Deployment Guide: Symantec Enterprise Vault with NetApp Storage Systems

Gangoor Sridhara, NetApp

TR-3500

Abstract

As the volume of e-mail and other unstructured data skyrockets, it has become increasingly clear that today's enterprises need a structured approach to archival. The combination of Symantec Enterprise Vault with NetApp storage systems provides enterprises the capability to archive and protect both business-critical e-mail and unstructured file system data in a simple to manage unified storage environment. This technical report discusses in detail the procedures required to complete the installation of Symantec Enterprise Vault in a NetApp unified storage environment.

Table of Contents

1. Introduction

Corporate data belongs to three major groups: structured, semi-structured, and unstructured data.

- **Structured data.** Data actively managed by a relational database application. A few examples of structured data are RDBMS data, ERP systems data, and so on.
- **Semi-structured data.** Data loosely managed by an application. An example of semi-structured data is a messaging/e-mail environment.
- **Unstructured data.** Data not controlled or monitored by any application or database server. Examples of unstructured data include a user's home directory, incoming fax document, prints, and Microsoft® Office files.

While structured data tends to have well-defined processes/procedures for data management such as backup, archival, and compliance, semi-structured and unstructured data is largely ignored. The Symantec Enterprise Vault Server product offers an efficient method to store messaging and file system data in a central archival location. Enterprise Vault manages the archival and retention of the data according to a set policy to a configured location and for a specified period for retaining the data.

In addition to the management of e-mail archival, Enterprise Vault also offers a complete solution for file system archival (FSA). This feature allows an Enterprise Vault Server to archive and manage file system data. This paper describes the steps required to deploy Symantec Enterprise Vault in combination with NetApp storage systems. The combination of Symantec Enterprise Vault and a NetApp storage system yields a highly available and scaleable solution ready to solve any enterprise's most demanding archiving and/or compliance challenges.

1.1. Background on Technical Issues

Symantec Enterprise Vault is a software solution designed to archive data, based on a fully configurable organization policy. This solution archives data from a primary application and storage system onto a secondary storage system, providing a fully indexed archive for retention while freeing primary storage capacity and performance. Enterprises without a centrally managed archival system for e-mail environments commonly face several challenges that can affect the usability of e-mail environments as well as the ability to protect user data. As the volume of e-mail increases, a common IT practice is to impose mailbox quotas on mailbox users. While archiving the result of maintaining a "high-water mark" for the volume size, quotas restrict the ability of users to conduct business. Quotas only push the message growth problem to a darker corner of the environment, forcing users to spend increasing amounts of time on managing their own ad-hoc archival of local PST files. These PST files are typically not included in an enterprise backup plan and therefore are unmanaged and at risk. Enterprises implementing a centralized archiving solution solve the problems of both mailbox growth and archive management while freeing valuable production/primary system resources and capacity, resulting in better performing systems and backup/recovery that meet the desired service levels. All of these benefits are provided without changing the user experience in their mail environment, because there are no quotas and no "do it yourself" archiving and cleaning chores. NetApp storage system solutions offer compelling advantages to this data management scenario. The ability to provision storage with primary and archive workload characteristics on a single system provides simplified management and leverages/minimizes IT skill sets, as users are required to only manage product and maintain a single system that is providing multiple service levels. In addition to the skyrocketing growth in e-mail volume, a number of compliance regulations recently enacted globally mandate the archival of e-mail and other corporate data. The requirement and the required ability to produce the data in a timely manner have driven enterprises to pursue a more structured and regulated archiving process.

1.2. Purpose and Scope

The purpose of this paper is to demonstrate the ease of product integration of Enterprise Vault and NetApp storage systems. It is important to note that this paper is not a substitute for the product documentation and release notes shipped with Symantec Enterprise Vault and/or the target NetApp storage system. It is very important to complete all the preinstallation tasks before attempting to install the software product. This paper will discuss steps required to prepare the operating system (OS) and NetApp storage systems ready for Enterprise Vault installation and configuration.

In addition to Symantec Enterprise Vault software, this paper will briefly discuss the installation of additional software products including the NetApp host attach kit (HAK) and SnapDrive software. For detailed procedures involved with installing these products as well as the SQL Server and Microsoft Exchange Servers required for a complete environment, please refer to the appropriate product documentation supplied with your release of software and hardware.

2. Infrastructure

In this section of the paper, we will describe the necessary infrastructure for deployment of an Enterprise Vault environment. Enterprise Vault can be configured to support compliance requirements as well as e-mail and file system archiving requirements. To support compliant retention of data, Enterprise Vault relies on the storage system solution's ability to lock data in an immutable store. This paper briefly describes the procedure to configure NetApp storage systems using NetApp SnapLock® to archive compliance data. For complete and detailed instructions on compliant data retention with NetApp SnapLock and Symantec Enterprise Vault, please refer to the detailed procedures found in configuring SnapLock with Enterprise Vault Server available on the NetApp Web site.

Deployment of Enterprise Vault requires server(s) running Microsoft Windows 2003 or Windows 2000 Server.Enterprise Vault also supports Exchange 2007 environment. In addition, Enterprise Vault requires either Microsoft SQL Server 2005 or SQL Server 2000 products. If you are deploying mailbox management, Enterprise Vault supports the following messaging systems:

- Microsoft Exchange 2003
- Microsoft Exchange 2007
- IBM Domino Server

For deployment of Enterprise Vault in Microsoft file system archiving applications, Microsoft Exchange is not required. Though not covered in this document Enterprise Vault also supports several other applications including Lotus Notes and Microsoft SharePoint. Information regarding Enterprise Vault archiving of these application deployments can be found on the Symantec Enterprise Vault Web site.

NetApp recommends the deployment of both Microsoft Exchange and SQL Server environments using either Fibre Channel SAN (FCP) or iSCSI protocol. Documentation and best practices for deploying IBM Domino server and several applications are available in the NetApp Technical Library section.

Best practices dictate the requirement to determine the number of Enterprise Vault Servers required for a given deployment. On most occasions, it is assumed to have one Enterprise Vault Server for every 4000 mailbox active users. Compliance accelerator and journal servers each require a dedicated Enterprise Vault Server. The number of Enterprise Vault Servers required is unique to each environment. This paper recommends seeking professional help while determining an optimal solution to fit your unique environment. It is also important to note that only one Exchange mailbox task can be set for each Enterprise Vault Server. This paper recommends considering this limitation of the number of Exchange tasks allowed per Enterprise Vault Server, while deciding on the configuration of Enterprise Vault and Exchange Servers.

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

Exchange Server: Windows 2003 Service Pack1 Enterprise Edition

SQL Server 2005 and Enterprise Vault Server: Windows 2003 Service Pack1 Enterprise Edition

E-mail archival and file system archival: NetApp FAS3050C storage system running Data ONTAP® 7.1.1

Exchange primary data: NetApp FAS980 storage system running Data ONTAP 7.1.

E-mail archival and FSA data migrating service: NetApp R200 storage system running Data ONTAP 7.1

Storage management software: NetApp SnapDrive software product version 4.1, NetApp SAN storage software product – Host Attach Kit 3.0, Emulex LP9002L fabric attached adapter card, and HBAnywhere software. For complete compatibility and support matrix, refer to the Compatibility and Configuration Guide for NetApp FCP and iSCSI Products.

2.1. Infrastructure-Related Tasks

Before attempting to install Enterprise Vault Server, it is a prerequirement to complete the setup tasks. This will prepare the systems for successful installation of Enterprise Vault software. Skipping any preinstallation tasks may adversely affect the Enterprise Vault Server installation and configuration.

This paper assumes that the NetApp storage setup needed a fresh install of storage area network (SAN) configuration. Configure the host attach kit software and the software on NetApp storage systems. For this purpose, we used host bus adapter (HBA) card LP9002L from Emulex to connect from Windows® Servers to the NetApp storage system. For details on supported HBA cards, visit the NetApp support Web site. If SAN configuration is already configured, determine the storage requirement and complete the storage setup.

To install the necessary applications such as Microsoft Exchange, SQL Server, and Enterprise Vault Servers, one may use the SAN or IP-based SAN storage configuration to configure the local disks on Windows Servers. This paper assumes that a new installation of Exchange, SQL Server, and Enterprise Vault Servers on NetApp storage area network (SAN) configuration occurs. Enabling the necessary product license is a prerequirement to use the storage.

To install SAN host attach kit Software follow the FCP Installation Guide available on the NetApp support site. Installing SAN Manager Software is optional. SAN Manager provides end-to-end Fibre Channel SAN management that enables NetApp customers to securely monitor and manage their enterprise storage infrastructure. To discover and monitor NetApp storage devices, SAN Manager requires a DataFabric® Manager server.

2.1.1. SnapDrive Software Installation

After installing SAN HBA software, prepare for installing SnapDrive software. Verify that the HBA has the supported version of driver and firmware and upgrade if necessary. To download the necessary driver and firmware, appropriate links to HBA vendor are available on NetApp support site.

It is also important to install the necessary hot fixes on the Windows Server. The necessary hot fix required on Windows 2003 Server is given in Appendix A. These hot fixes are required to complete the storage configuration. SnapDrive software integrates with the Windows Volume Manager. This allows NetApp storage systems to serve as virtual storage devices for application data in Windows Server environments. The SnapDrive application tool manages virtual disks available as local disks on Windows hosts. SnapDrive allows Windows machines to interact with the virtual disks as if they belong to a directly attached Redundant

Array of Independent Disks (RAID) array. SnapDrive software supports both Fibre Channel and IP based iSCSI protocols. It provides the dynamic storage management feature. For detailed procedures to install SnapDrive software, refer to the SnapDrive installation and administration guide. This paper recommends to have the systems connected Windows host reside in the same broadcast domain. Refer to SnapDrive Rules and Guidelines documentation on the NetApp support Web site. The NetApp support Web site requires the necessary user permissions. If you do not have access to the NetApp support Web site and require additional information, contact your NetApp sales team.

During our test install, the SnapDrive installation wizard displayed the FCP HBA driver and firmware information. On our test setup, the following figure displayed the available HBA driver and firmware version along with the status information.

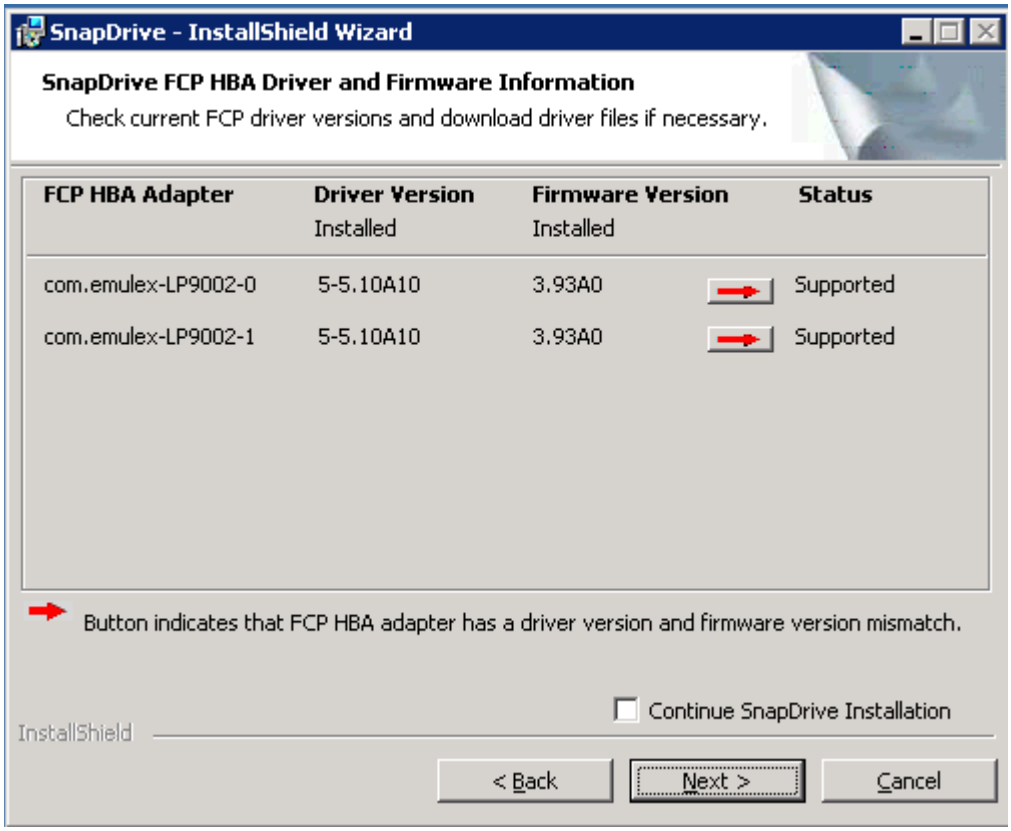

Figure 1) SnapDrive FCP HBA Driver and Firmware Information

After checking the driver and firmware-supported version, the install wizard checks the management driver information to support the MPIO feature. If required, this process installs the appropriate driver version. After installing the SnapDrive software, use the Windows management tool (MMC) console to configure the local drive. SnapDrive requires additional hot fixes from Microsoft before configuring the local drives. These patches are listed in Appendix A. In our test setup, we configured three virtual local disks on Enterprise Vault Server and two local disks on Exchange Server systems. Figure 2 displays the screen shot of computer management after the local disk configurations completed.

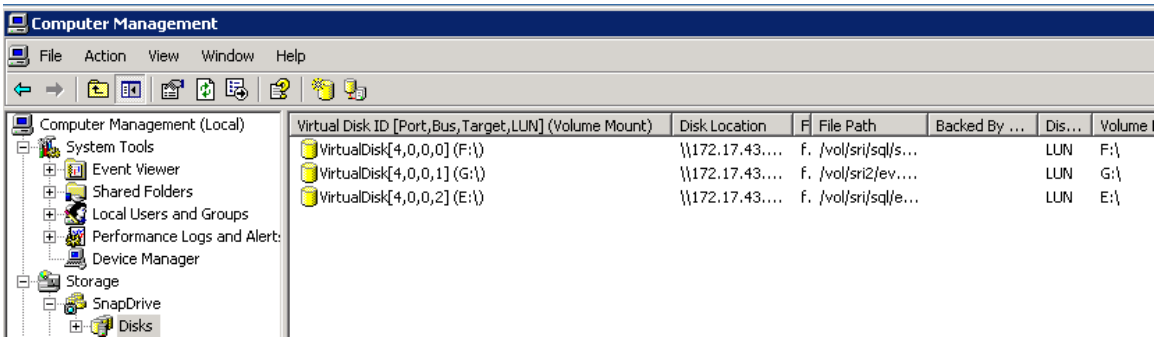

Figure 2) Fibre Channel SAN Configuration on Enterprise Vault Server as Shown in Computer Management

2.1.2. Installing Microsoft Exchange Server

In an Enterprise Vault environment, it is safe to assume that the Microsoft Exchange Server is installed and configured. If so, skip this section. However, for completeness of information, this paper assumes that Microsoft Exchange Server is installed as a new install before installing Enterprise Vault software. Using the SnapDrive tool, we created two virtual local disks on the Exchange 2003 Server. Before installing Exchange Server, our test setup completed the ForestPrep install task and applied the necessary Windows OS patches. New Exchange 2003 installation requires Windows 2003 SP1, Windows 2000 SP3, or later or Windows Advance Server SP3 or later. It is required to install certain services such as NNTP, SMTP, and World Wide Web, and enable these services on Windows Server. Before running the Exchange installation wizard, run ForestPrep to extend the Active Directory schema. DomainPrep will prepare the domain for Exchange 2003. Domain administrator privilege is required to complete these tasks. Note that Enterprise Vault also supports Microsoft Exchange 2007 server configuration. Following diagram shows the components selected for installing Exchange Server on our test setup.

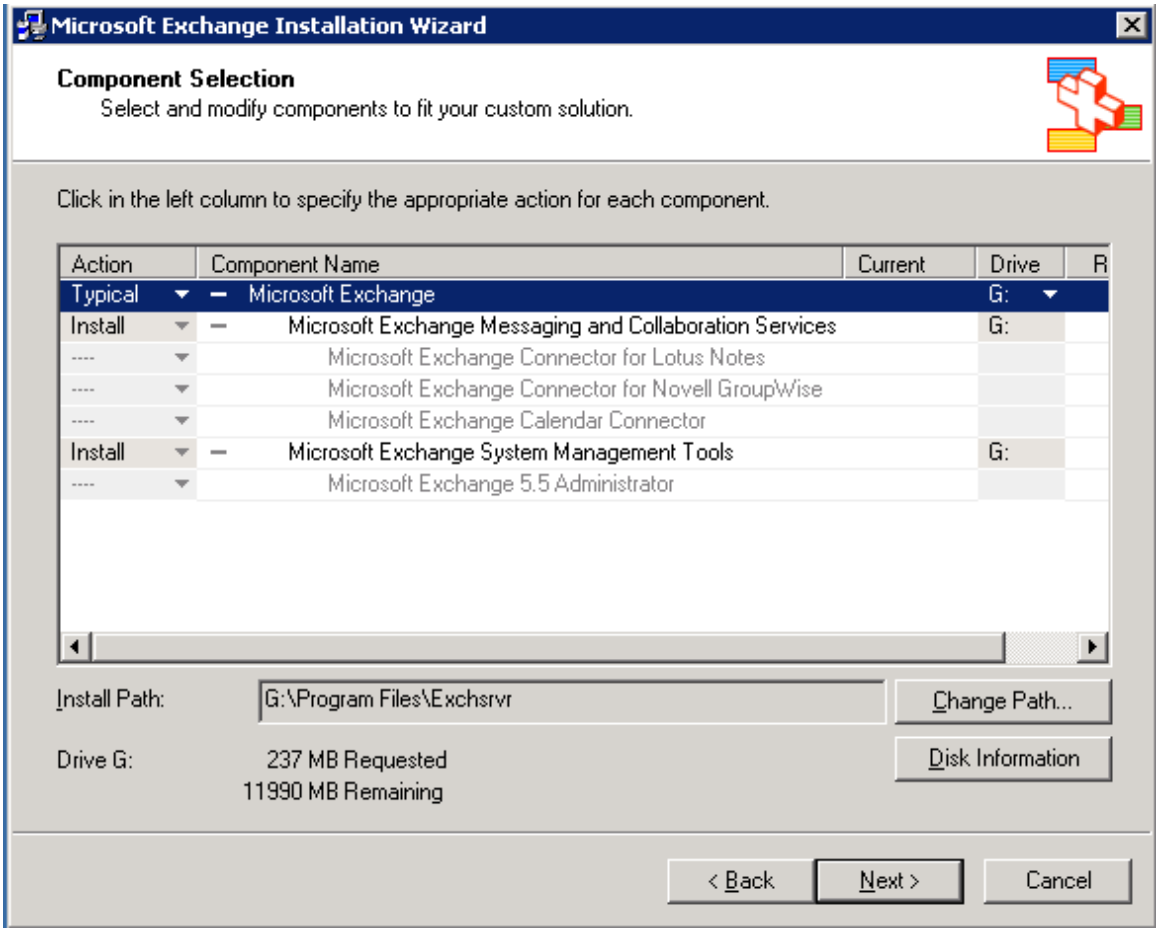

Figure 3) Microsoft Exchange Installation Wizard- Component Selection

Using the SnapDrive software tool, the storage administrator has the ability to scale the storage space dynamically. Note that the storage size configured in our test setup was only for informational purposes. You are allowed to create larger than 2TB logical unit numbers (LUNs) (and hence the size of local disks). Exchange installation continues to install the selected components as shown below.

