Technical report:

Implementing Symantec Enterprise Vault with IBM System Storage N series

Best-practices integration guide

Document NS3500-0

May 22, 2008

Table of contents

Abstract

As the volume of e-mail and other unstructured data skyrockets, it is increasingly clear that today's enterprises need a structured approach to archival. The combination of Symantec Enterprise Vault with IBM System Storage N series 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 an IBM System Storage N series unified storage environment.

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 relational database management system (RDBMS) data, enterprise resource planning (ERP) systems data, and so on by vendors like Oracle, IBM, Microsoft®, and others.

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 Enterprise Vault in combination with IBM® System Storage™ N series. The combination of Enterprise Vault and an N series storage system yields a highly available and scalable solution ready to solve any enterprise's most demanding archiving and/or compliance challenges.

Background on technical issues

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.

N series 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. The Enterprise Vault and N series combination provides such a solution.

Purpose and scope

The purpose of this paper is to demonstrate the ease of product integration of Enterprise Vault and IBM N series storage systems. It is important to note that this paper is not a substitute for the product documentation and release notes shipped with Enterprise Vault and/or the target N series 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 N series storage systems ready for Enterprise Vault installation and configuration.

In addition to Enterprise Vault software, this paper will briefly discuss the installation of additional software products including the IBM System Storage N series with Host Attach Kit (HAK) and IBM System Storage N series with SnapDrive® software. For detailed procedures involved with installing these products as well as the Microsoft 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.

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 FSA 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 N series storage systems using IBM System Storage N series with SnapLock® to archive compliance data.

Deployment of Enterprise Vault requires servers running Microsoft Windows® 2003 or Windows 2000 Server. Enterprise Vault also requires Microsoft SQL Server 2005 or SQL Server 2000 products. If you are deploying mailbox management, Enterprise Vault supports the following messaging systems:

- Exchange 2003
- Exchange 2000

- IBM Lotus® Notes® for Journal Archiving.

For deployment of Enterprise Vault in Microsoft FSA applications, 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 Enterprise Vault product website (at the time of this report writing, located at www.symantec.com/business/products)..

It is recommended that the deployment of both Exchange and SQL Server environments using either a Fibre Channel (FC) or iSCSI protocol storage area network (SAN).

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 4,000 active user mailboxes. Symantec Enterprise Vault 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 to determine an optimal solution to fit your unique environment. It is also important that only one Exchange mailbox task 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 (i.e., the infrastructure combination used for the purposes of this report but not necessarily the most current versions of all components at any time):

- 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 FSA: IBM System Storage N series N5500 storage system running IBM System Storage N series with Data ONTAP® 7.1.1
- Exchange primary data: IBM System Storage N series running Data ONTAP 7.1.
- E-mail archival and FSA data migrating service: IBM System Storage N series N3700 (NearStore) storage system running Data ONTAP 7.1, Storage management software: N series SnapDrive 4.1, N series SAN HAKit 3.0, Emulex LP9002L host bus adapter (HBA) card, and HBAnywhere software.

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 N series storage setup needed a fresh install of SAN configuration. Configure the HAK software and the software on N series storage systems. For this purpose, an Emulex HBA LP9002L card was used to connect from Windows Servers to the N series storage system. If SAN configuration is already configured, determine the storage requirement and complete the storage setup.

To install the necessary applications such as 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 N series SAN configuration occurs. Enabling the necessary product license is a prerequirement to use the storage.

Installing SAN Manager Software is optional. SAN Manager provides end-to-end FC SAN management that enables N series customers to securely monitor and manage their enterprise storage infrastructure. To discover and monitor N series storage devices, SAN Manager requires an IBM System Storage N series with DataFabric® Manager server.

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.

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 N series 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 FC and iSCSI protocols. It provides the dynamic storage management feature. This paper recommends having the systems connected Windows host reside in the same broadcast domain. During this test install, the SnapDrive installation wizard displayed the FC protocol HBA driver and firmware information. On this test setup, the following figure displayed the available HBA driver and firmware version along with the status information.

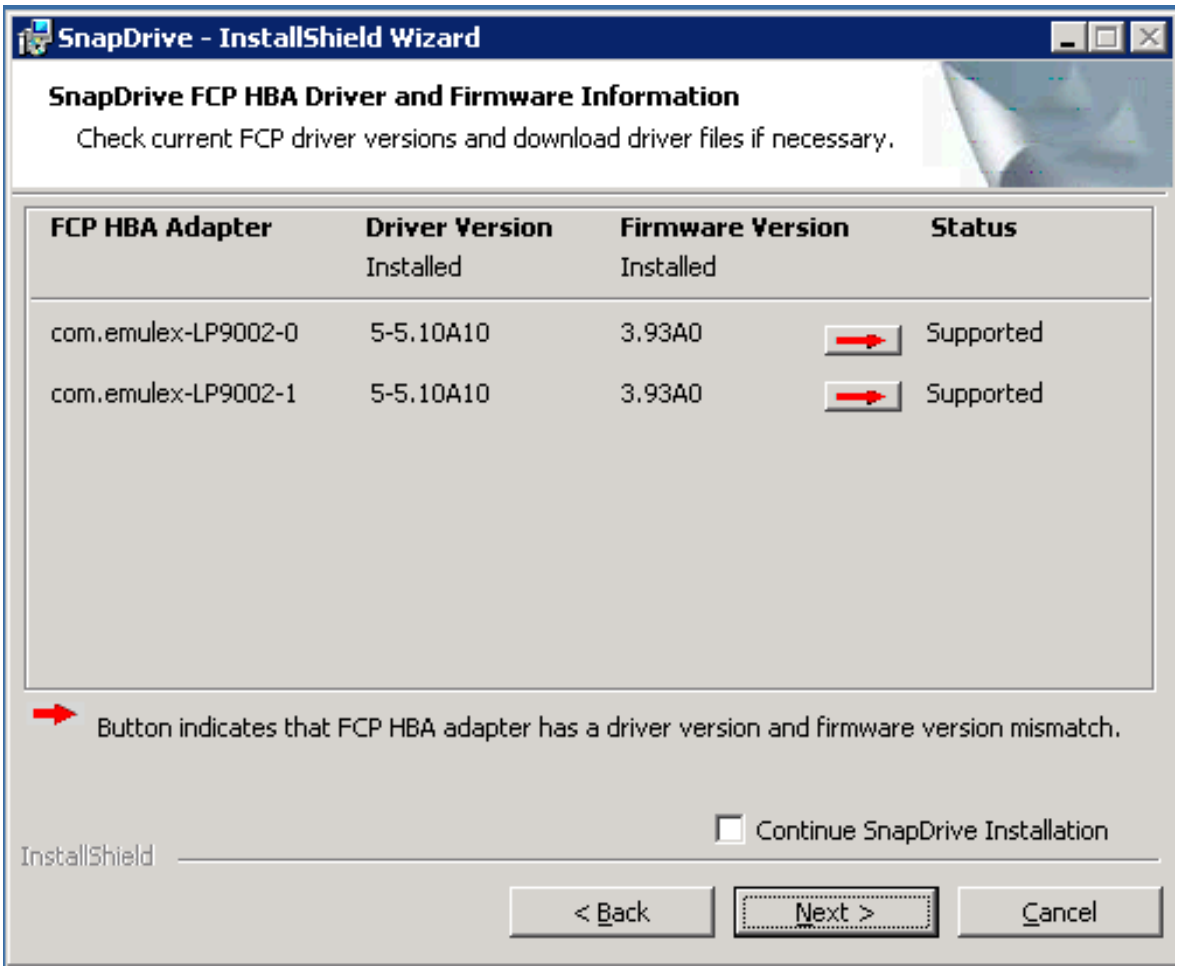

Figure 1) SnapDrive FC HBA driver and firmware information.

After checking the driver and firmware-supported version, the install wizard checks the management driver information to support the Microsoft Multipath I/O (MPIO) feature. If required, this process installs the appropriate driver version. After installing the SnapDrive software, use the Windows Microsoft Management Console (MMC) tool 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 this test setup, three virtual local disks were configured 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.

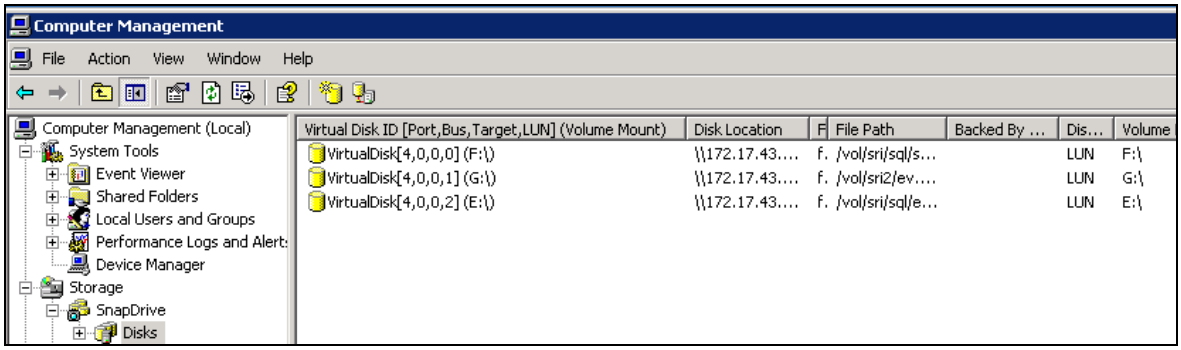

Figure 2) FC SAN configuration on Enterprise Vault Server as shown in MMC.

Installing Exchange Server

In an Enterprise Vault environment, it is safe to assume that the Exchange Server is installed and configured. If so, skip this section. However, for completeness of information, this paper assumes that Exchange Server is installed as a new install before installing Enterprise Vault software. Using the SnapDrive tool, two virtual local disks were created on the Exchange 2003 Server. Before installing Exchange Server, this 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 (AD) schema. DomainPrep will prepare the domain for Exchange 2003. Domain administrator privilege is required to complete these tasks. The following diagram shows the components selected for installing Exchange Server on this test setup.

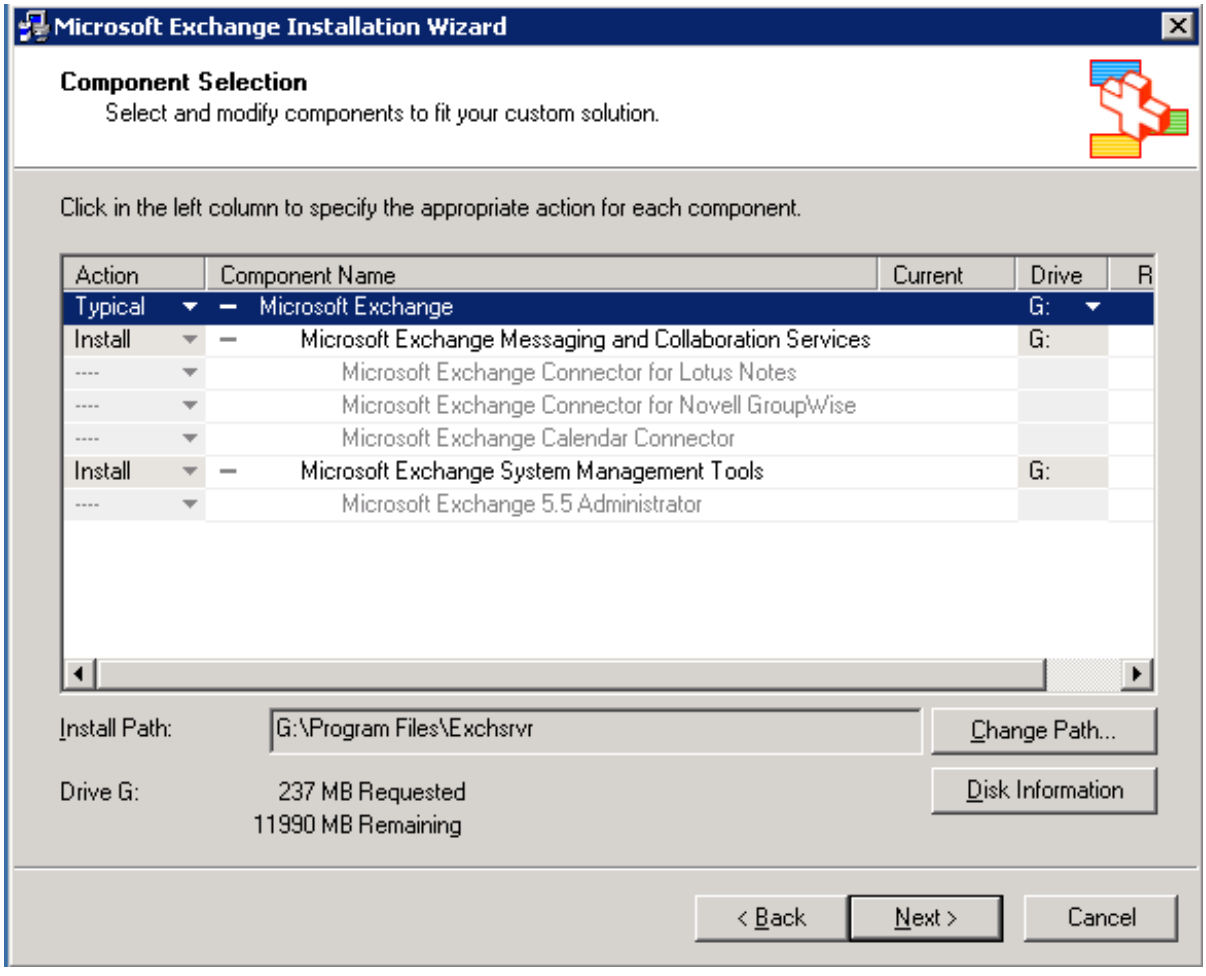

Figure 3) Exchange Installation Wizard component selection.

Using the SnapDrive software tool, the storage administrator has the ability to scale the storage space dynamically. Note that the storage size configured in this 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.

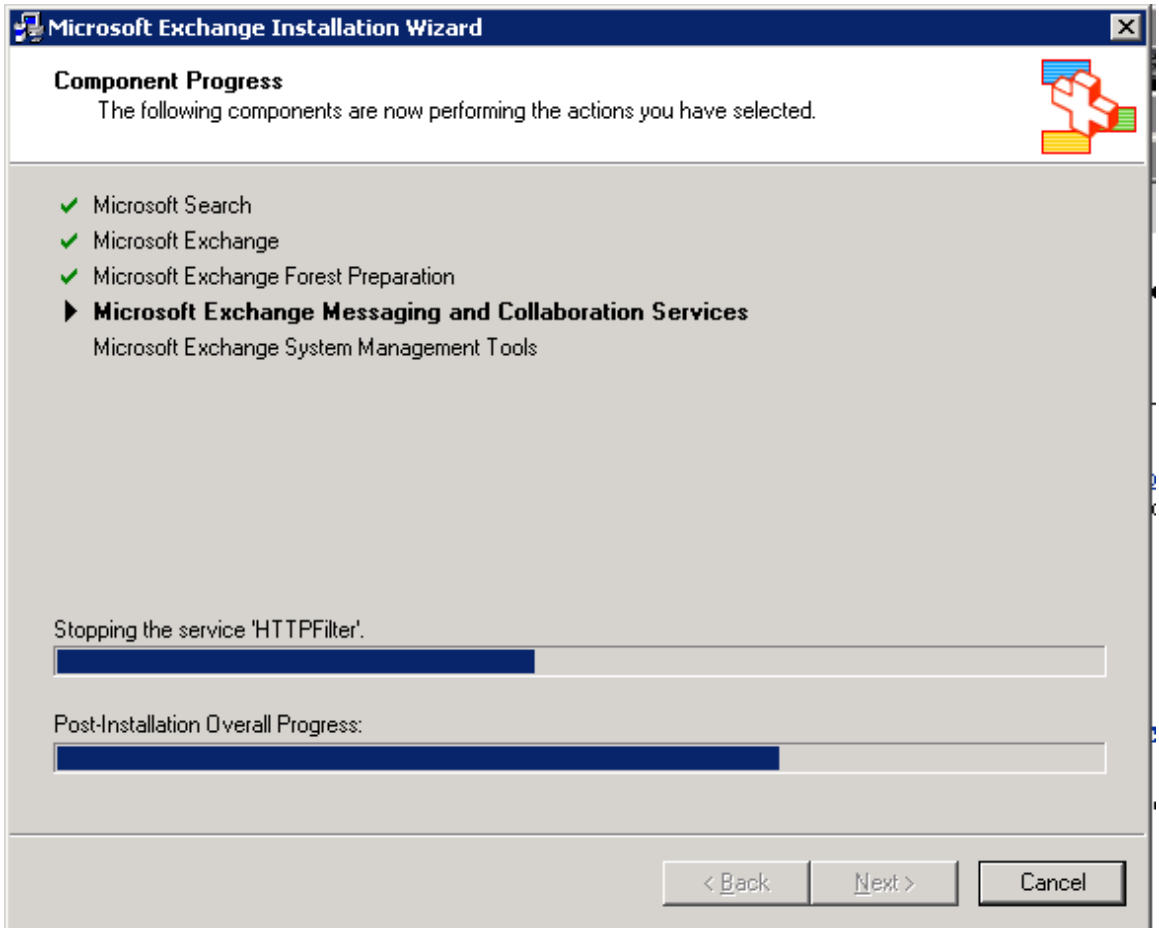

Figure 4) Exchange components install status.

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

SQL Server

Enterprise Vault requires SQL Server 2005 or SQL Server 2000 SP3 Server. A large Enterprise Vault environment may need a dedicated SQL Server on Windows Server. IBM System Storage N series with 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, an SQL Server 2005 was used to create 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.

