Technical report:

Symantec Enterprise Vault and IBM System Storage N series with SnapLock

Best-practice integration

Document NS3501-0

January 22, 2008

Table of contents

Abstract

Increased acceptance of electronic communication requires an efficient method of storing and managing the data. For legal and compliance purposes, enterprise customers require electronic data be archived and safely secured. Regulations require requested data be collected within a reasonable time. The Symantec Enterprise Vault application enables an organization to store messages and file system data onto central archives. Managing semi-structured data as well as unstructured data (file system) is a challenging task for enterprises. By deploying Enterprise Vault with IBM N series storage system(s), electronic data can be archived to meet compliance regulations using IBM System Storage N series with SnapLock features and capabilities. This paper covers solution deployment aspects, including the procedures required to configure Enterprise Vault and to set up IBM N series with SnapLock archival procedures.

Introduction

In addition to e-mail archival, the file-system archival (FSA) feature of Symantec Enterprise Vault™ allows the Enterprise Vault Server to archive and manage file system data. Enterprise Vault offers efficient ways to manage and intelligently archive e-mail and file-system data.

By taking advantage of the strengths of an IBM® System Storage™ N series solution in combination with Enterprise Vault, enterprise customers can fully address information life cycle management issues. This paper discusses the procedure to integrate Enterprise Vault Server with IBM System Storage N series with SnapLock® solutions.

Background on technical issues

A number of regulations enacted globally mandate content archiving along with the ability to produce specified data in a timely manner. In addition to compliance purposes, companies are adopting policies to protect their data. While many policies focus on e-mail data, a large percentage of enterprise data is file-system data. There is a business need to manage file-system data efficiently by archiving it onto a central archiving device that provides a data-indexing capability. Joint solutions from IBM N series and Symantec Enterprise Vault address such issues.

Purpose and scope

The purpose of this paper is to demonstrate the procedure to configure Enterprise Vault and IBM N series storage systems. This paper assumes that Enterprise Vault and IBM N series storage systems are installed and that you are ready to configure the Enterprise Vault store and vault store partition. This paper recommends that you refer to appropriate installation and configuration materials.

Infrastructure

This section describes the necessary infrastructure in the Enterprise Vault environment. Enterprise Vault is supported in the Microsoft® Windows® environment. In addition to using appropriate operating systems, it requires a supported version of a relational database product from Microsoft and Exchange server products. Even though Enterprise Vault supports compliance, it relies on a storage system solution for retaining the data. This paper shows steps to configure the IBM N series with SnapLock feature to archive compliance data.

At the time of this writing, Enterprise Vault requires Microsoft Windows 2003 or Windows 2000 Server. Microsoft SQL Server 2005 or 2000 is supported. It also requires Microsoft Exchange 2003 or 2000 Server for mailbox management. IBM Lotus® Notes® journaling feature is supported at this time. Microsoft SharePoint Server is required if the SharePoint Portal archiving feature is used. If Enterprise Vault Server is configured just for archiving the file system data, the use of Exchange Server is not required.

As a best practice and for supporting reasons, it is important that enterprises use either a storage-attached network (SAN) using the fibre channel (FC) protocol or an Internet protocol (IP)-based storage area network (IP-SAN) configuration for installing the SQL server and Exchange server in addition to installing Enterprise Vault. IBM System Storage N series with SnapDrive® software improves storage management. IBM System Storage N series with SnapManager® for SQL Server makes it possible to address SQL server backup and restore needs. Similarly, SnapManager for Exchange server helps in Exchange server systems.

In our test setup, we used the following inventory:

- Windows 2003 Service Pack1 Enterprise Edition for Installing Exchange Server
- Windows 2003 Service Pack1 Enterprise Edition for Installing SQL Server and Enterprise Vault Server
- An IBM N series N5500 storage system with Data ONTAP® 7.1.1 for archiving e-mail and FSA data
- An IBM N series running Data ONTAP 7.1 for SAN configuration
- An IBM N series with NearStore running Data ONTAP 7.1 for archiving e-mail and FSA data (and for migrating service),
- SnapDrive software product version 4.1 for storage management
- SAN storage software product – Host Attach Kit 3.0
- Emulex LP9002L fabric-attached adapter card and HBAnywhere software.

Infrastructure-related tasks

To install the SAN host attach kit software, follow the appropriate installation guide. Additionally, SAN Manager software, including Operations Manager, may also be installed. SAN Manager provides end-to-end FC SAN management that enables IBM N series users to securely discover, monitor, and manage their enterprise storage infrastructure. If an Operations Manager Server is required, you should also upgrade the host bus adaptor (HBA) driver and firmware.

SnapDrive software installation

After installing SAN HBA software, prepare for installing the SnapDrive software. Verify that the HBA has the supported version of the driver and firmware; upgrade the driver and firmware, if necessary.

SnapDrive supports both FC and iSCSI protocols. It allows the ease of dynamic storage management. For installing SnapDrive software, refer to the appropriate installation guide. This paper suggests that any IBM N series storage system connected to a host needs to reside in the same broadcast domain as the Windows server. This configuration will avoid the need for traverse router hops.

Microsoft SQL Server

Enterprise Vault requires Microsoft SQL Server 2005 or SQL Server 2000 SP3. For a large Enterprise Vault environment, a dedicated SQL server on a separate Windows server is recommended. If the IBM N series SAN or IP-based SAN storage configuration is used, this paper suggests using SnapDrive, a storage management utility. SnapManager for SQL Server allows database backup and recovery easily. In a production environment, several scenarios cause the Enterprise Vault index to be corrupted. Although this corruption is not common, still there exists a possibility. In case of index corruption, the administrator has to restore the data from the backup using SnapManager for SQL Server and SnapDrive if required.

Domain users account information

Enterprise Vault installation requires Domain Administrator privilege and an administrator user in the domain. This administrator should have the domain administrator privilege. On our test setup, we used a domain called “IOP” and created a user called ‘evadmin’.

Mapping the network share

Enterprise Vault requires an NT file system (NTFS)-supported file system as the archival destination. This includes local disks, configured virtual disks (with or without SnapDrive) using IBM N series storage systems or a network-mapped share. Network connectivity between Enterprise Vault Server and IBM N series storage systems must be configured. Once the network connectivity is established, create a volume of the desired size. Data ONTAP 7.1 or later provides greater flexibility in storage configuration to define and configure volume sizes. It also allows for scaling the storage dynamically. Depending on the need and growth of data, a particular volume can be expanded or shrunk.

Before creating a network share, verify that a common internet file system (CIFS) license is enabled and the CIFS setup is complete. On our test setup, we used two storage systems, one IBM N5500 system, and another IBM N series with NearStore system. On each system, we created the necessary CIFS shares. On our N5500 system, the following figure shows the CIFS shares created.

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

Figure 1. CIFS shares created on IBM N series storage system for Enterprise Vault archival.

Configuring Write Once, Read Many storage using SnapLock software

In order to successfully archive and retain the contents in its state as read-only for the specified time, a volume with SnapLock license must be configured. On the IBM N series storage system, the appropriate SnapLock product license must be enabled. Currently, there are two types of supported SnapLock features. The SnapLock license supports a stricter version of compliance volumes where the file cannot be disposed until the retention period expires. Another version of the license, known as SnapLock for Enterprise, allows the storage administrator to have the control over that volume. To create a SnapLock volume, you may follow these steps:

- Create a Snaplock supported aggregate on the IBM N series storage system (use the storage system console to create a Snaplock aggregate). An example of a command to create an aggregate is as follows:

  ```
  aggr create <aggrname> -r <raidgroupsize> -t <raidgrouptype> -L
  [<snaplock> or <enterprise>] <number of disks>
  ```

  Where: raidgrouptype is either raid_dp or raid4.

- Create a Snaplock volume using the previously created (Snaplock) aggregate.
- Create Qtree on this volume (If needed).
- Create a CIFS Share on the Snaplock volume.
- Verify that network security is enabled to run rsh from the Windows server.