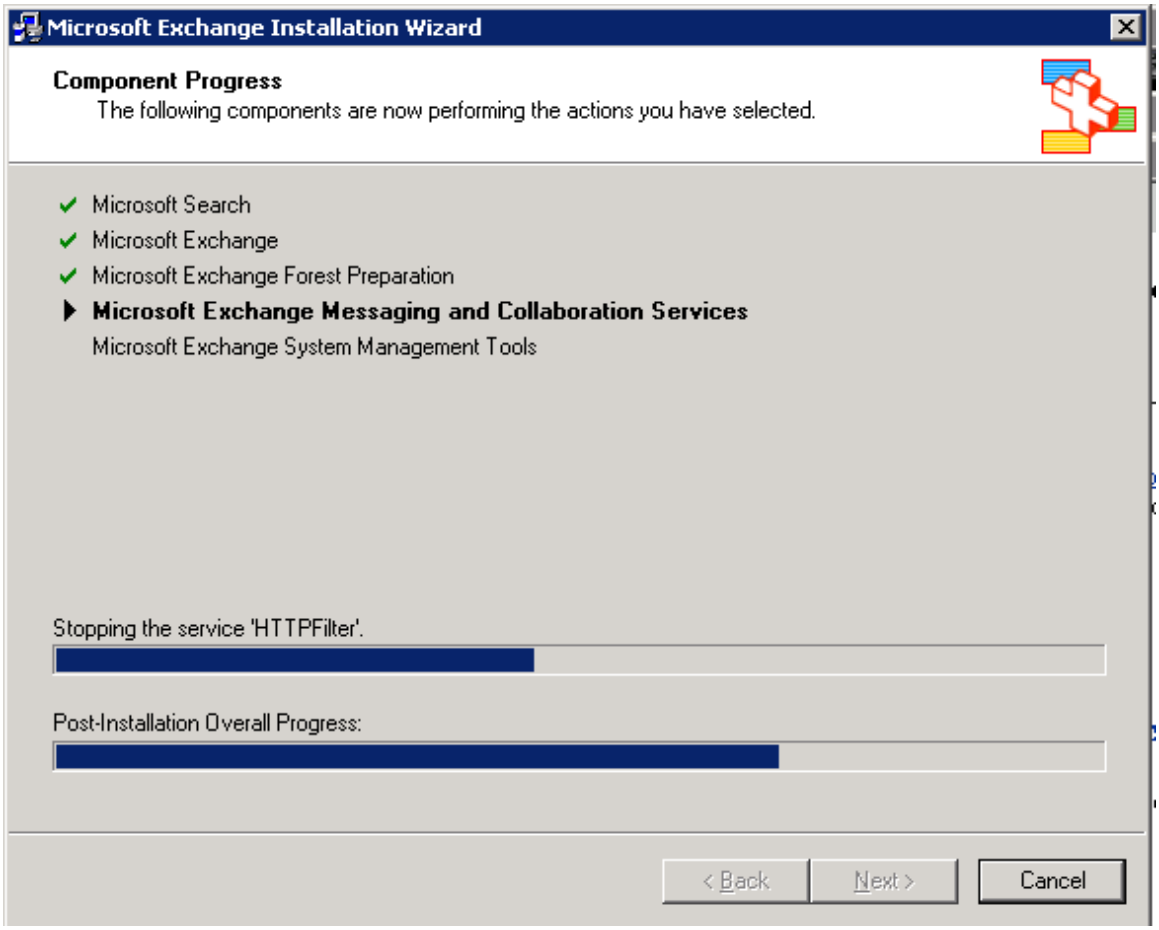

Figure 4) Microsoft Exchange Components Install Status

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.

2.1.3. 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, we used SQL Server 2005 and created a 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.

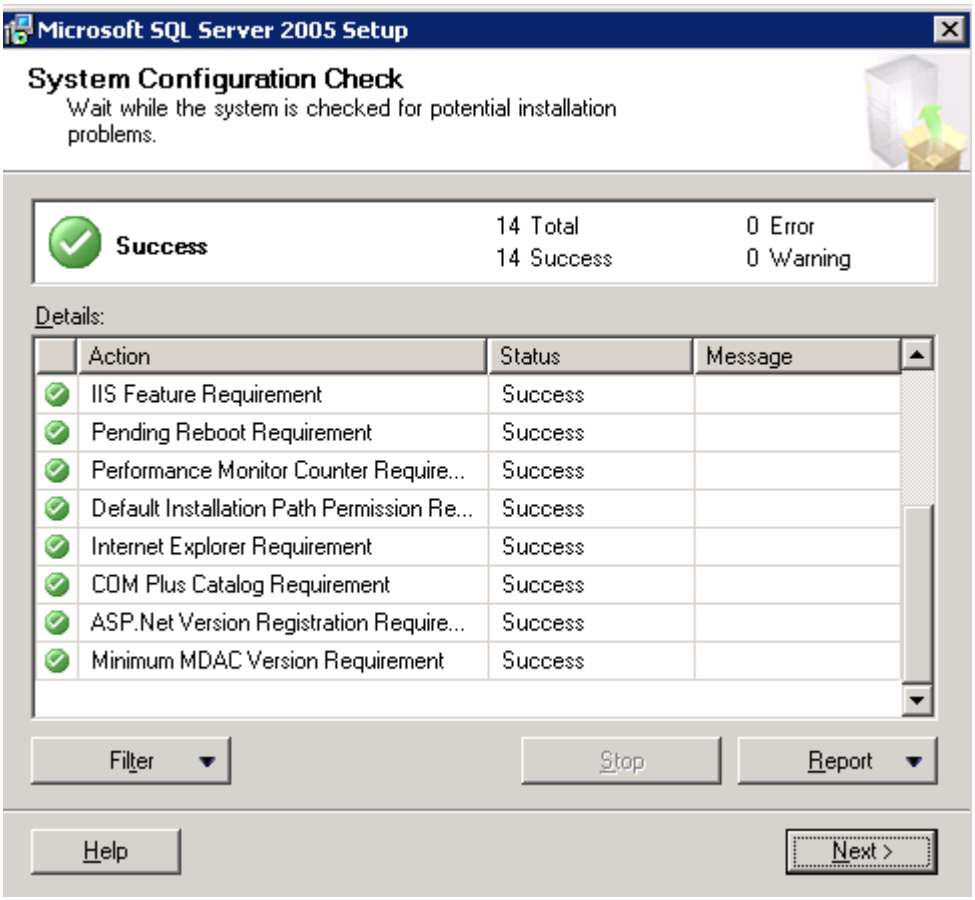

Figure 5) System Configuration Check for SQL Server 2005 Installation

After the system configuration check, the installation wizard starts the installation process. Select the SQL Server authentication mode that specifies the security used when connecting to SQL Server. There are two authentication modes, Windows authentication mode and mixed mode, which includes the Windows authentication as well as SQL Server authentication. During our test setup, we selected Windows authentication mode. During the SQL Server installation, select the components to install such as SQL Server database servers and analysis services. It may be relevant to select *Dictionary order, case-insensitive collations* settings. Report server information allows configuring the report server, virtual directories, and SSL settings. The installation wizard in our setup displayed the following figure showing the server type, server name, and authentication mode.

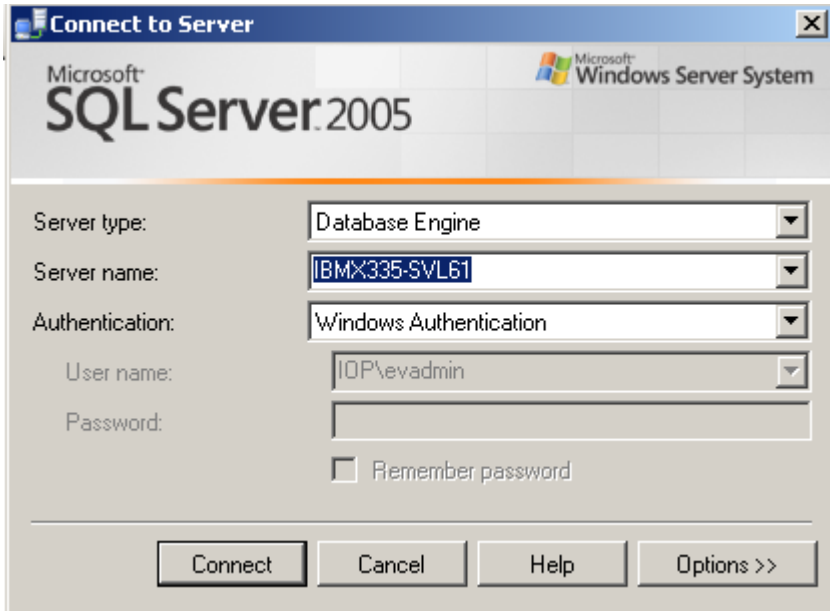

Figure 6) SQL Server 2005 Information

Verify that SQL Server has been installed successfully and start the SQL Server to complete the database configuration tasks.

2.1.4. Domain Users Account Information

Successful installation and configuration of Enterprise Vault Server requires an Enterprise Vault administrator user in the domain. This Enterprise Vault administrator need not have the domain administrator privilege. Best practices dictate avoiding giving the domain administrator privilege to the Enterprise Vault administrator account. On our test setup we used a domain called IOP and created a user called ‘evadmin’. In addition to this, we created multiple users to enable mailbox accounts.

2.1.5. Mapping the Network Share

Enterprise Vault requires an NTFS supported file system for archival destination. This includes local disks, configured virtual disks using NetApp storage systems, or a network-mapped share. Establish the network connectivity between the Enterprise Vault Server and NetApp storage system(s). Once the network connectivity is established, complete the storage configuration. Data ONTAP provides a greater flexibility in storage configuration in defining and configuring volume sizes. Dynamic scaling of storage is a supported feature. Based on the need and growth of data, a particular storage volume can be expanded or shrunk if needed.

Before creating a network share, verify that CIFS license is enabled and CIFS setup is complete. On our test setup, we used two storage systems, one FAS3050C system and an R200 storage system. On each system, we created the necessary CIFS shares. On our FAS3050C system, the following figure shows the configured CIFS shares.

```
ilm             /vol/ilm
                          everyone / Full Control
ilm1            /vol/ilm/ilm1
                          everyone / Full Control
vs3             /vol/sri                          Vault Store Partition 3
                          everyone / Full Control
```

Figure 7) CIFS Shares Created on FAS3050C Storage System for Enterprise Vault Archival

2.1.6. Configuring Write Once, Read Many Storage Using SnapLock Software

Companies require the ability to successfully archive and retain the contents in its state as read-only for a specified retention period. A SnapLock enabled volume meets this requirement. On the NetApp storage system, enable the appropriate SnapLock license. Note that certain configurations support both types of SnapLock licenses on the same NetApp storage system at the same time. Currently there are two types of supported SnapLock features. SnapLock license supports a stricter version of compliance volumes where the WORM committed files remains in an immutable state until the retention period expires. Another version is known as "SnapLock for Enterprise," and the storage administrator will have the control over that volume. Based on defined retention policy, configure the appropriate SnapLock volumes. Considering the effect of WORM features, this paper strongly advises users to seek professional help while configuring and testing SnapLock volume(s). Hands-on experience with a NetApp software simulator helps to understand the properties of SnapLock. Necessary Data ONTAP simulator software is available on the NetApp support Web site. The "Using SnapLock Compliance and SnapLock Enterprise with Data ONTAP 7G" paper discusses the SnapLock product in detail, and this paper recommends getting additional information. Note that any misconfigurations or settings with SnapLock volume may be irreversible, and hence NetApp professional help is strongly recommended.

2.2. Enterprise Vault Server Architecture

In this section, we briefly discuss the Enterprise Vault architecture and NetApp storage systems and Enterprise Vault integration methods. Enterprise Vault comes with several service components to perform the task of archiving, indexing, storing, and restoring the contents. The Enterprise Vault administration tool provides the configuration and management of Enterprise Vault services, tasks, and archives. Active Server Page (ASP) Web access components enable users to access the content from archives. Microsoft Outlook users have the capability to access the archived content from their Outlook client.

In addition to archiving e-mail data, Enterprise Vault supports additional features for file system archival, SharePoint archiving, and SMTP message archiving. File servers are used to store the file system archiving by using Enterprise Vault placeholder service. SharePoint archiving components enable archiving and restoring documents on SharePoint servers. Similarly, SMTP archiving component processes messages from third-party messaging services. Major focus of this paper will be e-mail management in Microsoft Exchange Server environment.

Enterprise Vault is composed of vault directory and vault store database that uses SQL Server databases. The relational database holds the Enterprise Vault configuration data and information about the archives. Some of the Windows tasks include:

- Scanning the server for archival pending items
- Storing the items in archival
- Indexing item attributes
- Retrieving the content from archives

Enterprise Vault architecture includes Windows Servers, Microsoft Exchange Server(s), Microsoft SQL Server, Enterprise Vault Servers, Lotus Domino server (Journaling feature), and the necessary storage system(s). In this architecture, three NetApp storage systems are used for:

- Configuring the storage area network (SAN) systems
- Configuring the network shares for content archival using Enterprise Vault on FAS3050C system
- Configuring the network shares for content archival using Enterprise Vault on R200 system

The test setup used near-line storage R200 for moving the items after archiving for a specified time. This architecture allows the items to be migrated from primary to the secondary storage destination. The following figure illustrates the Enterprise Vault system.

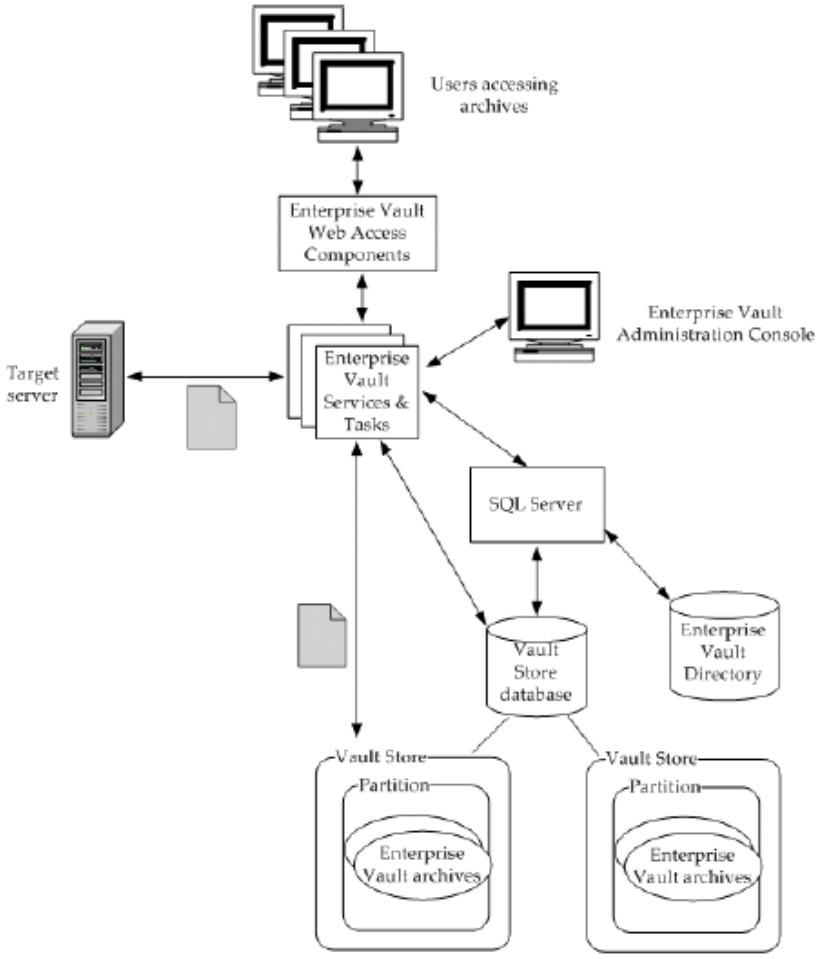

Figure 8) Enterprise Vault System Architecture

Enterprise Vault task performs the search and returns a list of results to the users. Then the user selects a particular link and the request goes to Enterprise Vault tasks and services, which in turn provide the HTML version of the item. Following figure explains how users access the stored items.

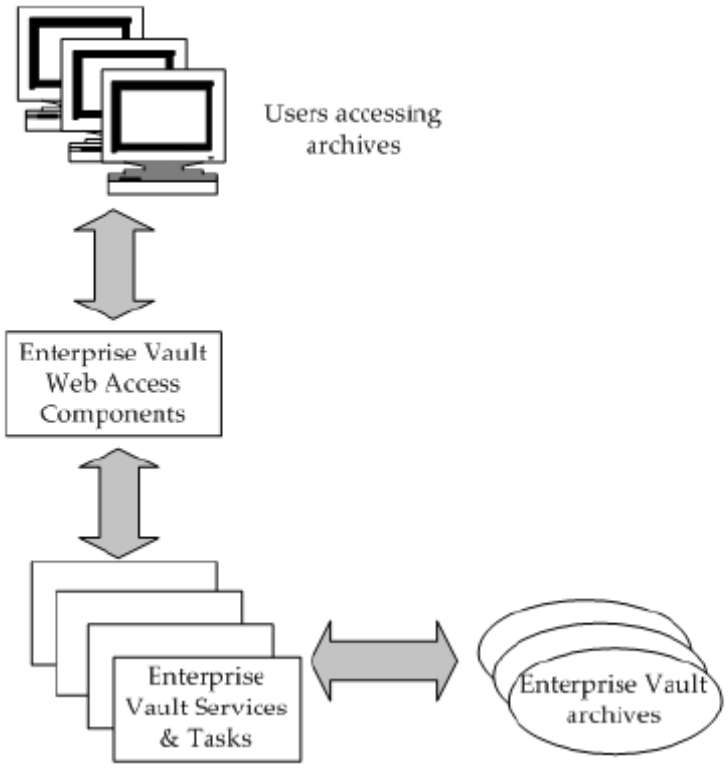

Figure 9) Process explaining how users can access stored items

2.3. Microsoft Exchange Server

Enterprise Vault configuration requires Exchange Server and SQL Server installations. Availability of Microsoft Exchange Server and SQL Servers is a requirement for Enterprise Vault archival configuration. If the architecture includes Microsoft Exchange Server on NetApp storage system, this paper recommends using SnapManager for Exchange to manage Exchange data. Similarly, SnapManager for SQL from NetApp enables the SQL Server database backup and recovery in an efficient way.

