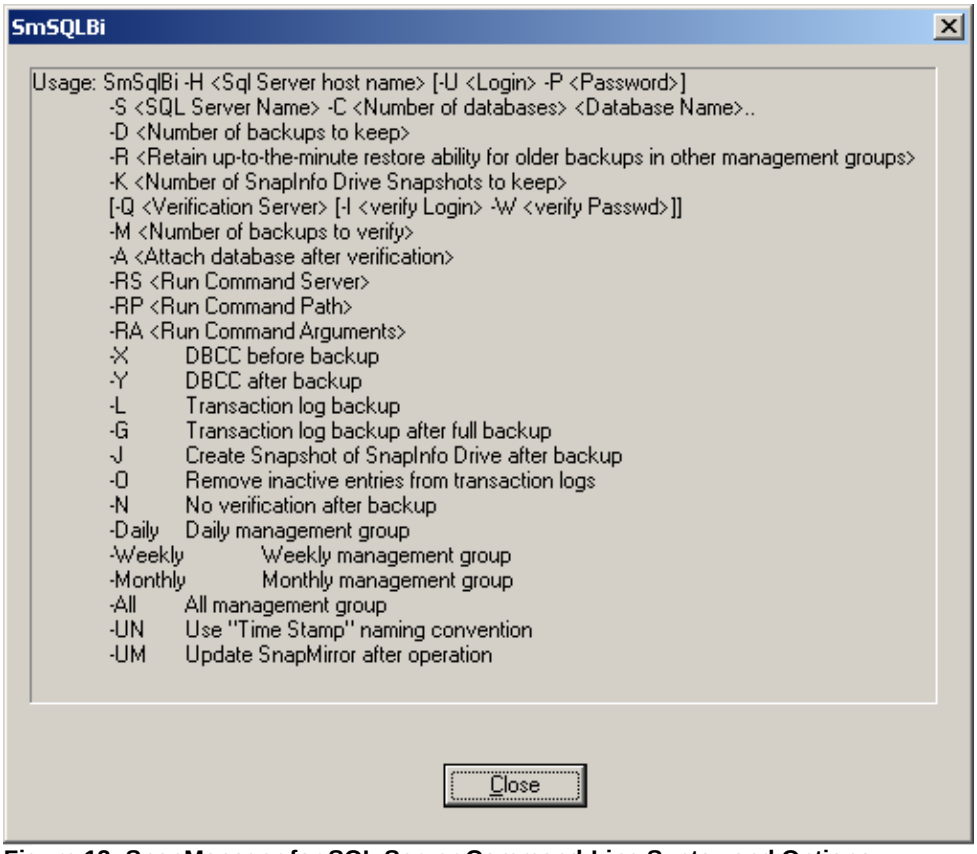

Figure 13: SnapManager for SQL Server Command-Line Syntax and Options

Use SnapDrive to Back Up Enterprise Vault Indexes and Archive Items

If the Enterprise Vault Index and Shopping services are located on SnapDrive created LUNs, data can be backed up using the SnapDrive tool. Backup can be achieved either by using the SnapDrive backup and restore wizard or by commands in batch file. On our test setup, Enterprise Vault Index services and Shopping Service files were located on a LUN, and we used the SnapDrive tool to create a Snapshot copy of the LUN as shown below.

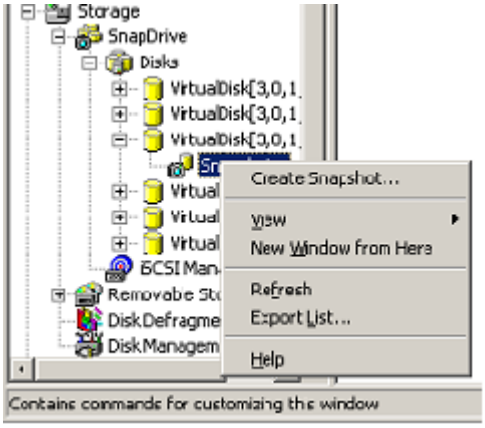

Figure 14: Creating the Backup of Enterprise Vault Index Files

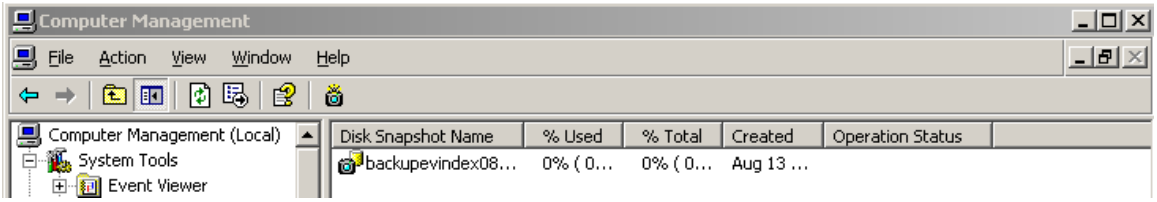

Figure 15: Enterprise Vault Index Backup Copy Created Using SnapDrive Snap-In Tool

You may also use SnapDrive supported CLI-based commands to back up the data of Enterprise Vault Indexes and Shopping services as shown below.

Use MMC Snap-in tool to create a Snapshot copy of the LUN:

Or '*SDCLI snap create –s <snapshot name> -D <mount point/ Drive letter>*'

If SnapMirror configuration is complete to replicate the backup data of the LUN to a different system, you may use the following command:

SDCLI snap update_mirror –m machinename –d mountpoint/driveletter

Backing Up of Archival Items

Archive files on Volume Not from SnapLock

If the archived items are not stored on SnapLock, use the NetApp FilerView® wizard to back up the data by creating a Snapshot copy of the volume. It can also be backed up by creating a Snapshot copy by using the remote shell command as shown below:

rsh <NetApp device name> -l user:password snap create –V <vol-name> <snapshot-name>

Archive Files on SnapLock Volume(s)

If the archive items are stored on a SnapLock volume, backup strategy has to be changed, as NetApp storage systems do not support restoring the backup copy to a previous point in time. Hence, a qtree level SnapMirror configuration has to be used. By using qtree level SnapMirror, data on the target system can be resynchronized with the next backup data set. This approach will maintain the compliance requirements as the file retention properties are maintained on the backup data. To set up qtree level SnapMirror, please refer to SnapLock documents at the NetApp portal. A brief method is given below.

Step 1. Create a SnapLock volume on the target NetApp storage system with sufficient storage.

Step 2. Use the QTREE structure to archive items on the source location to support qtree level SnapMirror.

Step 3. Configure SnapMirror on both NetApp storage systems.

Step4. Create a Snapshot copy of the archived items on the source volume.

Step 5. Start SnapMirror process to replicate the data using a qtree level SnapMirror of the Snapshot copy created. By using SnapMirror with the Snapshot copy, backup window is reduced significantly instead of waiting for the SnapMirror operation to complete before proceeding to the next task in the backup process.

Release Enterprise Vault from Read-Only Mode

Once all the components of the Enterprise Vault data set have been backed up, the server is ready to be released from its read-only mode. By releasing into read-write mode, users will be able to resume their normal tasks as opposed to read-only mode. Before putting Enterprise Vault into read-write mode, corresponding Enterprise Vault services have to be stopped to enable the registry key changes. To stop Enterprise Vault services, use the EVService command as shown below:

EVservice stop “Enterprise Vault Task Controller Service”

EVservice stop “Enterprise Vault Storage Service”

EVService stop “Enterprise Vault Shopping Service”

EVService stop “Enterprise Vault Shopping Service”

Verify that the Enterprise Vault services are stopped and then make registry changes to put Enterprise Vault into read-write mode. To change the registry keys, edit a registry file called BackupModeKeysNormal.reg with the following keys:

"EnableArchive"=dword:00000001

"EnableCrawler"=dword:00000001

"EnableExpiry"=dword:00000001

"EnableFileWatch"=dword:00000001

"EnablePSTMigrations"=dword:00000001

"EnableReplayIndex"=dword:00000001

“EnableRestore”=dword:00000001

Use the regedit command or other tools to change the registry keys; start Enterprise Vault services as shown below:

REM Now release Enterprise Vault Server from read-only mode

REM make proper entries to Enterprise Vault computer name to start services

EVService start IBMX336-SVL21 “Enterprise Vault Storage Service”

EVService start IBMX336-SVL21 “Enterprise Vault Index Service”

EVService start IBMX336-SVL21 “Enterprise Vault Shopping Service”

REM Starting Enterprise Vault Tasks

EVService start IBMX336-SVL21 “Mailbox Archiving task for IBMX336-SVL24”

EVService start IBMX336-SVL21 “Journal task for IBMX336-SVL24”

EVService start IBMX336-SVL21 “Public Folder task for IBMX336-SVL24”

EVService start IBMX336-SVL21 “PST Locator task”

EVService start IBMX336-SVL21 “PST Collector task”

EVService start IBMX336-SVL21 “PST Migrator task”

Verify Enterprise Vault Services

At this stage, the Enterprise Vault server is configured to run in read-write mode and all data has been backed up. Verify that the Enterprise Vault server is functioning properly. Restart any services if they are not started.

Removing Safety Copy

In an Enterprise Vault environment, it is normal to purge the archived e-mails from the Exchange Server for easier Exchange or Domino Server management. When an e-mail is archived, a copy is retained on the Exchange server until the command is executed to remove the safety copy, leaving a shortcut or a pointer to the original message. In Enterprise Vault 2007 server, an XML file is used instead of an IgnoreArchiveBitTrigger.txt file. However, if the files are archived onto a SnapLock volume, this setting differs from a volume that is not a SnapLock volume. Note that the Enterprise Vault behavior changes to safety copies when files are archived onto a SnapLock volume. This is due to the fact that a SnapLock volume maintains the WORM status and does not allow files to be modified or deleted until the expiration of the retention period. On our test setup, we configured to delete the safety copy immediately after the e-mails are archived onto a SnapLock volume, as shown below.