Enterprise Vault Server architecture

Enterprise Vault is comprised of Vault Directory and a Vault Store database that uses SQL server databases to hold the Enterprise Vault configuration data and information about the archives. Windows services and tasks perform background tasks. These tasks include scanning servers for items to be archived, storing the items in archival, indexing item attributes, and retrieving the content from archives.

The Enterprise Vault architecture includes Windows servers, Microsoft Exchange server(s), a Microsoft SQL Server, Enterprise Vault Servers, a Lotus Domino® Server (if the Notes Journal feature is used) and the necessary storage system. In this architecture, three IBM N series storage systems were used, one to configure the SAN system and network shares for archiving the contents using Enterprise Vault on another IBM N series and an IBM N series with NearStore systems. This test setup used nearline secondary storage (the NearStore feature) to move the items after archiving for a specified time. This architecture lets items be migrated from the primary storage destination to the secondary storage destination.

Enterprise Vault tasks perform a search and return 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 provides the HTML version of the item.

IBM N series Storage Systems

It is important to plan a careful architecture of Enterprise Vault regarding storage configuration. Enterprise Vault requires either local disks or virtual local disks for installing the SQL server, Enterprise Vault and Microsoft Exchange server. Either a SAN or an IP-based SAN satisfies the requirement. The necessary software and hardware configuration topics are discussed in earlier sections of this paper. In the test setup, we used an IBM N series storage system to configure local disks on both the Exchange server and

Enterprise Vault Server. For the archival destination, we used an IBM N series cluster configuration and an IBM N series with NearStore nearline storage to migrate the items after a specified period.

Configuration

The Enterprise Vault configuration requires the storage system to be presented as an NTFS file system. This includes the NTFS volume, the Network Share, and the IBM N series with SnapLock-enabled volume. Data may be migrated to secondary or tertiary locations. The Enterprise Vault configuration requires Vault Directory Database (VDD) to install the Enterprise Vault components.

Operating system information

Enterprise Vault is a Windows application. Enterprise Vault supports the 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 7.1 or later releases to support the its features. This includes the ability to remove the retention of expired items from the SnapLock volume. Enterprise Vault configuration requires Microsoft Exchange 2003 or Exchange 2000 and SQL server 2005 or SQL Server 2000.

Enterprise Vault configuration information

It is necessary to install and configure transmission control protocol (TCP)/IP on the Windows machine. This computer should have an IP address registered with 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 from Enterprise Vault Server.

By default, any file that is larger than 4MB is prevented from being downloaded by Microsoft Internet Information Services (IIS) on Windows 2003. To allow downloading files larger than 4MB, open the IIS manager and change the value in the AspBufferingLimit parameter. It is also important to understand the Enterprise Vault components to help configure them after the installation process:

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

The Vault Service account

Enterprise Vault uses the vault service account to access the Windows server operating system. The Enterprise Vault services are installed as Windows services. All Enterprise Vault computers share this account. This account must be a member of the Active Directory (AD) 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 a 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, the DNS alias is created by entering the CNAME parameter.

Installation

This section briefly covers the installation of Enterprise Vault Server. For detailed procedures, refer to the appropriate installation guide.

This section describes the steps involved with installing Enterprise Vault Server. Preparing the Windows servers with the appropriate operating system and all required HotFixes is the basic step in this stage. In the following sections, this paper describes the steps involved in our test setup. Installing SQL Server on a dedicated server will improve performance. On our setup, we installed both Enterprise Vault Server and SQL server on the same system.

Enterprise Vault Server

In our test setup, it was a fresh install of Enterprise Vault. After verifying the availability of Microsoft Exchange Server and SQL Server, the following Enterprise Vault components were installed. An installation wizard will install the Administration Console on Enterprise Vault Server.

After selecting the Enterprise Vault components to install, the installation wizard prompts you 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. In order to use Enterprise Vault, postinstallation tasks were completed after restarting the computer.

Postinstallation tasks

Preparing the system and completing the preinstallation tasks are significant steps when 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 will list the steps involved in the postinstallation activities.

Enterprise Vault configuration

Start the Enterprise Vault Configuration wizard. It allows creating a new Vault Directory on this computer. If you have an existing Vault Directory, select that Vault Directory. On our setup, we configured a new Vault Directory and provided the user authentication information for Enterprise Vault services. We provided the SQL Server that was used for the Vault Directory. In our case, the SQL Server entry was ‘IBMX335-SVL61’. The Configuration wizard proceeded after granting the necessary Vault Service account user permissions, as shown later.

Having granted the necessary user rights to Vault Service Account, Vault Directory Database and transaction log locations are required. In our test setup, we provided the virtual disk path (SAN) created by the SnapDrive storage management tool, as shown later. Administrators should select the locations for database and transaction logs according to their policy and may be on a separate disk path.

Before creating a new Vault Site, verify that a DNS alias for the new Vault Site is available. On the DNS server with administrator privilege, create a DNS alias. If the DNS server is also a Windows server, use **Administration -> tools -> DNS task** to create a DNS alias. Alternatively, if the DNS server is UNIX based, the DNS alias for the Enterprise Vault Server is created by CNAME entry in the DNS table. Giving

a meaningful name for the DNS alias is helpful. On our test setup, we created a DNS alias as 'vaultserver' because the Windows server was running the Enterprise Vault application. Entering a fully qualified name instead of a DNS alias will display a warning message about the recommendation to use the DNS alias. During this process, it detects the Enterprise Vault services installed on Enterprise Vault Server.

This paper assumes that a vault site has been created and is available for configuring Enterprise Vault for archiving. After creating a new Vault Site, it recognizes the services installed and default Enterprise Vault services for the computer. New services can be added by using the Configuration utility, either 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 that have been added, such as Indexing and Shopping. On our test setup, we selected the SnapDrive-configured local disks, as shown later. While creating the Vault Site, verify the settings for Storage service on the computer. Then, configure the appropriate numbers for the archive and restore process.

Configuring Enterprise Vault for archiving

A Vault Store is used to define the storage that is allocated to the partitions and the archives that it contains. Each Vault Store uses its own databases to hold the details of the archives within the Vault Store. To archive the items, at least one partition must be available. This partition is known as the Vault Store partition. At any time, only one Vault Store partition can be opened for archiving. Create a new Vault Store partition after preparing the IBM N series storage systems for archival.

Configuring IBM N series Storage System for archival destination

For installing Exchange Server 2003 and SQL Server and Enterprise Vault, we used the SAN configuration from IBM N series. Local disks were configured using IBM N series with SnapDrive storage management software. We are now ready to configure the Enterprise Vault archival destination and migration location on the IBM N series storage system(s). In our test setup, we used the IBM N5500 storage system and IBM N series with NearStore feature to configure the archive locations.

If the IBM N series storage system(s) are not installed and configured already, now is the time to configure the storage systems. On our setup, we checked the IBM N series storage system status and volume details.

You must enable the required IBM N series product licenses. This may include protocol licenses such as CIFS and FC protocol. Based on your company policy, you must prepare the storage. If the CIFS protocol is used, configure the CIFS setup and have the necessary CIFS shares available. If a decision is made to use the block protocol or SAN storage, configure the LUNs and necessary virtual local disks that are available on the system. In Enterprise Vault archival scenarios, network share may offer a better solution. Complete the same setup for additional IBM N series storage systems.

On our test setup, we decided to follow these steps –

- Create the appropriate Volume size using IBM System Storage N series with FlexVol™ and IBM System Storage N series with RAID-DP™ configuration
- Create the QTREE
- Create the CIFS shares
- Configure the network security

- Map the network shares on the Enterprise Vault computer
- Verify the universal naming convention (UNC) paths accessed from the computer (we used Computer Management, connected to another computer, and entered the IBM N series storage system name [or IP address].)