This paper recommends configuring Microsoft SQL Server on a separate Windows Server and not on the same Exchange Server. For a smaller environment and demonstration setups, installing SQL Server on the Enterprise Vault Server works fine.

2.4. NetApp Storage Systems

Enterprise Vault requires either local disks or virtual local disks for installing the SQL Server, Enterprise Vault, and Microsoft Exchange Server. Either SAN or IP-based SAN accomplishes the requirement. The necessary software and hardware configuration topics are discussed in earlier sections. For details, refer to NetApp support Web site. In our test setup, we used a FAS900 series storage system to configure local disks on both Exchange Server and Enterprise Vault Server. For archival destination, we used a FAS3050 cluster configuration and a near-line storage system R200 to migrate the items after a specified period.

3. Configuration

Enterprise Vault requires storage system be presented with NTFS file system configuration. NTFS volume, network share, and NetApp SnapLock enabled volume meet this requirement. Data may be migrated to secondary or tertiary locations depending upon the site policies. To install the Enterprise Vault components, Enterprise Vault configuration requires the availability of vault directory database.

3.1. Operating System Information

Enterprise Vault is a Windows based application. Enterprise Vault supports Windows 2003, Windows 2000 with SP3, and Windows 2000 Advanced Server with SP3 platforms. On our test setup, we used two Windows 2003 SP1 Servers, one for installing Microsoft Exchange 2003 Server and the other one for installing Enterprise Vault Server and SQL Server 2005 products.

Enterprise Vault requires Data ONTAP 7.0 or later releases supporting Enterprise Vault features. This includes the ability to remove the retention expired items from SnapLock volumes. Enterprise Vault configuration requires Microsoft Exchange 2003 or Exchange 2000 and SQL Server 2005 or SQL Server 2000. Note that earlier releases of Data ONTAP support Enterprise Vault 5.0 SP3 and later.

3.2. Enterprise Vault Configuration Information

It is required to install and configure TCP/IP on the Windows machine. This computer should have an Internet Protocol (IP) address registered with the domain name system (DNS). For performance reasons, this paper recommends a minimum of 2GB of main memory. It is also important to have access to SQL Server to Enterprise Vault Server prior to the software installation phase.

By default, IIS service on Windows 2003 prevents a file larger than 4MB from being downloaded. To enable downloading files larger than 4MB, open the IIS manager and change the “AspBufferingLimit” parameter. It is also important to understand the Enterprise Vault components configuration as a postinstallation task. Enterprise Vault configuration involves the following:

- Vault directory database – SQL Server database
- Vault store databases – required by SQL Server; storage space to grow dynamically
- Vault stores - required on the storage service computer
- The indexes - required for indexing services
- Shopping baskets – required on shopping service computer

3.3. The Vault Service Account

Enterprise Vault uses the vault service account to access the Windows Server operating system. Enterprise Vault services are Windows services. All Enterprise Vault computers share a vault service account (VSA). This account must be a member of Active Directory domain if Exchange Server is used.

The vault site alias is a DNS entry for the Enterprise Vault site. Each Enterprise Vault site should have a vault site alias. If the DNS server is running Windows Server, you may use the administrator tool and create an alias for the computer where Enterprise Vault is installed. If a UNIX® server used as a DNS server, a DNS alias is created by entering CNAME parameter. Consult the system administrator to complete this task as the administrator has the necessary expertise and privileges.

3.4. SnapDrive Software Installation and Configuration

SnapDrive tool eases storage management on Windows Server. It integrates with Microsoft Windows management console utility. Using this tool, configure the required local drives and complete the storage configuration as needed. Section 2.1.1 described the procedure to install SnapDrive software.

3.5. Microsoft SQL Server Configuration

Enterprise Vault requires Microsoft SQL Server installed and configured properly. NetApp storage system's virtual local disks configured with SnapDrive support SQL Server. Section 2.1.3 described the details about Microsoft SQL Server installation.

4. Installation

This section discusses the procedure to install and configure Enterprise Vault Server. Knowledge of Windows operating system administrator tasks, SQL Server, Microsoft Outlook, Internet Information Services, and archival hardware and software tasks are a prerequisite to complete the installation. Additional product knowledge such as Domino and SharePoint portal may be required. In this section, we cover the topics about preinstallation tasks, Enterprise Vault Server installation, and postinstallation configurations.

4.1. Preinstallation Checklist

It is necessary to complete the operating system and storage requirements prior to installing the software. Enterprise Vault 6.0 supports the following operating systems:

- Windows Server 2003 Standard Edition or Enterprise Edition
- Windows 2000 Server, Advanced Server and Datacenter Server
- Administration console, user extensions, and Exchange forms may be installed on Windows XP or Windows 2000 Professional Servers.

Enterprise Vault installation requires steps to be done in the following order for successful configuration:

1. Installation of Windows Server, necessary service pack
2. Recommended Windows hot fixes, listed in Appendix A
3. Outlook 2003 and CDO components
4. SQL Server 2000 or 2005
5. Available Exchange Server 2000 or 2003
6. Exchange System Manager
7. MSXML - if not already installed
8. MDAC – if not already installed
9. .NET framework – if not already installed
10. Lotus Note Client – if Domino server configuration is used
11. IIS with Active Server Pages – include SMTP, NNTP services

12. MSMQ - if not already installed
13. User extensions on user's computer to be able to archive items from a mailbox
14. Other components configuration such as Microsoft Sharepoint Server

4.2. Preinstallation Tasks

At this time, we assume the preinstallation requirements mentioned in earlier sections are completed. For completeness, here is a review with a brief checklist related to preinstallation tasks.

1. Vault service account.
2. Assigning Microsoft Exchange Server permission – vault service account must have access to Exchange mailboxes.
3. Create a SQL login for vault service account using SQL Enterprise Manager. This is a requirement if the mixed mode authentication mode used while creating the database.
4. Vault site alias – use DNS manager to create an alias. If the DNS server is UNIX based, you may configure DNS alias for the Enterprise Vault Server by creating a CNAME entry.

4.3. Installing Enterprise Vault

This section describes the steps involved with installing Enterprise Vault Server. Preparing the Windows Servers with appropriate operating system and all required hot fixes is the basic step in this stage. Installing SQL Server on a dedicated server may improve performance. On our setup, we installed both Enterprise Vault Server and SQL Server on the same system.

4.3.1. Enterprise Vault Install

In our test setup, it was a fresh install of Enterprise Vault software. In our test setup, we checked the availability of Microsoft Exchange Server and SQL Server before attempting to install Enterprise Vault Server. The following Enterprise Vault components were installed. The installation wizard will install the administration console on the Enterprise Vault Server as shown in the following figure.

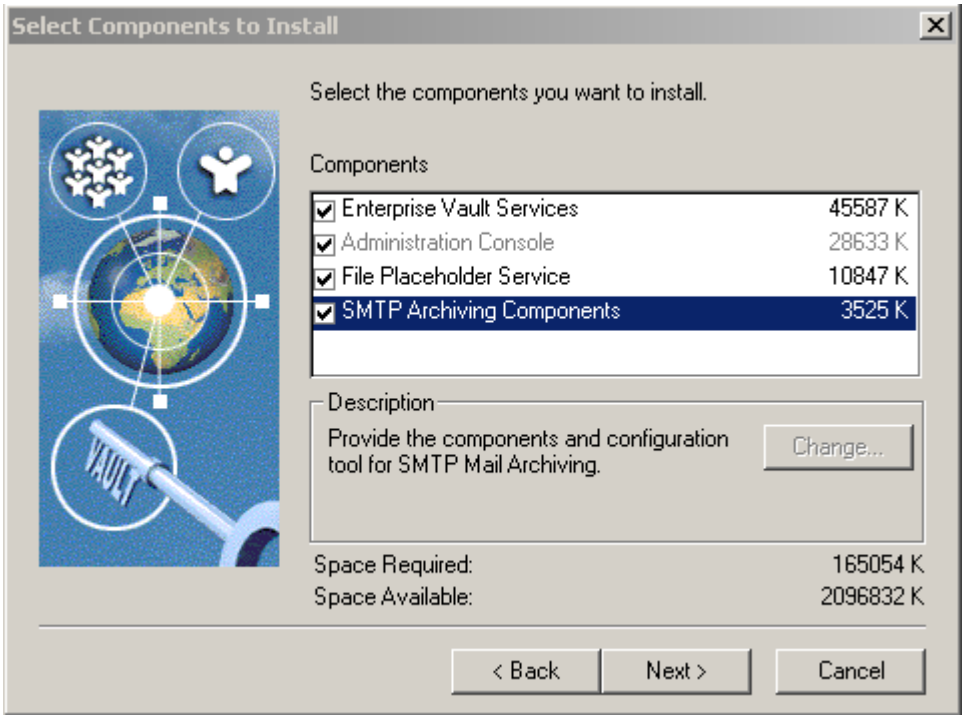

Figure 10) Enterprise Vault Components Installed

After selecting the Enterprise Vault components to install, the installation wizard prompts to enter the installation folder. In our test setup, we selected a SnapDrive created virtual local drive path, F:\EV, for installing Enterprise Vault Server.

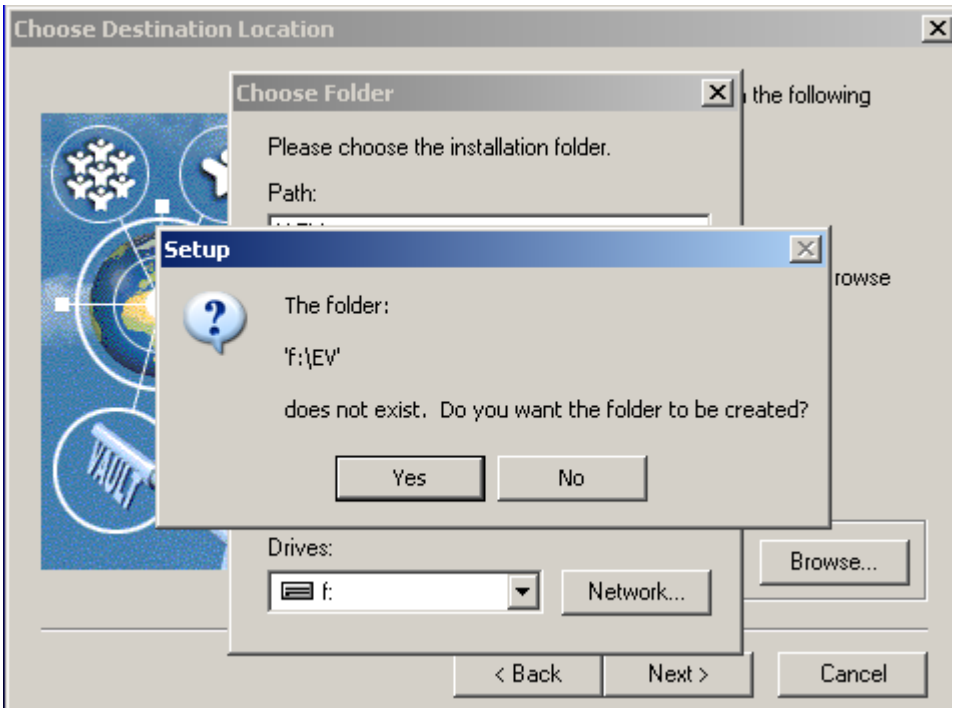

Figure 11) Choosing Enterprise Vault Destination Location

If the installation folder does not exist, it creates a new one. Installation utility continues with the installation after user agrees to the software license agreement. Next, select program folder for setup to add icons to a particular program folder. Observe the installation progress as shown in the following figure.

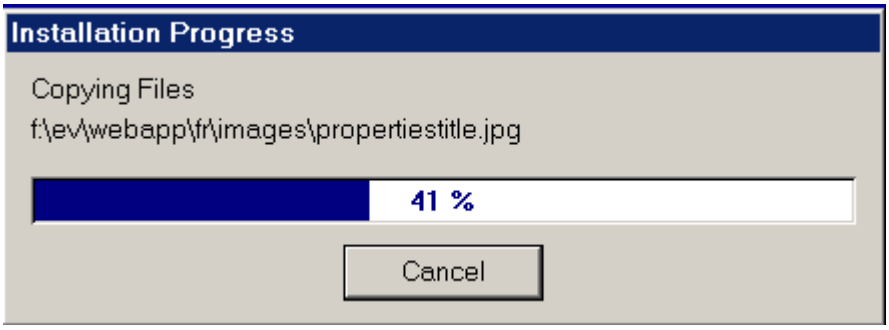

Figure 12) Monitoring Enterprise Vault Installation Progress

After copying the necessary files, it provides the installation summary with the information. This information includes the Enterprise Vault installation directory, program folder, Web alias, and the selected components for installation. Installation summary in our test setup is as shown in the following figure.

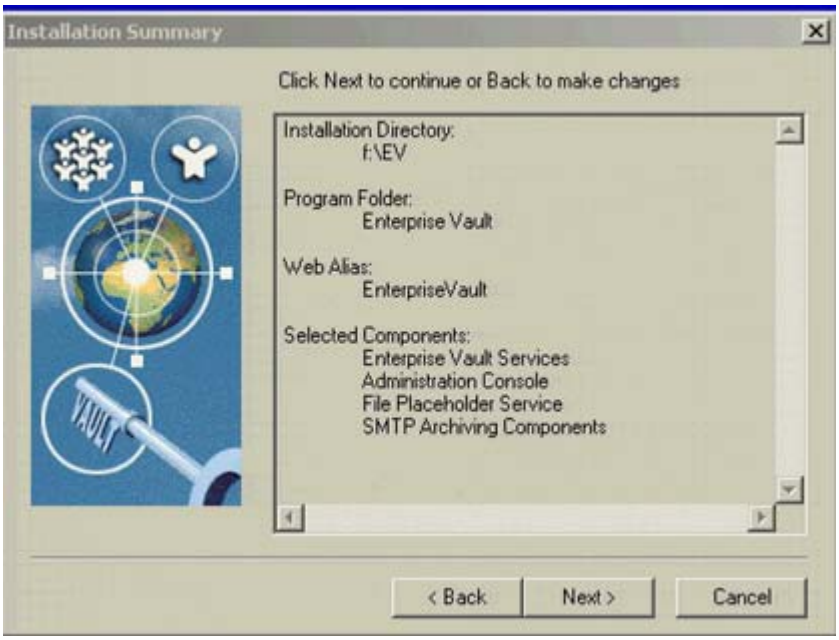

Figure 13) Display of Enterprise Vault Installation summary

Installation setup continues to install Enterprise Vault and may require restarting the Windows Server. After restarting the Windows Server, certain postinstallation tasks must be completed before being able to using the Enterprise Vault Server. On our setup, we restarted the computer and observed the following Enterprise Vault icons in the program folder.

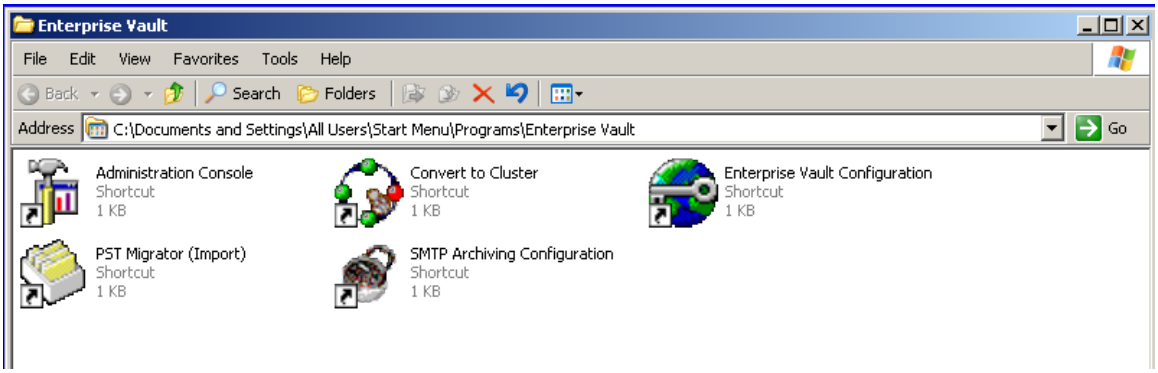

Figure 14) Program Files for Enterprise Vault

4.3.2. Postinstallation Tasks

Preparing the system and completing the postinstallation tasks are more significant steps than installing the Enterprise Vault software. Observe that the Enterprise Vault installation takes significantly less time compared to completing the preinstallation activities. In order to use Enterprise Vault, certain postinstallation and configuration tasks are to be completed. This section lists the steps involved with the postinstallation activities.

This section explains the procedure to configure for Web access application and distribute the Microsoft Exchange Server forms and the procedure to set up the administration console. Enterprise Vault installation utility sets the basic authentication method and integrated Windows authentication. The default authentication is configured by changing the IIS properties on the IIS computer. This task requires Windows administrator privilege. To set up the default authentication, follow these steps and continue to finish the task.

1. Start administrative tools and IIS.
2. Configure the Enterprise Vault Web access computer.
3. Default Web Site → Properties → Directory Security → Anonymous access and authentication.
4. Clear the checkbox and select Basic Authentication.
5. Integrated Windows Authentication → OK → Virtual Directory –Configuration.
6. Increase ASP Script Timeout → OK.