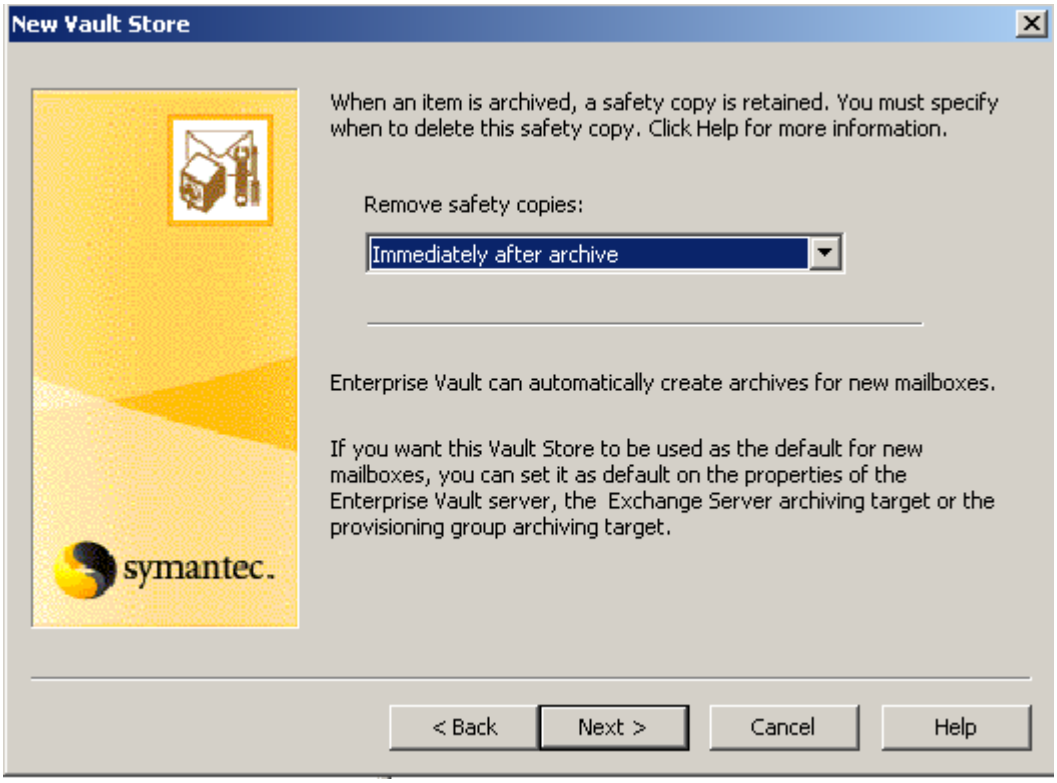

Figure 16: Remove Safety Copy After Archive onto SnapLock Volume

6.10. Automating Backup Process

Section 6.4 described the procedure to back up an Enterprise Vault data set, and the entire backup process could be automated for administration purposes. Following is an example of the script to back up Enterprise Vault Server.

EVService stop <EVserver name> "Enterprise Vault Task Controller Service"

EVService stop <EVServer name> "Enterprise Vault Shopping Service"

EVService stop <EVServer name> "Enterprise Vault Indexing Service"

EVService stop <EVServer name> "Enterprise Vault Storage Service"

regedit /s c:\temp\BackupModeKeysReadOnly.reg

EVService start <EVServer name> "Enterprise Vault Storage Service"

EVService start <EVserver name> "Enterprise Vault Indexing Service"

EVService start <EVserver name> "Enterprise Vault Shopping Service"

EVService start <EVServer name> "Enterprise Vault Task Controller Service"

REM smsqlbi command enables SQL Server database backup

REM change directory to SnapManager installation directory or

REM configure the SnapManager installation path to environment variable

REM See SnapManager for SQL Server manual to get the details of command options

smsqlbi -H Domain\Hostname -S Domain\EVservername -C 0 –D 7 -Recent -UM –N

Sdcli snap update_mirror –m machinename –d mountpoint/driveletter

Rsh destinationfiler –l root:password snapmirror update –S sourcefiler:sourcevolume destinationvolume

EVService stop "Enterprise Vault Task Controller Service"

EvService stop "Enterprise Vault Shopping Service"

EVService stop "Enterprise Vault Indexing Service"

EVService stop "Enterprise Vault Storage Service"

regedit /s c:\temp\BackupModeKeysNormal.reg

EVService start <EVServer name> "Enterprise Vault Storage Service"

EVService start <EVserver name> "Enterprise Vault Indexing Service"

EVService start <EVServer name> "Enterprise Vault Shopping Service"

EVService start <EVServer name> "Enterprise Vault Task Controller Service"

REM may not be required if set to delete after

REM archiving e-mails immediately

REM copy c:\temp\IgnoreArchiveBitTrigger.txt

REM J:\EVStores\EXCH_VS01\IgnoreArchiveBitTrigger.txt

6.11. Offline Backup with Enterprise Vault Services Stopped

It is easier to maintain data consistency when Enterprise Vault services and tasks are stopped during the backup process. This section provides the procedure to back up Enterprise Vault data and related databases while Enterprise Vault services and tasks are stopped. With the SnapManager for SQL Server utility, there is no need to shut down SQL Server.

- Step 1: Stop the Enterprise Vault Admin service. All other Enterprise Vault services and tasks are automatically stopped when Enterprise Vault Admin service is stopped.
- Step 2: Stop MSMQ on the computer.
- Step 3: Perform a complete system and file backup using SnapDrive.
- To perform a system backup, use the SnapDrive snap-in tool located in the Computer Management Console (MMC) on the computer. Expand Storage under SnapDrive and right click the local disk where the Vault Directory database, Enterprise Vault Monitoring database, and FSA Reporting service are located and create a Snapshot copy. Back up the database and the corresponding transaction logs. Usually they are configured on separate locations.
- Step 4: Repeat step 4 for other Enterprise Vault databases for each Vault Store database and its corresponding transaction logs.
- Step 5: Repeat step 4 for other Master and msdb databases.
- Step 6: Use SnapDrive to create a Snapshot copy of Enterprise Vault Index services and files.
- Step 7: Use SnapDrive to create a Snapshot copy of Enterprise Vault Shopping Service files.
- Step 8: To back up vault store files, use a storage system console or a CLI interface to create a Snapshot copy of the volume where the vault store files are located.

If a new service or task is added to the Enterprise Vault environment, unscheduled backup requires backing up the Vault Directory database, master, and msdb databases and their corresponding transaction logs.

After creating Snapshot copies, the backed up data may be replicated to another NetApp storage system using SnapMirror on local or a remote site for additional data protection.

Procedure for Offline Backup

This section provides a brief explanation and commands to back up Enterprise Vault data.

- Identify LUNs where the SQL Server databases are located.
- SQL Server System databases on a separate LUN.
- Enterprise Vault Directory database on a separate LUN.
- Enterprise Vault Store Database on a separate LUN.
- Identify LUNs where Enterprise Vault Index Service, Storage services, and file locations are stored.
- Index can reside either on LUN or on a network share.
- Residing on LUN managed by SnapDrive.
- Network Share.

Index and Storage Services Reside on the Same LUN

This section provides the steps involved to back up Enterprise Vault data when Index Services, Storage services, and files reside on the same LUN.

- Just create a single Snapshot copy to have the backup of all data on the LUN.
- If Index files reside on a network share, use a FilerView GUI or a CLI to back up data. If the LUN also contains the storage services data, just one backup of the LUN is sufficient.
- Identify the network share where Enterprise Vault Archived items are stored.

- For archived data on volume other than SnapLock, use a FilerView GUI or a CLI based command to back up data.
- For archived data on SnapLock volume, replicate the archived data to a different NetApp storage system using SnapMirror process. Restoring data from a Snapshot copy onto a SnapLock volume is not supported.
- Stop Enterprise Vault Services.
- Use Computer Management snap-in tool to stop Enterprise Vault Admin services.
- Use commands to stop Enterprise Vault services.
- Use EVService command tool.
- EVservice command allows stopping and starting as appropriate. Syntax of EVservice command is given below.
- Use Computer Management tool in MMC to stop the required services.
- Open MMC tool, expand Storage, and expand the local drives until you see Snapshot copies. Create a Snapshot copy using the SnapDrive wizard.
- Use 'net' command to stop Enterprise Vault services.
- Alternative to stop Enterprise Vault Services is to use 'net stop' command.
- Stop the Microsoft SQL Server.
- Use Microsoft SQL Management Studio, right click the SQL Server instance, and stop the services.
- If the LUNs are created and managed by SnapDrive, use CLI based command to back up each LUN.

- Use MMC Snap-in tool to create a Snapshot copy of the LUN.
- Or '*SDCLI snap create –s <snapshot name> -D <mount point/ Drive letter>*'.
- Or *SDCLI snap update_mirror –m machinename –d mountpoint/driveletter.*

Back Up Enterprise Vault Archived Items

Use FilerView GUI to create a Snapshot copy of the volume.

Alternatively, use '*rsh –l root:passwd <storage system name> snap create –V <vol name> <snapshot name>.*

If the data is stored on a SnapLock volume, use qtree level SnapMirror to replicate the data to another NetApp storage system's SnapLock volume or to a different SnapLock compliant volume on the same storage system. On such volumes, data cannot be restored to a previous point-in-time status from the Snapshot copy created.

Replicate the Backed up data to a different NetApp storage system.

Best practices suggest replicating the data backed up to a different NetApp storage system at another location. If Vault store archive items are stored on SnapLock volume, such data has to be replicated using SnapMirror, using qtree level SnapMirror during the backup mode.

In the above section, we discussed the entire backup procedure to protect the data in an Enterprise Vault environment. This approach provides a quicker way to back up Enterprise Vault data. In the following paragraph, this paper provides a script that could be run as a batch process to create the backup copy of Enterprise Vault data while Enterprise Vault services and SQL Server are not running. For simplicity, the following script makes certain assumptions about the configuration.

REM This file lists the commands used to back up Enterprise Vault data in offline mode

REM it assumes the SQL Server system databases, Enterprise Vault Directory databases, and Vault store databases reside on separate LUNs

REM Compliance based archive files reside on NetApp SnapLock volume

REM Enterprise Vault Index service, Enterprise Vault Storage service, and file locations use the same LUN

REM Enterprise Vault Archive file (noncompliance) uses a volume other than SnapLock

REM Stop Enterprise Vault Services

REM Enables the control of services and Enterprise Vault tasks

REM Syntax evservice start|stop|pause|resume <computer name> <service> [<service>...]