Creating a new Vault Store

Verify that the necessary storage configurations are completed and that the IBM N series storage locations are available for creating a new vault store. Continuing with the Enterprise Vault Configuration wizard, select the computer on which the storage service for the new Vault Store will be used.

The new Vault Store requires a name and we recommend a meaningful name. The Vault Store database requires the SQL Server information, and in our setup, we provided the SQL Server location as IBMX335-SVL61.

A Vault Store is used to define the storage that is 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.The new Vault Store requires a SQL database location for the database and transaction logs. Start a new Vault Store by using the Create wizard — right-click **Vault Store** from the Administration Console. Then, select **'New Vault Store**, as shown in the following figure.

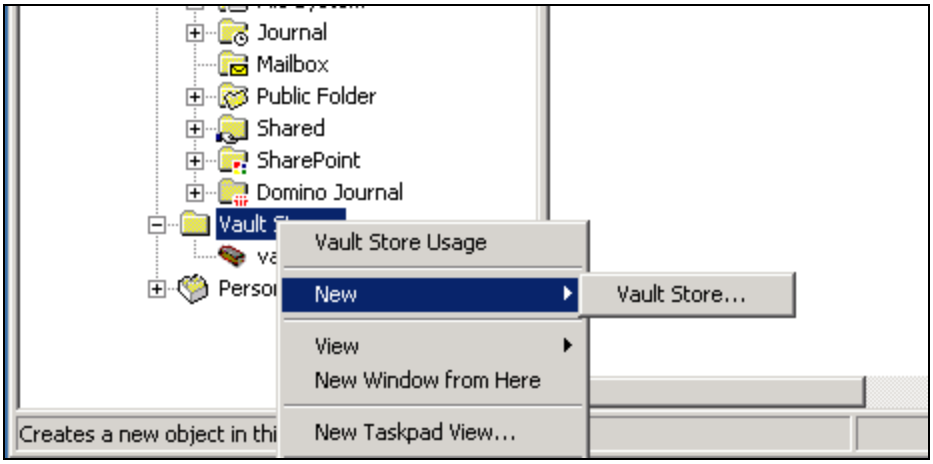


Figure 2. Enterprise Vault Administration Console to create a new Vault Store.

A Vault Store uses its own database to hold the metadata for the archives within the Vault Store. A new Vault Store requires creating new vault store partitions to enable the data archives. While creating the new vault store, select the computer that runs the Storage Service. The new Vault Store will use this storage service. Choose a name for the new Vault Store and the description helps to understand the type of Vault Store, as shown below.

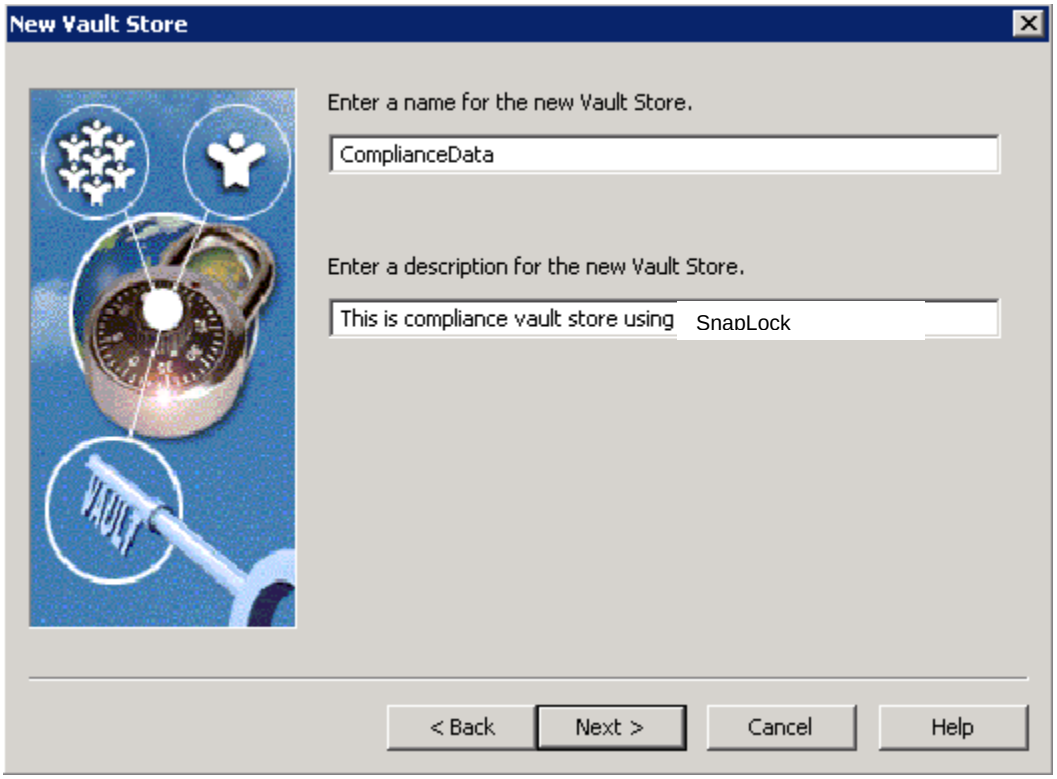


Figure 3. New Vault Store.

Enterprise Vault uses Microsoft SQL Server to store the metadata for the data archived. Each Vault Store uses its own database. Select the Vault Store database and transaction log locations. On our system, we selected the SnapDrive-created local drive, as shown below.

When an item or file is archived, a safety copy is retained. There are different options regarding the safety copy; select the appropriate options, according to your company policy. Configure the policy pertaining to the safety copy. For example, the safety copy can be retained forever or deleted after a backup and archival operation. Available options about safety copy policy are shown in the following figure.

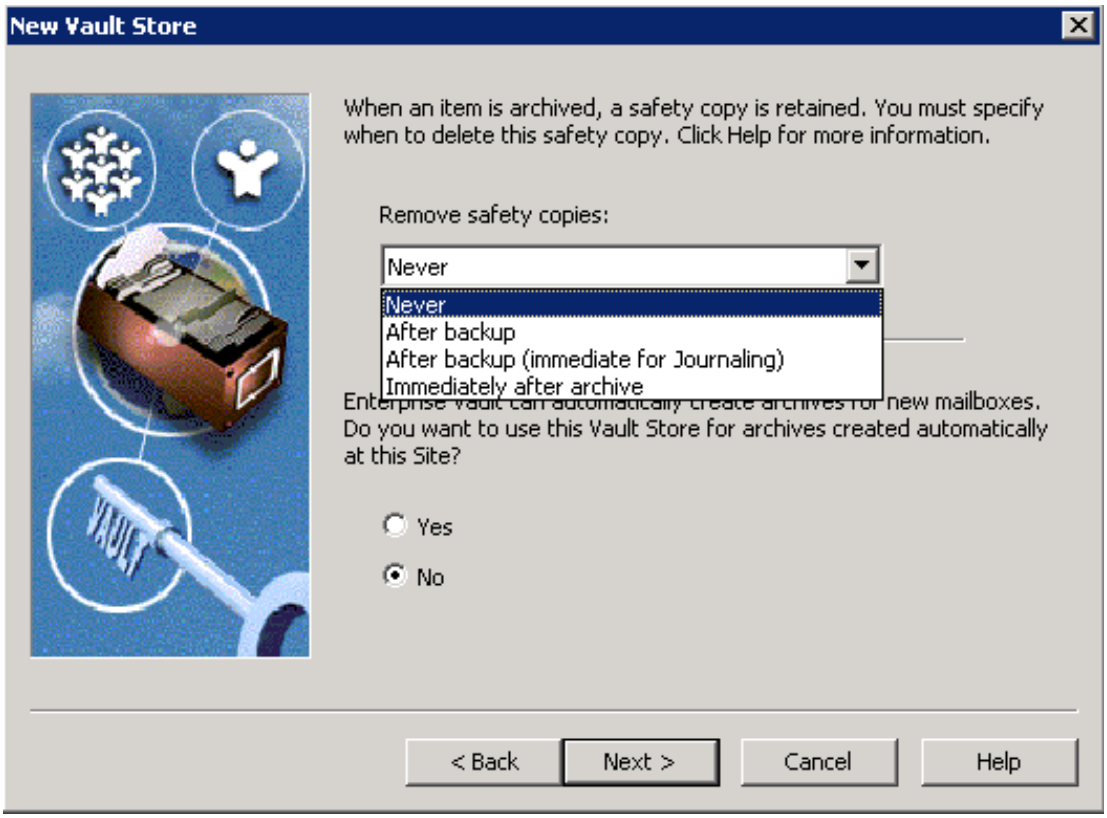


Figure 4. Retaining safety copy configuration.