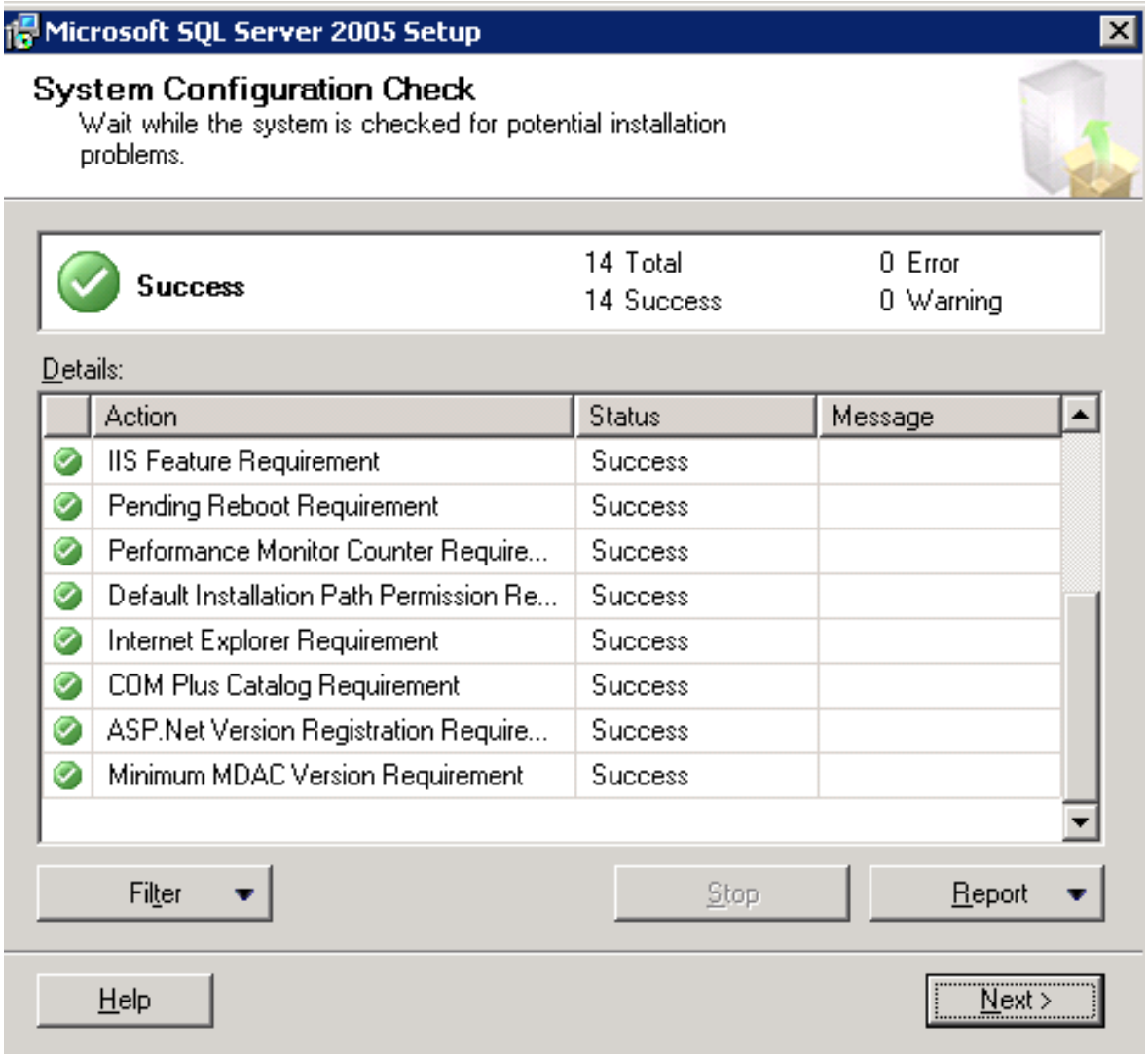

Figure 5) System configuration check for SQL Server 2005 installation.

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 this test setup, Windows authentication mode was selected. 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 this setup displayed the following figure showing the server type, server name, and authentication mode.

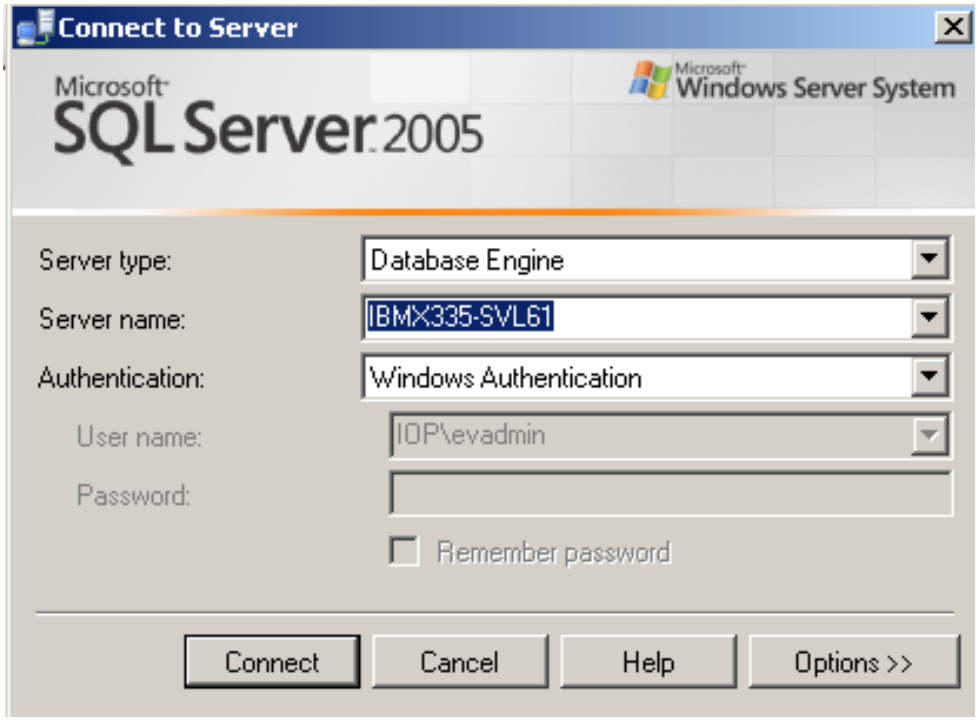

Figure 6) SQL Server 2005 information.

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

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 the test setup a domain called “IOP” was used to create a user called “evadmin.” In addition to this, multiple users were created to enable mailbox accounts.

Mapping the network share

Enterprise Vault requires an NTFS (NT file system) supported file system for archival destination. This includes local disks, configured virtual disks using N series storage systems, or a network-mapped share.

Establish the network connectivity between the Enterprise Vault Server and N series storage system(s). Once the network connectivity is established, complete the storage configuration. IBM N series with 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 Common Internet File System (CIFS) license is enabled and CIFS setup is complete. On this test setup, two storage systems were used, one N5500 system and an N3700 storage system. On each system, the necessary CIFS shares were created. On the N5500 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 the N5500 storage system for Enterprise Vault archival.

Configuring read-only 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 N series storage system, enable the appropriate SnapLock license. Note that certain configurations support more than one type of SnapLock license on the same N series storage system at the same time.

Currently there are two types of supported SnapLock features. A SnapLock license supports a stricter version of compliance volumes where the write-once-read-many (WORM) committed files remain in an immutable state until the retention period expires. Another feature, SnapLock for Enterprise, and the associated volume is controlled by the storage administrator. 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). Note that any misconfigurations or settings with a SnapLock volume may be irreversible, hence N series professional help is strongly recommended.

Enterprise Vault Server architecture

In this section, we briefly discuss the Enterprise Vault architecture and N series 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 FSA, SharePoint archiving, and SMTP message archiving. File servers are used to store the FSA 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. The major focus of this paper will be e-mail management in an Exchange Server environment.

Enterprise Vault is composed of an Enterprise Vault Directory and Enterprise 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, Exchange Server(s), SQL Server, Enterprise Vault Servers, Lotus Domino Server (with Journaling feature), and the necessary storage system(s). In this architecture, three N series storage systems are used for:

- Configuring the SAN systems
- Configuring the network shares for content archival using Enterprise Vault on an N5500 system
- Configuring the network shares for content archival using Enterprise Vault on an N3700 system.

The test setup used near-line storage N3700 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.

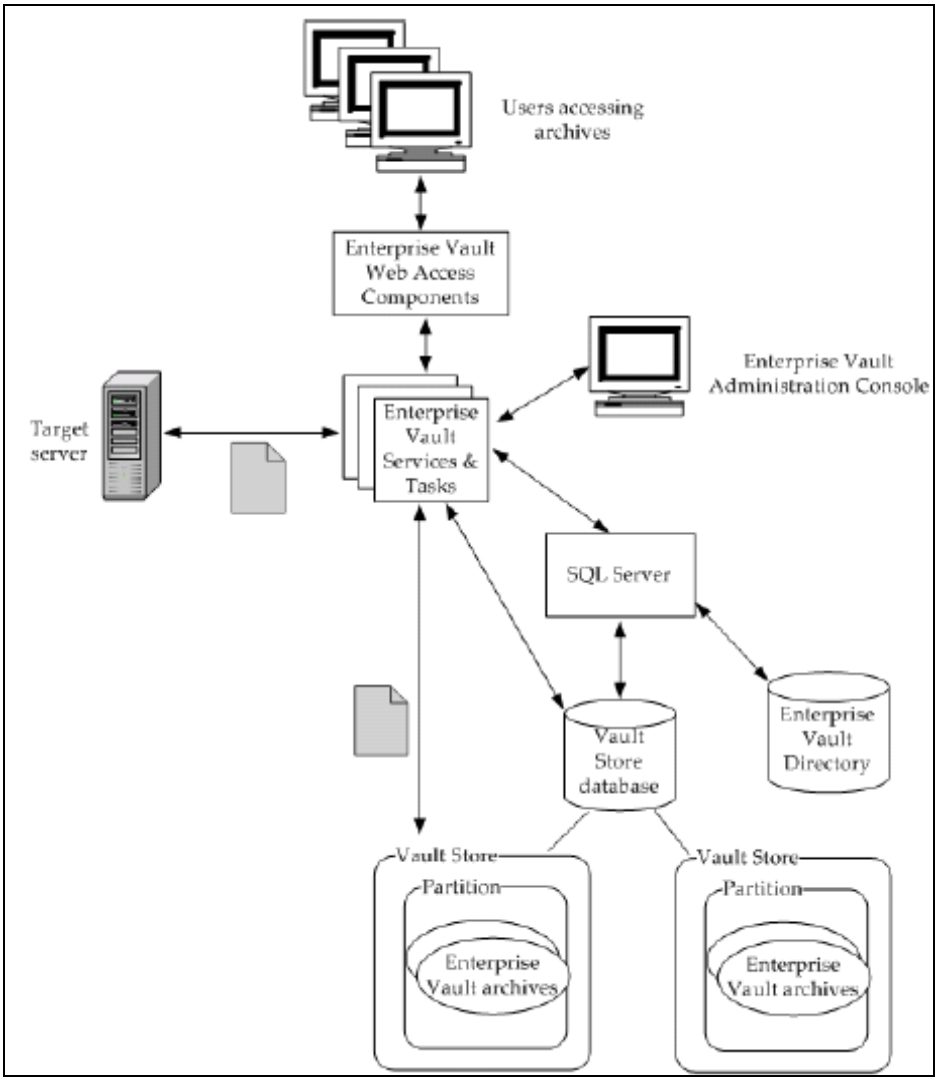

Figure 8) Enterprise Vault system architecture.

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. The following figure explains how users access the stored items.

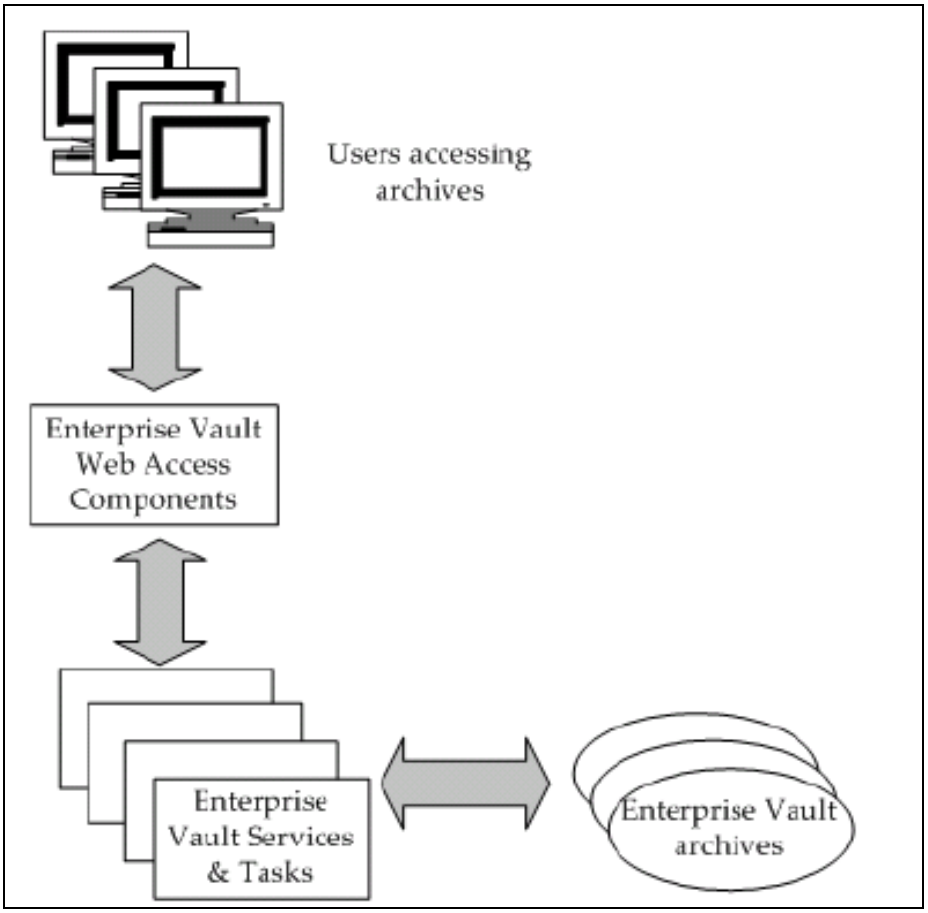

Figure 9) Process explaining how users can access stored items.

Exchange Server

Enterprise Vault configuration requires Exchange Server and SQL Server installations. Availability of Exchange Server and SQL Servers is a requirement for Enterprise Vault archival configuration. If the architecture includes Exchange Server on N series storage system, this paper recommends using IBM System Storage N series SnapManager for Exchange to manage Exchange data. Similarly, SnapManager for SQL from N series 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.

N series storage systems

Enterprise Vault requires either local disks or virtual local disks for installing the SQL Server, Enterprise Vault, and Exchange Server. Either SAN or IP-based SAN accomplishes the requirement. The necessary software and hardware configuration topics are discussed in earlier sections of this paper.

In this test setup, an IBM N series storage system was used to configure local disks on both Exchange Server and Enterprise Vault Server. For archival destination, an N series N5500 cluster configuration and a near-line storage system N3700 were used to migrate the items after a specified period.

Configuration

Enterprise Vault requires storage system be presented with NTFS file system configuration. NTFS volume, network share, and N series 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 (VD) database.

OS information

Enterprise Vault is a Windows-based application. At the time of this report writing, Enterprise Vault supports Windows 2007, Windows 2003, Windows 2000 with SP3, and Windows 2000 Advanced Server with SP3 platforms. On this test setup, two Windows 2003 SP1 Servers were used, one for installing Exchange 2003 Server and the other one for installing Enterprise Vault Server and SQL Server 2005 products.

Enterprise Vault requires N series with Data ONTAP 7.1 or later supporting Enterprise Vault features. This includes the ability to remove the retention expired items from SnapLock volumes. Enterprise Vault configuration requires at least Exchange 2003 or Exchange 2000 and SQL Server 2005 or SQL Server 2000.

Enterprise Vault configuration information

It is required to install and configure transmission control protocol/internet protocol (TCP/IP) on the Windows machine. This computer should have an 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, Internet Information Server (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
- Indexes – required for indexing services
- Shopping Baskets – required on shopping service computer.

The Vault Service Account

Enterprise Vault uses the Vault Service Account (VSA) to access the Windows Server OS. Enterprise Vault services are Windows services. All Enterprise Vault computers share a VSA. This account must be a member of AD domain if Exchange Server is used.

The Vault Site Alias (VSAlias) is a DNS entry for the Enterprise Vault site. Each Enterprise Vault site should have a VSAlias. 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 is 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.

SnapDrive software installation and configuration

The N series with SnapDrive tool eases storage management on Windows Server. It integrates with Windows MMC utility. Using this tool, configure the required local drives and complete the storage configuration as needed. A previous report section described the procedure to install SnapDrive software.

SQL Server configuration

Enterprise Vault requires SQL Server installed and configured properly. The N series storage system's virtual local disks configured with SnapDrive support SQL Server. A previous report section described the details about SQL Server installation.

Installation

This section discusses the procedure to install and configure Enterprise Vault Server. Knowledge of Windows OS administrator tasks, SQL Server, Outlook, IIS, 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.

Preinstallation checklist

It is necessary to complete the OS and storage requirements prior to installing the software. Enterprise Vault 6.0 was used in this test scenario. At the time of this report writing, Enterprise Vault 6.0 supported the following OSes:

- 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 collaboration data object (CDO) components

4. SQL Server 2000 or 2005
5. Available Exchange Server 2000 or 2003
6. Exchange System Manager
7. Microsoft XML Core Services (MSXML) – if not already installed
8. Microsoft Data Access Components (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. Microsoft Message Queuing (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 Sharepoint Server.

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. VSA (Vault Service Account)
2. Assigning Exchange Server permission – VSA must have access to Exchange mailboxes
3. Create a SQL login for VSA using SQL Enterprise Manager; this is a requirement if the mixed mode authentication mode is used while creating the database
4. VSAlias (Vault Site Alias) – Use DNS Manager to create an alias; if the DNS server is UNIX-based, you may configure the DNS alias for the Enterprise Vault Server by creating a CNAME entry.

Installing Enterprise Vault

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

Enterprise Vault install

In this test setup, it was a fresh install of Enterprise Vault software. In this test setup, the availability of Exchange Server and SQL Server were checked 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.

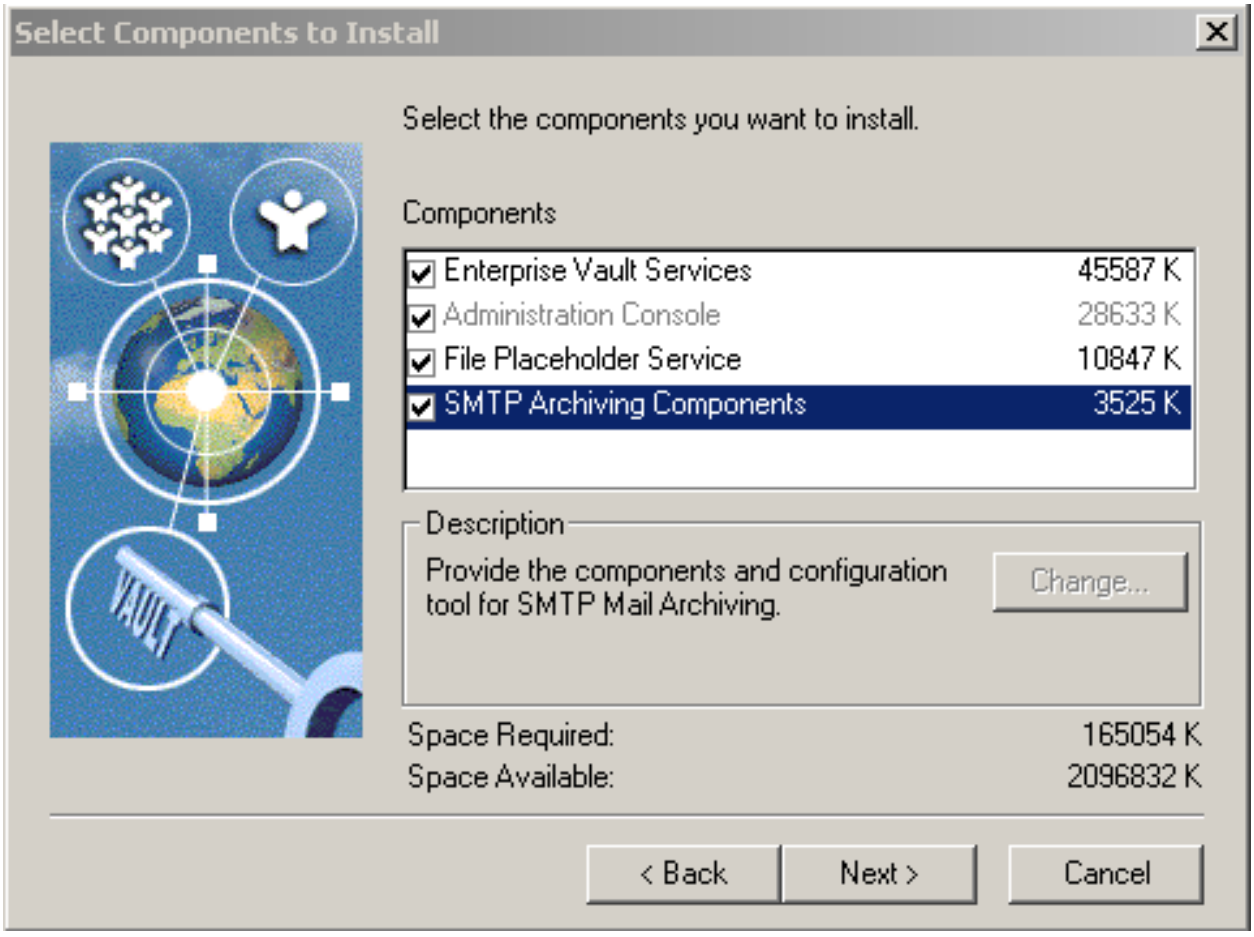

Figure 10) Enterprise Vault components installed.