EVservice stop “Enterprise Vault Task Controller Service”

EVservice stop “Enterprise Vault Storage Service”

EVService stop “Enterprise Vault Shopping Service”

EVService stop “Enterprise Vault Shopping Service”

REM Alternatively stopping Enterprise Vault Admin Services stops other Enterprise Vault services

REM and tasks

REM stop Microsoft SQL Server using SQL Server Management Studio

REM Connect to server and right on SQL Server and click Stop

REM Alternatively stop SQL Server services using MMC Snap-in console

REM Back up SQL Server databases residing on LUNs

REM SnapDrive supports CLI based command to back up data on LUN

REM SDCLI command syntax

REM sdcli snap create –m MachineName –s SnapshotName – D mount point list

Sdcli snap create –s August202007101005 –D E G H I

REM In the above command E drive has SQL system databases, G has Index services

REM and shopping services files, H has Vault Directory database and I has Vault Store

REM databases

REM Having backed up both databases, Enterprise Vault Index and shopping files, back up archived

REM items

REM rsh filername [-l login:password] snap create –V <Vol> -s SnapshotName

REM syntax sample Rsh fas3050-svl39 –l root:passwd snap create –V evj1 –s August202007101005

REM In our configuration, they used SnapLock volume

REM Replicate the backup data using SnapMirror to another location

REM first time replicate the data at base level and then update the changes

REM Sdcli snap update_mirror [-m MachineName] –d Mountpoint

Sdcli snap update_mirror –d E G H J

REM Destination path information available on SnapMirror setup configuration

REM Replicate the Enterprise Vault Archived items on the SnapLock volume

REM Use SnapMirror configuration to replicate the archive items maintaining the compliance properties

6.12. Online Backup While Enterprise Vault Services Running

This section describes a procedure to do an online data backup of Enterprise Vault Data as well as related Databases. SnapManager for SQL Server provides the ability to back up the SQL Server databases maintaining data consistency. In order to maintain data consistency in Enterprise Vault environment, this section exploits the possibility of putting Enterprise Vault server into read-only state during the backup operation. This section provides a procedure involved with Enterprise Vault online backup using NetApp storage solutions.

It is possible to back up Enterprise Vault data online, provided a user or process does not add new data to Enterprise Vault. In mission critical environments, it may not be possible to stop the Enterprise Vault services. This type of high demanding environments must meet the backup and recovery plan while the Enterprise Vault services are running. This section explains the procedure to back up databases using SnapManager for SQL Server in a consistent state and use SnapDrive to back up the Enterprise Vault data.

This section discusses procedure to back up SQL databases and Enterprise Vault data while Enterprise Vault services is running. During the online backup process, there is no need to stop Admin, Directory, and Shopping services. Backup procedure involves the following tasks:

Task 1: Use a batch file to stop all Enterprise Vault services.

Task 2: Use EVservice command to stop services.

Task 3: Put Enterprise Vault services to read-only status.

Task 4; Restart Enterprise Vault Services.

Task 5: Verify Enterprise Vault is in quiesce mode. Quiesce mode puts Enterprise Vault into read-only mode where the data is available for the users, but users cannot manipulate the shopping baskets or archive items.

Task 6: Back up vault store files to allow any updates to vault store database(s).

Task 7: Use SnapManager for SQL Server to back up related SQL databases except Vault store databases.

Task 8: Use SnapDrive to back up Index Services and files.

Task 9: Use SnapDrive to back up vault store archive files.

Above is the list of tasks required to achieve a consistent state of backup. In this section, let us discuss the procedure to back up data while maintaining Enterprise Vault Server online to improve higher availability. A first step is to develop a procedure to distinguish the normal and read-only mode setup.

6.13. Creating Registry Files for Registry Changes

Step 1: Create two registry files to automate the registry changes before and after backup of Enterprise Vault. Name this file BackupModeKeysNormal.reg for the normal operations of Enterprise Vault server for registry key.

HKEY_LOCAL_MACHINE\Software\KVS\Enterprise Vault\Storage and the contents of BackupModeKeysNormal.reg file on our test machine are shown below.

[HKEY_LOCAL_MACHINE\SOFTWARE\KVS\Enterprise Vault\Storage]

"ServiceId"="1597C4C67C0B1B64795CF4A74328FC6501e10000DRGVAULTSVL21"

"EnableArchive"=dword:00000001

"EnableCrawler"=dword:00000001

"EnableExpiry"=dword:00000001

"EnableFileWatch"=dword:00000001

"EnablePSTMigrations"=dword:00000001

"EnableReplayIndex"=dword:00000001

“EnableRestore”=dword:00000001

Registry keys with value 1 is the default setting for normal operation. Use the same file to make changes to the value of registry keys to 0 and save it as *BackupModeKeysReadOnly.reg* file. A sample output of *BackupModeKeysReadOnly.reg* file is given below.

"EnableArchive"=dword:00000000

"EnableCrawler"=dword:00000000

"EnableExpiry"=dword:00000000

"EnableFileWatch"=dword:00000000

"EnablePSTMigrations"=dword:00000000

"EnableReplayIndex"=dword:00000000

“EnableRestore”=dword:00000000

6.14. EVprebackup.bat File

Create a batch file to perform the following tasks and name it. On our test setup, we created a file called EVprebackup.bat. This file performs the following tasks:

- Step 1: Stop Enterprise Vault tasks.
- Step 2: Stop Enterprise Vault Services.
- Step 3: Put Enterprise Vault into read-only mode.
- Step 4: Start Enterprise Vault services.
- Step 5: Start Enterprise Vault Tasks.

This batch file stops the Enterprise Vault services on a Directory Service and other computers running Enterprise Vault services. An example of this scenario includes the Enterprise Vault Services running on the Directory Service computer and other computer with Enterprise Vault services running. Objective of this is to stop all Enterprise Vault services prior to putting into read-only mode. Read-only mode helps in maintaining data consistency. It also prevents data from updating during the backup process. This is where the NetApp storage system solution brings unique value to significantly reduce the read-only access time. With a NetApp disk-based solution, the entire backup process could be completed quickly. To achieve the tasks listed in step 2, create a file called EVprebackup.bat with the following content. Make necessary changes to computer names, services, and relevant information.

```
REM - - - - - -EVprebackup.bat
REM This batch file stops Enterprise Vault services running on Directory Service computer and
REM other computer(s).
REM After stopping services, it puts Enterprise Vault into read-only mode
REM Then it starts the Enterprise Vault services
REM stop Enterprise Vault tasks on Directory Service computer
EVService stop IBMX336-SVL21 “Mailbox Archiving task for IBMX336-SVL24”
EVService stop IBMX336-SVL21 “Journal task for IBMX336-SVL24”
EVService stop IBMX336-SVL21 “Public Folder task for IBMX336-SVL24”
EVService stop IBMX336-SVL21 “PST Locator task”
EVService stop IBMX336-SVL21 “PST Collector task”
EVService stop IBMX336-SVL21 “PST Migrator task”

REM If Enterprise Vault Services are running on the Enterprise Vault Server
EVService stop IBMX336-SVL21 “Enterprise Vault Storage Service”
EVService stop IBMX336-SVL21 “Enterprise Vault Index Service”
EVService stop IBMX336-SVL21 “Enterprise Vault Shopping Service”
REM Stop Enterprise Vault services running on servers other than Directory Service Computer
REM add EVService command syntax
REM If some Enterprise Vault services are running on other computers, remove the comments
REM  EVService start
REM Now put Enterprise Vault into read-only mode
REM Locate the registry key file path and make appropriate changes to the
REM following command
Regedit /s c:\windows\safereg\BackupModeKeysReadOnly.reg

REM Now release Enterprise Vault Server from read-only mode
```

REM make proper entries to Enterprise Vault computer name to start services

EVService start IBMX336-SVL21 “Enterprise Vault Storage Service”

EVService start IBMX336-SVL21 “Enterprise Vault Index Service”

EVService start IBMX336-SVL21 “Enterprise Vault Shopping Service”

REM Starting Enterprise Vault Tasks

EVService start IBMX336-SVL21 “Mailbox Archiving task for IBMX336-SVL24”

EVService start IBMX336-SVL21 “Journal task for IBMX336-SVL24”

EVService start IBMX336-SVL21 “Public Folder task for IBMX336-SVL24”

EVService start IBMX336-SVL21 “PST Locator task”

EVService start IBMX336-SVL21 “PST Collector task”

EVService start IBMX336-SVL21 “PST Migrator task”

Make modification to the above file to match the tasks and services running in your environment and save it as BackupModeKeysReadOnly.reg file. Verify that the file is not saved as a text file.

When executing this file, the Enterprise Vault server will be configured to run in read-only mode. During this mode users are able to access data. However, they will be unable to retrieve items from the archives. Hence it is critical to release the read-only as early as possible. If you are not yet ready with other files to run online backup, wait until all the scripts are available.

6.15. Procedure to Back Up Enterprise Vault Registry Entries

Procedure to back up registry entries is provided in this section.

Back up Enterprise Vault registry entries on all Enterprise Vault servers and all computers where vault service account is logged into a system. To back up registry key, tools such as regedit or other applications may be used. While using the ‘regedit’ command, expand the registry keys to that folder and export the keys to save it on a disk.

It is equally important to back up the Enterprise Vault registry entries on every Enterprise Vault server and back up the Enterprise Vault registry hive under the following key:

HKEY_LOCAL_MACHINE

\Software

\KVS

\Enterprise Vault

In addition to this, back up the registry entries on each server where the VSA is logged for the following key:

HKEY_CURRENT_USER

\Software

\KVS

\Enterprise Vault

6.16. Backup of Databases Using SnapManager for SQL Server

SnapManager for SQL Server offers a wizard to configure the setup, back up SQL Server databases, and restore one or more databases. This paper recommends using the SnapManager wizard while backing up or restoring the database(s). In addition to this tool, SnapManager for SQL Server also supports a command line interface (CLI) to back up and update the changes to SQL Server databases. Backup command syntax to backing up databases using SnapManager for SQL Server is given below:

REM smsqlbi command enables to back up the specified databases

REM change directory to SnapManager installation path

REM Add SnapManager path is added in the environment variable

cd \program files\netapp\snapmanager for SQL Server

REM smsqlbi – IBMX336-SVL22 –S IBMX336-SVL21 –C 0 –R 7 –Recent –UM –N

REM –Recent option renames Snapshot copy to generic name

REM –UM updates the SnapMirror destination

REM Hostname and SQL Server name may include the Windows domain and computer

REM name

REM Otherwise use SnapManager for SQL Server Backup/Restore wizard to configure and back up individual

REM or multiple databases residing on a single or multiple LUNs

6.17. Backup of Enterprise Vault Index and Shopping Services and File Locations

Enterprise Vault Index and shopping services files are stored either on SAN storage or on the network share. Following commands provide the details to back up Enterprise Vault Index and shopping services files.