A new Vault Store partition is required in order for a new Vault Store to be created. Enterprise Vault can create a new Vault Store partition, as shown on the next page.

A SnapLock storage device may not allow deleting the archived items until the retention period expires. You need to know how SnapLock devices affect the Enterprise Vault backups. The new Vault Store partition's Create wizard displays a warning as shown in the following figure. In order to provide the archival destination path, use the network share that is configured on the IBM N series storage system. Then create a folder at the network share level. An example would be to follow this procedure:

- Map the network share on the computer.
- Create a folder on top of that network share.
- Provide this path as the location for the new Vault Store partition.

Enterprise Vault has a feature to provide additional safety for the content, and we chose to remove the archived items from the primary after the backup is completed. Another option is provided so that the contents of the archived items are never deleted from the primary.

Next, the Create wizard will display the summary for creating a new Vault Store. On our test setup, this task created a new Vault Store as shown below.

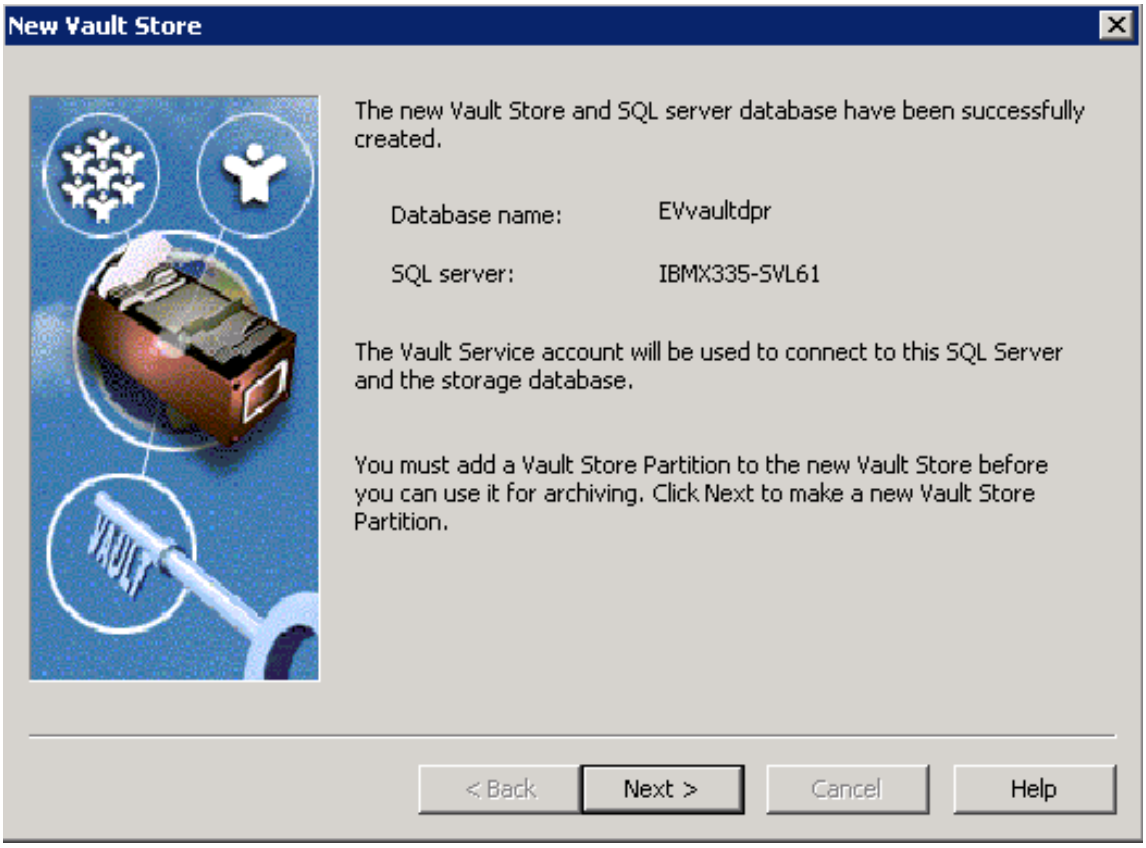


Figure 5) New Vault created with database name EVvaultdpr.

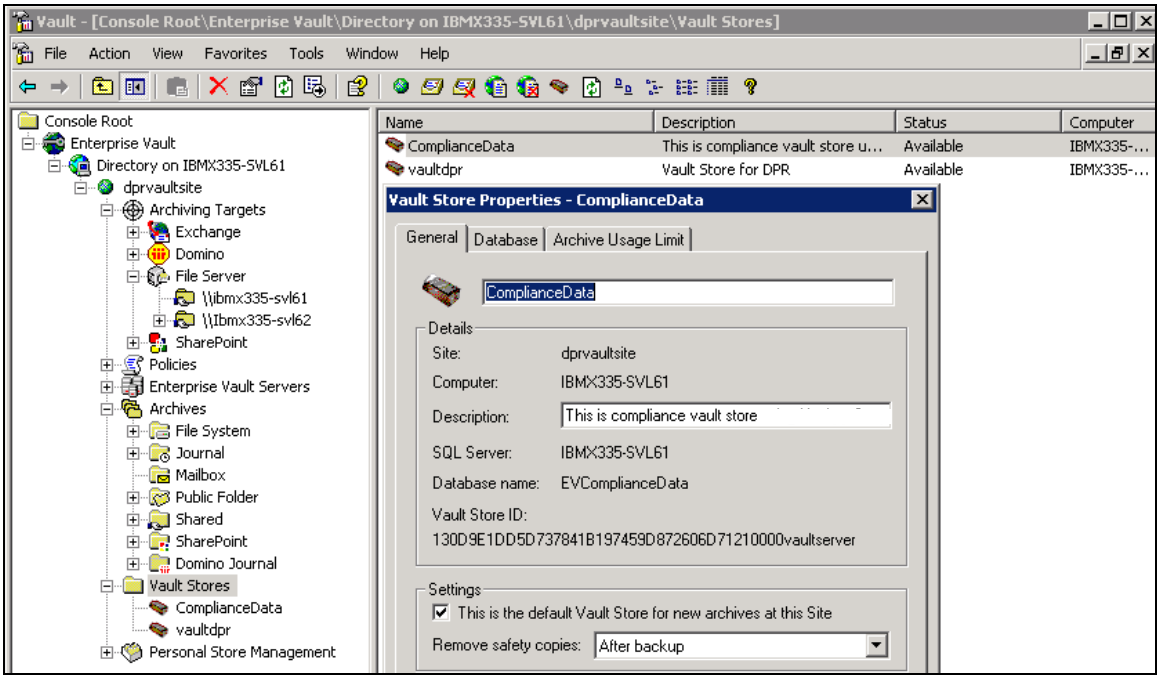


Figure 6. Properties of newly created Vault Store ComplianceData.