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

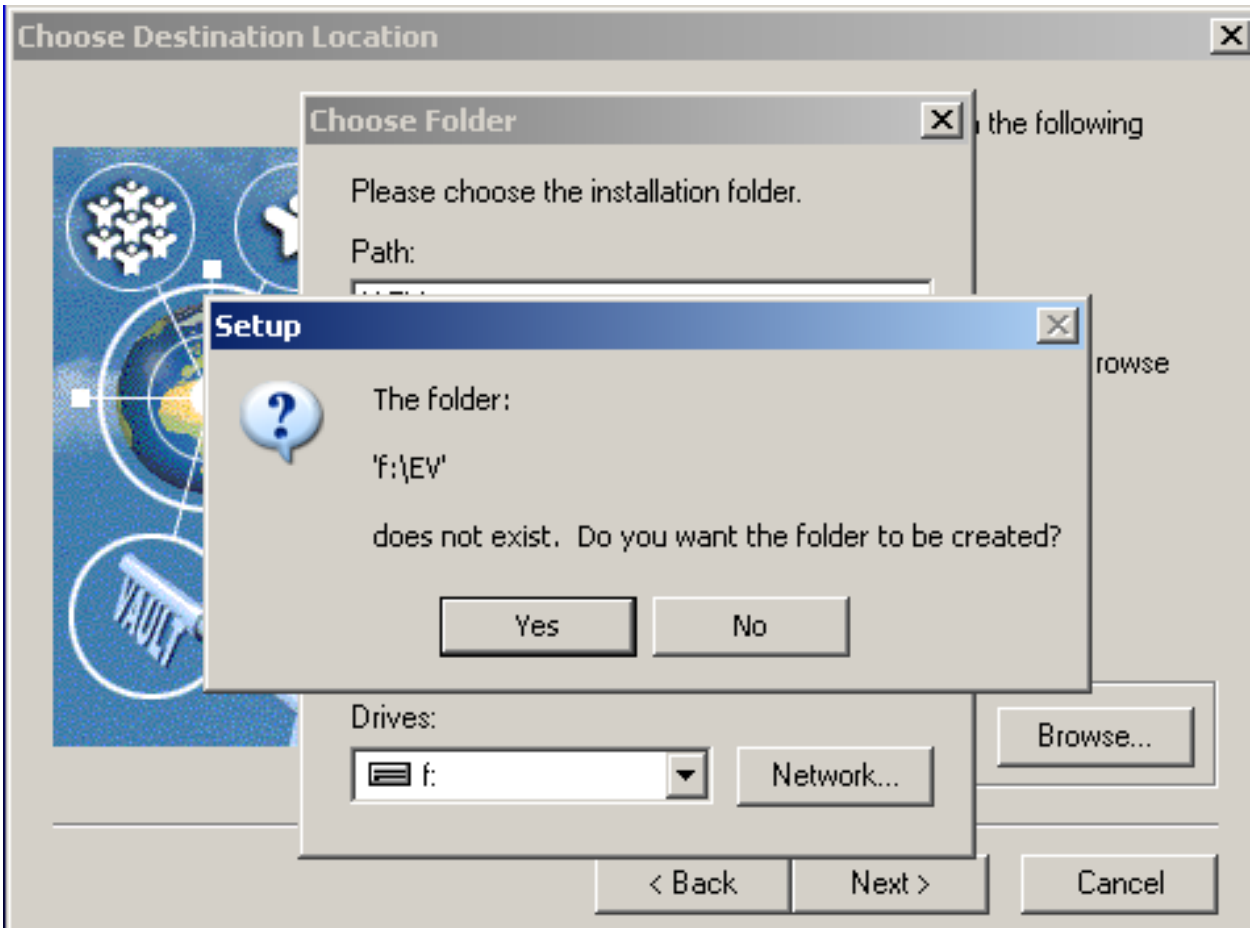

Figure 11) Choosing Enterprise Vault destination location.

If the installation folder does not exist, it creates a new one. The installation utility continues with the installation after the 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.

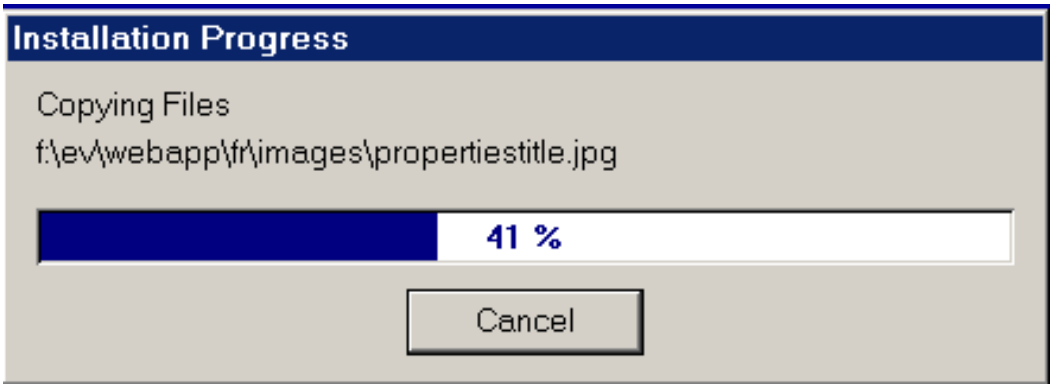

Figure 12) Monitoring Enterprise Vault installation progress.

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 this test setup is as shown in the following figure.

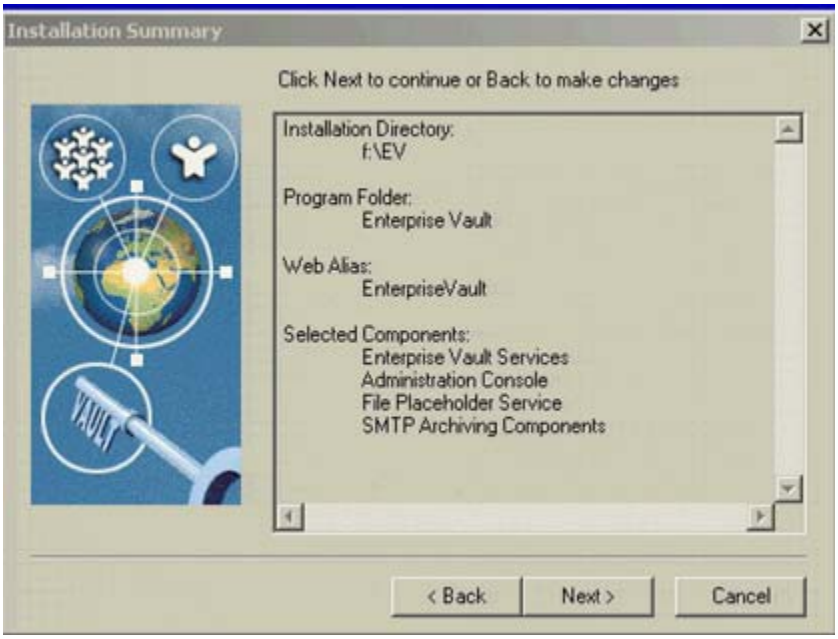

Figure 13) Display of Enterprise Vault installation summary.

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 this setup, the computer was restarted to observe the following Enterprise Vault icons in the program folder.

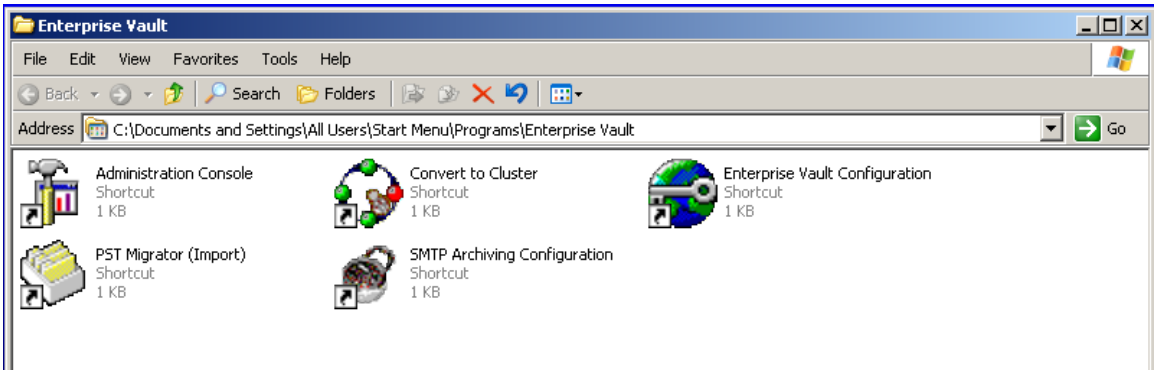

Figure 14) Program files for Enterprise Vault.

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 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.

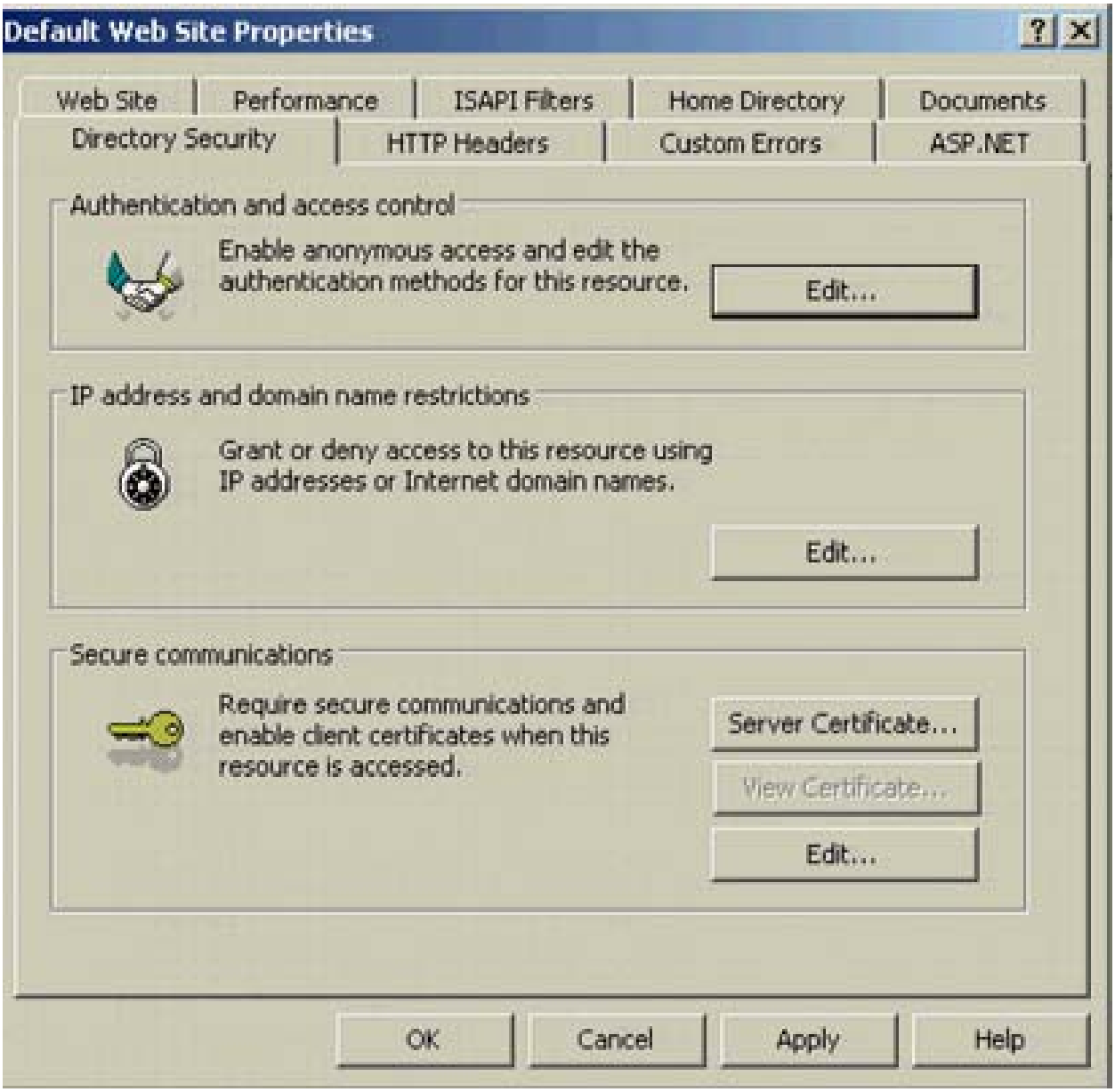

Figure 15) Default Website pProperties.

After setting Windows authentication security mode, complete the Exchange tasks for Enterprise Vault. On this system, a folder was created in the Organizations Forms library with access provided to all Exchange users. To create a folder, log in to the Exchange Server and open the Exchange System Manager. On this test setup, these steps were followed 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 VSA)
7. Roles → Owner → OK → OK → Close Exchange System Manager.

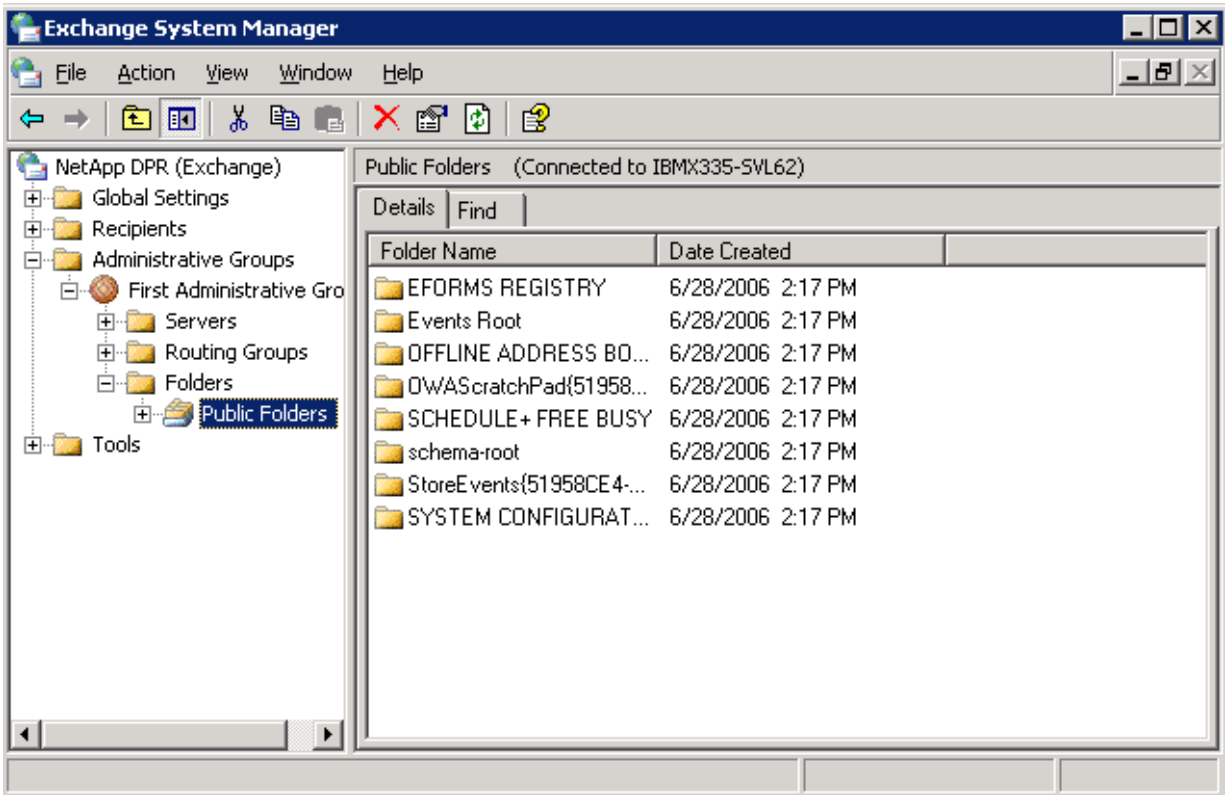

Figure 16) Exchange System Manager process to create a folder.

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

Enterprise Vault configuration

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

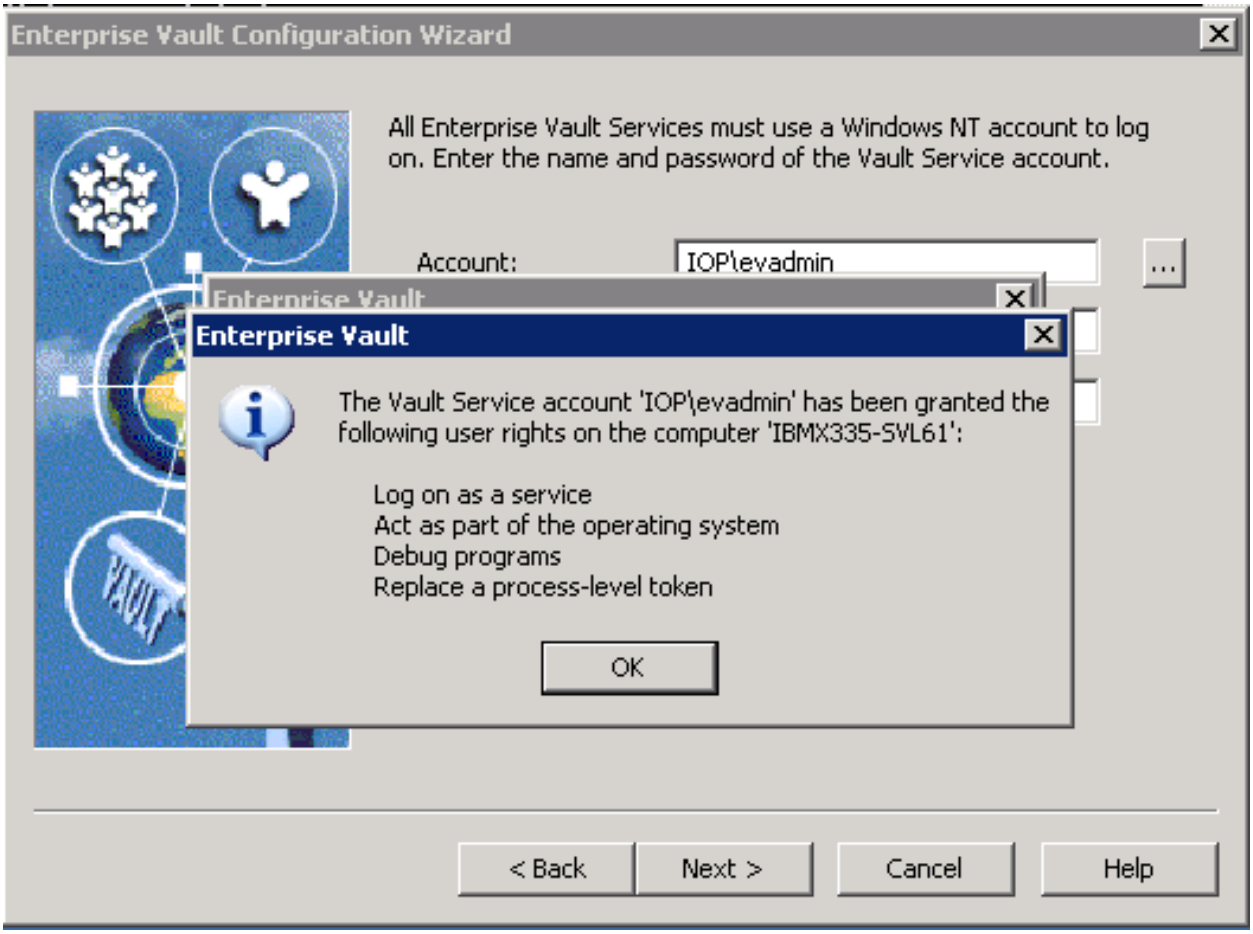

Figure 17) VSA user permissions.