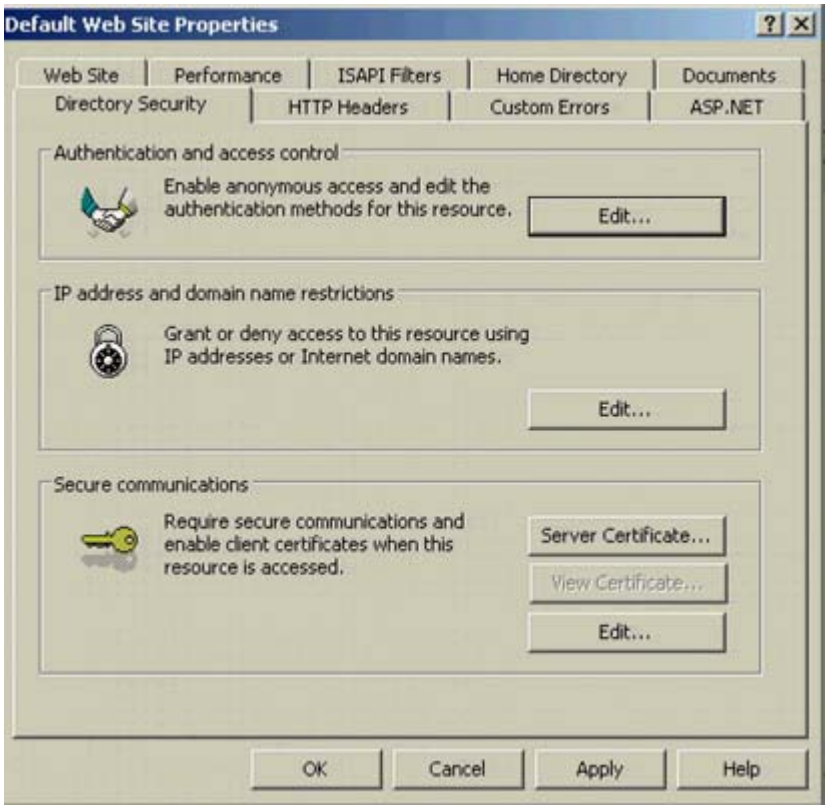

Figure 15) Default Web Site Properties

After setting Windows authentication security mode, complete the Microsoft Exchange tasks for Enterprise Vault. On our system, we created a folder in the Organizations Forms library with access provided to all Microsoft Exchange users. To create a folder, log in to the Exchange Server and open the Exchange System Manager. On our test setup, we followed these steps to create a folder.

1. Exchange System Manager → Organization and expand administrative Group → Expand Folders.
2. Expand the public folders (or right-click EFORMS REGISTRY) on the right-hand pane.
3. Complete Properties window.
4. Verify language that is appropriate and click OK (required if a different language to be set).
5. On Properties screen, click Permissions → client Permissions → Add.
6. Select the user name for the account for the ownership of forms (usually Enterprise Vault service account).
7. Roles → Owner → OK → OK → Close Exchange System Manager.

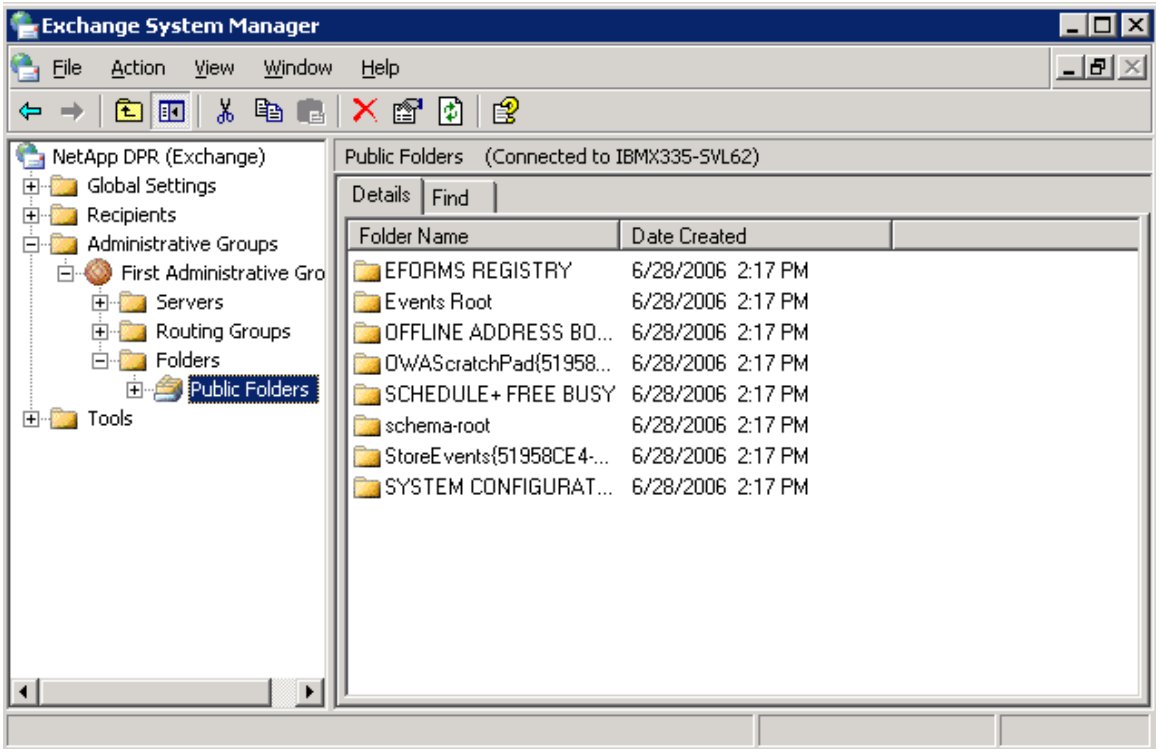

Figure 16) Exchange System Manager to Create a Folder

After creating the folder and setting the form's ownership, install the Exchange forms and customize user's desktop. In order to set a different font such as Japanese fonts, use the Enterprise Vault administration console.

4.3.3. Enterprise Vault Configuration

Start the Enterprise Vault configuration wizard. Create a new vault directory on this computer. If you have an existing vault directory, select that vault directory. On our setup, we configured to create a new vault directory and provided the user authentication information for Enterprise Vault services. We provided the details of SQL Server that were used for vault directory. In our case, SQL Server entry was "IBMX335-SVL61". The configuration wizard proceeded after granting the necessary vault service account user permissions as shown below.

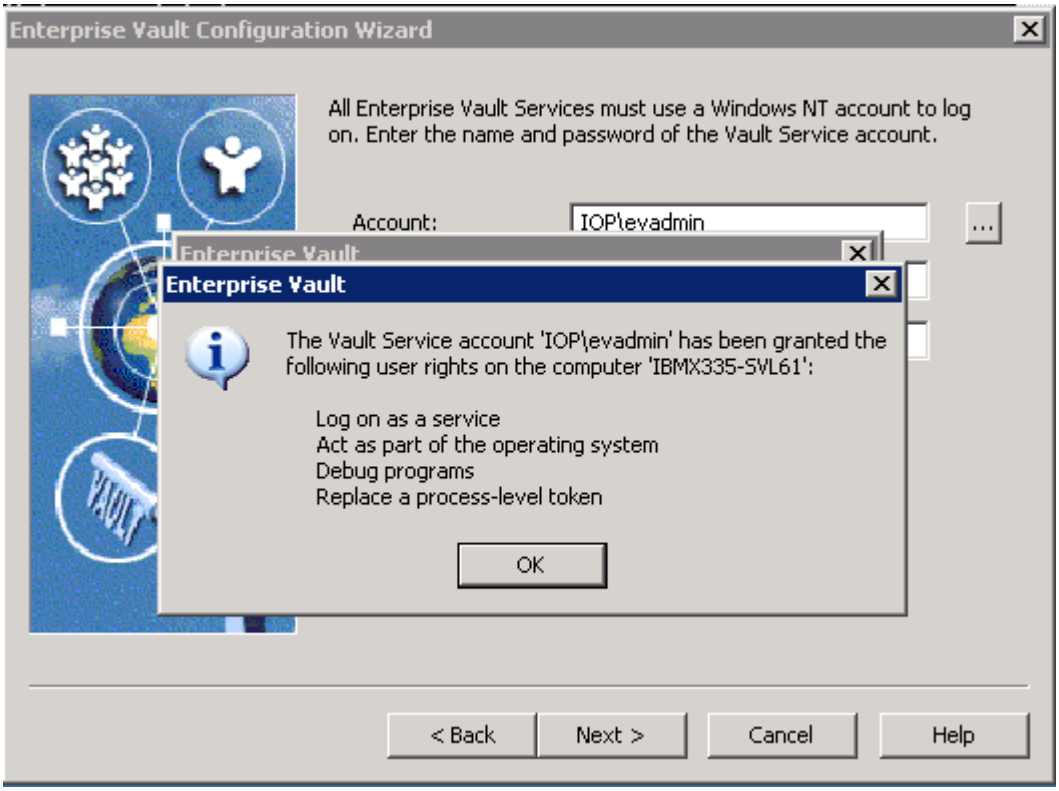

Figure 17) Enterprise Vault Service Account User Permissions

After granting the necessary user rights to the vault service account, vault directory database and transaction log locations information is required. In our test setup, we provided the virtual disk path (storage area network) created by SnapDrive storage management tool, as shown below. Locations for writing the database and transaction logs selected were based on a defined policy. These locations could be on the same or a separate disk path.

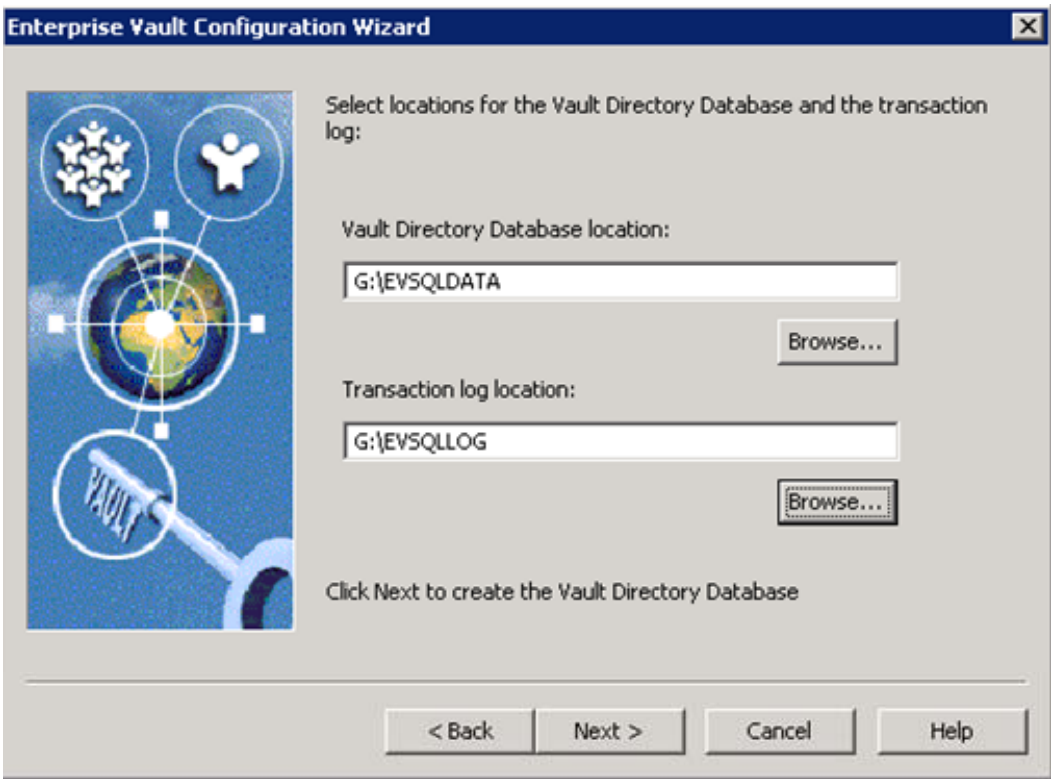

Figure 18) Enterprise Vault Directory Database and Transaction Log Locations

Before creating a new vault site, verify that a DNS alias for the new vault site is available. Create a DNS alias on the DNS server. This operation requires administrator privilege. Use the Windows administration tool to complete the operation. Giving a meaningful name for DNS alias would help. On our test setup, we created a DNS alias as ‘vaultserver’ as the Windows Server was running the Enterprise Vault application. Entering fully qualified name entry instead of DNS alias will display informing the advantage of using DNS alias. During this process, it detects the Enterprise Vault services installed on the Enterprise Vault Server. On our setup, this task displayed the following output with a new vault site name of “dprvaultsite”.

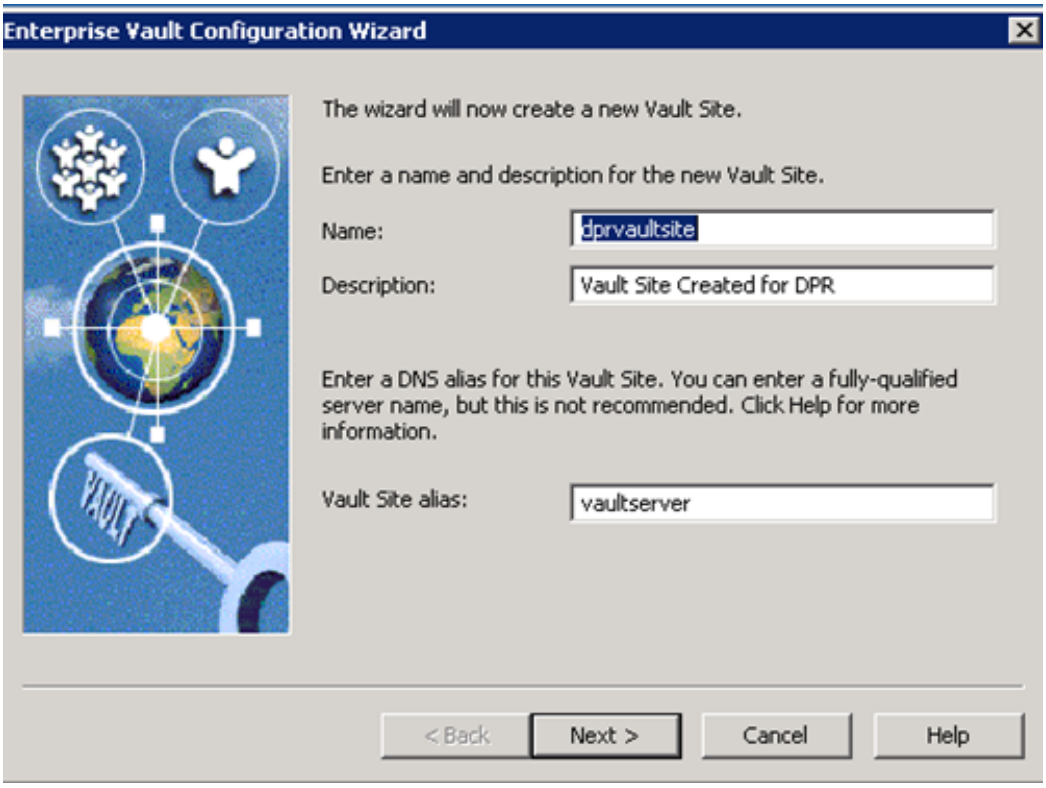

Figure 19) Creating a New Vault Site

After creating a new vault site, services installed, and the default, Enterprise Vault services for the computer are recognized. Using the configuration utility, new services are added at this time or later. It also lists the default Indexing service for the new archives and shopping services location information. It is important to verify storage locations for the services added such as indexing and shopping. While creating a new vault site, verify the settings for storage service on the computer. Then configure the appropriate numbers for archive and restore process. On our setup, we set the archive processes to five and restore process to one. On our test setup, we selected the SnapDrive configured local disks as shown below.

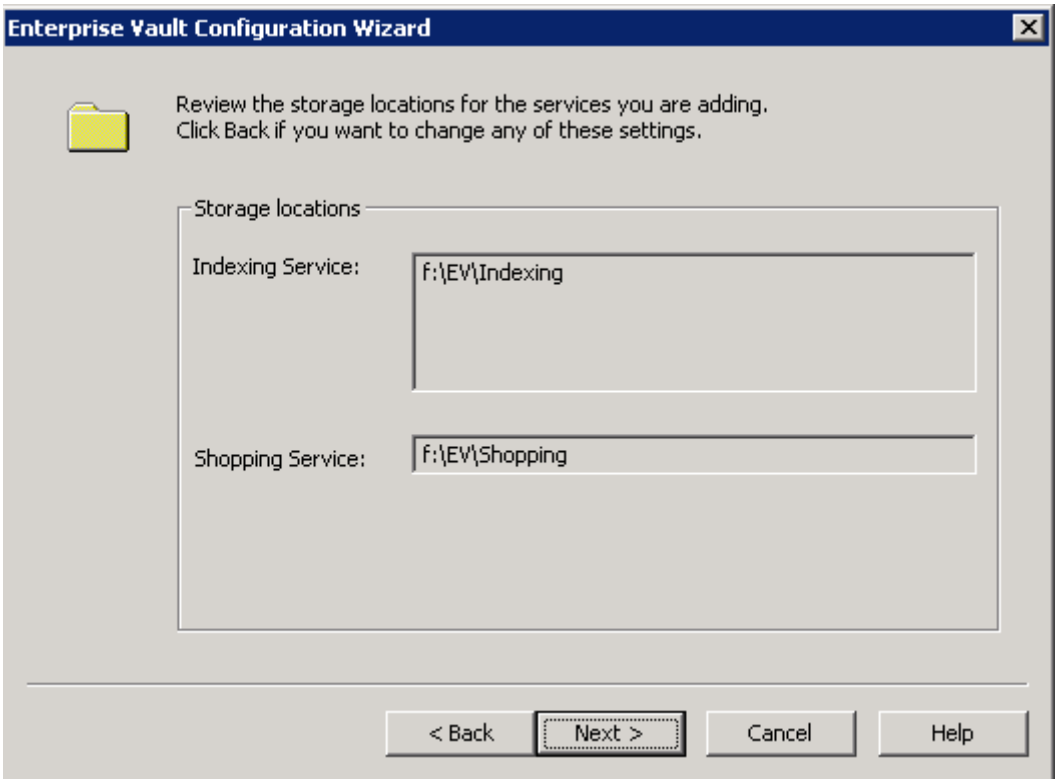

Figure 20) Storage Locations for the Services

Once the Enterprise Vault Server is configured, the installation wizard proceeds to start the Enterprise Vault services and data creation. In our setup, we checked the Enterprise Vault services status to verify the services enabled and started. Following figure displays the status of these tasks on setup.