Creating a Vault Store partition using IBM N series Storage System destination path

As discussed in Section 4.3.3.2, verify that the IBM N series storage systems are accessible from Enterprise Vault Server. Using the network share, map the appropriate IBM N series storage system's volume(s). Now, start the new Vault Store Partition wizard on the Enterprise Vault Administration Console. Note that only one partition is opened at a given time. Provide the Vault Store Partition name and description.

Following is a sample screen capture for entering the Vault Store Partition name and description into the wizard.

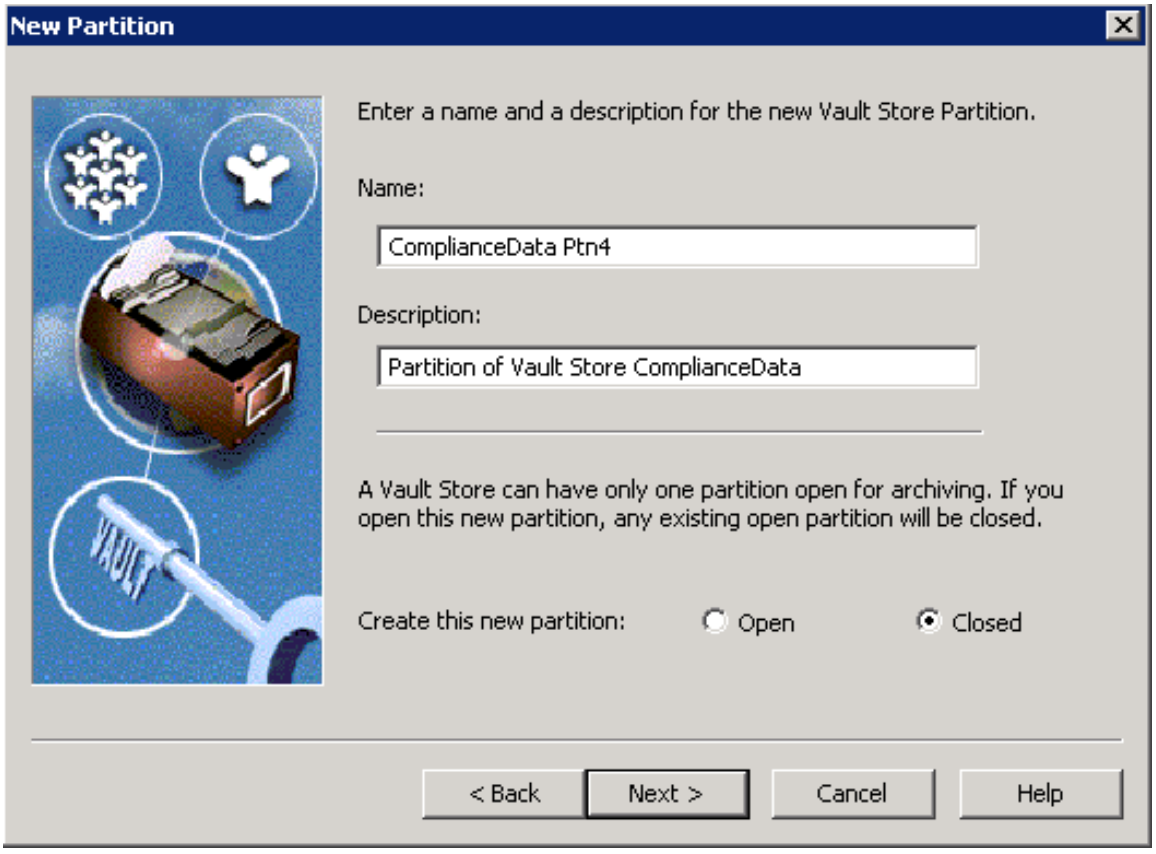


Figure 7. New Vault Store partition.

Continue with the process of creating a new partition by selecting the appropriate option for storage system. If you select the NTFS system, IBM N series configured volume must be mapped as a network share or configured as virtual local disk. For compliance purposes, select the IBM N series with SnapLock volume. On our setup, we followed this procedure to create a new Vault Store Partition.

- Create the appropriate volumes on the IBM N series storage system (N5500)
- Create Necessary Qtree(s) (Optional)
- Create CIFS Shares for the volume or the QTREE

- Map the above CIFS Share on Enterprise Vault Server or on the Administration Console computer (in our example, for mapping the network share, we mapped \\fas3050c-svl34\vs3 as vs3, the name of CIFS Share.)
- Create a folder at the root of the mapped drive. (For example, we created a folder called *store*.)

The above procedure is shown in the following three figures to demonstrate the process involved with creating a new Vault Store partition. It is important to note that at least one directory must be present above the CIFS share point. Creating a folder at the root of the share point will address this requirement. If you are attempting to provide the UNC path, verify that a folder exists at the share point level. In the following figure, we selected NTFS volume for the mapped drive.

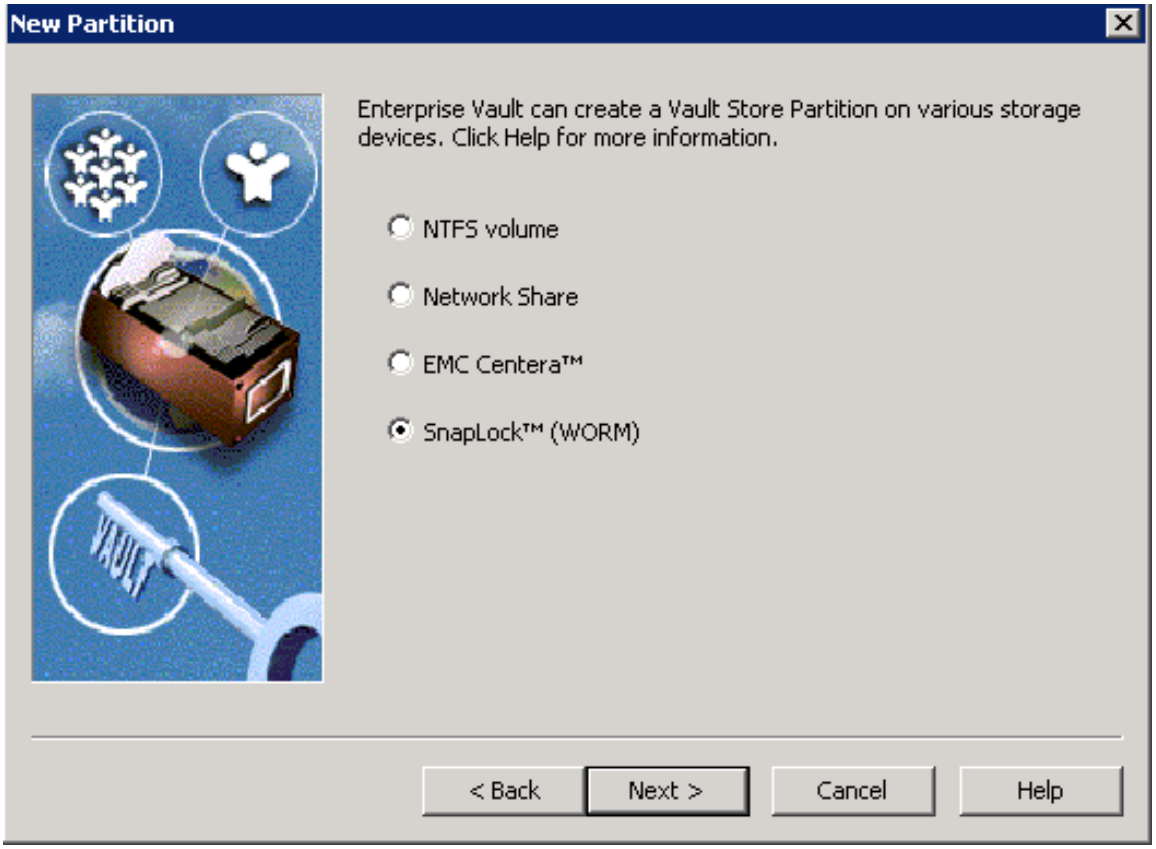


Figure 8. Vault Store partition on IBM N series storage system.