After granting the necessary user rights to the VSA, VD database and transaction log locations information is required. In this test setup, the virtual disk path (SAN) created by SnapDrive storage management tool was provided, 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.

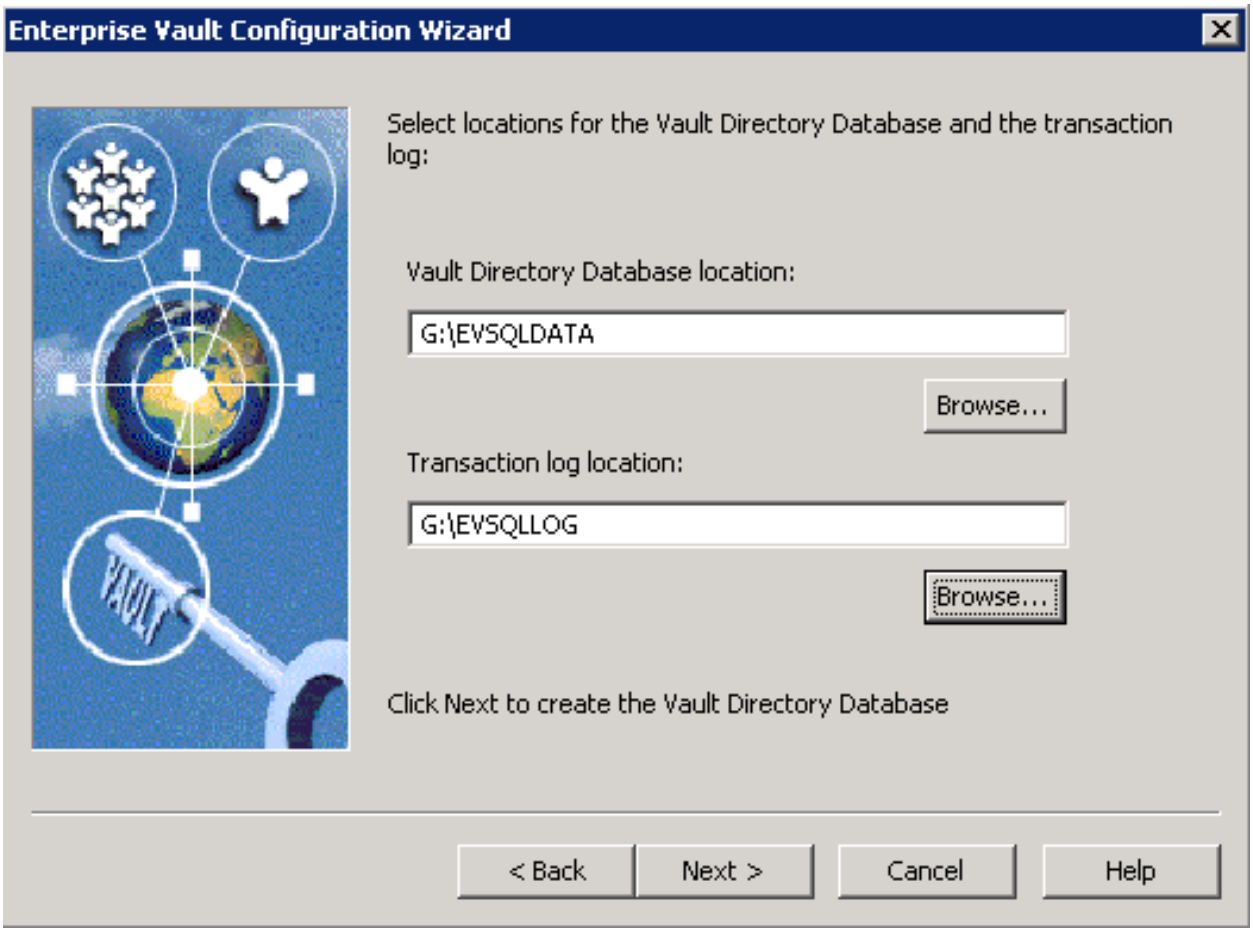

Figure 18) VD database and transaction log locations.

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 this test setup, we created a DNS alias “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 this setup, this task displayed the following output with a new vault site name of “dprvaultsite.”

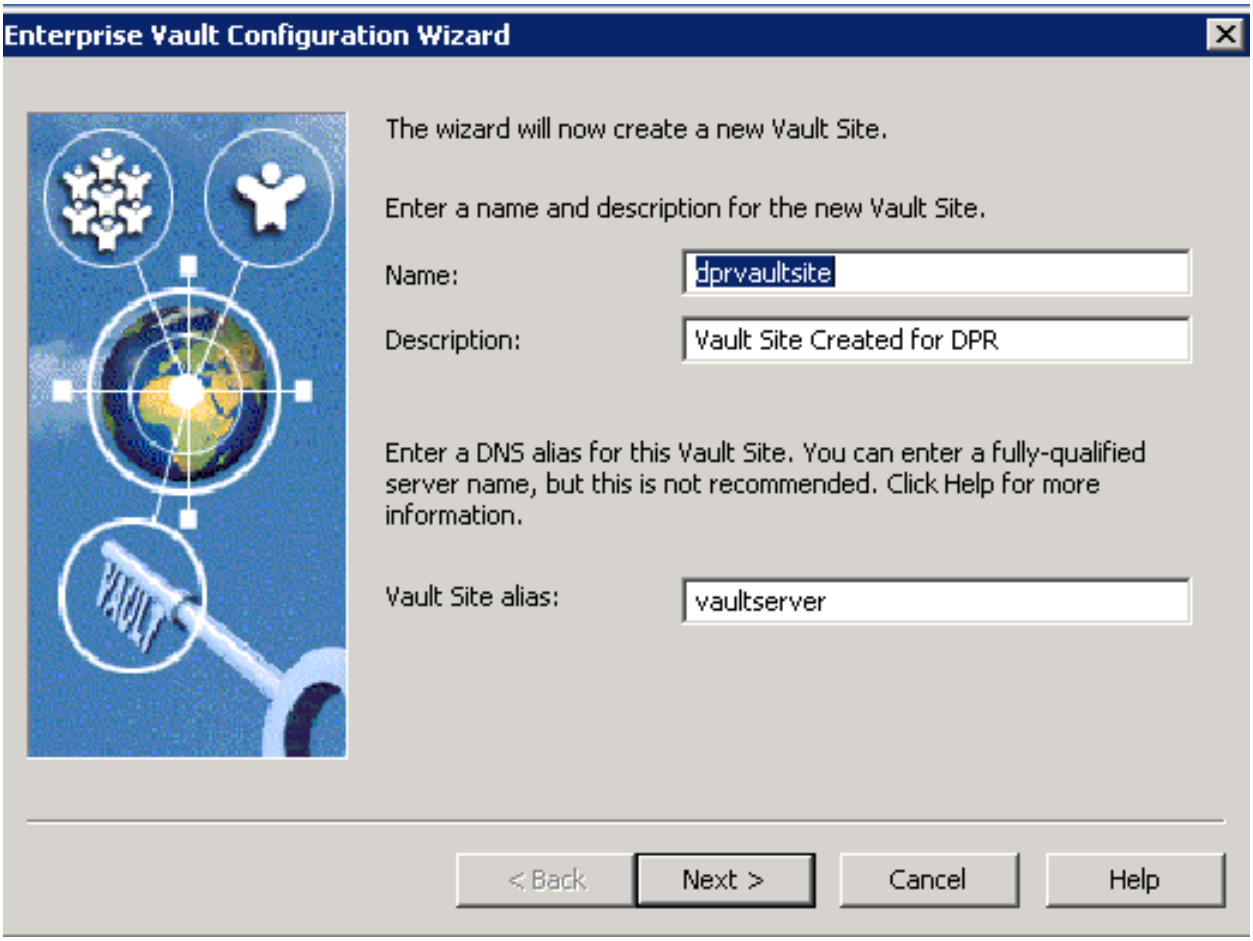

Figure 19) Creating a new vault site.

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 this setup, the archive processes were set to five and the restore process was set to one. On this test setup, the SnapDrive configured local disks was selected, as shown below.

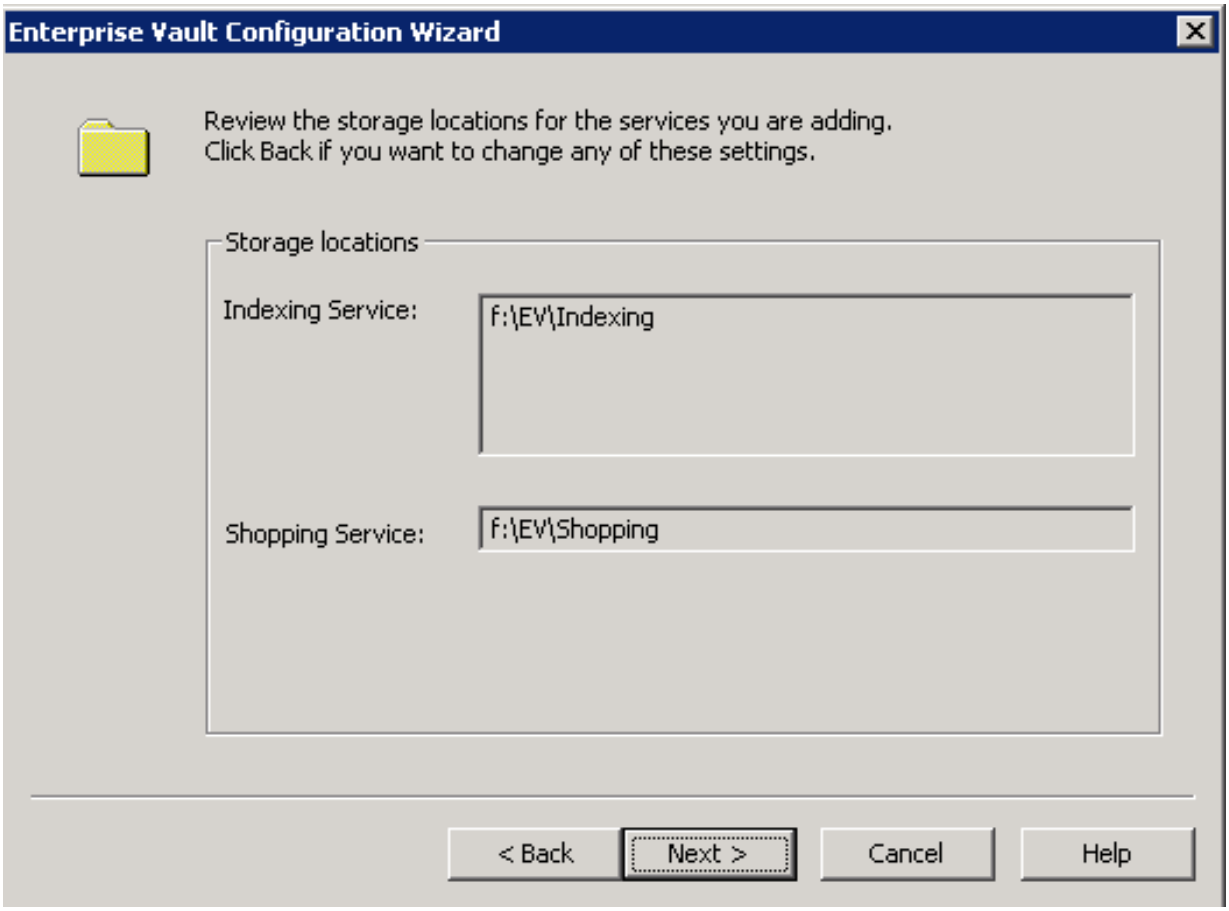

Figure 20) Storage locations for the services.

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

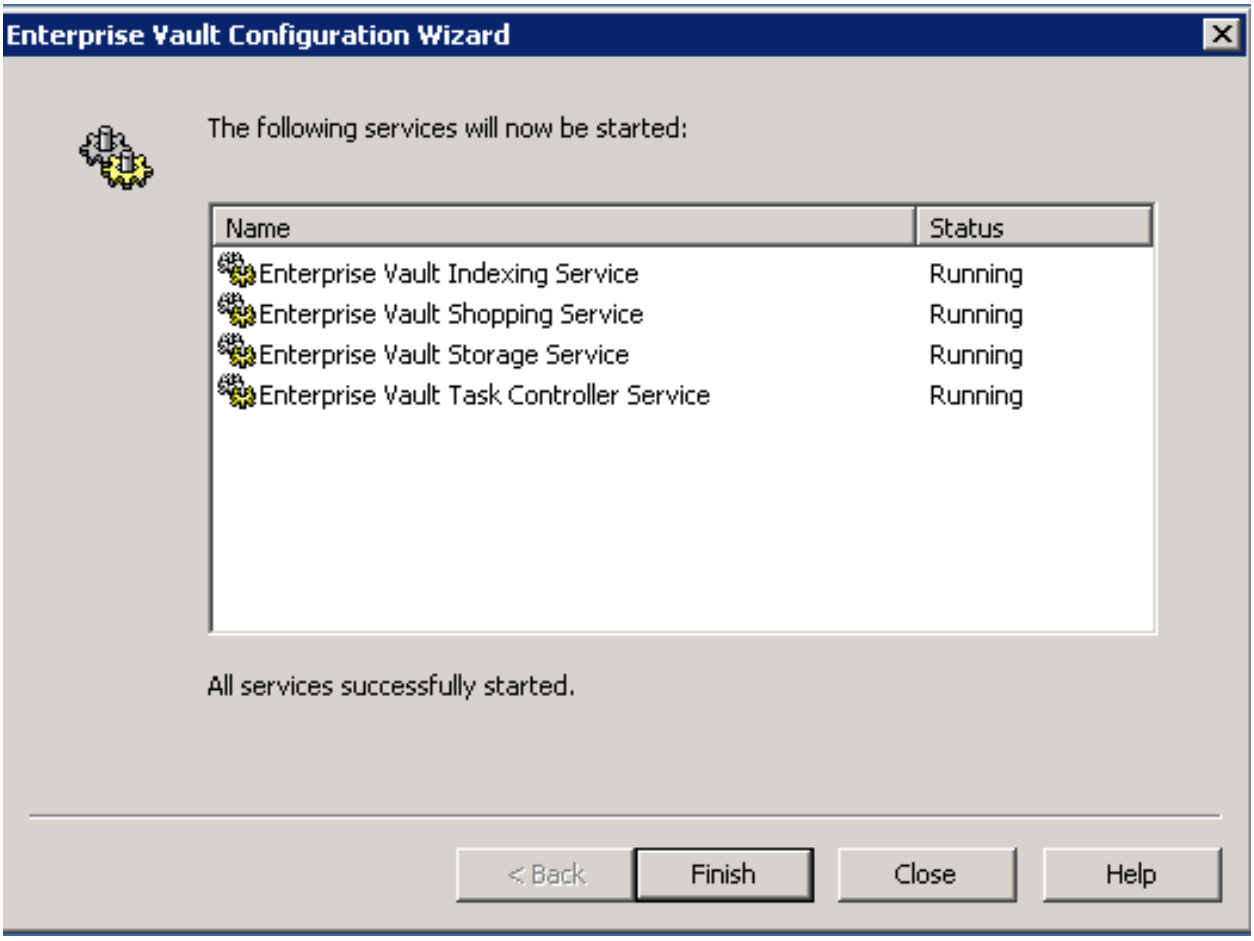

Figure 21) Status of Enterprise Vault services.

Now verify the VD 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.

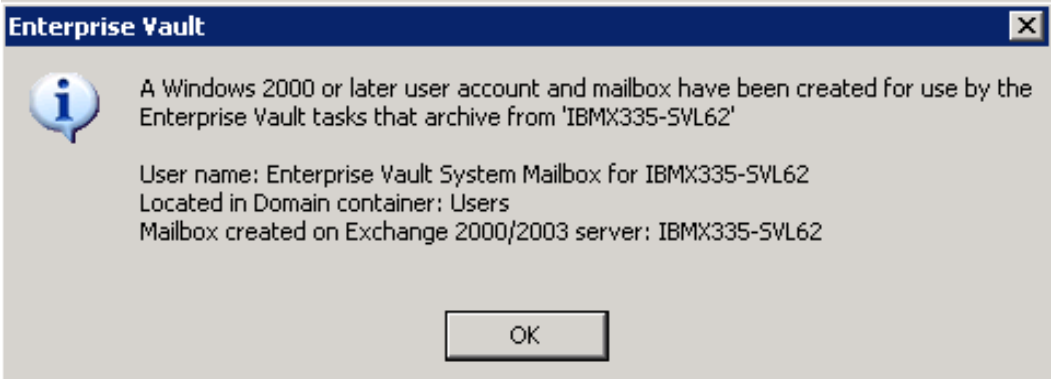

Figure 22) Mailbox information,

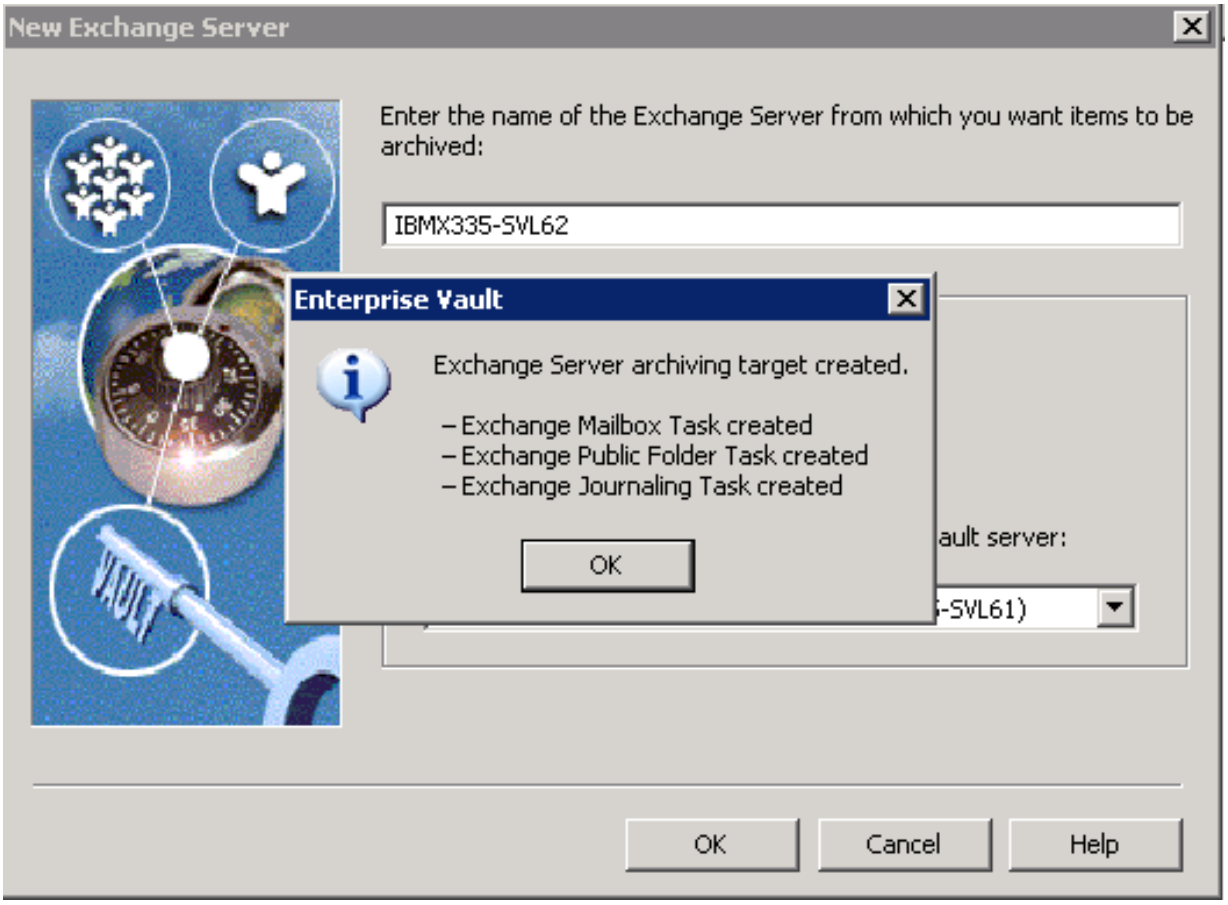

Figure 23) Exchange Server archiving target.