REM If the Index and Shopping service files are configured on LUN(s)

REM if SnapMirror configuration is set up, use the following command

REM Sdcli snap update_mirror <–m MachineName > -d mountpoint

REM example of above command is given below

REM Sdcli snap update mirror –m IBMX336-SVL21 –d G

REM in the above command IBMX336-SVL21 is the machine name where Index files

REM are located and G is the drive letter of Index files to be backed up

REM If SnapMirror config not used, create Snapshot copy with SnapDrive

REM Sdcli snap create <-m MachineName> -s SnapshotName -D mountpoint

Sdcli snap create –m IBMX336-SVL21 –s EVIndexBackupOn082220071531 –D G

REM above command will create a Snapshot copy of LUN mounted as G drive

REM If shopping service files located on different LUN, add that mount point

REM If multiple LUNs or network shares are configured to store Enterprise Vault Index files

REM add all the mount points to back up the data

6.18. Backup of Enterprise Vault Archive Files

Enterprise Vault archive files are stored in a network share including the compliance data. If the Enterprise Vault Archive files are located on the SnapLock volume, creating a Snapshot copy will not help as the data cannot be restored to a previous point in time on a SnapLock volume. In order to achieve the backup of Enterprise Vault Archive files on a SnapLock compliance volume, they must be replicated to another volume maintaining the compliance properties. For details to set up SnapMirror on SnapLock volumes, refer to documents on the NetApp information portal.

For backing up Enterprise Vault Archive files, create a backup using the rsh command. If there are any network access issues with rsh, use a storage system console or a FilerView GUI to create the Snapshot copy.

REM This part provides a command syntax to back up Enterprise Vault Archives

Rsh <filername> -l root:passwd snap –V <volname> snapshotName

REM If SnapMirror is configured

Rsh <filername> -l root:passwd snapmirror update –S fas3050-svl39:evstore1 fas3050-svl40:evstore1

Rsh <filername> -l root:passwd snapmirror update –S fas3050-svl39:evstore2 fas3050-svl40:evstore2

REM for archive files stored on SnapLock volume, ignore the above steps

REM for SnapLock volume – use qtree level SnapMirror

REM qtree SnapMirror will allow the data to be resynchronized at the next backup data set

REM to use qtree SnapMirror, you must have qtree created and archive file stored under a qtree and not at the volume root level

REM Resync of data is not supported at a volume level SnapMirror.

REM Note that it is not a disadvantage as long as the qtree is used for archival items

6.19. EVpostbackup.bat File

Next step is to create a file to temporarily stop the storage and indexing services to change the registry keys to their original settings. This file is named as EVpostbackup.bat. Following are the entries of EVpostbackup.bat file:

REM -- -- --

REM file name is called ‘EVpostbackup.bat’

REM stop the Enterprise Vault storage and indexing services

EVService stop IBMX336-SVL21 “Enterprise Vault Storage Service”

EVService stop IBMX336-SVL21 “Enterprise Vault Indexing Service”

REM now put Enterprise Vault in normal mode

Regedit /s c:\windows\safereg\BackupModeKeysNormal.reg

REM Start Storage and Indexing services

EVService start IBMX336-SVL21 “Enterprise Vault Storage Service”

EVService start IBMX336-SVL21 “Enterprise Vault Indexing Service”

Note that normal.reg file may reside on any location and it need not reside under the directory shown in the above EVpostbackup.bat file.

Alternatively, net stop and net start commands may be used to stop and start the same services. An example: to stop Enterprise Vault Task Controller Service, you would use a command as shown below. This is explained in Section 6.14

net stop /y “Enterprise Vault Task Controller Service”

6.20. Verify the Test Scripts

Once these files are created, it is important to test and correct the scripts to ensure they work as expected. After testing, schedule the batch files. Again, verify that the registry files are configured correctly. Incorrect registry key settings could affect the backup and recovery process.

6.21. Backup of SQL Server Databases and Enterprise Vault Data

SnapManager for SQL Server manages the database backup of several databases on the NetApp volume. It will ensure the database data consistency. This is a huge advantage to database administrators. Databases may reside under different LUNs and virtual local disks. Before creating the backup of SQL databases, ensure the Enterprise Vault application (and any other applications using the same SQL Server) into read-only mode. Without the use of SnapManager for SQL Server, utmost care is required to maintain data consistency.

SnapManager for SQL Server manages internally the tasks required to maintain data consistency and runs any ‘checkpoint database’ against all SQL Server databases. This procedure flushes any metadata from the cache to maintain data consistency.

Prior to backing up SQL databases, it is important to verify and run the following batch files.

Step 1: Verify BackupModeKeysNormal.reg file.

Step 2: Verify BackupModeKeysReadOnly.reg file.

Step 3: Verify the EVprebackup.bat file.

Step 4: Verify EVpostbackup.bat file.

Step 5: Verify you have the file locations and database names available.

Step 6: Verify Enterprise Vault Indexing services and file locations.

Step 7: Verify Enterprise Vault Shopping service and file locations.

Step 8: Verify the Vault store archiving files.

Step 9: Run EVprebackup.bat.

Step 10: Use SnapManager for SQL wizard to back up Enterprise Vault Directory database.

Step 11: Use SnapManager for SQL Server wizard to back up Enterprise Vault Store database(s).

Step 12: Use SnapManager for backup SQL databases.

Step 13: Use SnapDrive to back up Enterprise Vault Index services and files (and subfolders).

Step 14: Use SnapDrive to back up Enteprise Vault Archive Items

Step 15: Use SnapDrive to back up vault store files when data is on a volume other than SnapLock.

Step 16: Use Qtree level SnapMirror to replicate the Vault store archival files, including DVS files.

Step 17: Verify if the vault store archival files are to be resynchronized with the source data.

Step 18: Run EVpostbackup.bat.

SnapManager for SQL Server creates the backup of Enterprise Vault Directory database, EVMonitoringdatabase, FSAReportingdatabase, and Vault Store databases. Use SnapDrive to back up indexes and shopping service files. Note that these databases usually reside on several virtual local disks. Their corresponding transaction logs may reside in separate virtual local disks. SnapManager for SQL Server allows backup of the database and applying the transaction logs to update the database data.

SnapDrive is able to restore a virtual disk from the Snapshot copy created by SnapDrive.

6.22. Releasing Enterprise Vault from Read-Only Mode

It is time to release the Enterprise Vault server from read-only mode. To release read-only mode, run the EVpostbackup.bat batch file. This temporarily stops Enterprise Vault services, puts the registry entries to normal operation mode, and restarts the stopped Enterprise Vault services.

6.23. Procedure to Back Up Enterprise Vault Data While Enterprise Vault Services Stopped

In this section, we provide the details to back up Enterprise Vault data by stopping the related tasks and services to maintain data consistency. During this time, data is unavailable to users, and hence it is critical to complete the backup process with a minimal impact to end users. Using NetApp storage solutions, it is possible to create the backup almost instantly.

Backing up of Enterprise Vault data is similar to the procedure explained earlier. Steps involved with backing up Enterprise Vault data are given below.

a. Stop Enterprise Vault Admin Service (this will stop all Enterprise Vault services and tasks).

b. Use SnapDrive to back up vault store files.

c. Use SnapManager for SQL Server to back up Enterprise Vault related SQL databases.

- Enterprise Vault Directory database
- Vault Store database(s)
- Enterprise Vault Monitoring database
- FSA Reporting database (if FSA Reporting configured)

d. Use SnapDrive to back up Enterprise Vault Index services and files (including subfolders).

e. Use SnapDrive to back up Shopping service and file locations (including subfolders).

f. Back up Enterprise Vault registry entries.

6.24. Procedure to Back Up Using SnapDrive Without SnapManager for SQL Server Utility

To back up using SnapDrive without having SnapManager for SQL Server utility, steps are described below.

- Step 1: Note the Enterprise Vault Directory database and its location.
- Step 1-1: Directory database contains the Enterprise Vault configuration information. Back up the database depending on your company's backup policy. By default, it is recommended to back up at least once a week and truncate the transaction logs after the backup is over. When SnapManager for SQL Server is not installed to manage SQL Server databases and the databases reside on a single NetApp storage volume, SnapDrive may be used to back up the data. Use SnapDrive snap-in tool in Computer management console on the host server to back up the data.
- To back up Directory database, stop the Enterprise Vault admin service and use SnapDrive snap-in tool to create a Snapshot copy of the local disk (LUN) where SQL database EnterpriseVaultDirectory is located.
- Step 2: Note the Indexing service file locations.
- It is important to back up indexes stored in multiple locations. Get the properties of each Indexing service to determine the folders (local disk) to back up. If they are located across multiple local disks (multiple LUNs), use SnapDrive to create the necessary Snapshot copies. If the Shopping service is storing the files in the same local disk (LUN), make sure to stop the Shopping service before backing up the data.
- Step 3: Note the Shopping service file locations.
- Once the Indexing services and files are backed up, verify Shopping service is stopped so that users cannot use and manipulate the shopping baskets. Use SnapDrive to back up the Shopping service and files. If the Shopping service stores files in the same local disk (same LUN), it is done with the backup of Indexing Services and files.
- Step 4: Note the vault store SQL databases.
- Vault store database has to be backed up at the same time as the vault store files backup. This holds true for the restore process. This means, if the vault store database is restored, its corresponding vault store files must be restored at the same time.
- Determine the Vault store database name(s) and location of the Vault store files. As a first step, create a Snapshot copy of Vault store files of all locations (directory structure) using the SnapDrive tool. Prior to backing up Vault store databases to determine the Vault store associations with each Storage service and the location of vault store files.
- Use SnapDrive to back up Vault store files and the computer running Storage service. This will ensure to update all the archive pending items to shortcuts resulting in the vault store database update. Now use SnapManager for SQL Server to back up the vault store SQL database. The naming syntax of the vault store database is EV<vault store name>. In case of backing up application data, use SnapDrive SnapManager for SQL Server to back up master and msdb databases.
- Step 5: Note the Enterprise Vault Monitoring database location.
- It is assumed that Enterprise Vault Admin service is stopped prior to backing up Enterprise Vault Monitoring database. Use SnapManager for SQL Server to back up Enterprise Vault Monitoring

database. If the monitoring database is located under the same LUN as Directory database, it is already backed up. With SnapManager for SQL Server 2.1R1, it is possible to back up a specific database or all databases. However, best practices suggest backing up of all databases residing on a LUN.

- Step 6: Backing up FSA Reporting database.
- If FSA Reporting is configured, Enterprise Vault creates a database called FSA Reporting database. This is a SQL database that contains data from the Enterprise Vault File Collector service. If the FSA Reporting database is located under a different directory than Vault Directory database or locations previously covered, use SnapManager for SQL Server to back up the EnterpriseVaultFSAReporting database.
- Step 7: Back up Enterprise Vault Registry entries on all Enterprise Vault servers and any computer where vault service account is logged in.