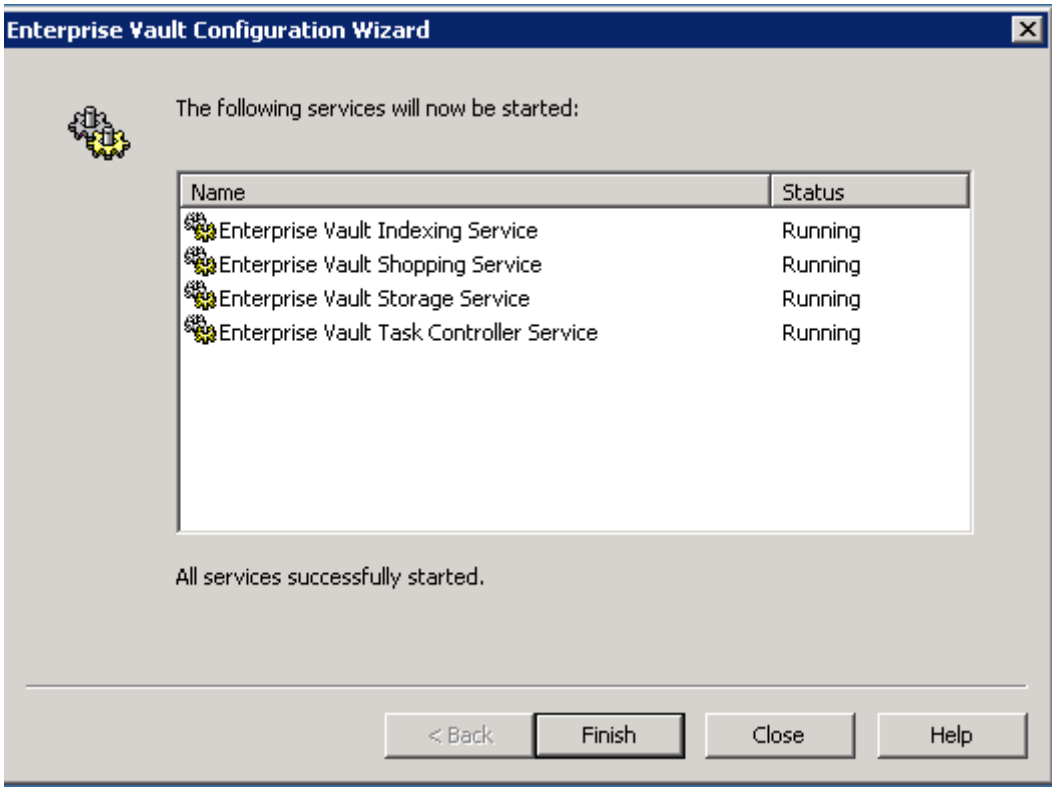

Figure 21) Status of Enterprise Vault Services

Now verify the vault directory is visible on the administration console. The next phase is to create the Exchange tasks for each Enterprise Vault, such as archiving tasks for Exchange mailbox tasks, and so on, as shown below. Enterprise Vault recognizes that user account and lists the user name and Exchange Server information as shown below.

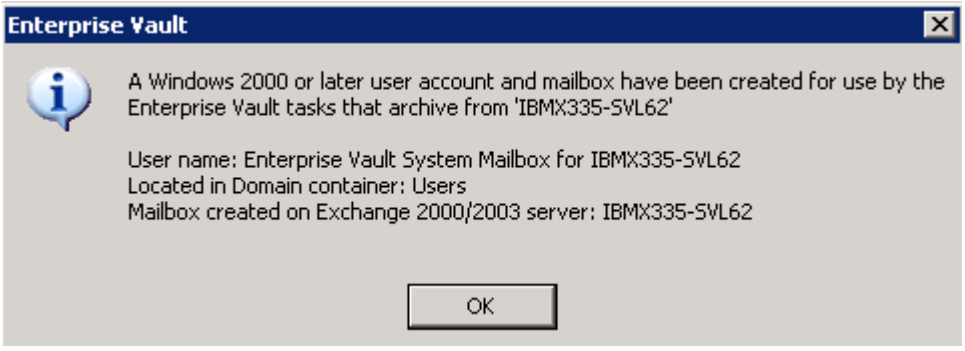

Figure 22) Mailbox Information

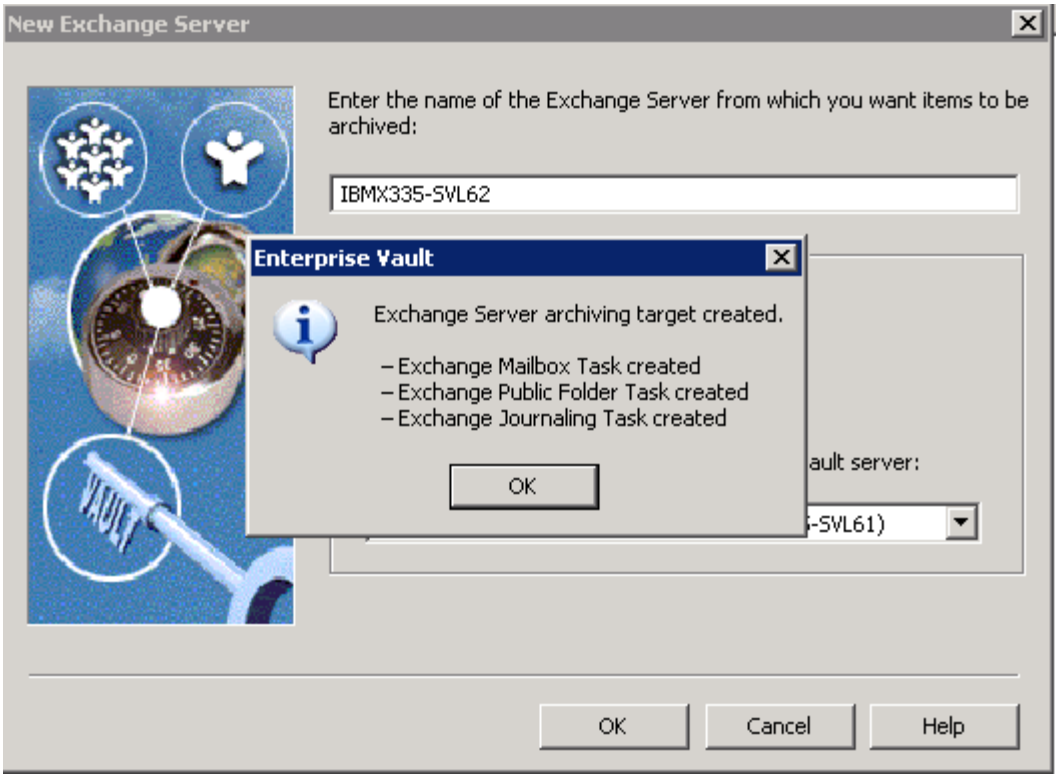

Figure 23) Exchange Server Archiving Target

4.3.3.1. Configuring Enterprise Vault for Archiving

A vault store is used to define the storage allocated to the partitions and archives. Each vault store uses its own databases to hold the details of the archives within the vault store. A new partition on the vault store allows the items to be archived. At any time, only one vault store partition is opened for archiving. Create a new vault store partition to set up archival configuration.

4.3.3.2. Configuring NetApp Storage System for Archival Destination

In our test setup, we used a SAN configuration from NetApp to install Microsoft Exchange Server 2003, Microsoft SQL Server, and Enterprise Vault products. Local disks were configured using NetApp SnapDrive storage management software. Once the storage configuration task is completed, configure the Enterprise Vault archival destination and migration location. On our test setup, we configured the Enterprise Vault archival destination and migration location on NetApp storage systems. In our test setup, we used FAS3050C storage system for archival and R200 for migration services. Using such configurations, specified items migrated from the primary storage to the secondary storage based on the archival policy set within Enterprise Vault. At this time, verify that the NetApp storage system(s) are configured and storage path available on the operating system servers.

On our test setup, NetApp storage system status and volume details were checked before configuring Enterprise Vault. Remember to enable the NetApp product licenses such as CIFS, iSCSI, and FCP. Based on your company policy, configure the storage systems. An example of the above is to configure CIFS setup and have necessary CIFS shares available if required. In a SAN storage environment, configure the LUNs and related virtual disks. SnapDrive software tool provides easier storage management capabilities. Network share configuration may offer some advantages in an Enterprise Vault environment. Configure additional NetApp storage systems, if needed.

On our test setup, we decided to follow the steps listed below:

Create the appropriate Volume size using FlexVol™ and RAID-DP™ configuration:

1. Create the qtree.
2. Create CIFS shares.
3. Configured the network security.
4. Mapped the network shares on the Enterprise Vault computer.
5. Verified that UNC paths are accessible from the computer. We used the computer management tool, then selected 'connect to another computer', and entered the NetApp storage system name (or IP address).

4.3.3.3. Creating New Vault

As mentioned in Section 4.3.3.2, verify that the necessary storage configurations are completed and NetApp storage systems available for creating a new vault store. Continuing the Enterprise Vault configuration wizard, select the computer on which the storage service the new vault store used. Following figure displays storage services configuration information.

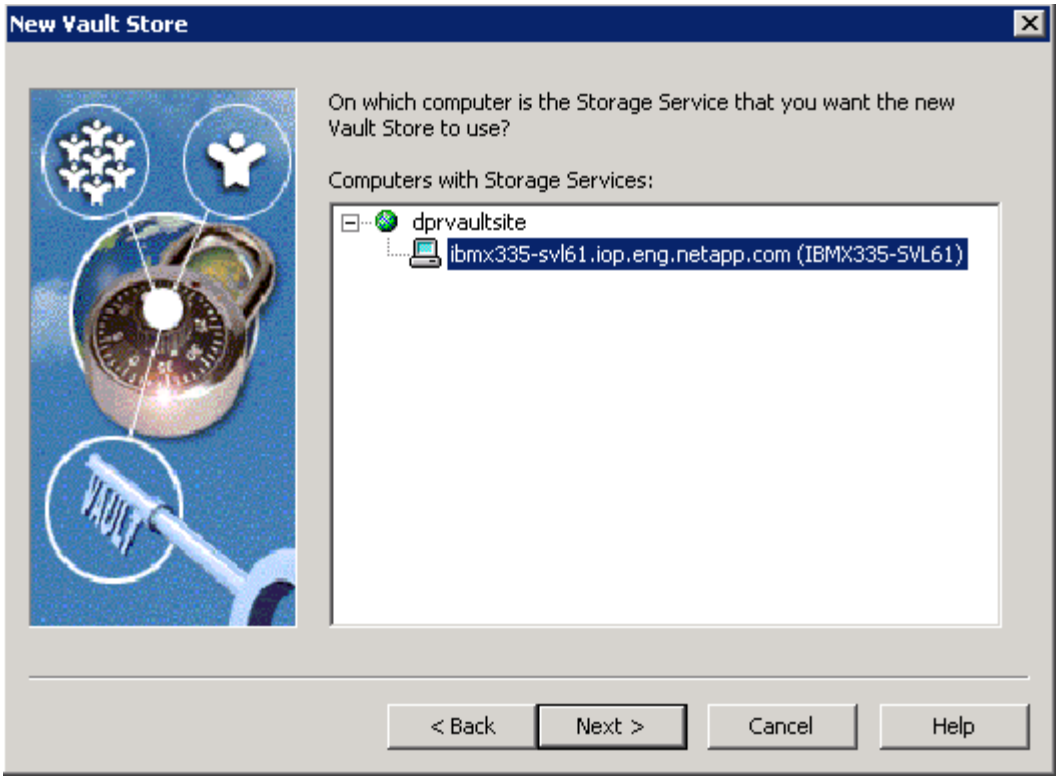

Figure 24) New Vault Store Configuration – Selecting the Computer for Vault Store Partition

A new vault store requires a name, and we recommend providing a meaningful name to help in understanding the archival configuration. A vault store database requires the SQL Server information, and in our setup, we provided the SQL Server location (IBMX335-SVL61).

A vault store defines the storage allocated to the partitions. Enter the vault store name and description for the new vault store. Provide the SQL Server information for using the vault store database. New vault store requires a SQL database location for database and transaction logs. On our setup, we selected the SnapDrive created local disk path as shown below.

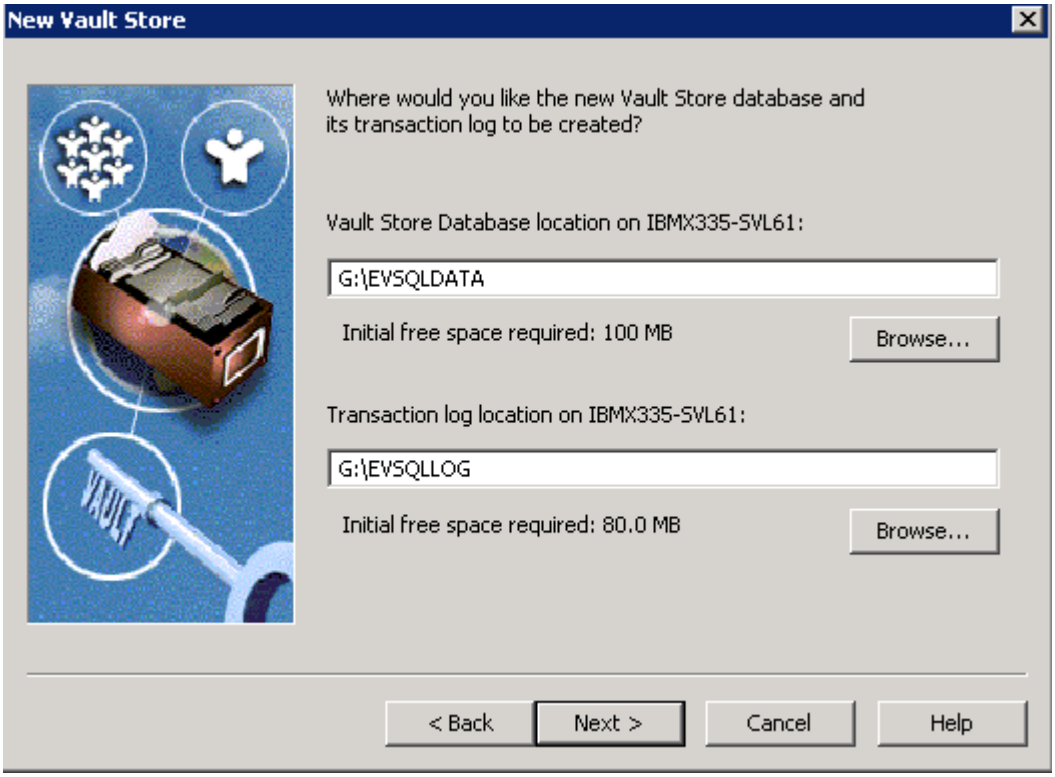

Figure 25) New Vault Store database Locations – SnapDrive Created Local Disk

Enterprise Vault has a feature to provide additional safety for the content. In our test setup, we chose to remove the archived items from the primary after the backup is completed. Another option allows the contents of the archived items to never be deleted from the primary storage. Next, it will display the summary for creating a new vault store. On our test setup, this task created a new vault store as shown below.

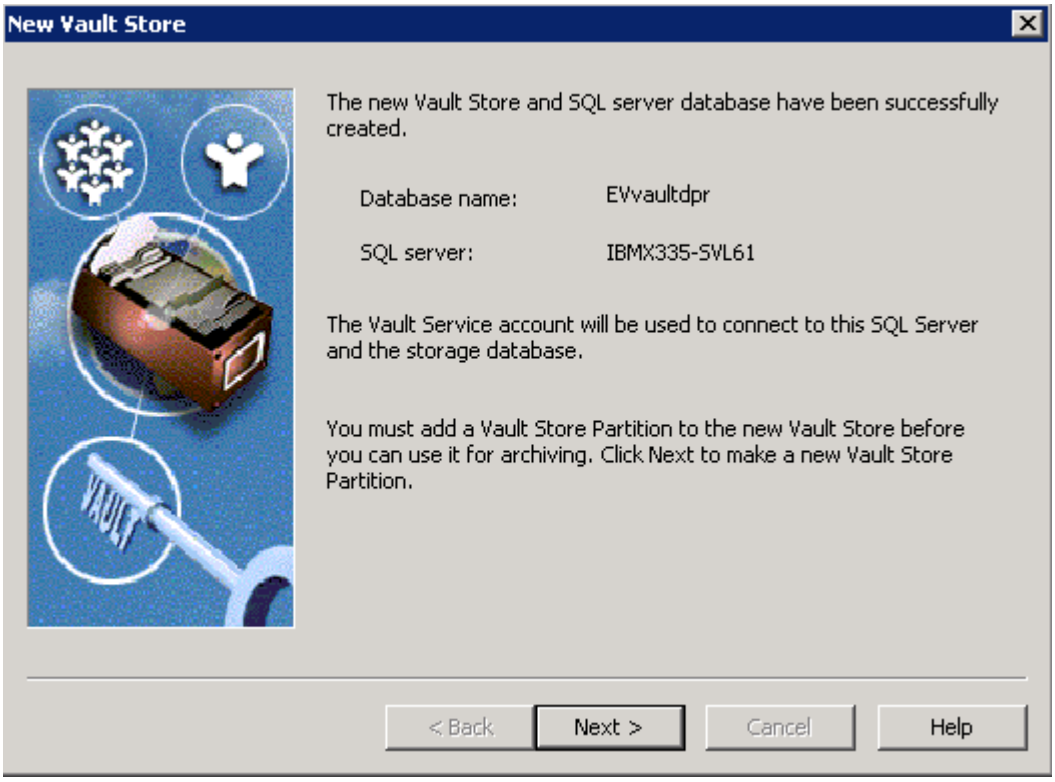

Figure 26) New Vault Created with Database Name EVvaultdpr

4.3.3.4. Creating a Vault Store Partition Using NetApp Storage System Destination Path

This paper assumes that the storage systems are configured and available at this time. Using the network share, map the appropriate NetApp storage system's volume(s). Use the Enterprise Vault administration console to start the new vault store partition create wizard. Only one partition should be opened at any given time. Provide the vault store partition name and description. The following figure shows new vault store partition name and description provided in our test setup.