Select an NTFS storage system of the mapped drive for configuring the non-WORM data archival. For compliance data archival, select the SnapLock (WORM) storage system to create a new Vault Store Partition.

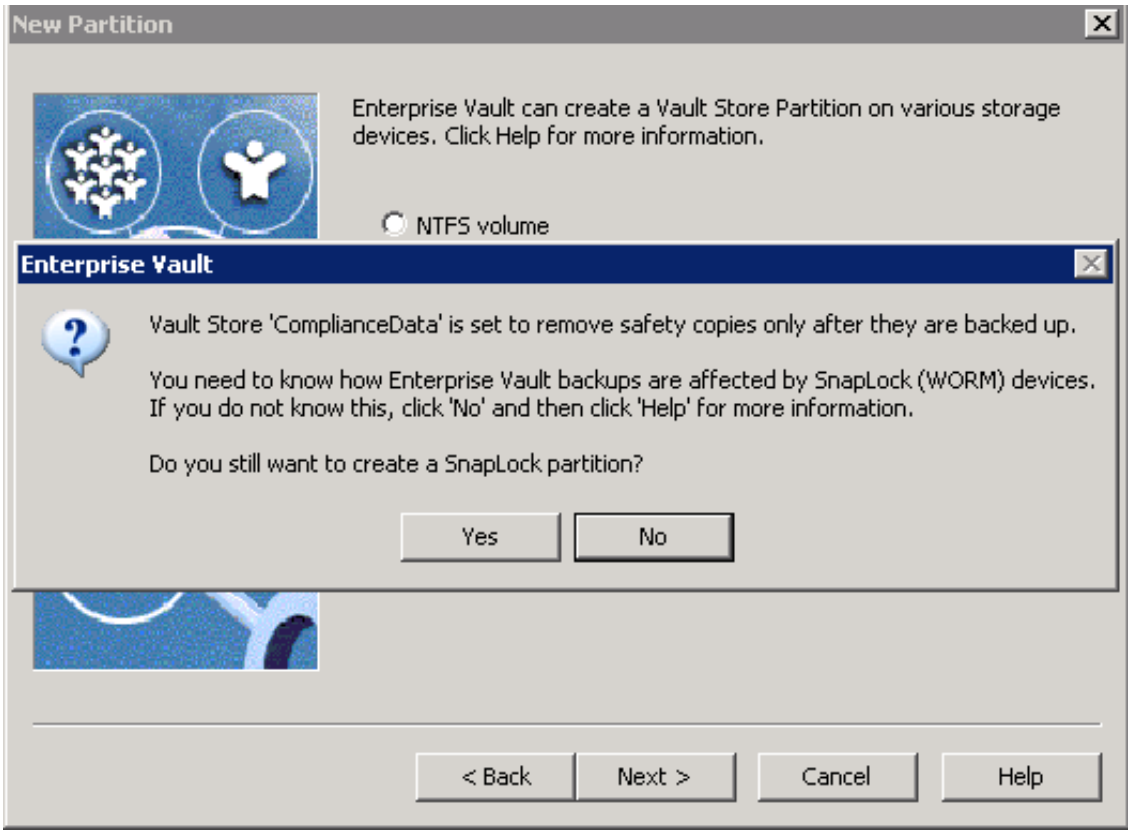


Figure 9. Storage location for the new Vault Store partition.

To create a Vault Store partition, the specified folder must be empty. Select that path and click **OK**.

Procedures to complete the New Vault Store Partition

Continue with creating Vault Store partition. Here is a brief systematic set of instructions to do so.

- Enterprise Vault can reduce space by archiving and migrating old files from the archives. Select your options.
- Enterprise Vault can integrate with file collection software. Choose this if required.
- Enterprise Vault can integrate with file migrator software. Choose the available software such as Enterprise Vault, Veritas NDMP back, or none.
- Select the daily file collection period. Choosing off-peak time is an option for most users.
- Select the age of files at which they will collected.
- Choose whether the migrator service needed. Again, the same choices are offered, including Enterprise Vault.
- Specify the age of the files to be collected, and select the option to remove collections from primary location, if that is your preference.
- Provide the secondary location using UNC path such as \\r200-svl07\ilm\store2
- After this, complete the Vault Store Partition and verify the creation of the new Vault Store Partition.

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 10. Vault Store partitions for Vault Store vaultdpr after creating a closed Vault Store partition.

Archival setup

This section describes the procedure to set up an archival of items from mailboxes. By completing these tasks, Enterprise Vault will be ready for archiving the items. Section 4.3.3.3 described the procedure to create a new Vault Store, where as section 4.3.3.4 explained the steps to create a new Vault Store partition. The 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. Here is the procedure to set up the Enterprise Vault archival.

Create the archive task

Using the Enterprise Vault Administration Console, create an archive task, as listed below.

- Expand the Administration Console until you see the Enterprise Vault Servers container.
- Expand Enterprise Vault Servers.
- Expand the name of the computer to which an archiving task will be added.
- Right-click **Tasks** and create a new Archiving Task.
- Complete the New Archiving Task wizard.

After creating the archiving task, verify the Site archiving settings by using the Administration Console and by selecting the Enterprise Vault site. After creating an archive task, our setup appeared as shown in Figure 11.

Create other archive tasks such as Journal task. Following figure lists the configured archive tasks.

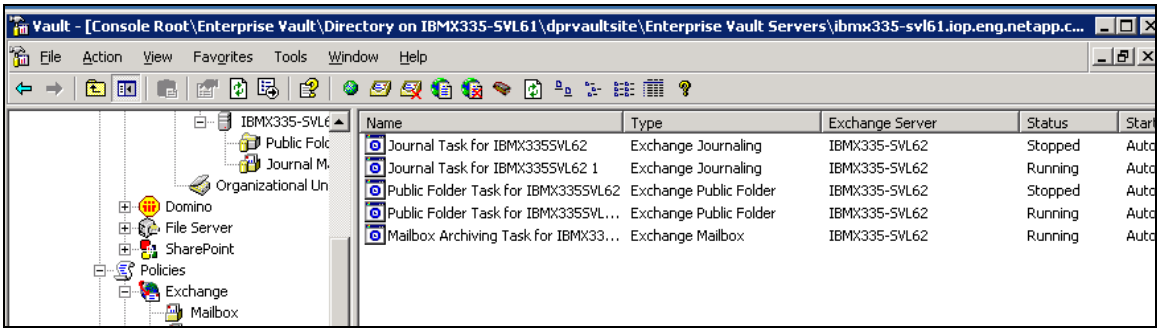


Figure 11. Archive tasks created.

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 and Microsoft SharePoint Portal data. 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.

Enterprise Vault supports various configurations and possible installation strategies, including the following:

- One Enterprise Vault site for each Exchange Server site
- One Enterprise Vault site for FSA (file system archival).

Other configuration possibilities, such as many Enterprise Vault sites for one Exchange Server or vice versa, result in some performance issues. An example is the ability to configure Exchange Mailbox task settings. There is a limit of one Mailbox task setting per Exchange Server.

This section discusses the procedure to configure the FSA component of Enterprise Vault on IBM 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 Enteprise Vault supports file system archival. Refer to Figure 13 for installing the file system archival component. Verify that the necessary network connectivity has been established between the operating system server and the IBM N series storage system(s). For file system archiving, network connectivity using CIFS protocol should work fine. If the decision has been made to archive onto a SnapDrive, the configuration of a local drive is also supported. Enterprise Vault requires the storage system to present its storage as an NTFS file system. File system archival works at the file level; network configuration may be an optimum solution.