It is equally important to back up the Enterprise Vault registry entries on every Enterprise Vault server and back up the Enterprise Vault registry hive under the following key:

HKEY_LOCAL_MACHINE

\Software

\KVS

\Enterprise Vault

In addition to this, back up the registry entries on each server where the vault service account (VSA) is logged for the following key:

HKEY_CURRENT_USER

\Software

\KVS

\Enterprise Vault

To back up the registry entries, open a registry editor such as ‘regedit’ and expand until the directory structure appears. Use the ‘export’ option to export the keys to a file.

7. Restoring the Enterprise Vault Data

This section provides the details to restore Enterprise Vault Server data sets. Restoring Enterprise Vault data involves preparing for the data recovery and execution of the procedure.

- Preparation

  It is important to prepare the Enterprise Vault server and NetApp storage systems prior to initiating the data recovery. It is critical to maintain data consistency and not corrupt the data set while recovering the data. This means handling the various Enterprise Vault data sets in a consistent manner. In order to achieve it, it is required to bring the Enterprise Vault server to offline mode. In most scenarios, Enterprise Vault servers (all Enterprise Vault Computers) are already in offline mode. Stop any Enterprise Vault services if they are still running. Stopping Enterprise Vault Admin Service will stop other services. Ensure the NetApp storage system are accessible and server connectivity is available.

- Execution

  Once the restore environment preparation work is complete, proceed with the data restoring from Snapshot copies and the database recovery using SnapManager for SQL Server.

- Procedure for Restoring Selective components

  Enterprise Vault has several data components. During the restore process, it is required to make a decision whether to recover an individual data component or all data sets required within Enterprise Vault environment. Individual components of Enterprise Vault dataset could be recovered from backup copies..

- Procedure for Restoring Entire Enterprise Vault Site

  There may be an occasion where all related Enterprise Vault data sets have to be restored from the backup. This type of requirement might arrive from a disaster or total loss of Enterprise Vault server and data. In such cases, it is possible to restore all components of the Enterprise Vault data set. Section 7.3 describes the procedure to restore from full backup copy.

7.1. Overview Restore Process

This section describes the procedure to recover Enterprise Vault server. It is assumed that Enterprise Vault server is not running on the server where the data being restored. Some of the recovery options are listed below.

- Option 1: Using full system backup
- Option 2: Using Enterprise Vault data backup
- Option 3: Enterprise Vault Component recovery

Enterprise Vault has several components of data sets to be considered before restoring the data from the backup. In this section, following restore processes are discussed.

a. Restore an Enterprise Vault Directory Database using SnapManager for SQL Server

b. Restore Enterprise Vault Store database

c. Restore EVMonitoring Database

d. Restore Enterprise Vault Index services and file locations

e. Restoring Enterprise Vault Shopping service and file locations

f. Restoring Enterprise Vault Archived items

7.2. Advantages of NetApp Storage System Solution

The joint solution of Enterprise Vault and NetApp storage offers a value in the ability to recover Enterprise Vault quickly.

7.3. Recovery of Enterprise Vault from Full System Backup Data

Using the Snapshot copy created with SnapDrive and the database backup created with SnapManager for SQL Server, restore the data. SnapDrive allows restoration of data to a point-in-time copy of the backup. SnapDrive has the ability to restore the data to the local disk from the Snapshot copy. It is important to note that SnapDrive manages only the Snapshot copies it created. Here are steps involved with the full system backup recovery process.

- Step 1: Verify Enterprise Vault Services are stopped prior to restoring the data.
- Step 2: Restore Index files and locations using SnapDrive.

- Step 3: Restore Shopping service files and locations using SnapDrive.
- Step 4: Restore Vault store files and locations.
- Step 5: Restore databases using SnapManager for SQL Server wizard.
- Step 6: Recover Enterprise Vault server.
- Step 7: Run Enterprise Vault Configuration Wizard to reconstruct the service and task information.

7.4. Recovery from a Disaster

It is possible to recover an Enterprise Vault environment from a disaster scenario. Steps involved to recover Enterprise Vault environment are given below.

- Step 1: Restore file system from backups.
- Step 2: Restore SQL Server backups.
- Step 3: Restore vault store files to their original locations on Storage service computer.
- Step 4: Restore Indexing files to their original locations on Indexing service computer.
- Step 5: Restore Shopping service files to their original locations on Shopping service computer.
- Step 6: Run archive operations since the last set of daily backups.
- Step 7: Cancel all archive pending items from mailboxes.
- Step 8: Repeat the retrieval requests that were made and not completed due to system failure.

7.5. Recovery of Enterprise Vault Using Data-Only Backup

Data-only backup involves the backing up the Enterprise Vault data, including the registry, without backing up the actual Enterprise Vault server system. In such cases, recovery of Enterprise Vault requires recent backups of the following:

- Directory database
- All vault store databases
- Monitoring database
- FSA Reporting database (if FSA Reporting is configured)
- Vault store saveset files
- Indexing data
- Shopping data

Here is the procedure to recover Enterprise Vault server:

- Install software on servers.
- Install Windows software.
- Install other applications software.
- Install Enterprise Vault software on all servers (new systems). Install into the same location as the previous configuration. Install the same version of Enterprise Vault software. Avoid running the Enterprise Vault Configuration program.
- Restore Enterprise Vault Directory database.

- Restore Vault store databases.
- Restore the Monitoring database.
- Restore FSA Reporting database.
- Enterprise Vault Server name changes
- Restore Enterprise Vault data files to their original locations.
- Directory database entries.
- Recreate services and tasks on the Directory service computer.
- Recreate services on other Enterprise Vault Computers.
- Web Access Application URL.
- Registry Entries.

7.6. Recovery of an Enterprise Vault Component

Section 7.4 explained the procedure to recover Enterprise Vault in a disaster scenario. Section 7.5 explained the procedure to recover Enterprise Vault server when Enterprise Vault data-only backup is available. This section provides the procedure to recover a component of Enterprise Vault server. Care must be taken while recovering an Enterprise Vault component from a previous backup and it is not recommended in a production environment. Components that can be recovered are listed below.

- Directory service SQL database
- Stop Enterprise Vault Admin service on all computers
- Use SnapManager for SQL Server to restore the Directory database
- Start Directory service
- Open Admin Console

SQL Server system databases reside on a SQL Server environment. To restore system databases, the Enterprise Vault Admin service and SQL service must be stopped on all SQL Server computers to maintain data consistency. SnapManager for SQL Server will be leveraged to restore SQL Server databases from the last known backup copy.

While using the SnapManager for SQL Server for restoring the SQL databases, it is required to specify the SQL Server information where the databases were backed up. SnapManager for SQL Server provides the ability to restore the databases from the database backups created by it on a different SQL Server. However, usually the Enterprise Vault environment uses the same SQL Server and not any other SQL Servers. On our test setup, it is shown below.

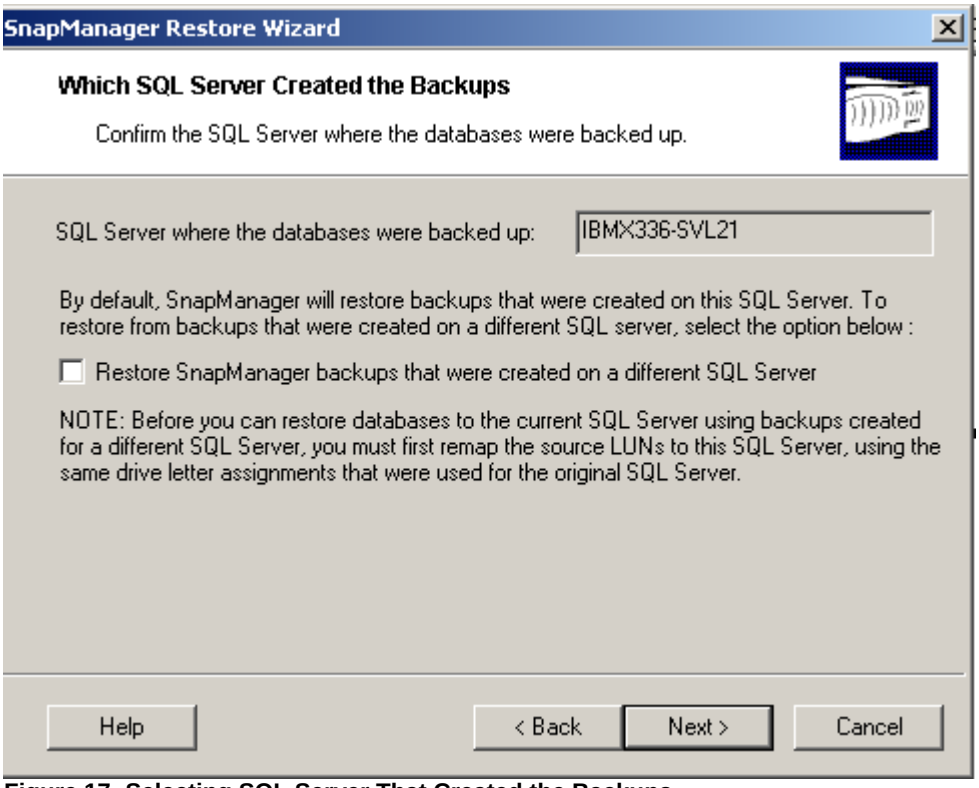

Figure 17: Selecting SQL Server That Created the Backups

Once the SQL Server where the database backup was performed is selected, select the backup of the databases and transaction logs that needs to be restored. Double clicking a SQL Server displays the available databases and the LUNs where the database backups are available. On our test setup, it is shown in Figure 18.