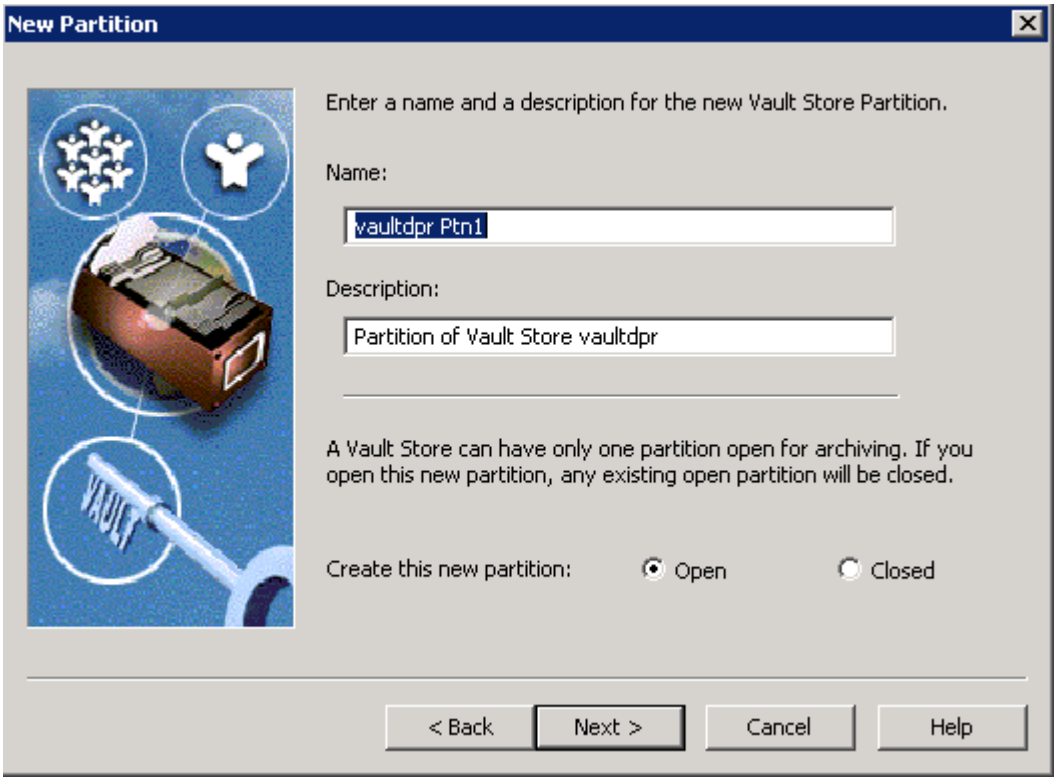

Figure 27) New Vault Store Partition

Continue with the creating new partition wizard and select the appropriate option for your storage system. If you select the NTFS system, NetApp will configure the volume as a network share or as virtual local disk (network shared drive). For compliance purposes, select NetApp SnapLock volume. Refer to the Configuring SnapLock with Enterprise Vault technical report, available on our Web site. We followed this procedure to create a new vault store partition before creating a new vault store partition:

1. Create the appropriate volumes on NetApp storage system (FAS3050C).
2. Create necessary qtree(s) (optional).
3. Create CIFS shares for the volume or the qtree.
4. Map the above CIFS share on the Enterprise Vault Server or on the administration console computer.
5. Example for mapping the network share mapped was \\fas3050c-svl34\vs3, where vs3 is name of CIFS share.
6. Create a folder at the root of the mapped drive. For example, we created a folder called ‘store’ on the mapped drive.

The following three figures demonstrate the procedure described above to create a new vault store partition. It is important to note that at least one directory must be present above the CIFS share point level. To meet this requirement, create a folder at the root of the share point. If you are planning to provide the Universal Naming Convention (UNC) path, verify that a folder exists at the share point level. This requirement is similar to network share environment. In our test setup, we selected NTFS volume for the mapped drive to specify the network path connectivity to the NetApp configured storage path. Following figure shows the selection of network configuration.

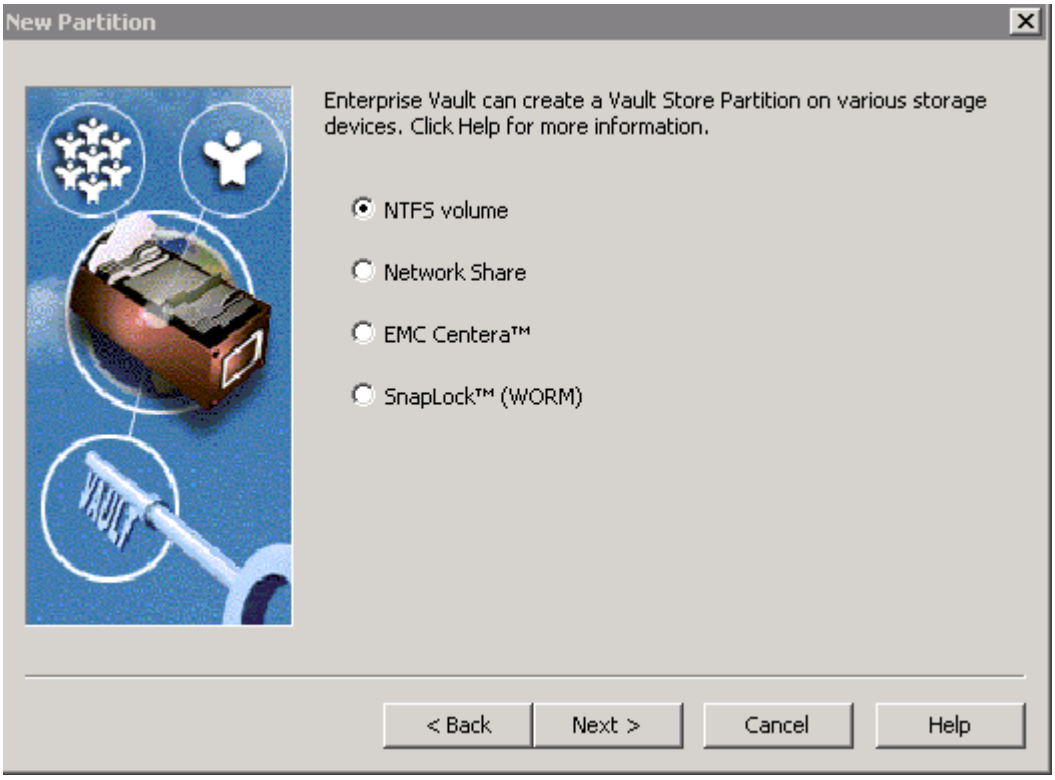

Figure 28) Vault Store Partition on NetApp Storage System

Select an NTFS volume for configuring the non-WORM data archival. For compliance data archival, select the SnapLock (WORM) storage configuration to create a new vault store partition. The SnapLock Configuration with Enterprise Vault technical report discusses the SnapLock and file system archival configuration.

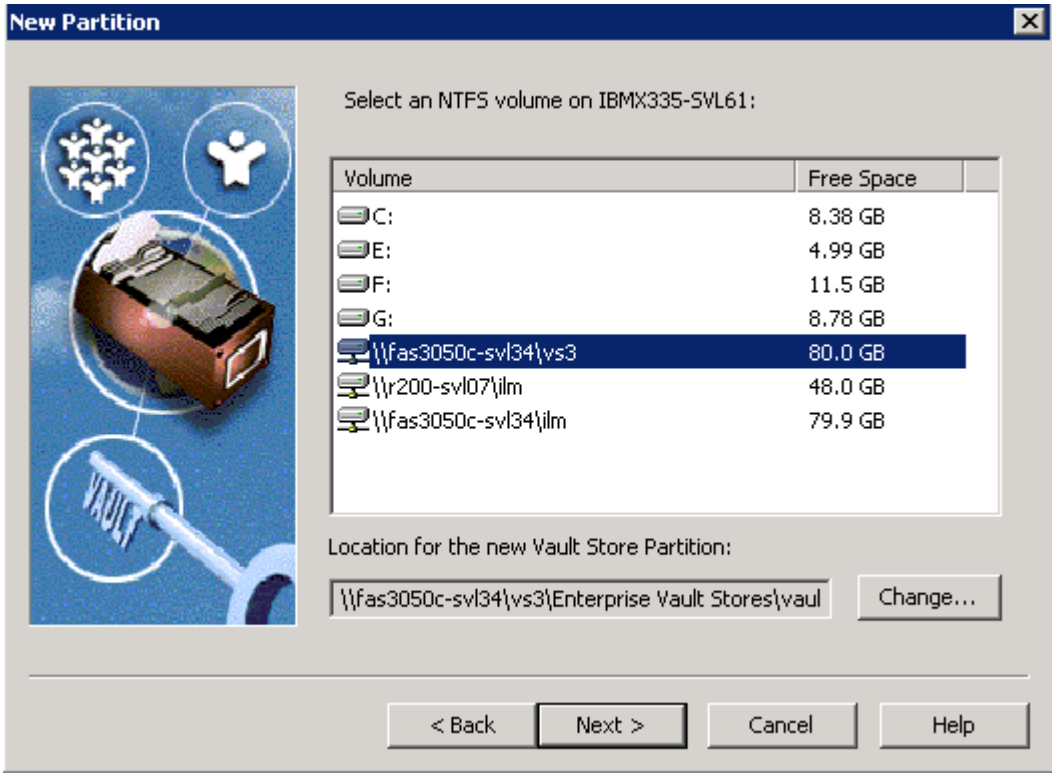

Figure 29) Storage Location for the New Vault Store Partition

The vault store partition requires the specified folder to be empty; select the folder path that meets this requirement, and then click OK.

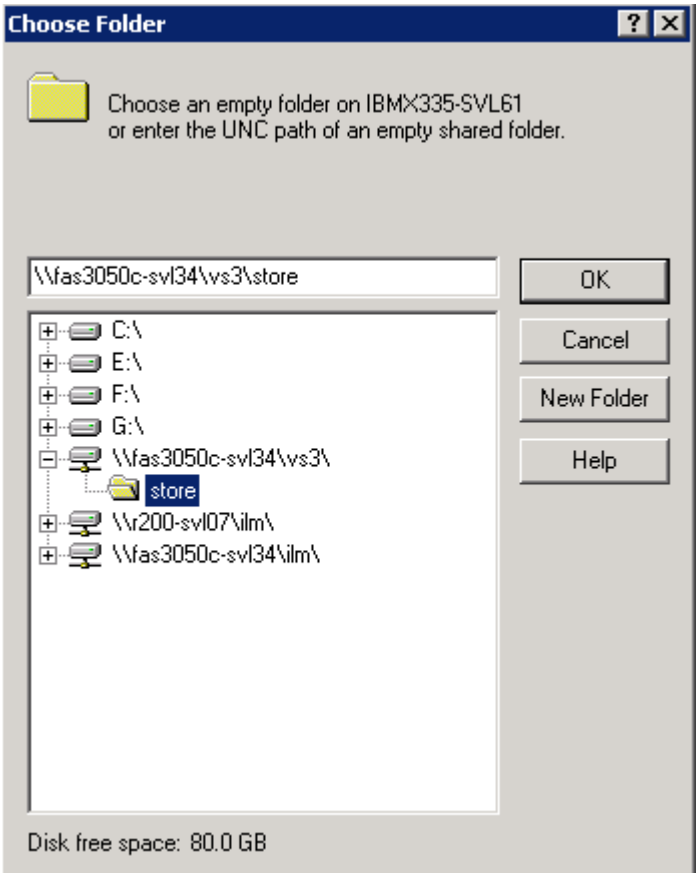

Figure 30) Selecting Vault Store Partition Storage Location

Following are the steps to complete the new vault store partition

1. Enterprise Vault can reduce space by archiving and migrating old files from the archives. Select your options.
2. Enterprise Vault can integrate with file collection software and choose if required.
3. Enterprise Vault can integrate with file migrator software. Choose the available software such as Enterprise Vault, Veritas® NDMP back, or none.
4. Select the daily file collection period. Choosing off-peak time may be an option for most customers.
5. Select the age of files at which they will be collected.
6. Choose if migrator service is needed, and again we have the same choices, including Enterprise Vault.
7. Specify the file age to be collected and option to remove collections from primary location.
8. Provide the secondary location using UNC path such as \\r200-svl07\ilm\store2.
9. After this, complete the vault store partition and verify that the new vault store partition is created.

ription	Status	Device Type	Collector Type	Migrator Type
tion of Vault Store vaultdpr	Closed	Network Share	Enterprise Vault	None
tion of Vault Store vaultdpr	Open	Network Share	Enterprise Vault	None
tion of Vault Store vaultdpr	Closed	Network Share	Enterprise Vault	Enterprise Va

Figure **31) Vault Store partitions for Vault Store vaultdpr after creating a closed Vault Store Partition**

5. Archival Setup

This section describes the procedure to set up to archive items from mailboxes. After completing archival setup tasks, Enterprise Vault will be ready for archiving the items. Section 4.3.3.3 described the procedure to create a new vault store, whereas section 4.3.3.4 explained the steps to create a new vault store partition. Vault store and vault store partition must exist before enabling the mailboxes for archiving. A vault store supports multiple vault store partitions. At any given time, only one vault store partition is active, and the remaining partitions are closed. This section discusses the procedure required to set up the Enterprise Vault archival.

5.1. Create Organizational Unit and Archive Task

Using the Enterprise Vault administration console, add an Exchange organizational unit, Exchange Server, and task controller service. Organizational unit consists of a mailbox and PST migration policies. Exchange organization allows selecting a default retention category for archiving such as business. Also, note that Enterprise Vault Server allows configuring a single Exchange task per Exchange Server. This means a single Enterprise Vault Server supports only one Exchange mailbox task. If your environment runs multiple Enterprise Vault Servers, an equal number Exchange Servers are required to set up the same number of Exchange mailbox tasks. Following is a screenshot of our setup while creating a new organizational unit.

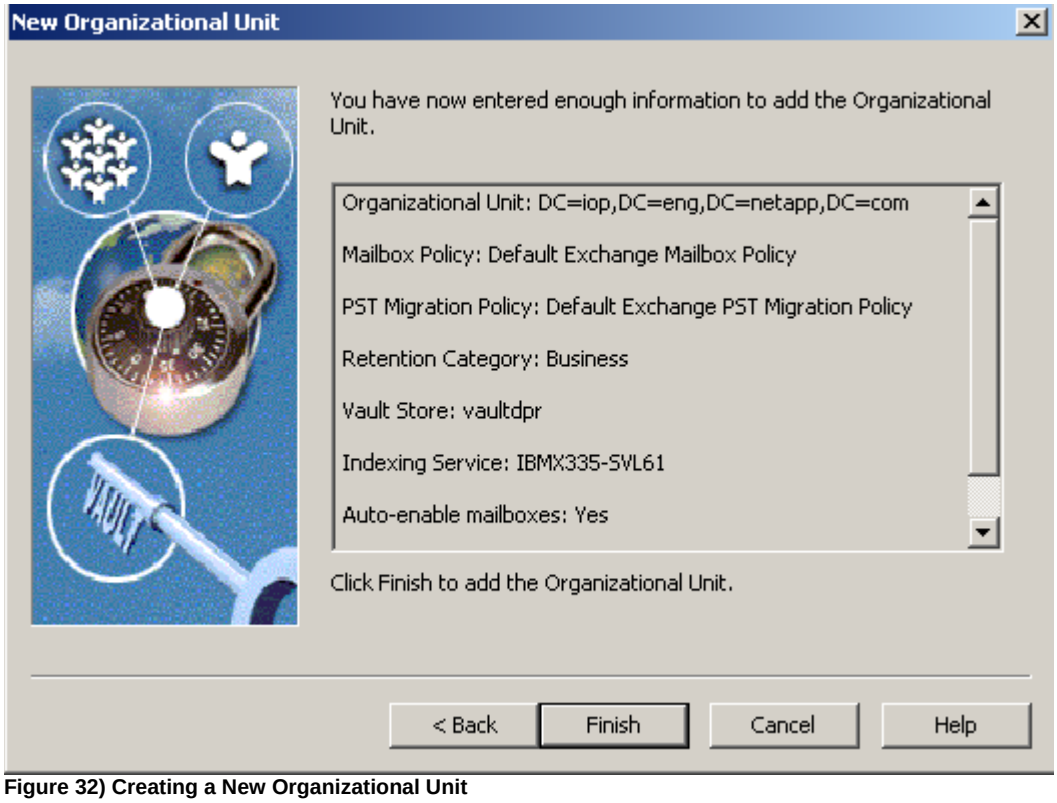

Figure 32) Creating a New Organizational Unit

Continue to add an archiving task using the administration console. A sample Exchange organizational unit is DC=pri,DC=dept,DC=company,DC=com for the domain pri.dept.company.com. By default, Enterprise Vault creates a few retention categories such as business. New retention categories can be created using Enterprise Vault administration console. In our setup, we created a new retention category called 'datacompliance' to archive the data to a SnapLock compliance storage location. When a mailbox is enabled for archiving, Enterprise Vault creates an archive in the vault store.

Use the Exchange task wizard to create new mailboxes. This task allows the Exchange Server to manage e-mail communication. Selected mailboxes require new archives created to use a vault store. Configure the archiving policy for this setup.

Here is the procedure to create an archiving task.

1. Expand the administration console until Enterprise Vault Servers container.
2. Expand Enterprise Vault Servers.
3. Expand the name of the computer to which an archiving task is to be added.
4. Right-click Tasks and create a new archiving task.
5. Complete the new archiving task wizard.

Now use the administration console to verify the site archiving settings. After creating an archive task we had the our setup shown below.