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 (VSP) is opened for archiving. Create a new VSP to set up archival configuration.

Configuring IBM N series for archival destination

In this test setup, an N series SAN configuration was used to install Exchange Server 2003, SQL Server, and Enterprise Vault products. Local disks were configured using SnapDrive storage management software.

Once the storage configuration task is completed, configure the Enterprise Vault archival destination and migration location. On this test setup, the Enterprise Vault archival destination and migration location was configured on N series storage systems. In this test setup, an N series N5500 storage system was used for archival and an N3700 was used 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 N series storage system(s) are configured and storage path available on the OS servers.

On this test setup, the N series storage system status and volume details were checked before configuring Enterprise Vault. Remember to enable the N series product licenses such as CIFS, FC, and iSCSI protocols. 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. The SnapDrive software tool provides easier storage management capabilities. Network share configuration may offer some advantages in an Enterprise Vault environment. Configure additional N series storage systems, if needed.

On this test setup, the steps listed below were followed:

1. Create the appropriate volume size using IBM System Storage N series with FlexVol™ and IBM System Storage N series with RAID-DP™ configuration
2. Create the qtree
3. Create CIFS shares
4. Configure the network security
5. Map the network shares on the Enterprise Vault computer
6. Verify that universal naming convention (UNC) paths are accessible from the computer; the computer management tool was used, then “connect to another computer” was selected, and the N series storage system name (or IP address) was entered.

Creating a new vault

As mentionedpreviously, verify that the necessary storage configurations are completed and N series storage systems are available for creating a new vault store. Continuing the Enterprise Vault configuration wizard, select the computer on which the storage service for the new vault store is used. The following figure displays storage services configuration information.

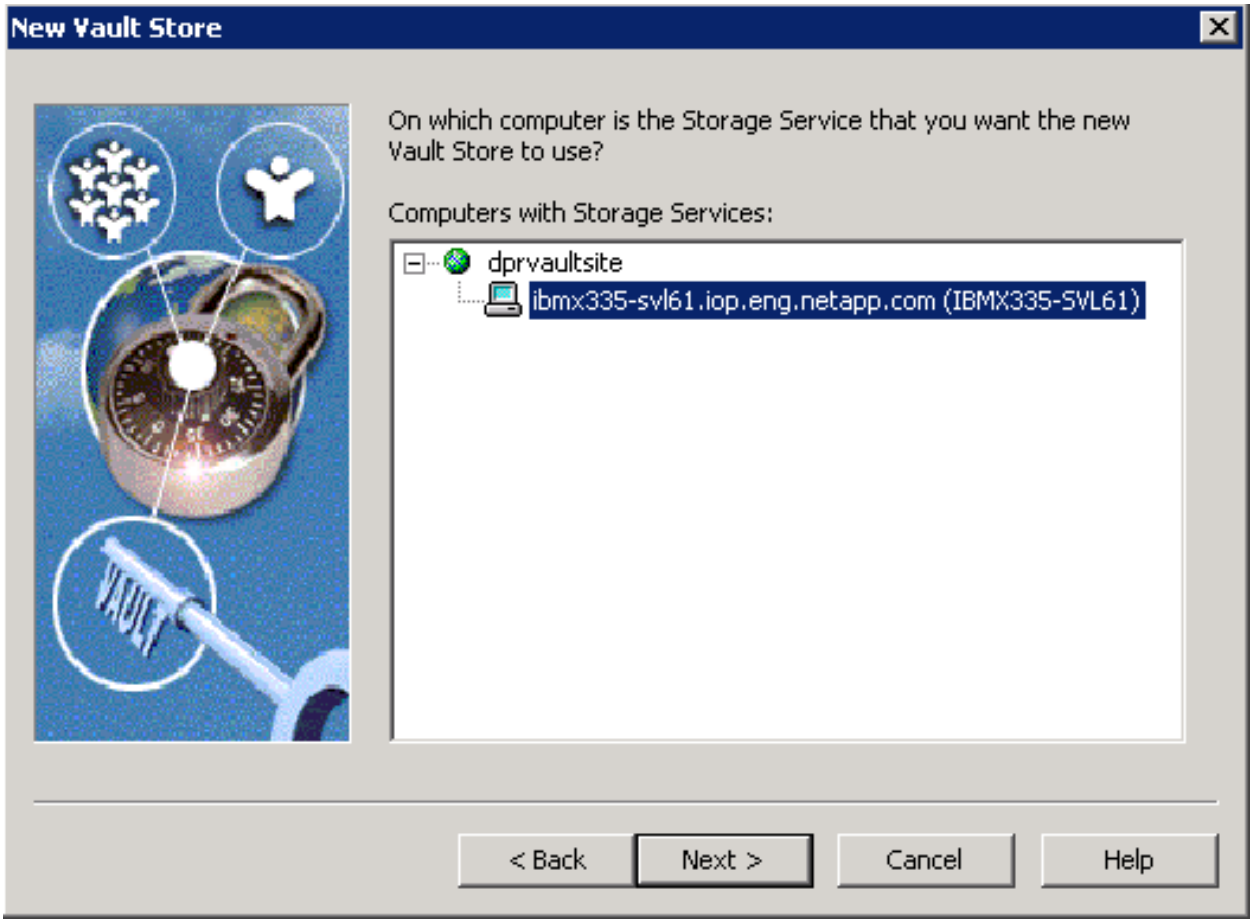

Figure 24) New vVault store configuration – selecting the computer for vault store partition.

A new vault store requires a name, and it is recommended that a meaningful name is provided to help in understanding the archival configuration. A vault store database requires the SQL Server information, and in this setup, the SQL Server location (IBMX335-SVL61) was provided.

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. A new vault store requires a SQL database location for database and transaction logs. On this setup, the SnapDrive created local disk path was selected, as shown below.

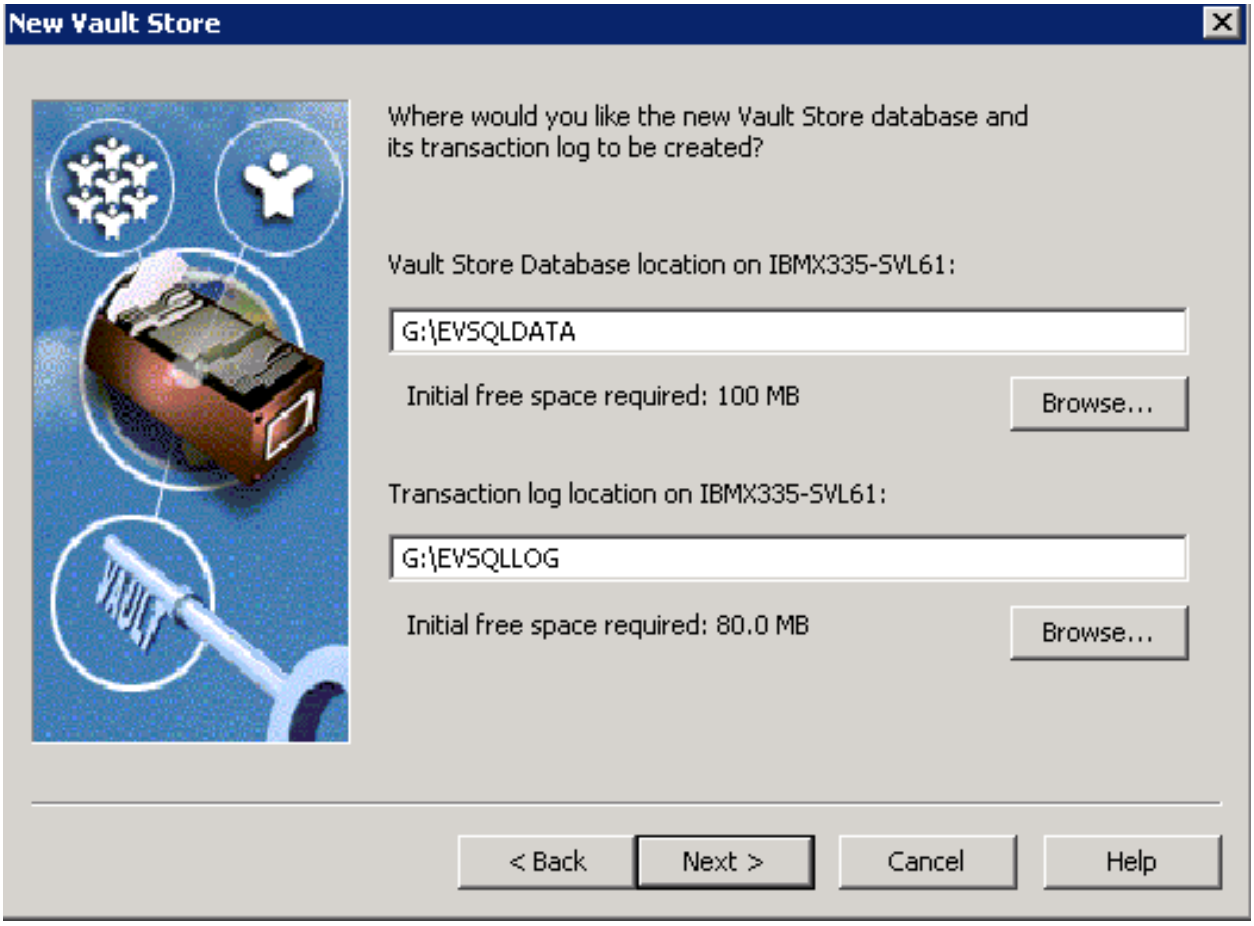

Figure 25) New vault store database locations – SnapDrive created local disk.

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

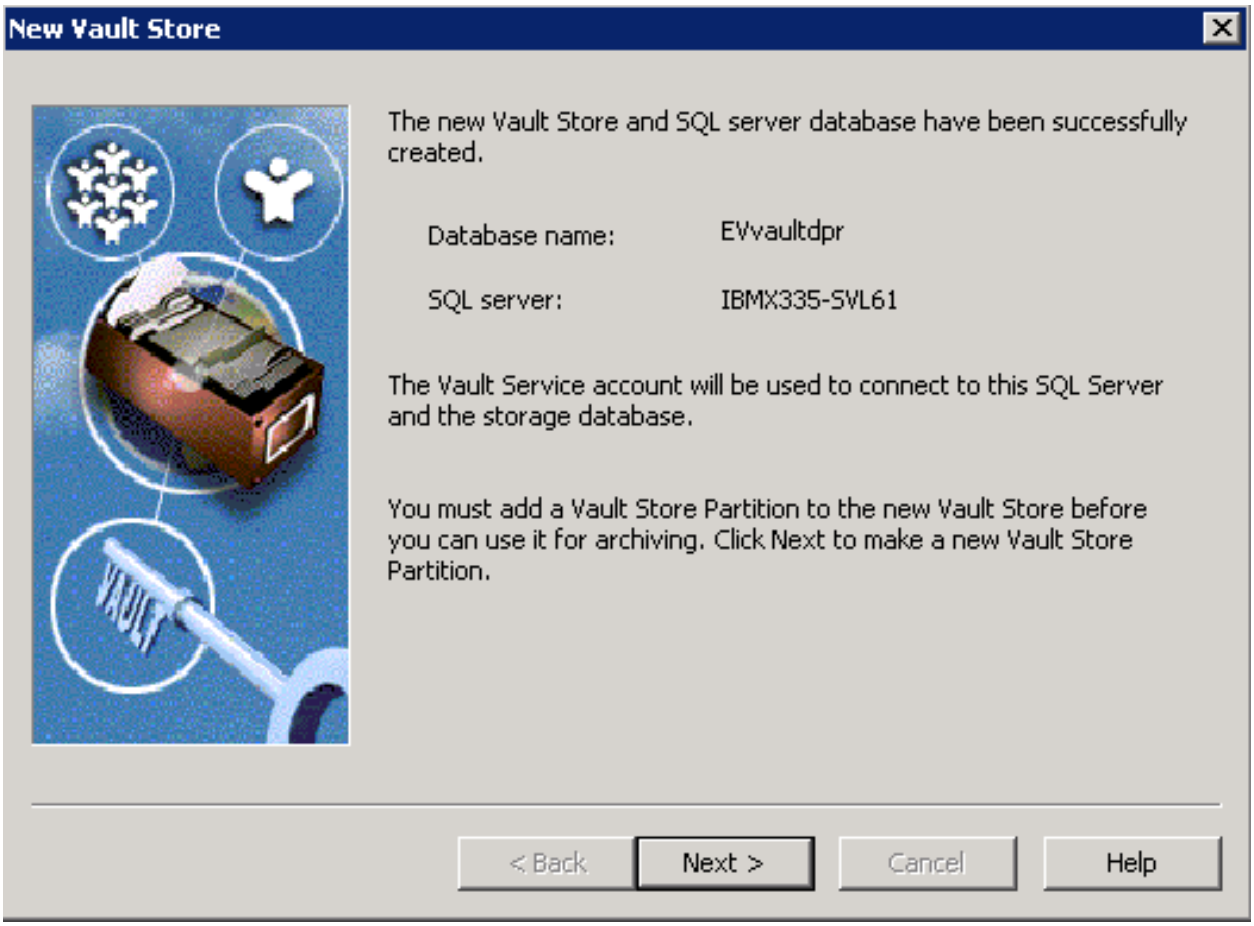

Figure 26) New vault created with database name EVvaultdpr.

Creating a vault store partition using an N series 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 N series storage system's volume(s). Use the Enterprise Vault administration console to start the new VSP create wizard. Only one partition should be opened at any given time. Provide the VSP name and description. The following figure shows the new VSP name and description provided in this test setup.

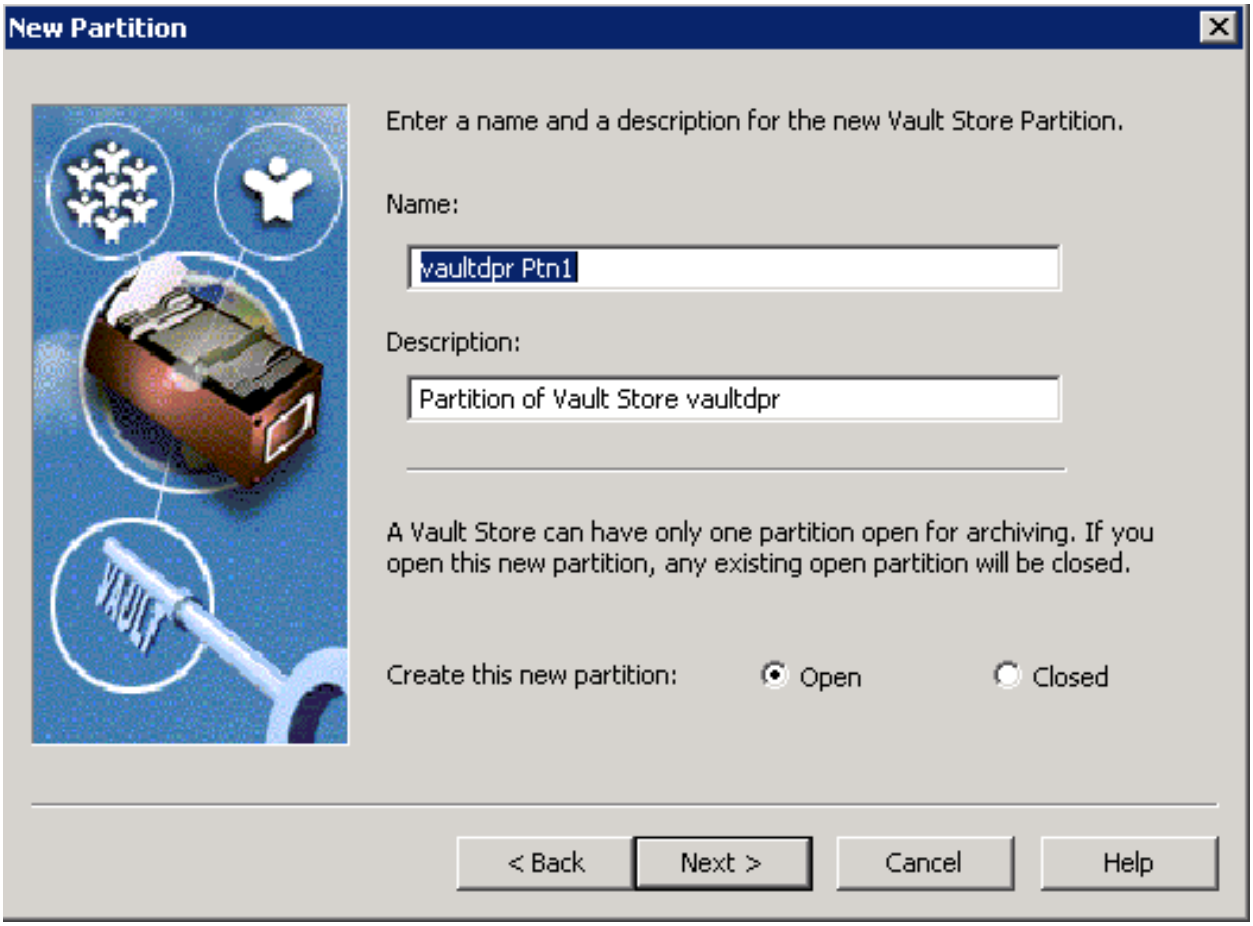

Figure 27) New VSP.