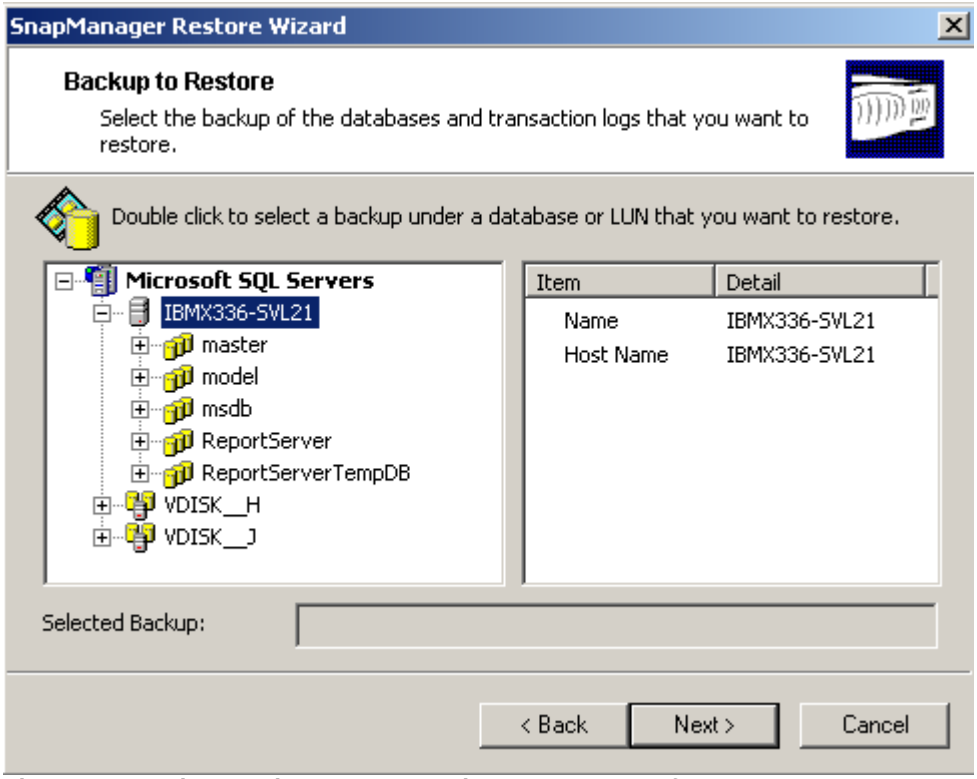

Figure 18: Starting Database Restore Using SnapManager for SQL Server

In order to display the details of the SnapManager for SQL Server backup for a particular database, expand the available database backups as shown in the following figure. SnapManager for SQL Server allows restoring a particular database and selecting a particular database for the database restore if needed.

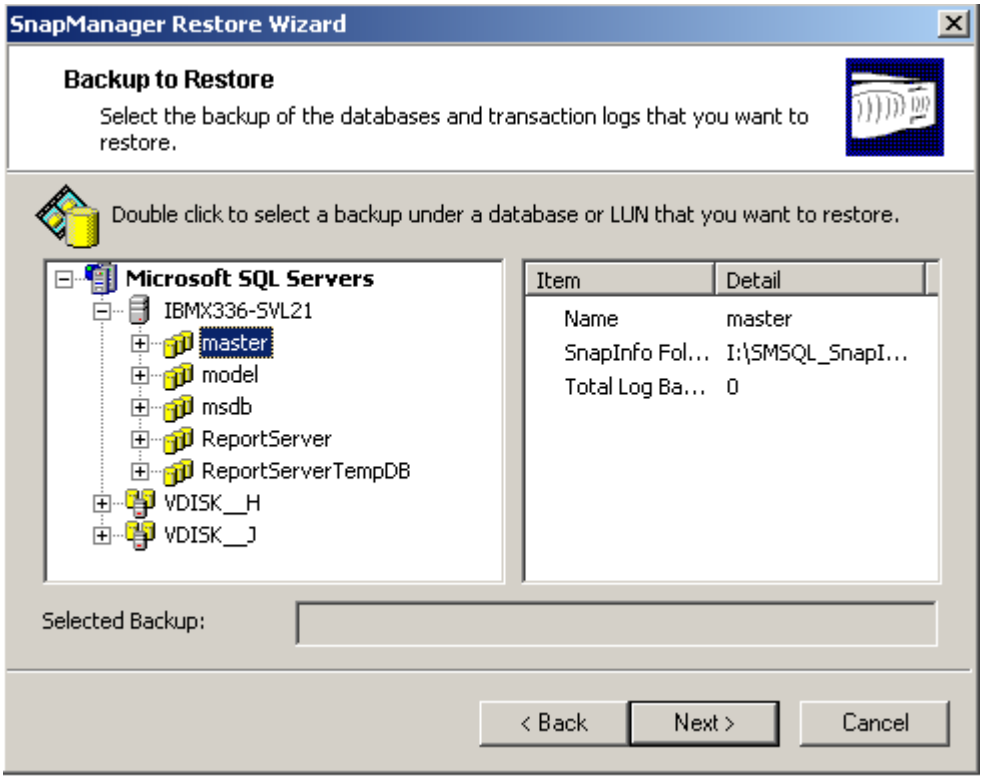

Figure 19: Selecting a Particular Database for the Database Restore

Expanding the databases lists the available database backups. Select from the list of available database backups. SnapManager for SQL Server restores the specified databases using a stream mode. If you need to restore all databases on the same LUN, use the SnapManager for SQL Server tool to restore the LUN instead of selecting individual databases. On our system, selecting the latest available backup listed the mode of database restoration for the specified database, as shown below.

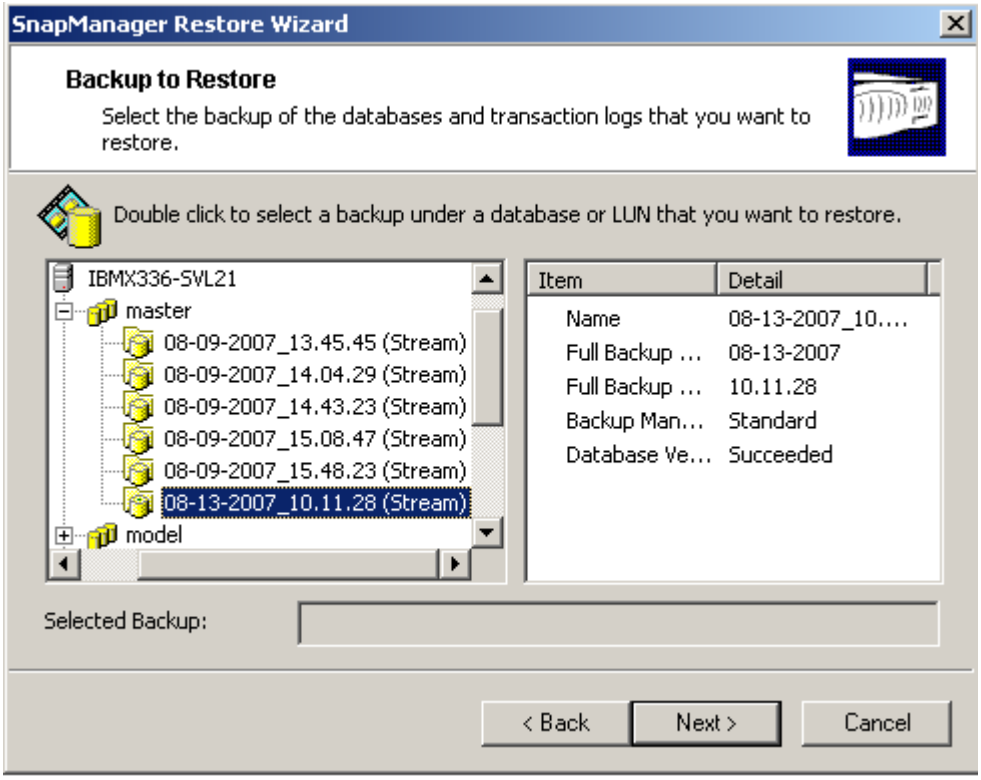

Figure 20: Selecting the Database Data Set for Restoring Master Database

- Directory service computer
- Restore system backup
- Restore Directory Service SQL database
- Restore of other Enterprise Vault services on this computer from backups

The Enterprise Vault Directory database is a SQL Server database and resides on the Directory database server. To restore this database, Enterprise Vault Admin service must be stopped on all Enterprise Vault servers prior to restoring the database. The restore process uses SnapManager for SQL Server to recover the Directory database and mount the database from the available database backup. It is important to note that SnapManager for SQL Server will be able to restore the database from its previous backup data sets. SnapManager for SQL Server will not support database recovery from backups from other third-party applications.

- Stop the Enterprise Vault Admin service on all Enterprise Vault servers.
- Launch SnapManager for SQL Server on the SQL Server and select the Restore option.
- Expand the data set to be restored
- Once the Directory database is restored, continue to restore other databases as needed in your environment. Do not start Enterprise Vault Admin service until all Enterprise Vault components or a specific component is restored. In our test setup, Enterprise Vault Services were stopped until all

components of Enterprise Vault data sets were recovered. To stop the Enterprise Vault service, use the EVService command, as explained in earlier sections.

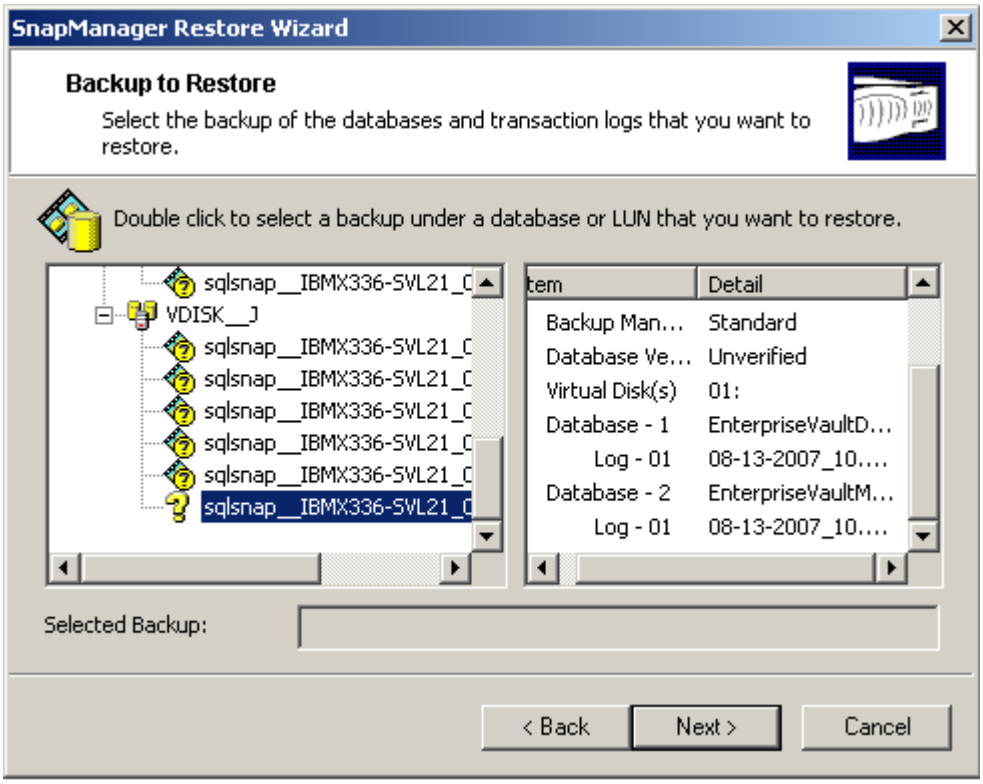

Figure 21: Selecting the Enterprise Vault Directory Database Backup Data set

- Step 1: Vault store SQL database.
- Step 2: Recover the vault store SQL database by restoring the computer running the Storage service and replace the vault store files.
- Step 3: Restore the vault store's SQL database, master and msdb databases.
- Step 4: Restore backups of other Enterprise Vault services that run on the restored Storage service computer.
- Step 5: Enterprise Vault Store database(s) reside on a SQL Server. To restore this database, Enterprise Vault Storage service must be stopped on the Enterprise Vault server being recovered prior to restoring the database(s). SnapManager for SQL Server is being used to restore the Vault Store database(s). To recover the Vault store databases, follow these steps.
- Step 6: Stop Enterprise Vault Storage Service if it is not already stopped by using the EVService stop "Enterprise Vault Storage Service" command.
- Step 7: Launch SnapManager for SQL Server tool.
- Step 8: Expand the backup set to be recovered. It is important to make sure that SQL system databases such as master, msdb databases, and Enterprise Vault Directory database are all restored prior to restoring Vault store databases.
- Step 9: Now start Enterprise Vault Storage service by using the "*EVService start <EVservername> "Enterprise Vault Storage Service*" command.