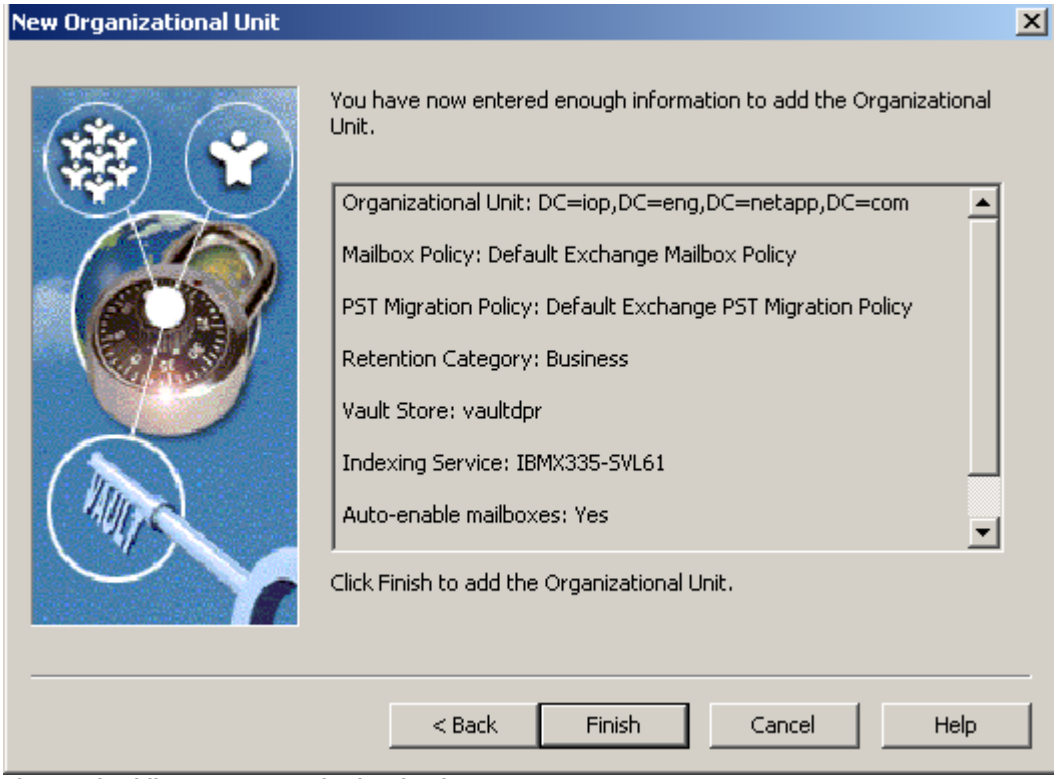

Figure 33) Adding a New Organizational Unit

Create a new public folder archive task using the administration console by specifying the vault store. This requires the Indexing service for the archive to be enabled. In our test setup, we created a new public folder archive task as shown below.

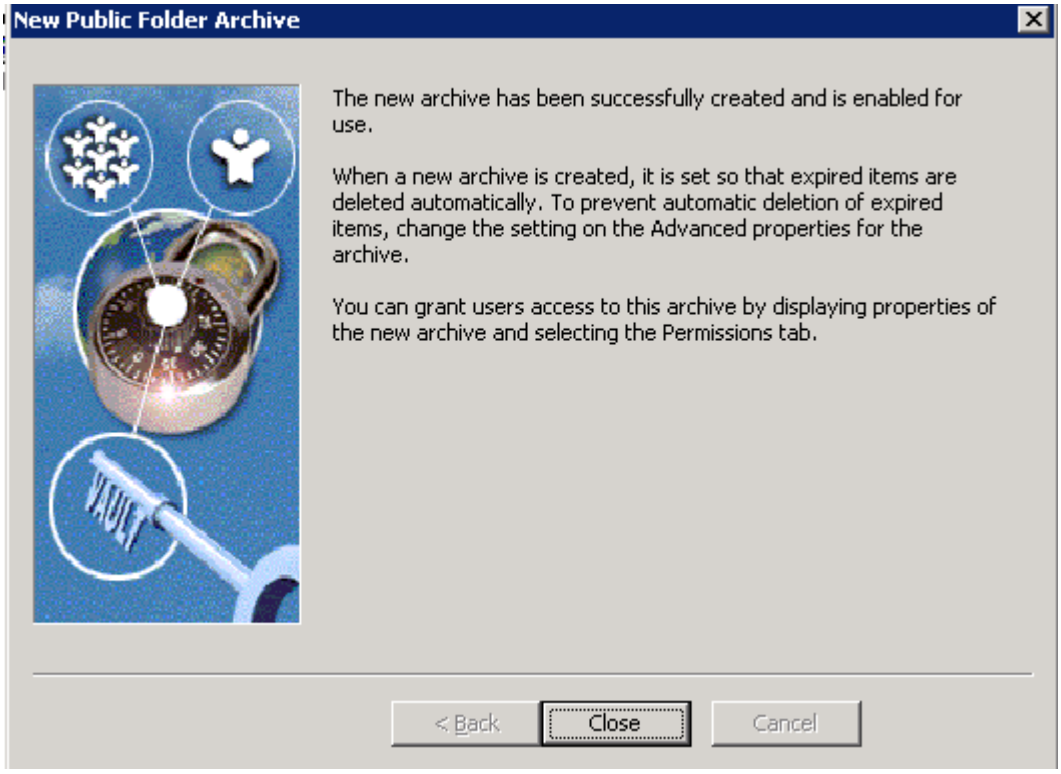

Figure 34) Creating a New Public Folder Archive Task

Create other archive tasks such as a journal task. The following figure lists the configured archive tasks created on our test setup.

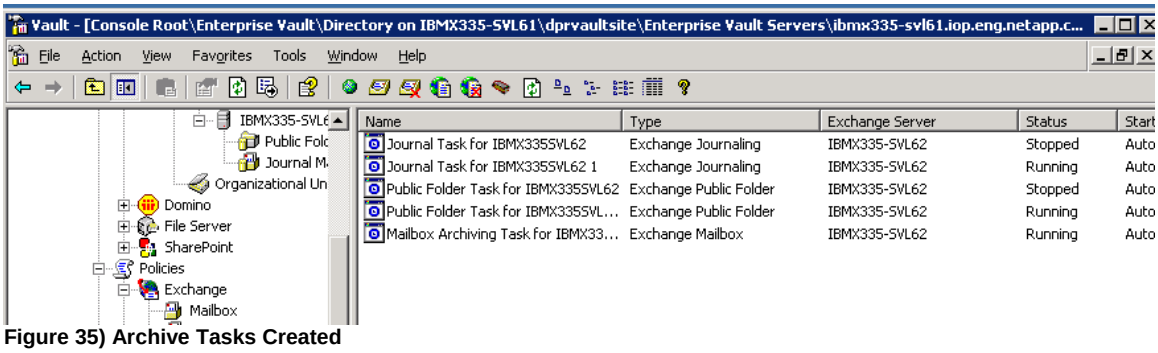

Figure 35) Archive Tasks Created

5.2. File System Archiving

Enterprise Vault Server is designed to archive items from Exchange Server mailboxes and public folders. In addition to these tasks, it supports archiving file system, mailbox journaling archival of Lotus Notes, and Microsoft SharePoint portal data. This section briefly discusses the procedure to configure a file system archival component. Enterprise Vault supports file archiving with two product offerings. The basic version simply archives the data from the file system into Enterprise Vault according to a set policy. The advanced version supports indexing the content in addition to the ability to move the content into the Enterprise Vault system. An Enterprise Vault site computer runs one or more Enterprise Vault services by sharing the same configuration.

It is important to understand all the configuration possibilities while deploying Enterprise Vault Server. Some possible Enterprise Vault configurations and installation strategies are listed below. For additional information, refer to Enterprise Vault product documentation available on the Symantec Web site.

- One Enterprise Vault site for Each Exchange Server site
- One Enterprise Vault site for file system archival
- One Enterprise Vault site for each Exchange Server site

Other configuration possibilities include several Enterprise Vault sites for one Exchange Server or vice versa. This configuration may have some consequences. An example is the ability to configure Exchange mailbox task settings. There is a limit of one mailbox task setting per Exchange Server. However, Microsoft Exchange configuration is optional. Exchange Server configuration is required in an Exchange e-mail environment.

This section discusses the procedure to configure the file system archival (FSA) component of Enterprise Vault on NetApp storage system(s). This paper recommends analyzing the file system archival requirement such as the server and storage requirements. The file placeholder service component of Enterprise Vault supports file system archival. Refer to Figure 13 for installing the file system archival component. Verify that the necessary network connectivity is established between the operating system server and NetApp storage systems. For file system archiving, a network connectivity using CIFS protocol configuration is supported. Configuring the SnapDrive enabled local disk is also supported for file system archiving. This means that archiving to network storage or local storage is a supported configuration. Enterprise Vault requires the storage system to present its storage as an NTFS file system. Since the file system archival works at the file level, a network configuration is ideal for archiving file system data.

This section provides the steps to set up file system archiving.

1. Install file placeholder service.
    a. Select *File Placeholder Service* component from the install wizard.
2. Configure the placeholder service.
    a. Verify Enterprise Vault has file system archiving license enabled.
    b. Program files → Enterprise Vault → file system archiving configuration.
    c. Introduction --> vault service account details.
    d. Verify that the advanced user rights are granted.
    e. Setup file permissions to have full control access to the network shares and files that are archived.
3. Create a volume policy.
4. Create a folder policy.
5. Create new volume on the file server and apply volume policy.
6. Create archive points to control archived folders.

Using the above procedure, set up the file system archiving by selecting the placeholder configuration wizard. File placeholder service configuration is shown in the following figure for our test setup.

Figure 36)File Placeholder Service Configuration Wizard

Configuration requires Windows user authentication information to grant the necessary user rights such as:

- Log on as a service
- Act as part of operating system
- Debug programs
- Replace a process-level token

After granting the necessary user rights on the computer running the configuration, file system archiving setup gets completed. On our system the configuration wizard displayed the information shown below.

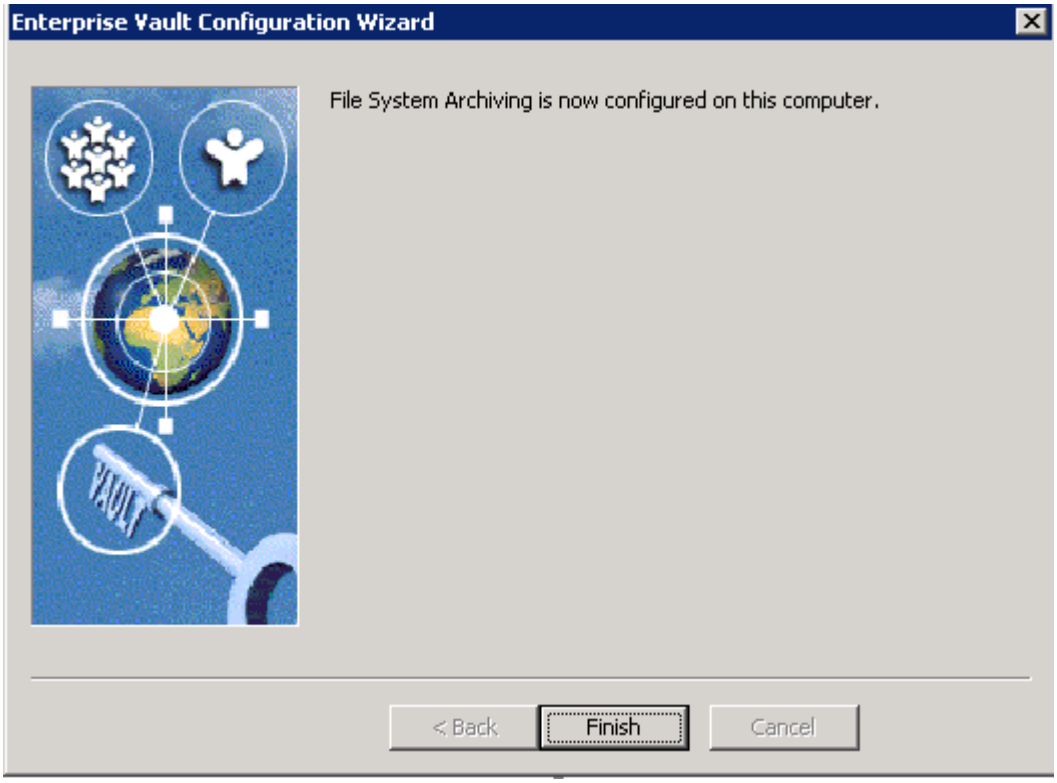

Figure 37) File Placeholder Configuration Completion

Having successfully configured the file system archiving, file server archiving policy has to be created. Archiving policy requirement is similar to creating a mailbox archiving policy. There are two possible types of archiving policies, one being volume archiving policy and the other one, a folder level archiving policy. Using the Enterprise Vault administration console, create a volume archiving policy by providing the policy name and the description. On our test setup, the archiving policy name and description were entered as shown in the following figure.

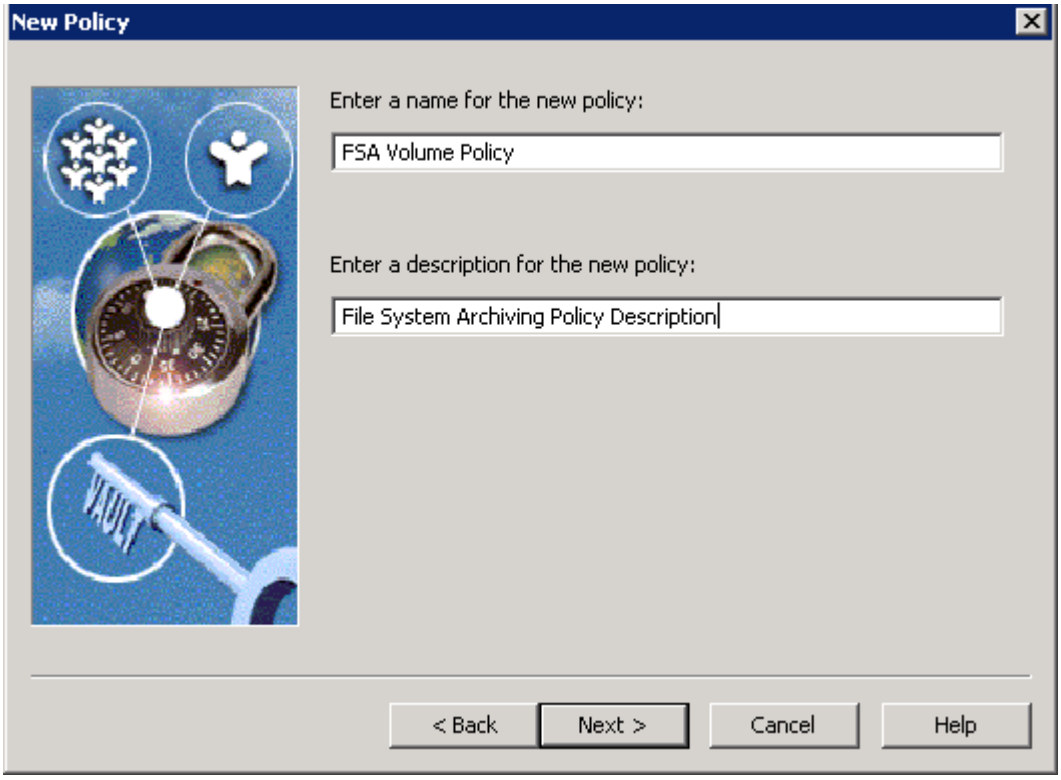

Figure 38) Creating New Volume Archiving Policy

Continue with the wizard to configure quota enable or disable management, start, and stopping of archiving process settings. Using this configuration, the archiving process runs after a predefined percent of data usage. Select a retention category for this volume policy to be applied. Choose whether to leave a shortcut to the archived file. Archiving policy allows specifying the type of files archived onto the Enterprise Vault Server. File system archiving applies to the permissions of the folder archived from the system. Change the settings if necessary while creating the rules.