Continue with the creating new partition wizard and select the appropriate option for your storage system. If you select the NTFS system, N series will configure the volume as a network share or as virtual local disk (network shared drive). For compliance purposes, select N series SnapLock volume. This procedure was followed to create a new VSP:

1. Create the appropriate volumes on N series storage system (N5500)
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 \\n5500-svl34\vs3, where vs3 is name of CIFS share
6. Create a folder at the root of the mapped drive (fFor example, a folder called “store” on the mapped drive).

The following three figures demonstrate the procedure described above to create a new VSP. It is important to note that at least one directory must be present above the CIFS SharePoint level. To

meet this requirement, create a folder at the root of the SharePoint. If you are planning to provide the UNC path, verify that a folder exists at the SharePoint level. This requirement is similar to network share environment. In this test setup, the NTFS volume was selected for the mapped drive to specify the network path connectivity to the N series configured storage path. The following figure shows the selection of network configuration.

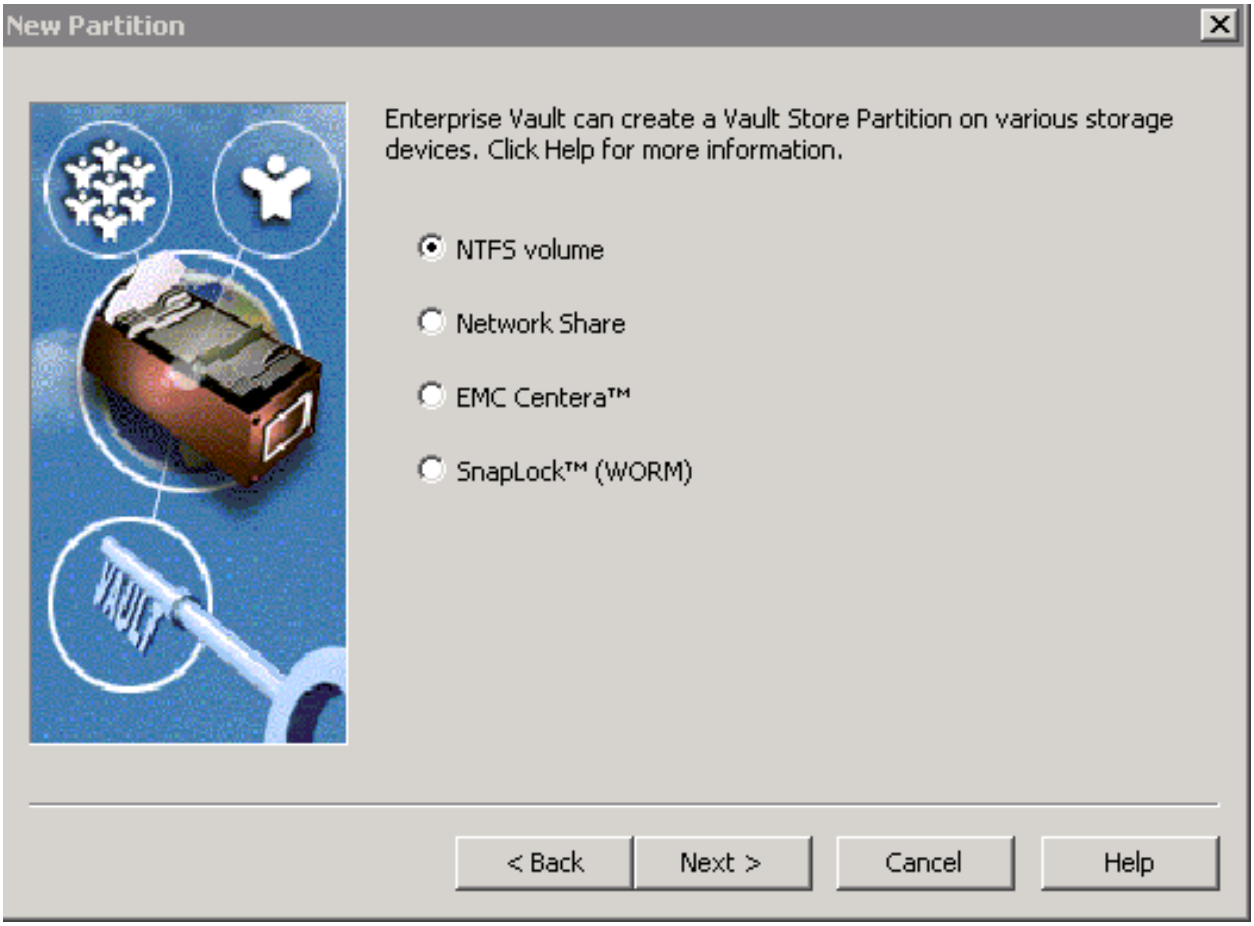

Figure 28) VSP on N series system.

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 VSP.

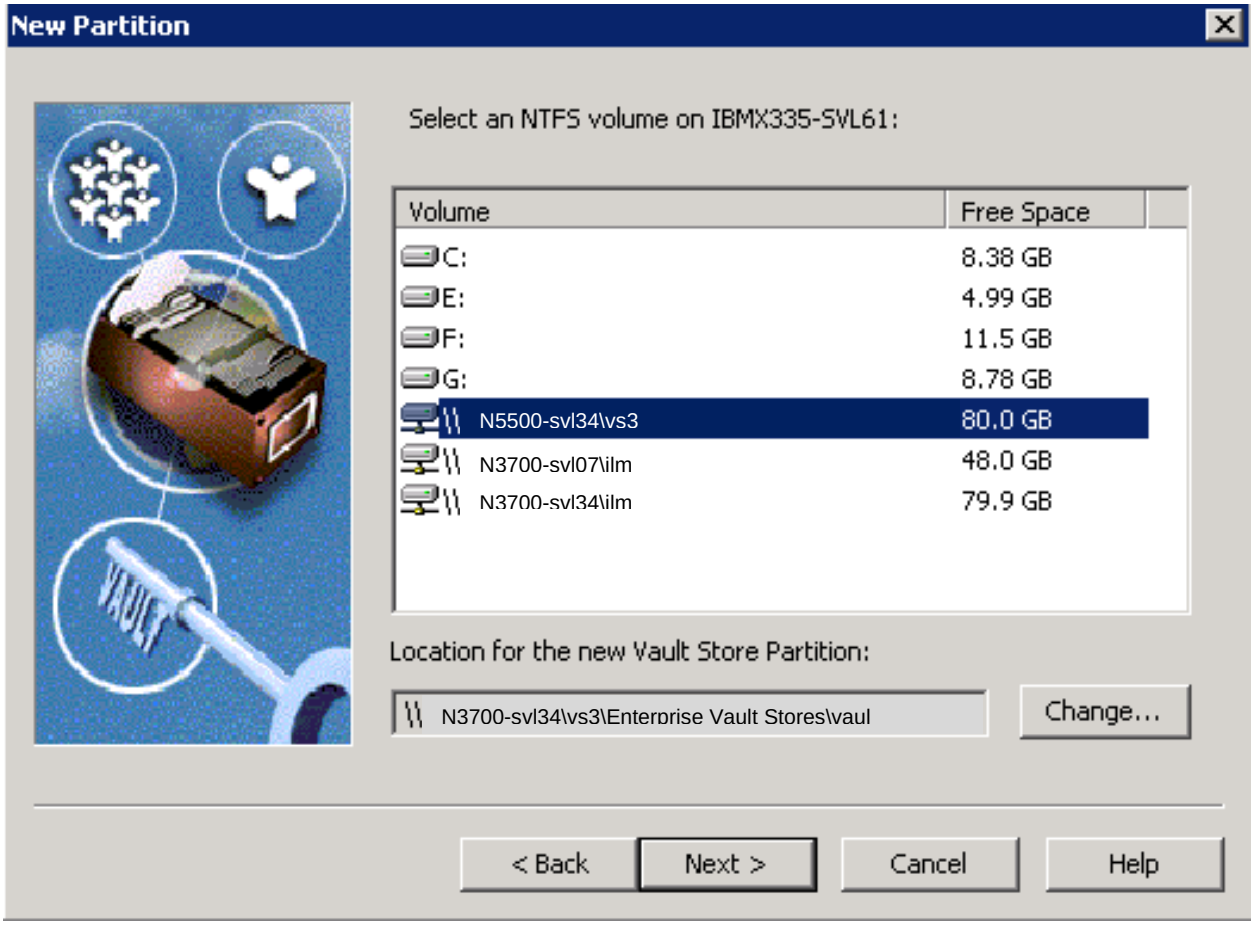

Figure 29) Storage location for the new VSP.

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

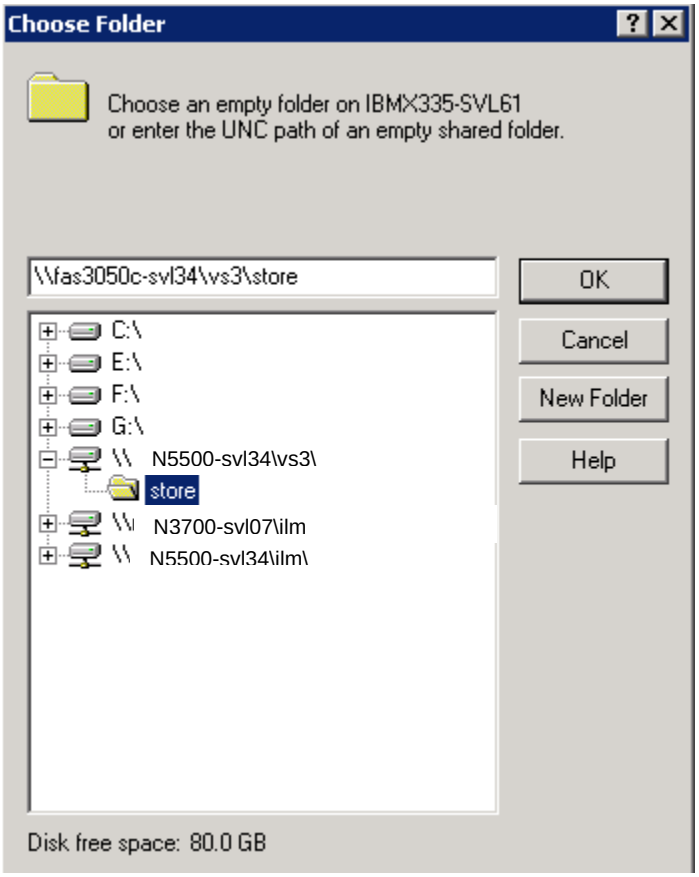

Figure 30) Selecting VSP storage location.

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 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 what choice(s)
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 \\N3700-svl07\ilm\store2
9. After this, complete the VSP and verify that the new VSP 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) VSPs for vault store "vaultdpr" after creating a closed VSP.

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. A prior section 4.3.3.3 described the procedure to create a new vault store, whereas another section explained the steps to create a new VSP. Vault store and VSP must exist before enabling the mailboxes for archiving. A vault store supports multiple VSPs. At any given time, only one VSP is active, and the remaining partitions are closed. This section discusses the procedure required to set up the Enterprise Vault archival.

Create organizational unit and archive task

Using the Enterprise Vault administration console, add an Exchange organizational unit, Exchange Server, and task controller service. An 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 this setup while creating a new organizational unit.

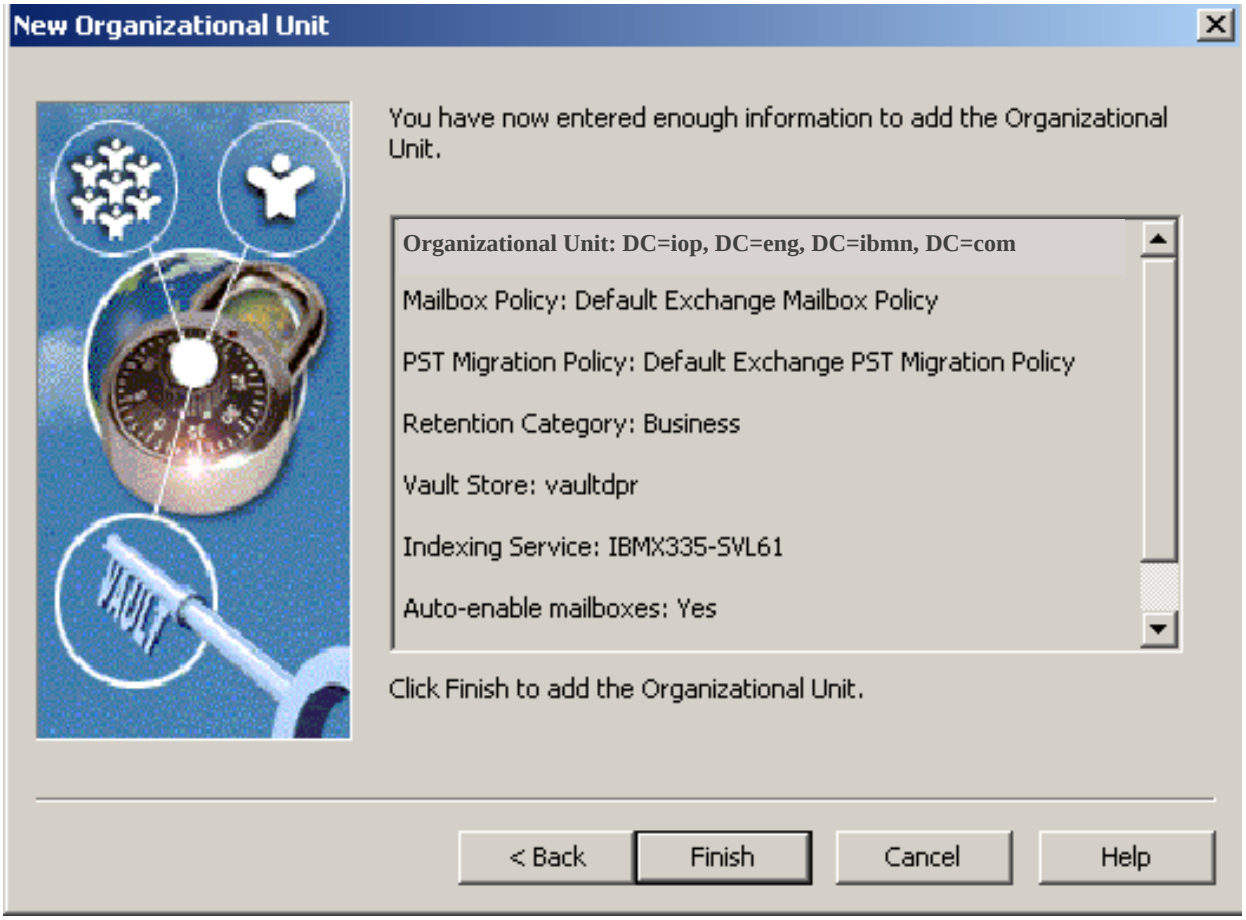

Figure 32) Creating a new organizational unit.

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 this setup, a new retention category called “datacompliance” was created 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 to include the 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 the setup was as shown below.

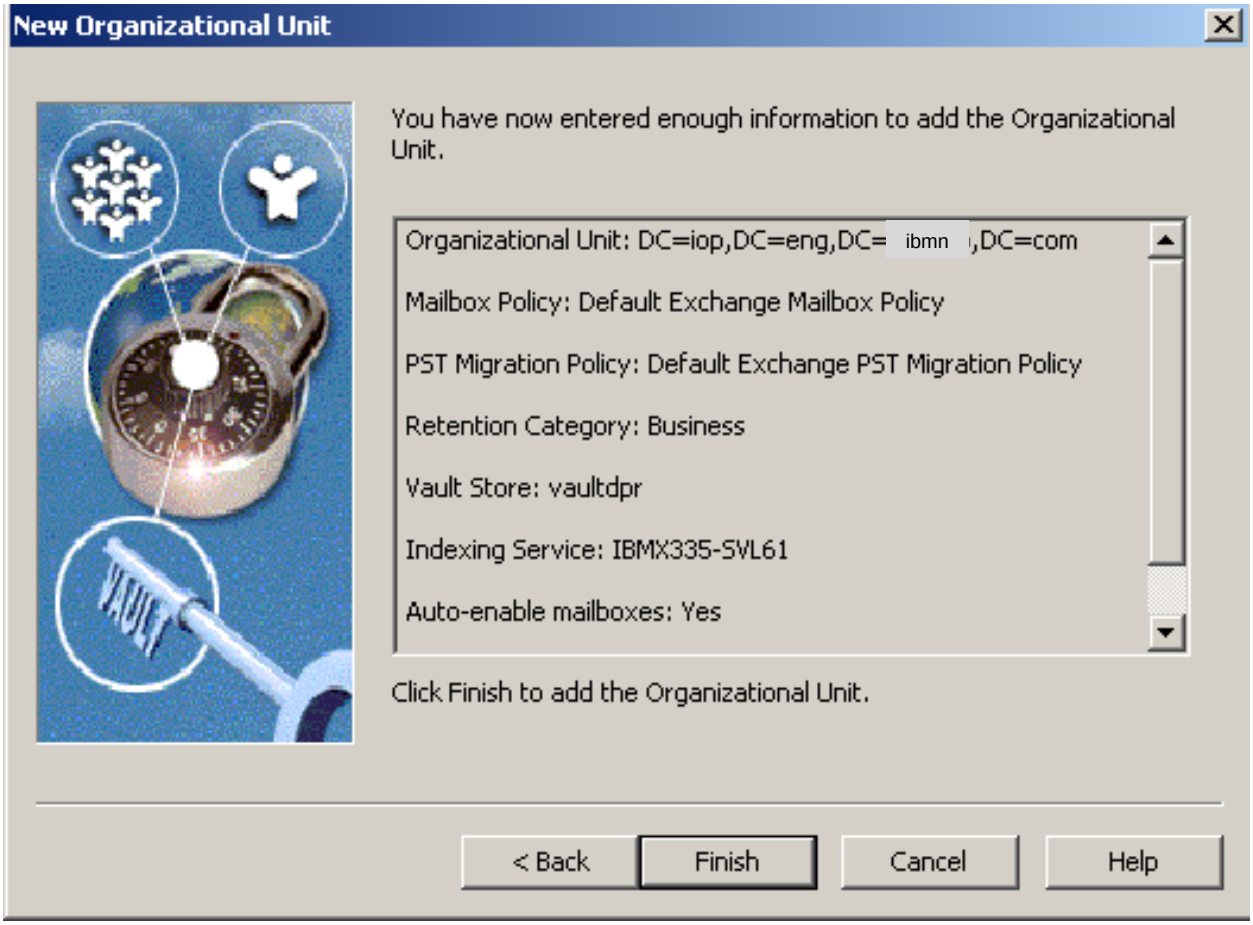

Figure 33) Adding a new organizational unit.

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 this test setup, a new public folder archive task was created, as shown below.