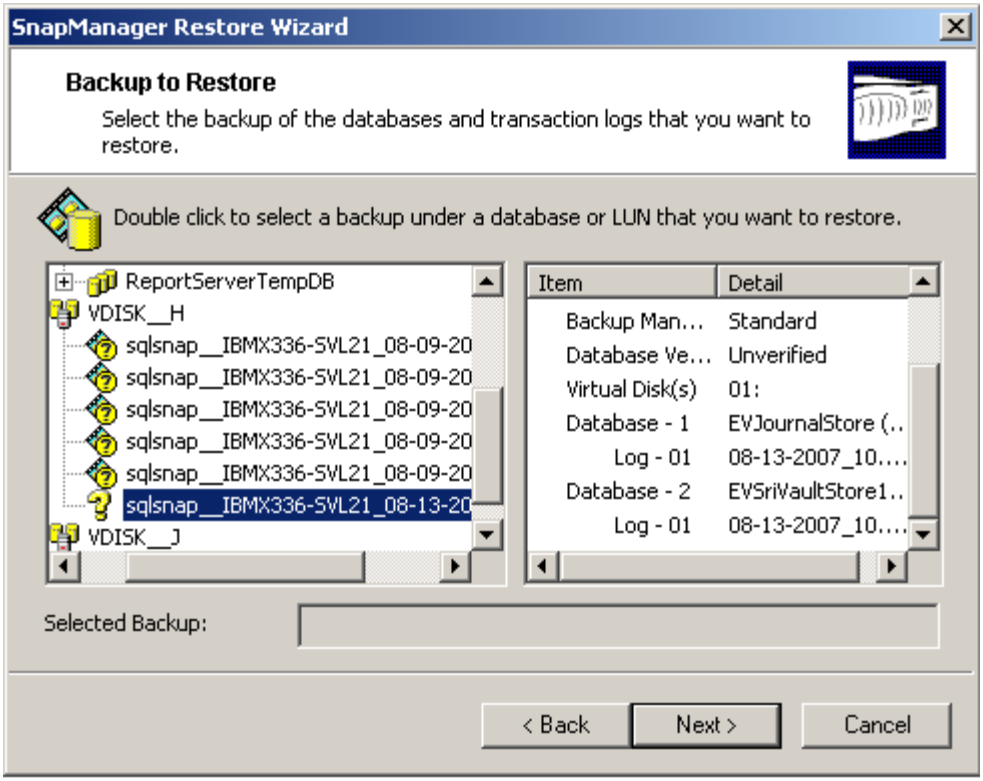

Figure 22: Selecting the Backup Data Set for Vault Store Database Recovery

- Use Enterprise Vault Admin Console to verify all Enterprise Vault Services are operating properly.

Index File Locations

- Verify the service is stopped.
- Restore the system backup of the computer running the Indexing service.
- Restore the backups of other Enterprise Vault services that run on this computer.
- On our test setup, we configured a LUN with the SnapDrive tool to store Enterprise Vault Indexes. Restoring Enterprise Vault Index services and file locations was done with THE storage management tool called SnapDrive.
- Once the Enterprise Vault Services are stopped, use the SnapDrive Snap-in tool to expand the LUN containing the Index Services and files to be restored from the Snapshot copy. This can be restored either using the SnapDrive snap-in or sdcli command line interface. EVService stop IBMX336-SVL21 “Enterprise Vault Storage Service”.
- EVService stop IBMX336-SVL21 “Enterprise Vault Index Service”
- EVService stop IBMX336-SVL21 “Enterprise Vault Shopping Service”
- EVService stop IBMX336-SVL21 “Enterprise Vault Task Controller Service”

Before restoring the Enterprise Vault Index files, verify the path where the Index files are located, and on our system, it is stored on a LUN configured as a local drive by the SnapDrive tool as shown below.

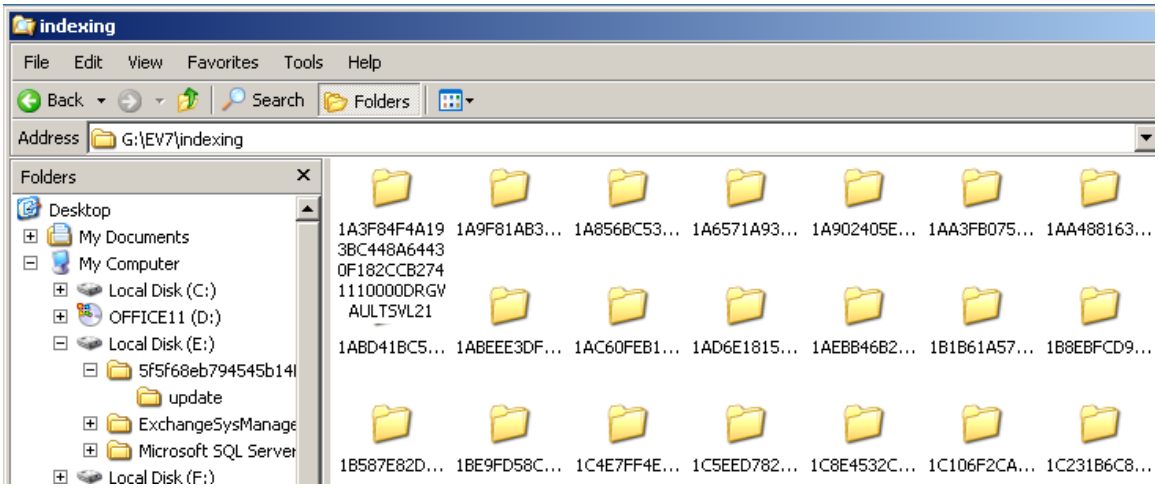

Figure 23: Verifying the Enterprise Vault Index File Locations Prior to Restoring the Enterprise Vault Index Data

Expand the storage, SnapDrive, and disks, and click the available Snapshot copy from which the data is to be restored as shown below.

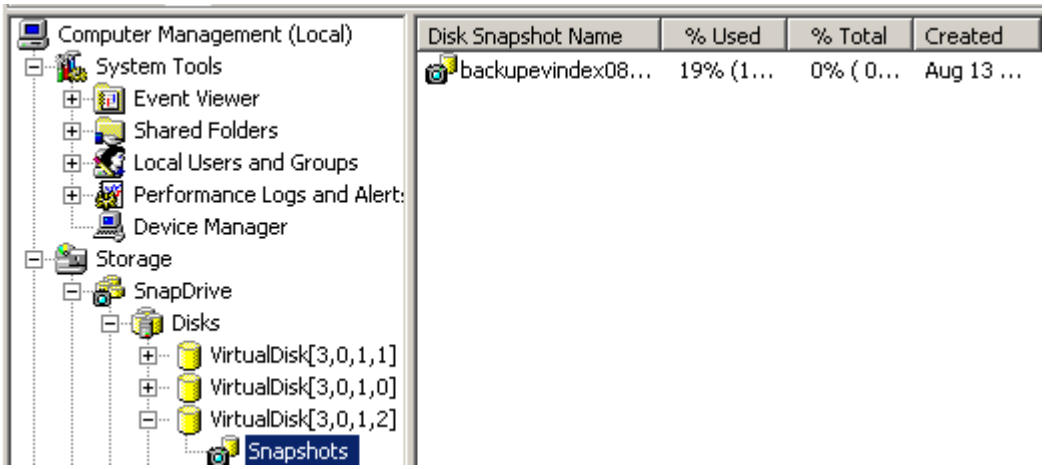

Figure 24: Checking for Available Snapshot Copy Prior to Restoring Enterprise Vault Indexes and File Locations

List the available Snapshot copies for restoring the Enterprise Vault Indexes, and on our test setup, there was one Snapshot copy available. To restore the data from this Snapshot copy, right click and select the restore disk from this Snapshot option, as shown below.

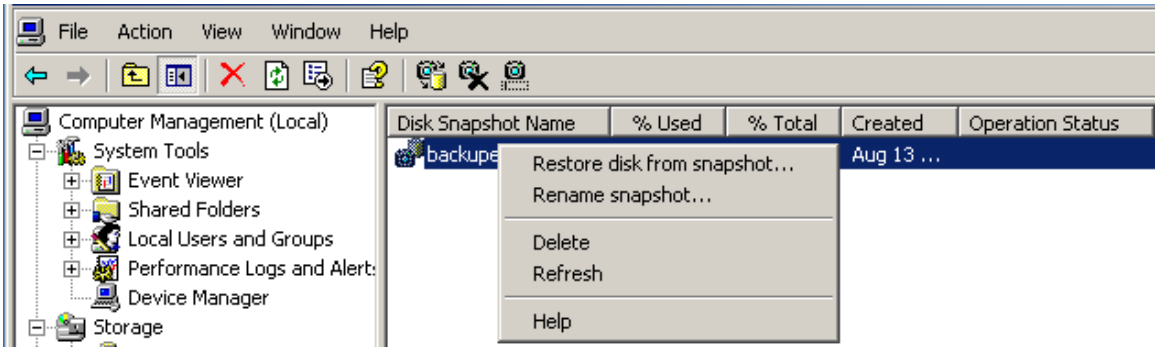

Figure 25: Restoring Enterprise Vault Index Service and File Locations from Snapshot Copy

SnapDrive will enable restoring the data to the point-in-time copy. You may verify the data restored on the disks.