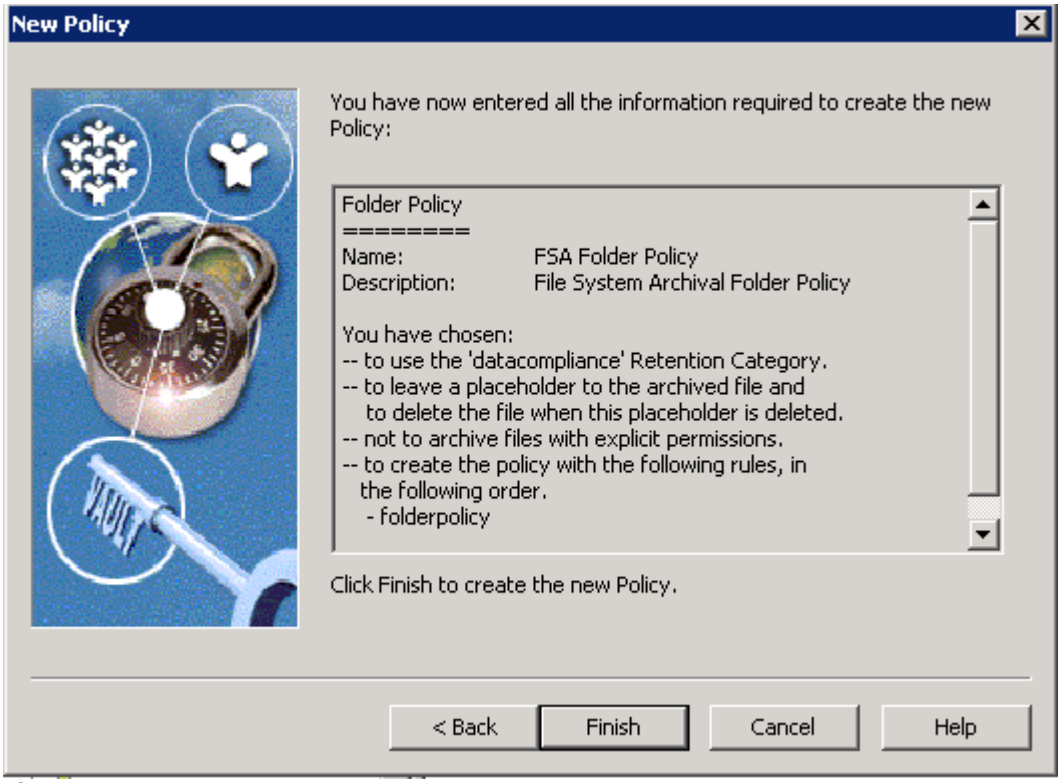

Figure 39) Information Required to Create the New Archiving Policy

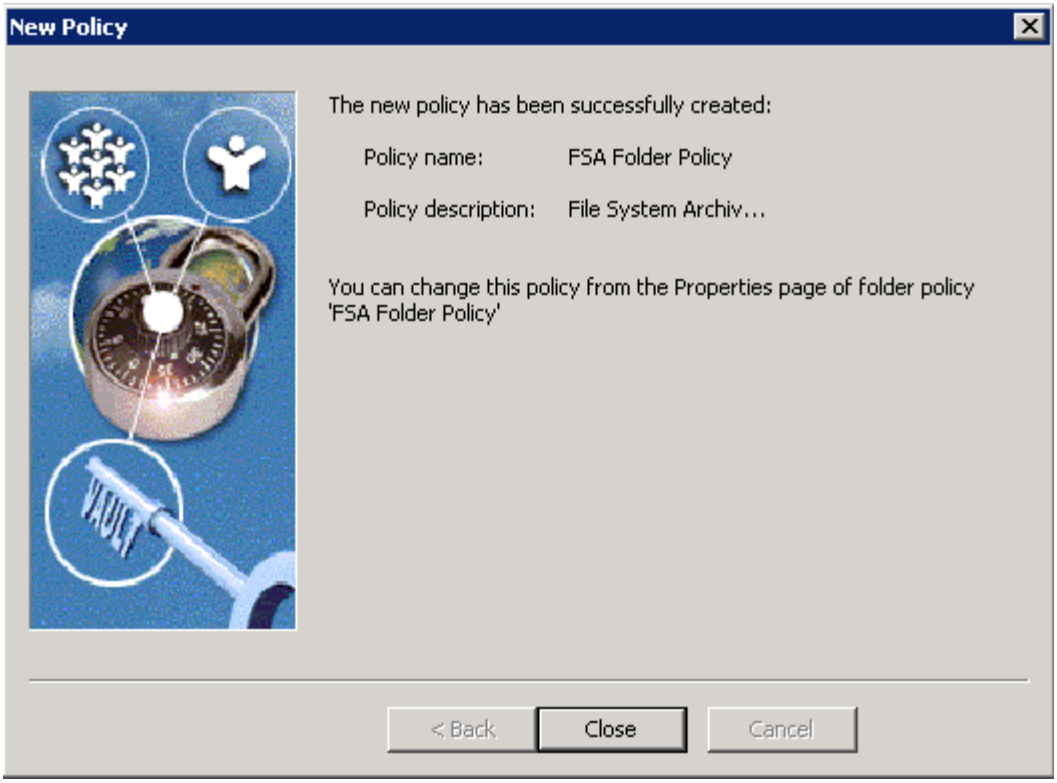

Figure 40) New Policy for File System Archiving

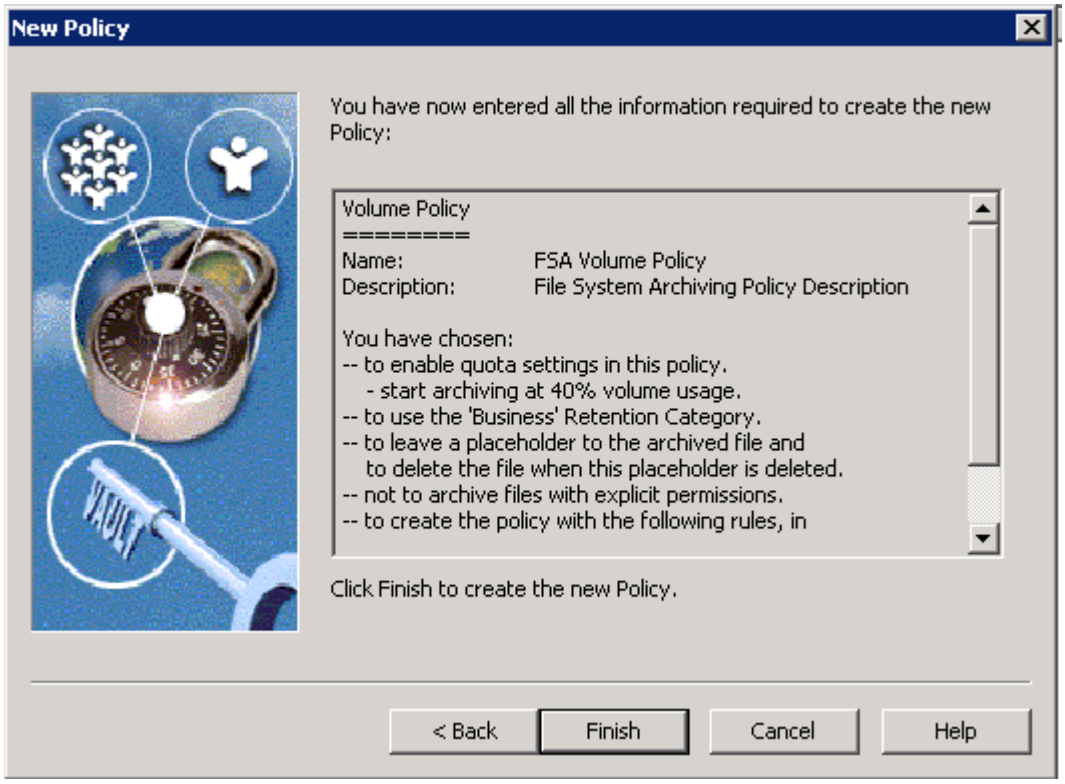

Figure 41) New Archiving Policy Settings

After creating the file archiving policy, it is important to add a file server using its fully qualified DNS name (FQDN) for the file server. It is a good idea to browse the file server from the available servers. Select the computer running the shopping service and continue with the configuration as shown in the following figure.

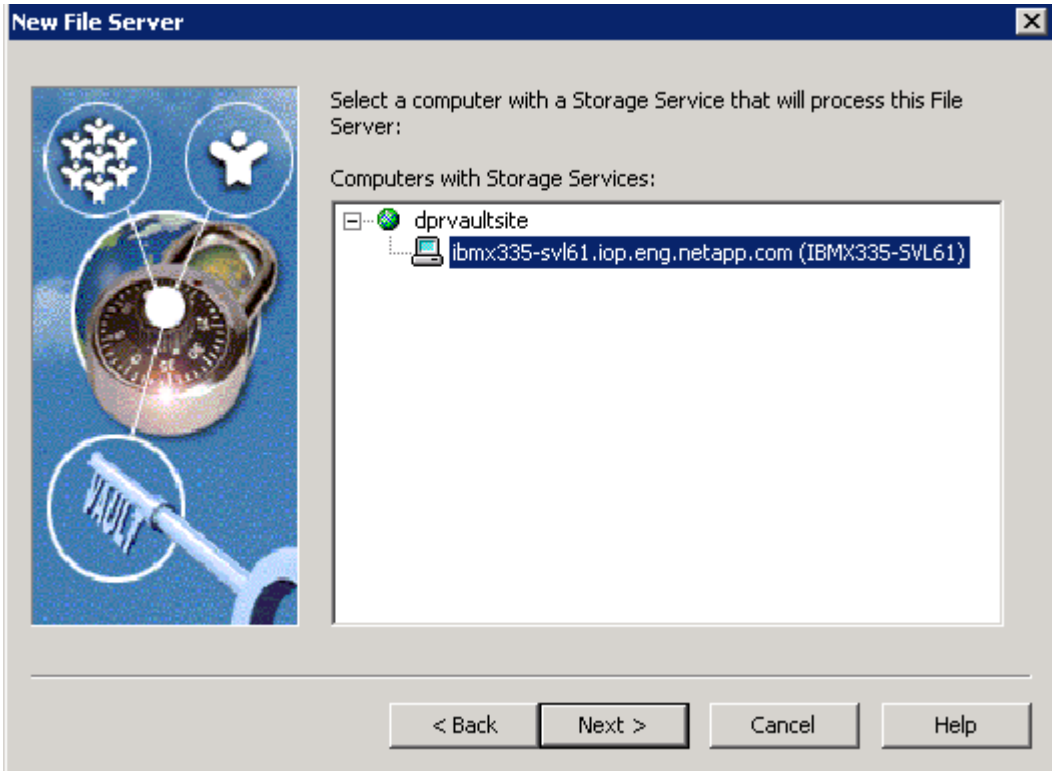

Figure 42) Selecting the Computer Running Storage Service

The file placeholder service component installed on the storage system presents itself as an NTFS file server, and leave placeholder shortcuts. The placeholder service component does not run on the NetApp storage system(s). Instead, it runs on the Windows Server and is configured using the administration console. This service can run a different Windows Server than the Enterprise Vault Server. File archiving filter driver is not required on the NetApp storage system. An archive point in each folder is created when a new volume is created using the administration console. To create a volume, expand archiving targets, to see the file server, and right-click the available file server.

To complete the file archiving setup, follow these instructions.

1. Open the Enterprise Vault administration console,
2. Expand the file server.
3. Select the file server as shown in the following figure and continue with creating the volume.

Note that there are two types of shares to browse while selecting a Windows share. Selecting the hidden type share displays the drive letters available as archival points.

The following figure shows the command to create a new volume for file server archiving targets on our test setup.

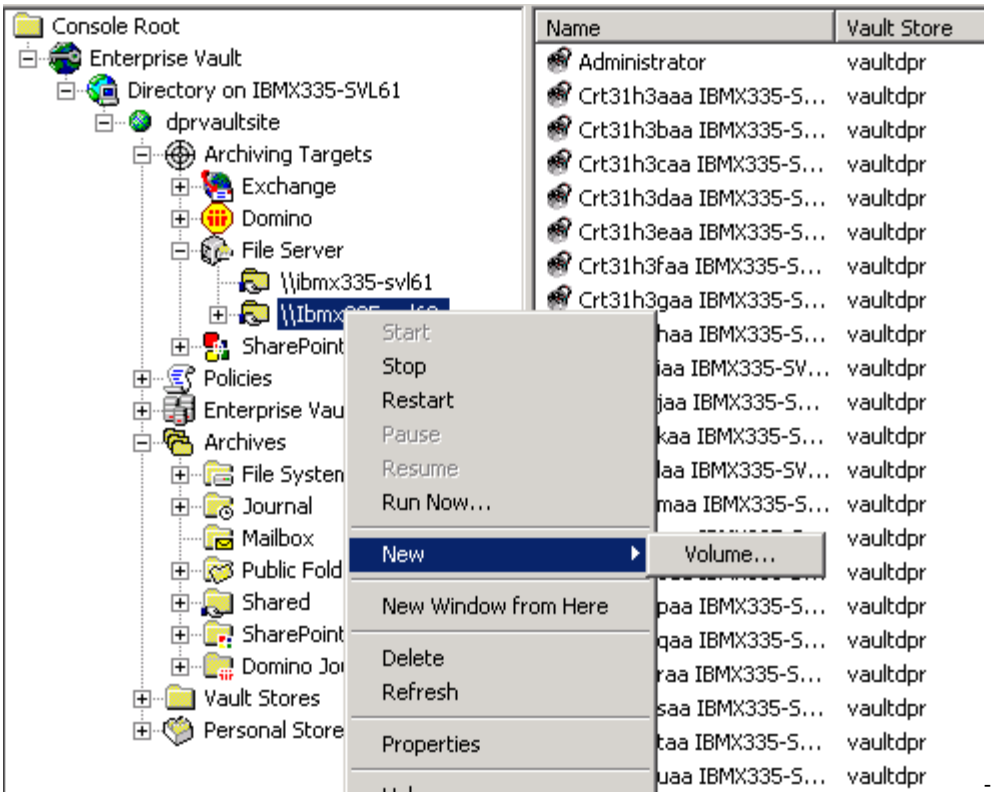

Figure 43) Creating a New Volume for File Server Archiving Targets

Browsing the hidden type of share will display the directory path. Select a folder archiving target from the displayed directory path. Apply the volume policy for the archiving target and select the required vault store on the processing computer. On our test setup, the following figure displayed information required to create the archiving volume.

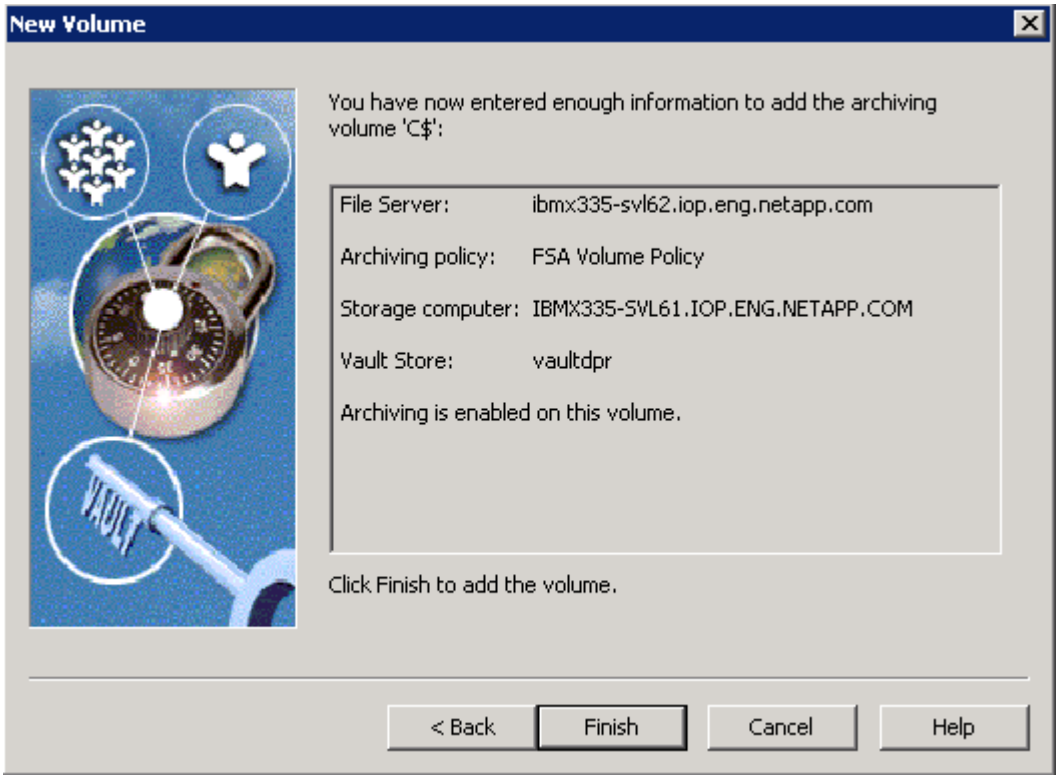

Figure 44) Creating New Archiving Volume for File Server

Create the necessary archiving targets for all the folders that require file system archiving. The following figure shows the available file server archiving targets on our test setup. Note that C$ share on the file server shown corresponds to a particular directory path as configured in the file server archiving targets. This means C$ need not refer to the root directory of local drive C:\, and it may correspond to other folders in the file server.

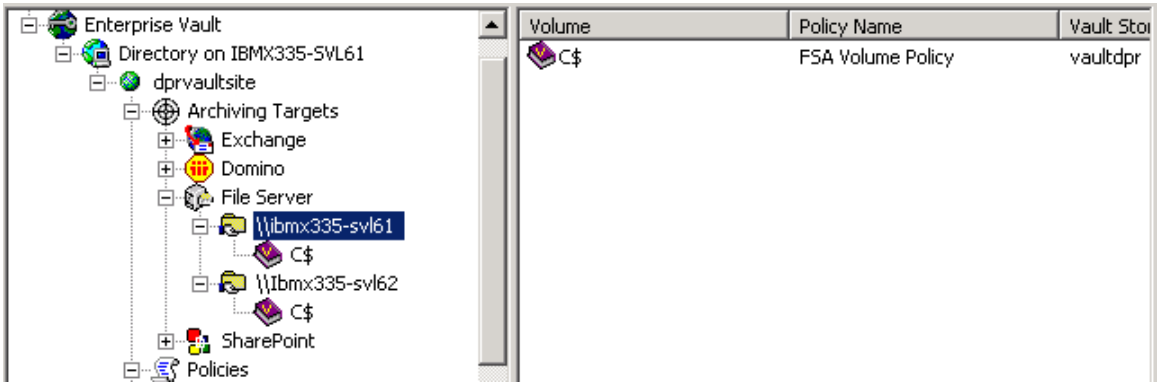

Figure 45) Available Archiving Targets on File Servers (File System Archiving)

6. Summary

Enterprise Vault supports archiving messages from Exchange Server. It can archive Lotus Domino servers for journaling feature in addition to the ability to archive file system and SharePoint portal data. Using NetApp storage systems, data can be archived onto a network share or as a configured local disks. Using NetApp SnapLock software, data archived by Enterprise Vault achieves the compliance goal. This paper discussed the procedure to deploy Enterprise Vault Server with NetApp storage systems. This paper covered the topics to configure the storage area network as well as NTFS file systems. Storage configured as virtual local disks was used to install and configure Microsoft Exchange Server, Microsoft SQL Server, and Enterprise Vault Server. Enterprise Vault used NetApp storage systems configured as network shares for archiving the data from the primary to 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 recovered from the backup copy loses all the recently archived items. Data replication could take a significant amount of time and resources. Creation of an HTML file archive reduces the space savings from archiving and compression. Restoring a corrupted database could be disastrous in an enterprise environment. Joint solutions of Enterprise Vault and NetApp storage system deployment address the shortcomings mentioned.

NetApp storage solutions effectively address the shortcomings explained previously. Symantec Enterprise Vault and NetApp product integration design offers highly available and exceptional performance at very low total cost of ownership. The ability to provision storage with primary and archive workload characteristics on a single system provides simplified management and leverages/minimizes IT skill sets, as users are required to only manage the product and maintain a single system that is providing multiple service levels. In addition to the skyrocketing growth in e-mail volume, a number of compliance regulations recently enacted globally mandate the archival of e-mail and other corporate data. This requirement and the required ability to produce the data in a timely manner have driven enterprises to pursue a more structured and regulated archiving process.

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 available 24x7.

NetApp offers complete solutions for Enterprise Vault Server environments. SnapManager for Exchange is ideal to manage Exchange Server data such as backup and recovery. SnapManager for SQL allows creation of consistent and quick backup copies. The same also allows restoring the database backup from Snapshot™ created with SnapManager for SQL Server product. SnapDrive for Windows provides an efficient and easy way of data storage management on Windows Server.

In conclusion, the recommendations made in this paper are intended to be an overview of best practices for most environments. This paper serves as a starting guide when designing and deploying Symantec Enterprise Vault in a NetApp environment. To ensure a supported and stable environment, become familiar with the products of Enterprise Vault and NetApp storage systems. During the design phase, involve the Microsoft Exchange and SQL Server specialists along with Enterprise Vault experts. This paper strongly recommends seeking professional help from respective vendors.

7. 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 NetApp. Do not attempt to seek help from NetApp Global Support for procedures listed in this document.

8. Appendix

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

8.1. Operating System Required Patches

The section lists the hot fixes 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 hot fixes are required on Windows 2003 SP1 Server.

- Q916531-hbaapi
- Q916048-storport
- Q913648-vss
- Q912593-classpnp
- Q910048-ntoskrnl

8.2. References

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

- "Deployment Guide for VERITAS Enterprise Vault from Symantec: NetApp Storage Solution"
- "Integrating VERITAS Enterprise Vault with NetApp Storage Solution File Archival"
- "Enterprise Vault 6.0 SP2 Product Documentation from Symantec Manuals"
- "Symantec Enterprise Vault"
- "SnapDrive for Windows: Best Practices"
- "Using SnapLock Compliance and SnapLock Enterprise with Data ONTAP 7G"