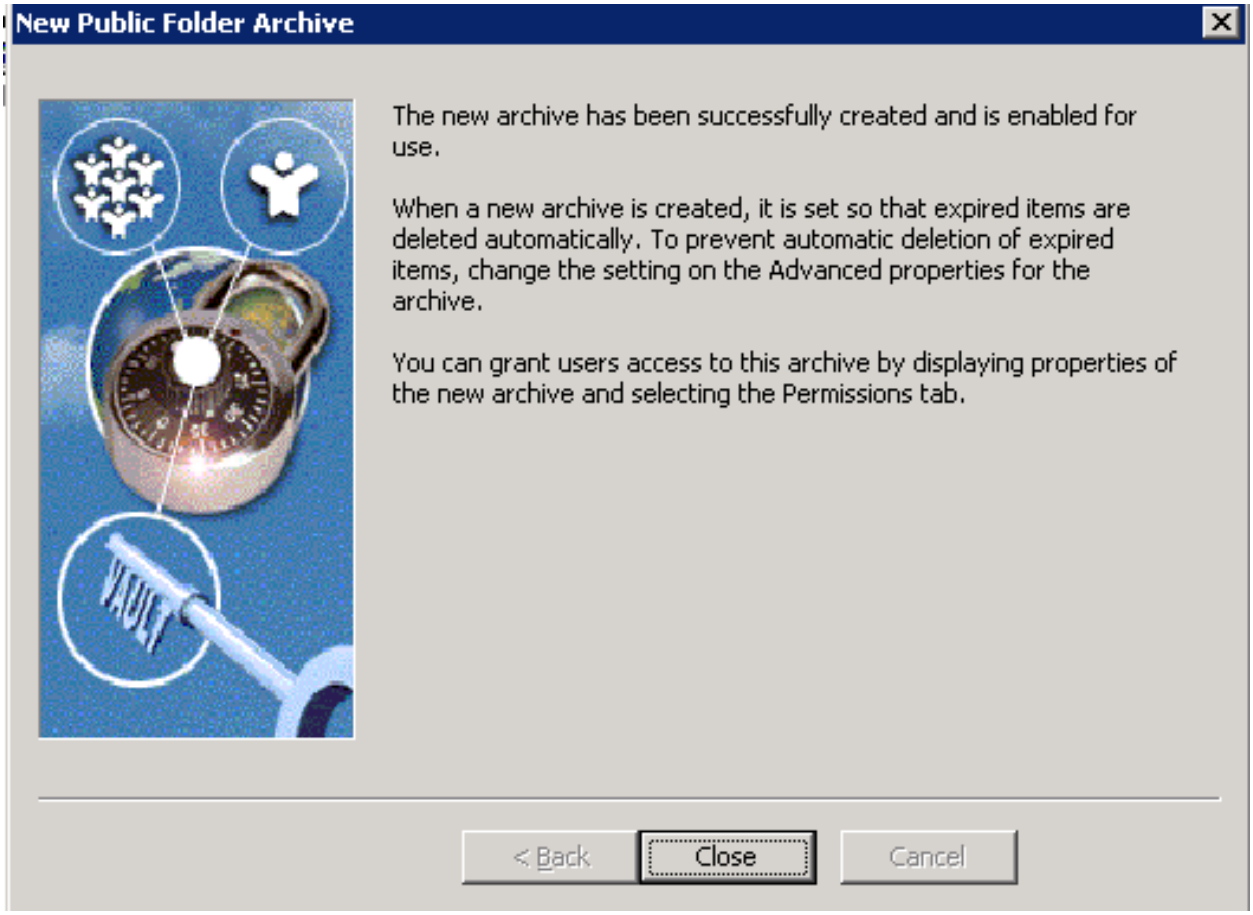

Figure 34) Creating a new public folder archive task.

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

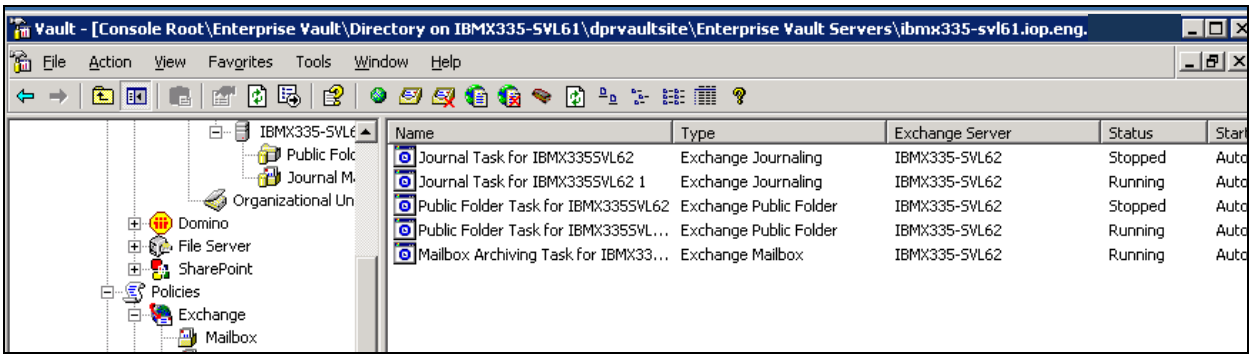

Figure 35) Archive tasks created.

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 SharePoint portal data. This section briefly discusses the procedure to configure an FSA component. Enterprise Vault supports file archiving with two 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. For additional information, refer to documentation available on the Symantec Web site. Some possible Enterprise Vault configurations and installation strategies are listed below:

- One Enterprise Vault site for each Exchange Server site

One Enterprise Vault site for FSA.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, Exchange configuration is optional. Exchange Server configuration is required in an Exchange e-mail environment.

This section discusses the procedure to configure the FSA component of Enterprise Vault on N series storage system(s). This paper recommends analyzing the FSA requirement such as the server and storage requirements. The file placeholder service component of Enterprise Vault supports FSA. Refer to Figure 13 for installing the FSA component.

Verify that the necessary network connectivity is established between the OS server and N series 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 FSA. 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 FSA 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
    b. Verify Enterprise Vault has the FSA license enabled
    c. Program files → Enterprise Vault → file system archiving configuration
    d. Introduction --> vault service account details
    e. Verify that the advanced user rights are granted
    f. 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 FSA by selecting the placeholder configuration wizard. File placeholder service configuration is shown in the following figure for this 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 OS
- Debug programs
- Replace a process-level token.

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

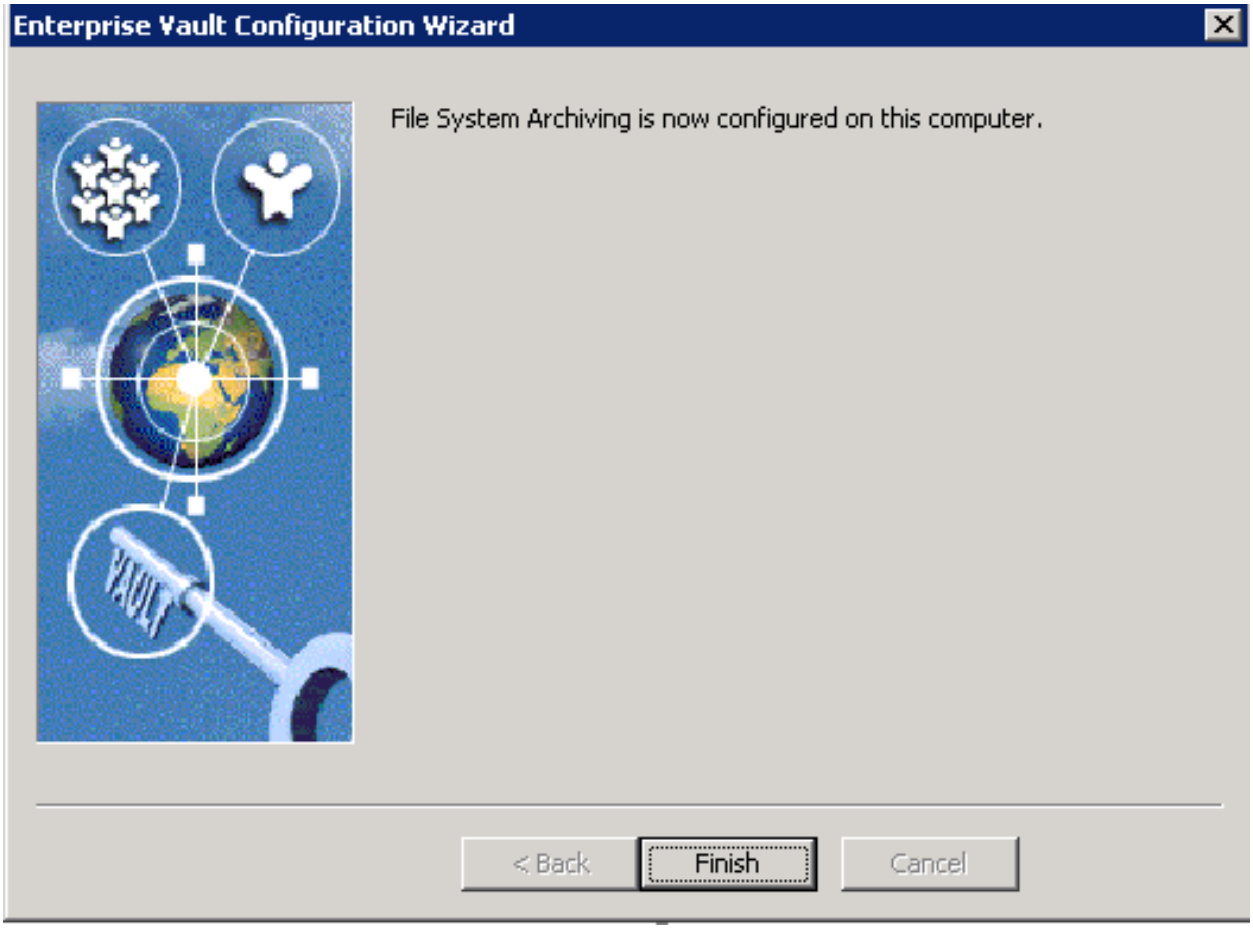

Figure 37) File placeholder configuration completion.

Having successfully configured the FSA, FSA 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 this test setup, the archiving policy name and description were entered as shown in the following figure.

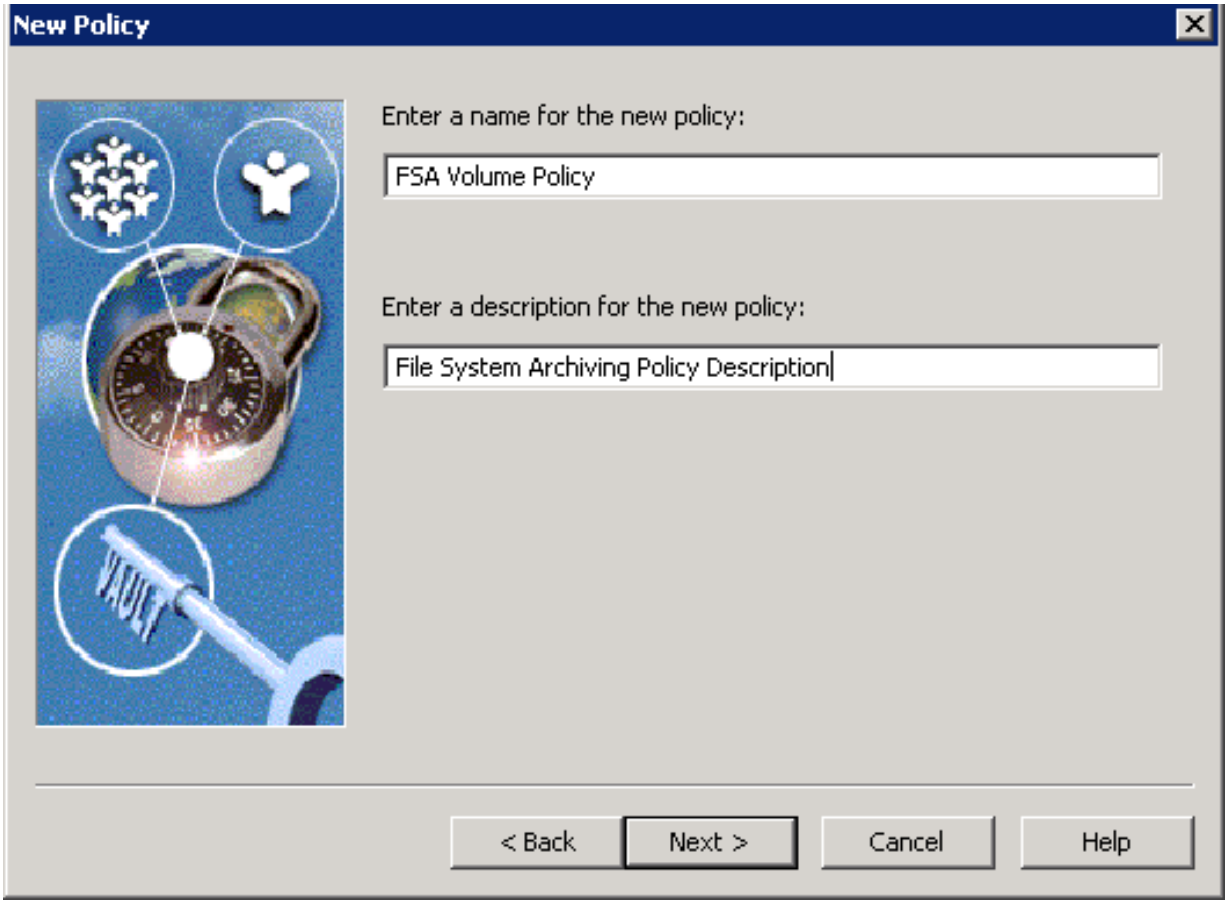

Figure 38) Creating a new volume archiving policy.

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. FSA applies to the permissions of the folder archived from the system. Change the settings if necessary while creating the rules.

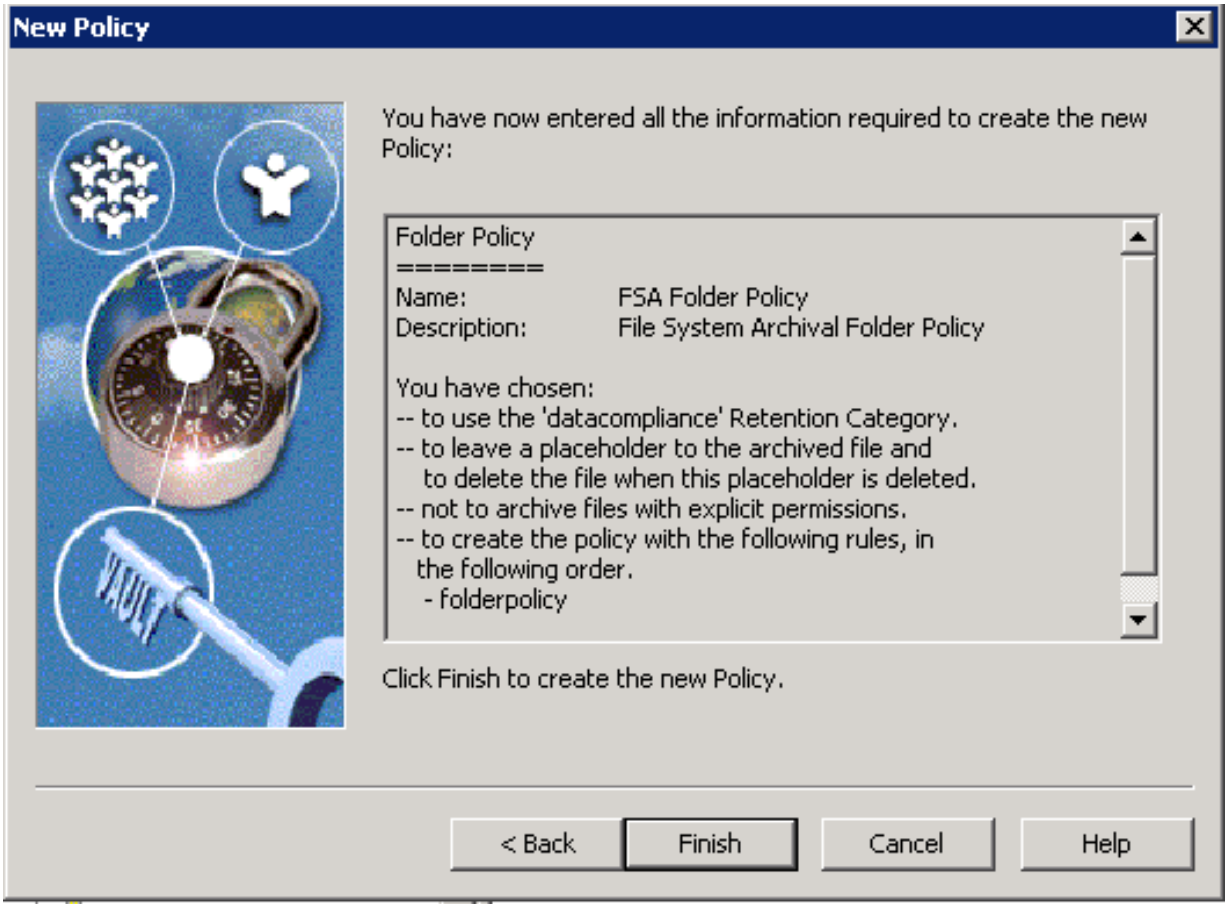

Figure 39) Information required to create the new archiving policy.

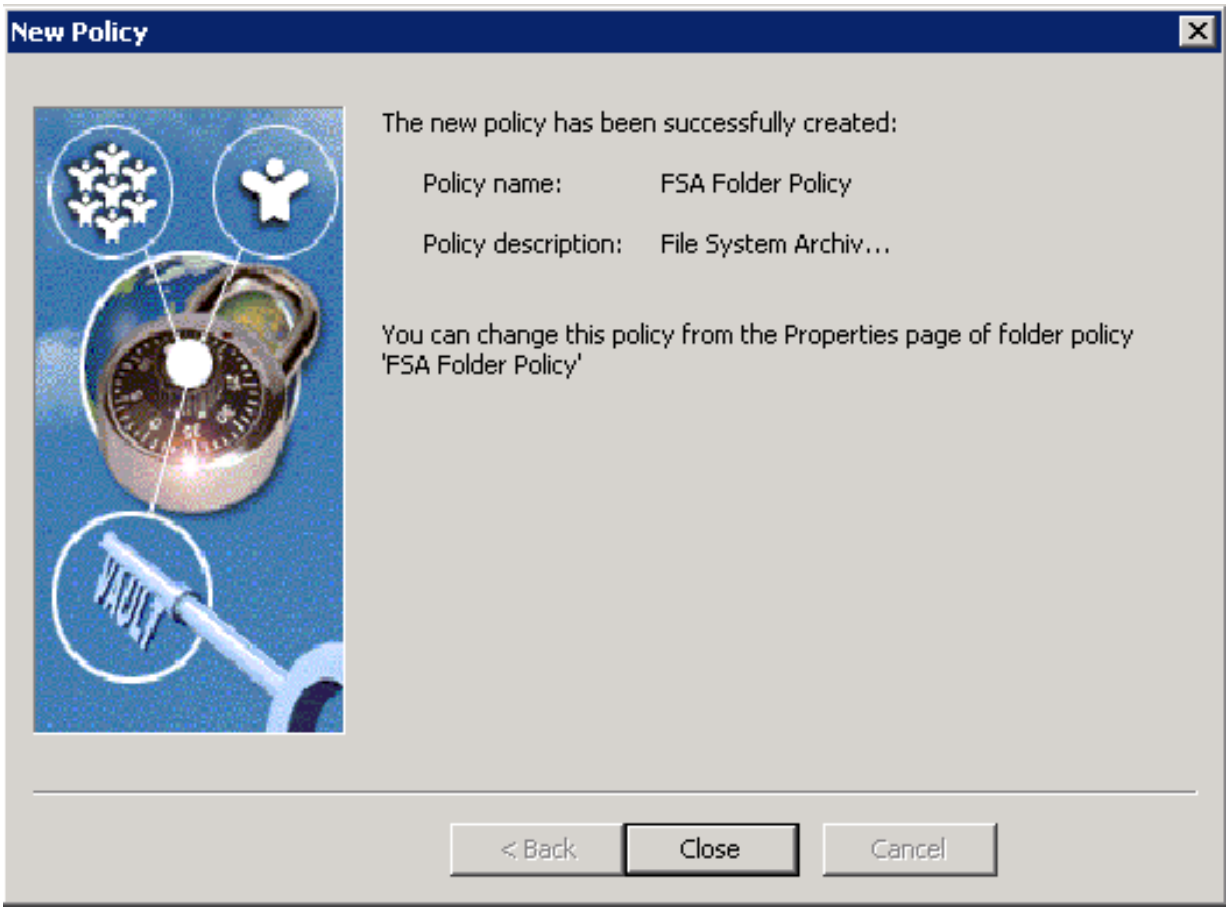

Figure 40) New policy for FSA.