Backing Up Shopping Service Files

- Step 1: Verify Shopping service is stopped.
- Step 2: Restore Shopping data to its original location.
- Step 3: Start Shopping service.
- Step 4: Verify User's ability to use the existing shopping baskets.
- Step 5: If Enterprise Vault Shopping service and file locations are configured on the same LUN as Enterprise Vault Index services and file locations, it is already backed up with the Enterprise Vault indexes. If Shopping service and file locations are stored on a separate LUN, restore from the relevant backups.
- Step 6: Vault store archive files.
- Step 7: Restore each system running a Storage service (system recovery).
- Step 8: Restore Vault store files into their original locations.
- Step 9: Restore vault store SQL database.
- Step 10: Restore backups of any other Enterprise Vault services that run on the restored Storage service computer.
- Step 11: The Enterprise Vault Shopping service resides on each Enterprise Vault server. To restore the data, the Enterprise Vault Shopping service must be stopped prior to recovering the data. SnapDrive is leveraged to restore the Shopping services data residing on a LUN from the previous backup copy.
- Step 12: Restore Vault Store Archive Items.

Restoring the Vault store items procedure depends on the storage location of the source data. If the archive items are stored on a volume other than SnapLock, use a storage system console or telnet session to restore the data from the previous Snapshot copy while Enterprise Vault services are stopped.

- *EVService stop IBMX336-SVL21 "Enterprise Vault Storage Service"*
- *EVService stop IBMX336-SVL21 "Enterprise Vault Index Service"*
- *EVService stop IBMX336-SVL21 "Enterprise Vault Shopping Service"*
- *EVService stop IBMX336-SVL21 "Enterprise Vault Task Controller Service"*

Once the Shopping service is stopped, expand the disks on the SnapDrive snap-in tool to the LUN containing the Shopping service and file locations, expand the disks, and click Snapshot. Right click the recent Snapshot copy and select to restore the Shopping service and files.

Alternatively, restore the data using the SDCLI command-line interface (CLI). A command syntax of SDCLI to restore data is given below.

- *SDCLI snap restore –d mountpoint/driveletter –s snapshotname*
- Now start Enterprise Vault Services by using the EVService command.
- Verify the service operations from Enterprise Vault Admin Console.

To restore a Snapshot copy, use the following command on the storage system console:

Filerprompt> snap restore –V [-f] [-t vol] –s <snapshot-name] [-r <restore-as-path>] <vol-name> |<restore-from-path>

It can also be restored from a computer using the rsh command. Syntax for using the rsh command to restore from a Snapshot copy is shown below.

Rsh <filername> -l root:password snap restore –V [-f] [-t vol] –s <snapshot-name] [-r <restore-as-path>] <vol-name> |<restore-from-path>

The above paragraphs explained the procedure to restore the archive items stored on a volume other than SnapLock. On the other hand, if these vault store archive items are stored on a SnapLock volume to maintain the WORM properties, data has to be restored by replicating the data from the backup copy using qtree level SnapMirror. SnapRestore from Snapshot is not supported on SnapLock volumes. To initiate the SnapMirror process, use the previous SnapMirror setup and change the source and destination path configuration. Initiate the replication after ensuring the SnapMirror source and destination paths to ensure the data recovery from the right place.

8. Takeaways

Procedure and tools explained in this paper mean a lot in managing complex Enterprise Vault backup and restore issues. Managing several different data sets maintaining data consistency across all data sets is a challenge to an enterprise environment. In an enterprise environment, bringing the Enterprise Vault application to offline may not be an option to most customers. Without a NetApp storage solution, the Enterprise Vault server has to be offline or in a read-only state for a larger time window. Putting Enterprise Vault offline causes the data to be queued up within the e-mail server, data accessibility issues, and lost productivity. In today's world, making data unavailable for an extended period has a business impact. Certain businesses require the Enterprise Vault server to be online all the time. This requirement seems like a tall order. By exploiting NetApp storage solutions, the joint solution of Enterprise Vault and NetApp provides unique advantages to customers.

Another example: If Enterprise Vault Index is corrupted, rebuilding the Enterprise Vault Index could take days or even weeks in a normal environment. Considering the nature of the Enterprise Vault Index and the way it is heavily accessed, it is possible to corrupt the Enterprise Vault index. By using the NetApp storage solution, such data can be restored very quickly without the need to rebuild or going through system performance degradation while building the Enterprise Vault Index.

Another issue with Enterprise Vault in enterprise data centers relates to 2/3 tier storage architecture. This type of architecture adds complexity and cost to the setup. NetApp addresses this issue by offering a unified storage architecture. This means that NetApp storage systems may be carved out to configure the storage

for various Enterprise Vault data components as well as other optional applications on a single box. An example includes configuring the Enterprise Vault archival data on SATA drives, Enterprise Vault Index on FC or SATA drives, Database on SAN storage, and compliance data on a volume enabled by SnapLock. Use NetApp storage management solutions such as SnapManager for SQL Server to manage the database backup and recovery, SnapDrive to manage storage data, and SnapMirror to replicate the data to another/same system to have simple disaster recovery solution.

This paper discussed the procedure to back up Enterprise Vault server data in a NetApp storage system configuration. It covered the topics to back up full system data, Enterprise Vault data only, and registry entries backup. It also discussed the procedure to recover Enterprise Vault in various situations from the backup data. It explained the procedure and ease of using storage management solutions such as SnapManager for SQL Server and SnapDrive tools. To install and configure Microsoft Exchange Server, Microsoft SQL Server, and Enterprise Vault server, we used the SnapDrive configured local disks on our test setup. Enterprise Vault used NetApp storage systems configured as network shares for archiving the data from the primary to the secondary.

Enterprise Vault server has several drawbacks in terms of data availability and dependability. To access the data of archived files or to access the files, SQL Server must always be up and running. In case of database corruption, data has to be recovered from a backup copy, losing all the recently archived items. Data replication could take a significant amount of time and resources. Restoring a corrupted database could be disastrous in an enterprise environment. This paper briefly explained the procedure to recover Enterprise Vault server from a disaster scenario.

NetApp storage solutions effectively address the shortcomings explained previously. The Symantec Enterprise Vault and NetApp product integration offers highly available and exceptional performance at the lowest total cost of ownership in the industry.

NetApp and Symantec are committed to providing Enterprise Vault users with superior solutions designed to meet business objectives. NetApp storage system solutions ensure protection of Enterprise Vault data 24x7 and provide the ability to recover the data quickly.

9. Conclusion

This paper 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 joint solution story relates better together, and the NetApp storage solution complements the Enterprise Vault capabilities in backup and restores areas.

The procedures made in this paper are intended to be an overview of the Enterprise Vault backup and recovery architecture. This paper serves as a starting guide when designing and deploying backup and recovery of Symantec Enterprise Vault in a NetApp storage system environment. During the design phase, involve Microsoft Exchange and SQL Server specialists along with Enterprise Vault experts and discuss the deployment plans and requirements with appropriate Symantec and NetApp professional services teams. For details, refer to appropriate product manuals.

10. Caveat

NetApp has not tested all possible combinations of hardware, storage architecture, and software solutions. If you use a different Windows Server OS or a different version of Enterprise Vault, then significant differences in your configurations could exist. These differences may alter the procedures necessary to achieve the objectives outlined in this document. If you find that any of these procedures do not work or find any errors, we suggest contacting the author immediately. If you need additional information or have any questions, contact the Web administrator of Network Appliance. Do not attempt to seek help from NetApp Global Support for procedures listed in this document.

11. Appendix

This section provides additional information that helps successful installation and configuration of an Enterprise Vault system on a Windows server.

11.1. Operating System Required Patches

The section lists the hotfixes that must be installed before configuring the NetApp storage system using Fibre Channel Protocol and SnapDrive software. The Microsoft support team provides these patches directly to its customers.

If you install and configure local drives using SnapDrive in a Fibre Channel Protocol environment, the following Windows hotfixes are required on Windows 2003 SP1 server:

1. Q916531-hbaapi
2. Q916048-storport
3. Q913648-vss
4. Q912593-classpnp
5. Q910048-ntoskrnl

11.2. SnapManager for SQL Server

SnapManager for SQL Server 2.1R1 or later releases support the capability to restore a single database using streaming mode.

11.3. Infrastructure Used in the Test Setup

Following are the details of our infrastructure used to test the environment. Please note that these configurations may not reflect any best practices suggested in product documentation. Refer to Enterprise Vault and NetApp product manuals and technical reports to understand the best practices configuration to fit your unique setup needs.

- Path for all data components including
  - SQL Databases for Vault Stores
    1. LUN Configured on NetApp Storage System
  - NetApp Storage System for compliance data archival
    1. SnapLock Compliance Volume on qtree ‘evstoreslc1’
  - SQL Databases for Vault Store Logs
    1. LUN Configured on NetApp Storage System as drive H:\
  - SQL Directory Database
    1. LUN Configured on NetApp Storage System as drive J:\
  - SQL Directory Logs
    1. LUN Configured on NetApp Storage System as drive E:\
  - Indexes for all Vault Stores
    1. LUN Configured on NetApp Storage System as drive G:\
- Names for Aggregates, Volumes, LUNs
  - Aggregate
    1. Available aggregates on NetApp Storage system(s)
  - Volumes
    1. Available Volumes on NetApp Storage system(s)
  - LUNs
    1. Available LUNs on NetApp Storage system(s)
- Names of all shares
  - Available CIFS Shares on NetApp Storage system(s)
- Size of all LUNs, Volumes, Aggregates
  - LUNs

1. LUN Details on all NetApp Storage system(s)

    - Volumes
    - Aggregates

- IP Addresses for FAS systems
    -
- Windows Servers Used
    - Windows 2003 Server for Enterprise Vault Server
    - Windows 2003 Server for SQL Server
    - Windows 2003 Server Exchange 2003 Server
    - Windows 2003 Server
    - Windows 2000, Windows XP, and Windows 2003 for Enterprise Vault Client applications

12. References

This section provides additional information that helps provide successful installation and configuration of an Enterprise Vault system on Windows Server.

Enterprise Vault Server configuration with NetApp storage systems involves several components to achieve a backup and recovery solution. Please use appropriate product manuals of each storage management tools prior to attempting Enterprise Vault backup and recovery in a NetApp storage system environment.

The following technical reports and system manuals were referred to while developing this paper. For detailed procedures, refer to their respective documents.

- ”Implementing Symantec Enterprise Vault with Network Appliance Storage Systems”
- “Integrating Veritas Enterprise Vault with NetApp Storage Solution File Archival”
- “Enterprise Vault 2007 Product Documentation from Symantec Manuals”
- “Symantec Enterprise Vault”
- “SnapDrive for Windows: Best Practices”
- “Using SnapLock Compliance and SnapLock Enterprise with Data ONTAP 7G”