Setting up of file system archiving involves the following steps:

- Install the File Placeholder Service
  - Select **File Placeholder Service** component from the install wizard
- Configure the Placeholder Service
  - Verify that Enterprise Vault has FSA License enabled
  - **Program Files → Enterprise Vault → File System Archiving Configuration**
  - **Introduction --> Vault Service Account details**
  - Verify that the advanced user rights are granted
  - Set up the file permissions to have full control access to the network shares and files that are archived
- Create a volume policy
- Create a folder policy
- Create a new volume on the file server and apply the volume policy
- Create archive points to control the archived folders.

Using the above procedure, to set up the file system archiving, use the Enterprise Vault File Placeholder Configuration wizard. The File Placeholder service configuration is shown in the following figure.

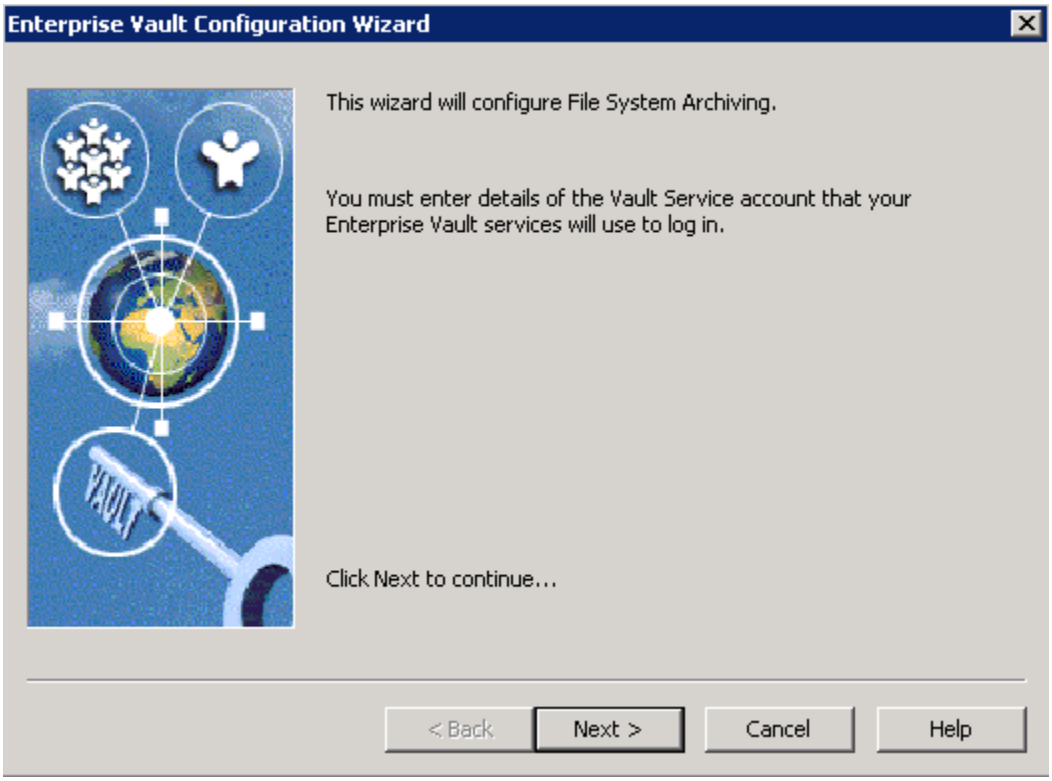
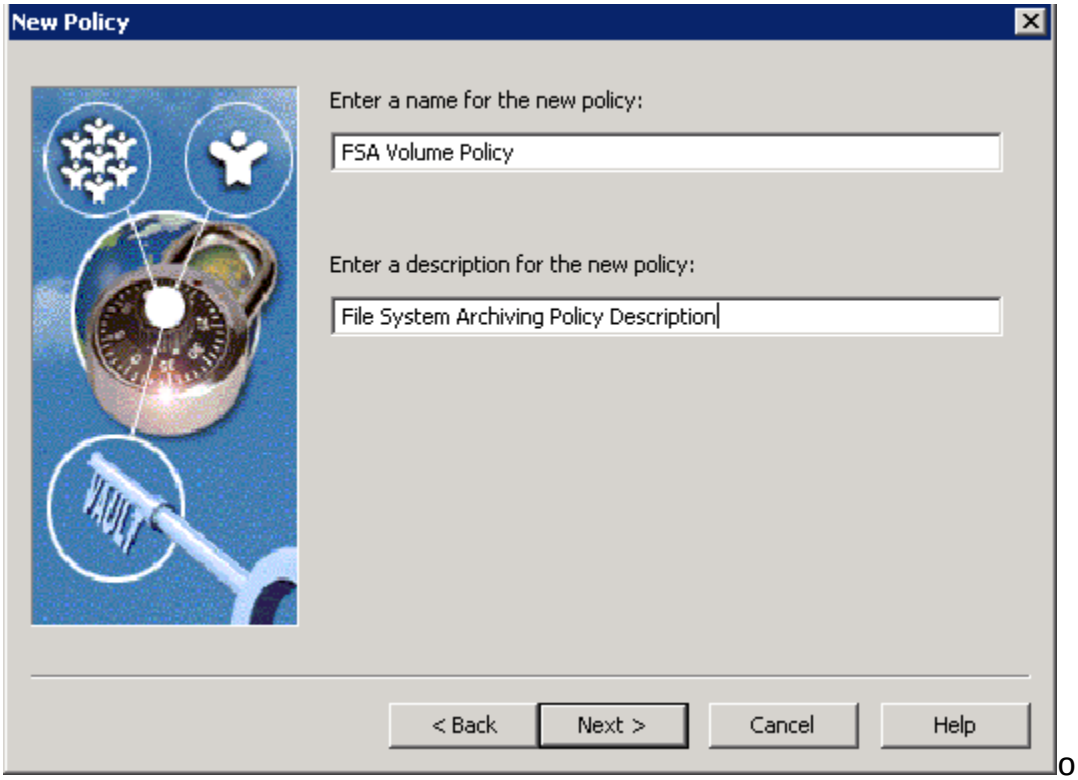


Figure 12. File Placeholder Service configuration wizard.

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

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

After granting the necessary user rights, file system archiving is configured on the computer that is running the configuration. After the file system archiving is configured, create a file server archiving policy. There are two possible types of archiving policies: a volume archiving policy and a folder-level archiving policy. Create a volume archiving policy by providing the policy name and the description, as shown in the following Figure 13.



othe

Figure 13. Creating a new FSA volume policy.

Follow through the wizard to configure quota enable or disable management and to establish the settings for starting and stopping the archiving process. Using this configuration, the archiving process can start after a certain percentage of data use. Select a retention category to be applied for this volume policy. Choose whether to leave a shortcut to the archived file. Specify the rules for archiving, such as the type of file to be archived. File system archiving applies to the permissions of the folder archived from the system. Change the settings if necessary while creating the rules.