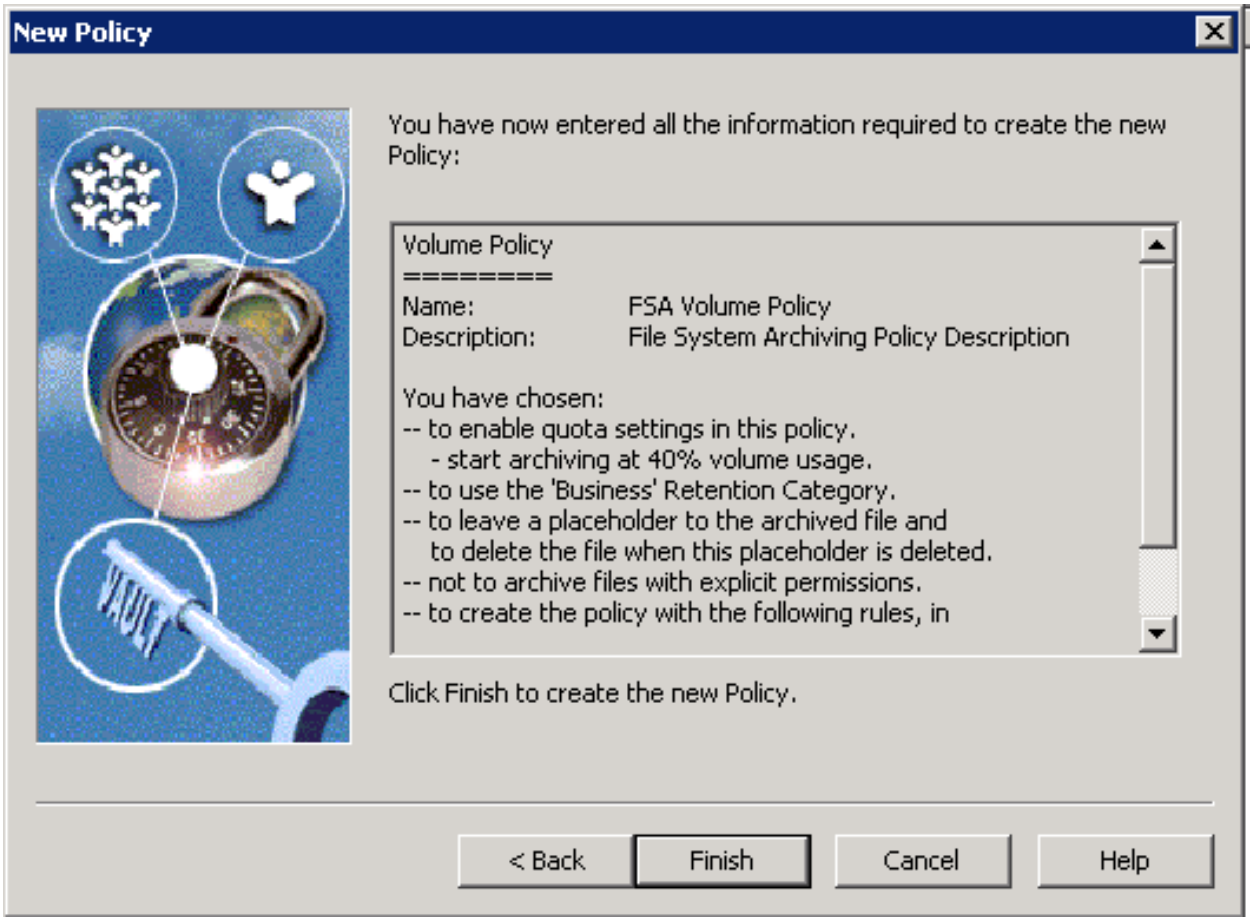

Figure 41) New archiving policy settings.

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.

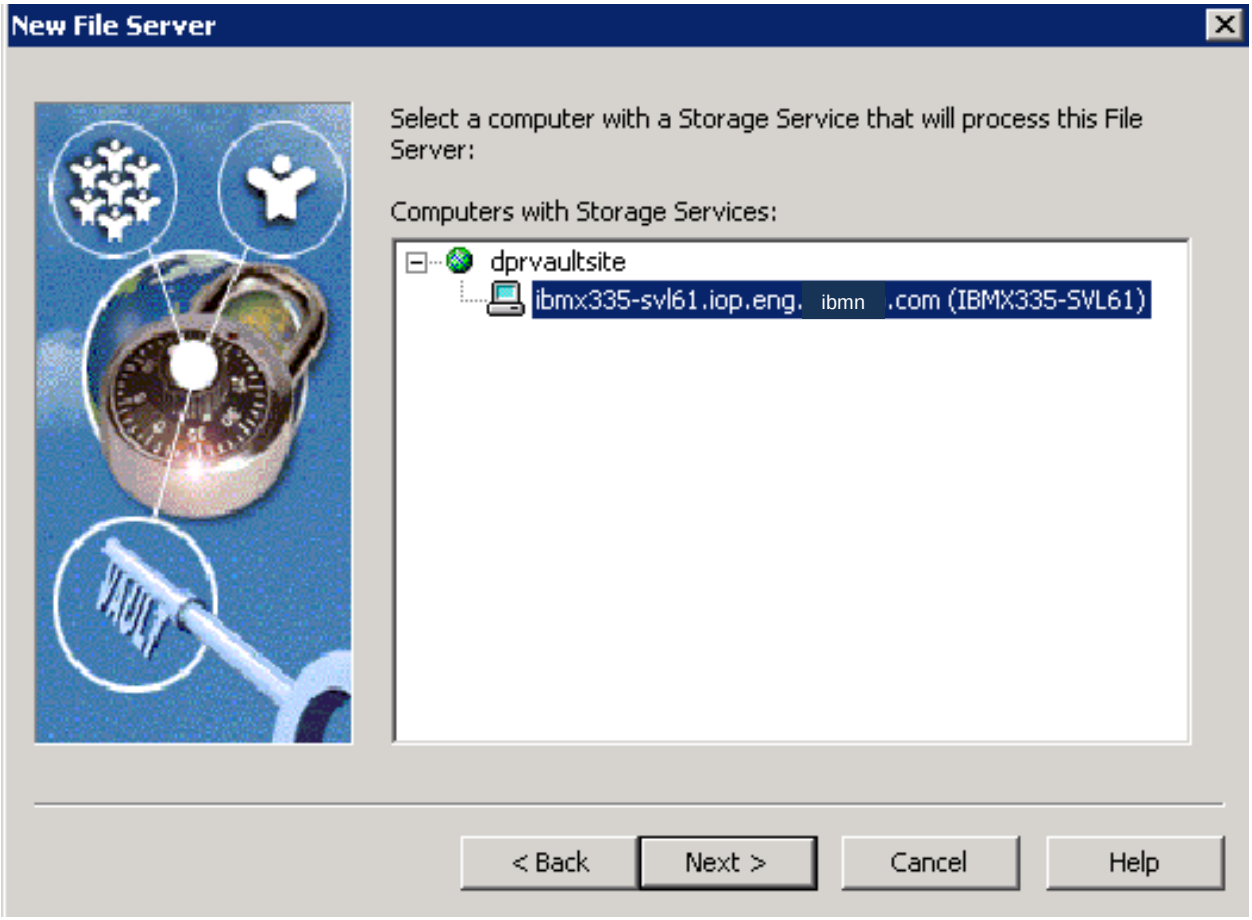

Figure 42) Selecting the computer running storage service.

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 N series 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 N series 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 FSA targets on this test setup.

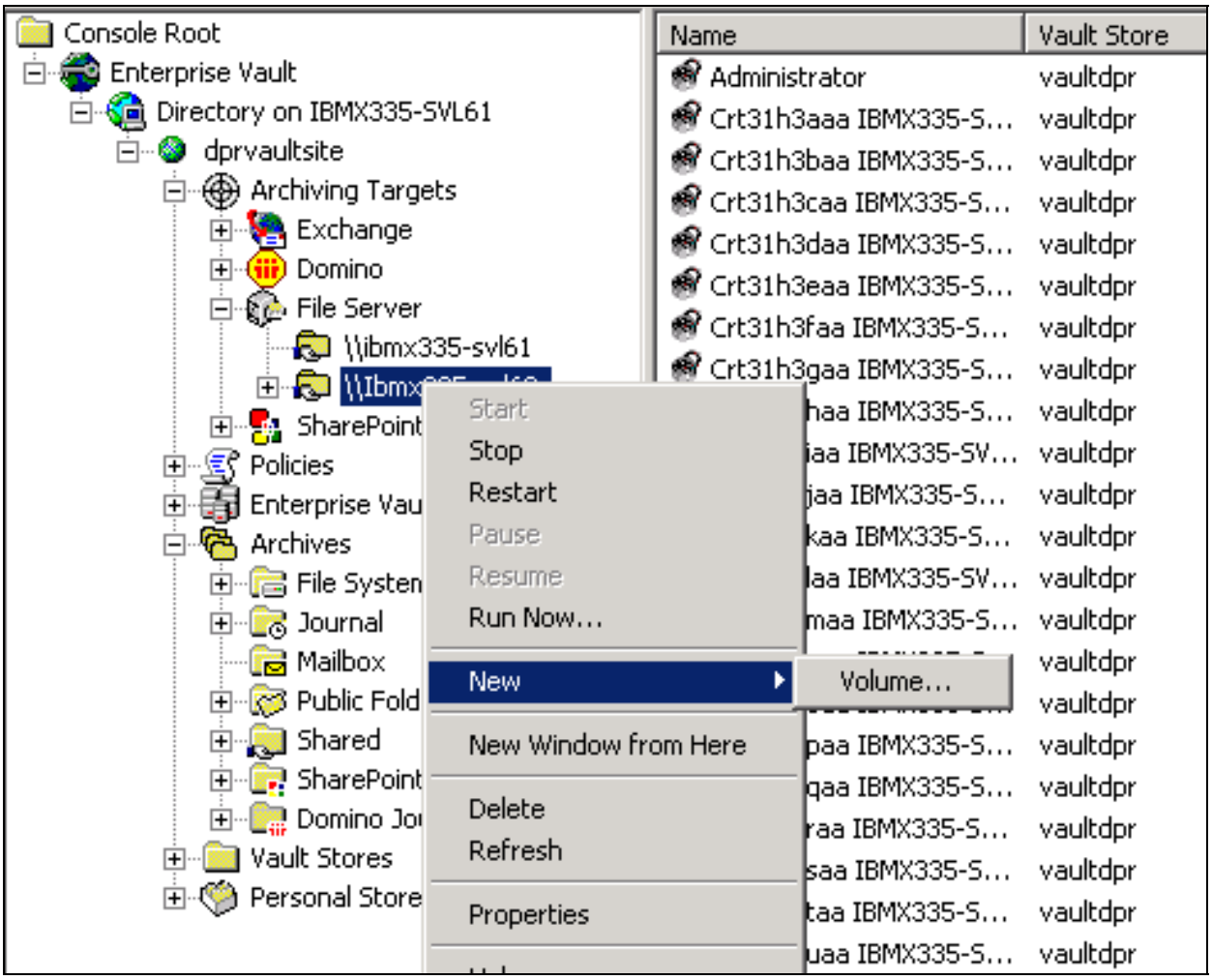

Figure 43) Creating a new volume for FSA targets.

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 this test setup, the following figure displayed information required to create the archiving volume.

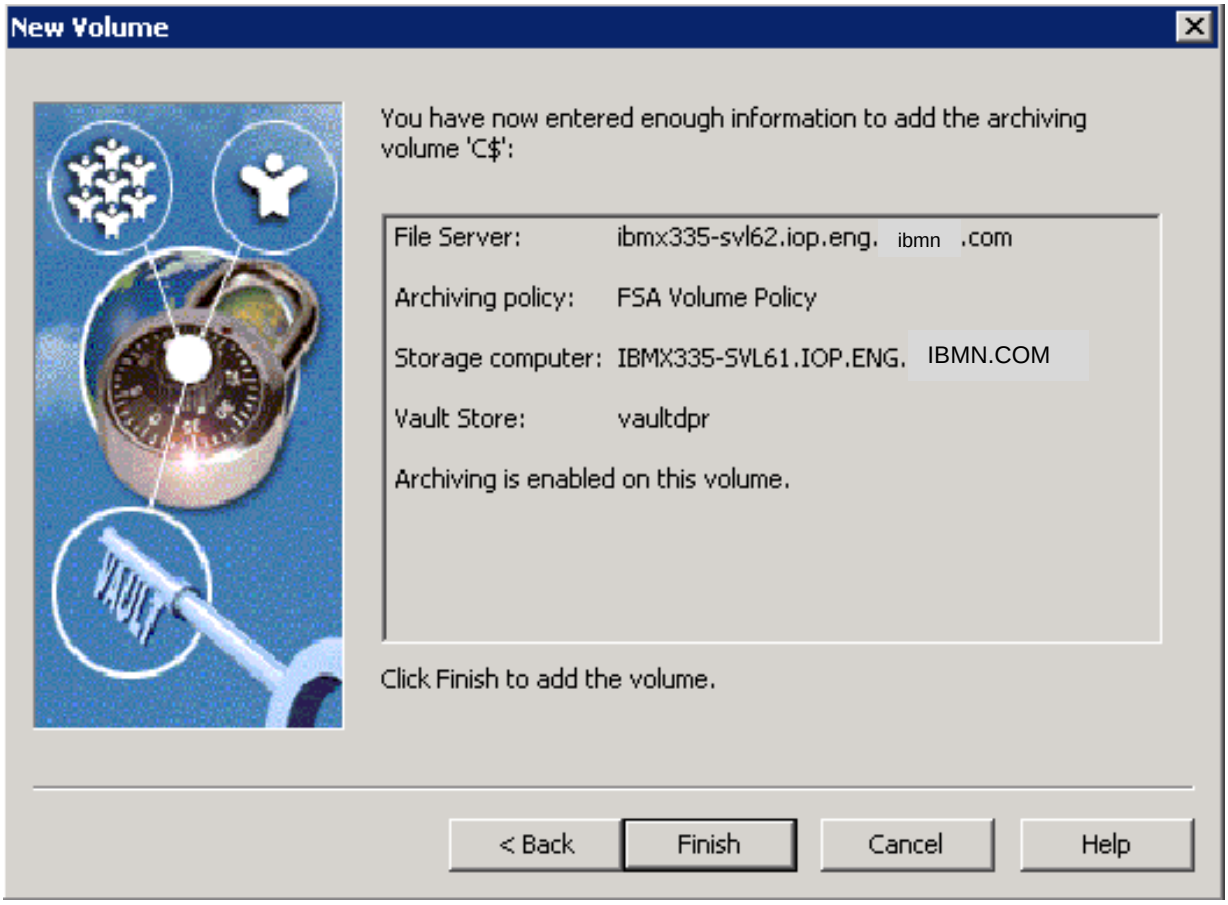

Figure 44) Creating new archiving volume for file server.

Create the necessary archiving targets for all the folders that require FSA. The following figure shows the available file server archiving targets on this 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.

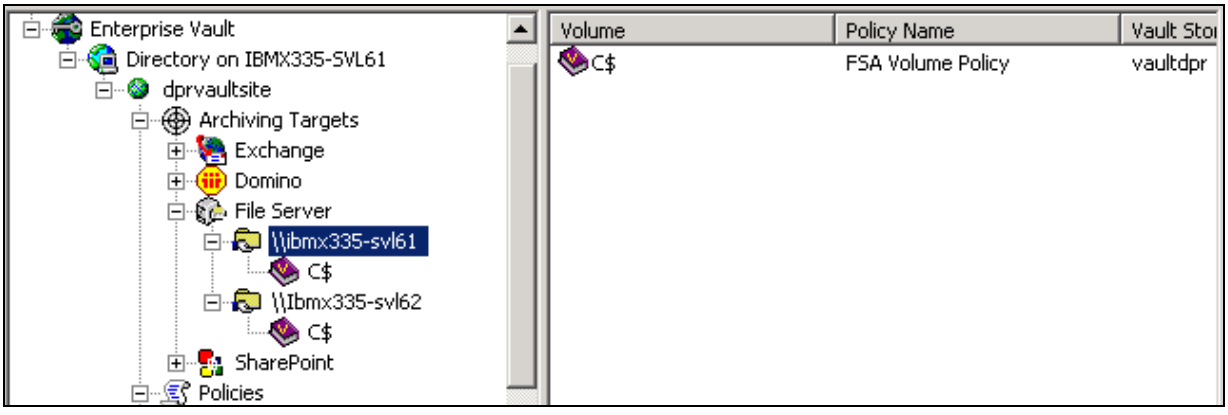

Figure 45) Available archiving targets on file servers (FSA).

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 N series storage systems, data can be archived onto a network share or as configured local disks. Using N series with SnapLock, data archived by Enterprise Vault achieves the compliance goal. This paper discussed the procedure to deploy Enterprise Vault Server with N series storage systems. This paper covered the topics to configure the SAN as well as NTFS file systems. Storage configured as virtual local disks was used to install and configure Exchange Server, SQL Server, and Enterprise Vault Server. Enterprise Vault used N series storage systems configured as network shares for archiving the data from the primary to secondary.

At the time of this report writing, 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.

Enterprise Vault with IBM N series storage solutions effectively addresses the shortcomings. Symantec Enterprise Vault and the N series 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.

IBM N series and Symantec are committed to providing Enterprise Vault users with superior solutions designed to meet business objectives. N series storage system solutions ensure protection of Enterprise Vault data available 24x7.

IBM N series 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 snapshots created with SnapManager for SQL Server. 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 Enterprise Vault in an N series environment. To ensure a supported and stable environment, become familiar with Enterprise Vault and N series storage systems. During the design phase, involve Exchange and SQL Server specialists along with Enterprise Vault experts. This paper strongly recommends seeking professional help from respective vendors.

Caveat

All possible combinations of hardware, storage architecture, and software solutions have not been tested. 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.

Appendix

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

OS required patches

The section lists the hot fixes that must be installed before configuring the N series storage system using FC 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 FC protocol environment, the following Windows hot fixes are required on Windows 2003 SP1 Server:

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

Trademarks and special notices