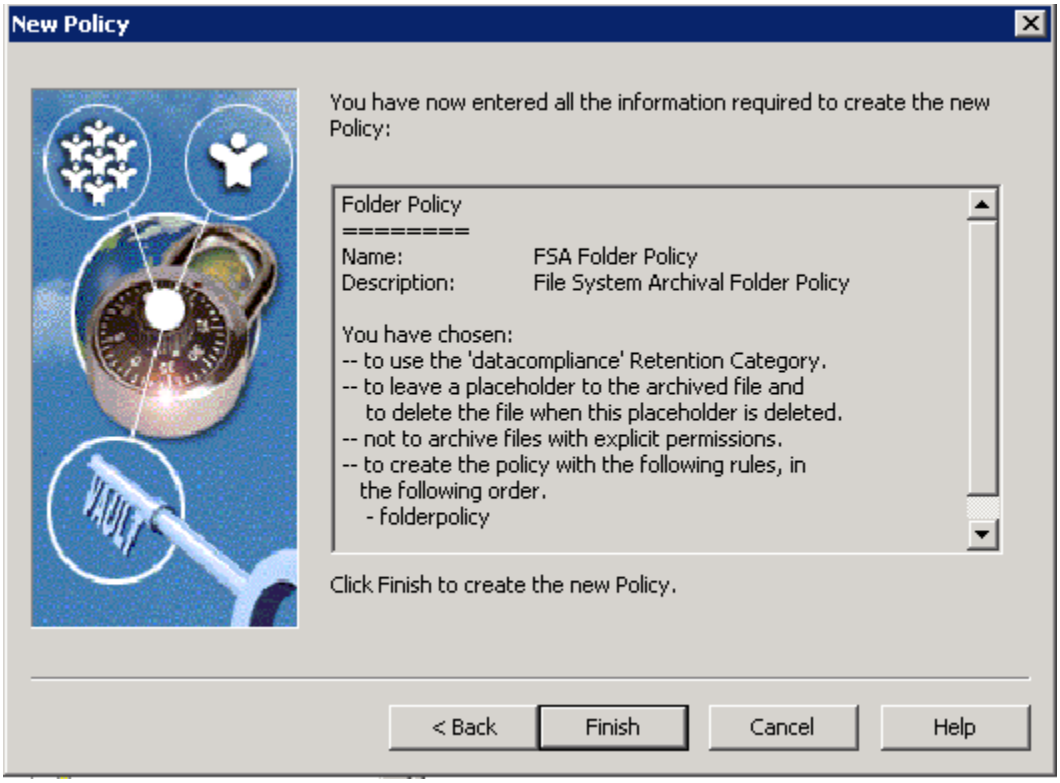


Figure 14. Information required to create the new FSA policy.

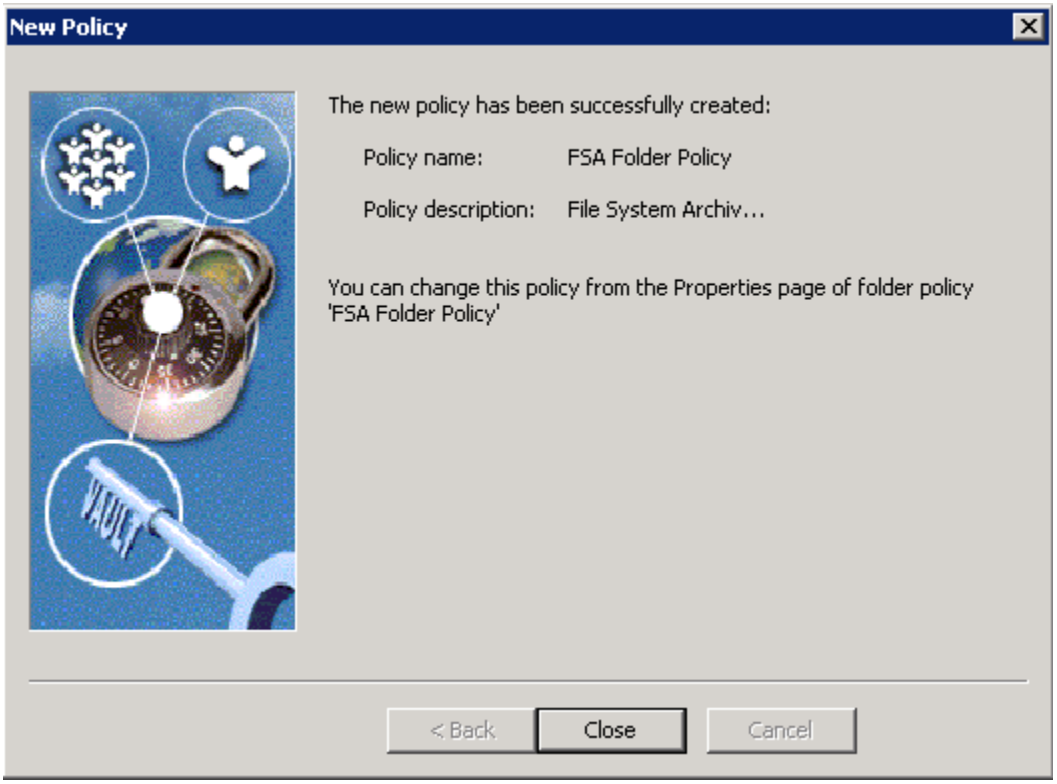


Figure 15. New FSA policy.

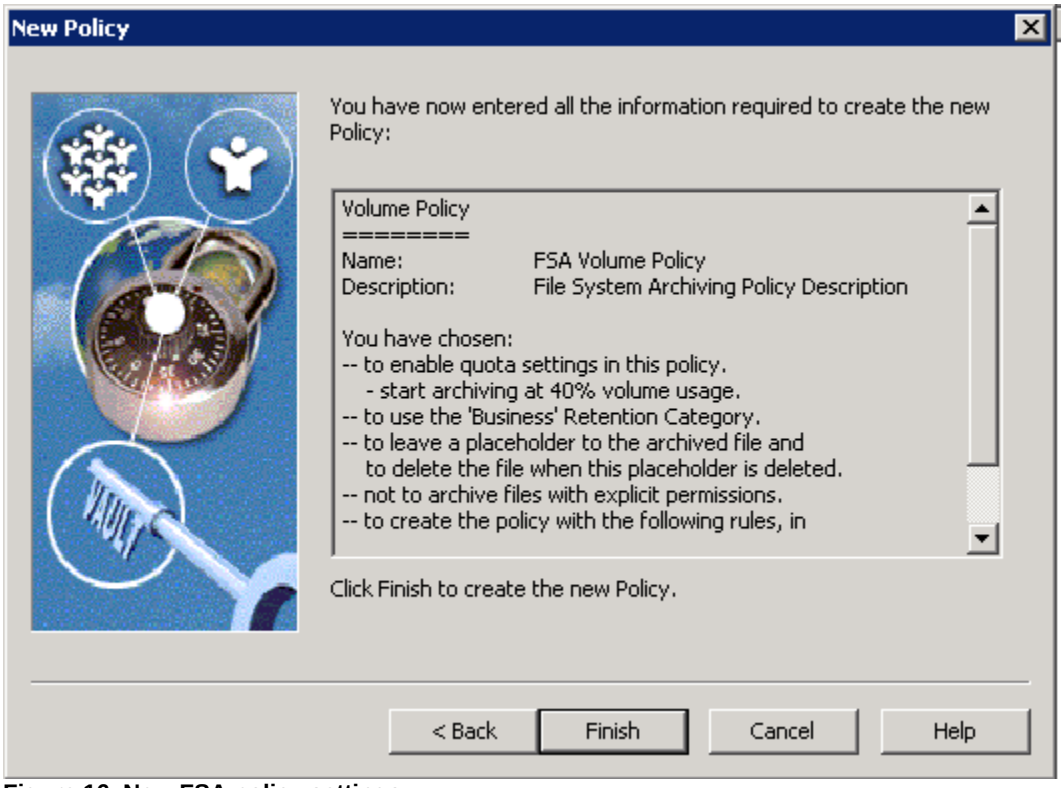


Figure 16. New FSA policy settings.

After creating the file archiving policy, it is important to add a file server — being sure to use the 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 that is running shopping service and continue with the configuration.

On a storage system that presents itself as an NTFS file server, the File Placeholder Service component is installed and leaves Placeholder shortcuts. The Placeholder service component does not run on the IBM N series storage system. Instead, it runs on the Windows server and is configured by using the Administration Console. This service can run a different Windows server than Enterprise Vault Server. A file archiving filter driver is not required on IBM N series storage system. An Archive Point in each folder is created when a new volume is created using Administration Console. To create a volume, expand **Archiving Targets -> file server** and right-click the available file server.

To complete the file archiving setup, open the Enterprise Vault Administration Console, expand the file server, and select the file server (as shown in Figure 17). Continue creating the volume. There are two types of shares to browse while selecting a Windows share. Selecting the hidden type of share displays the drive letters of the available archival points.

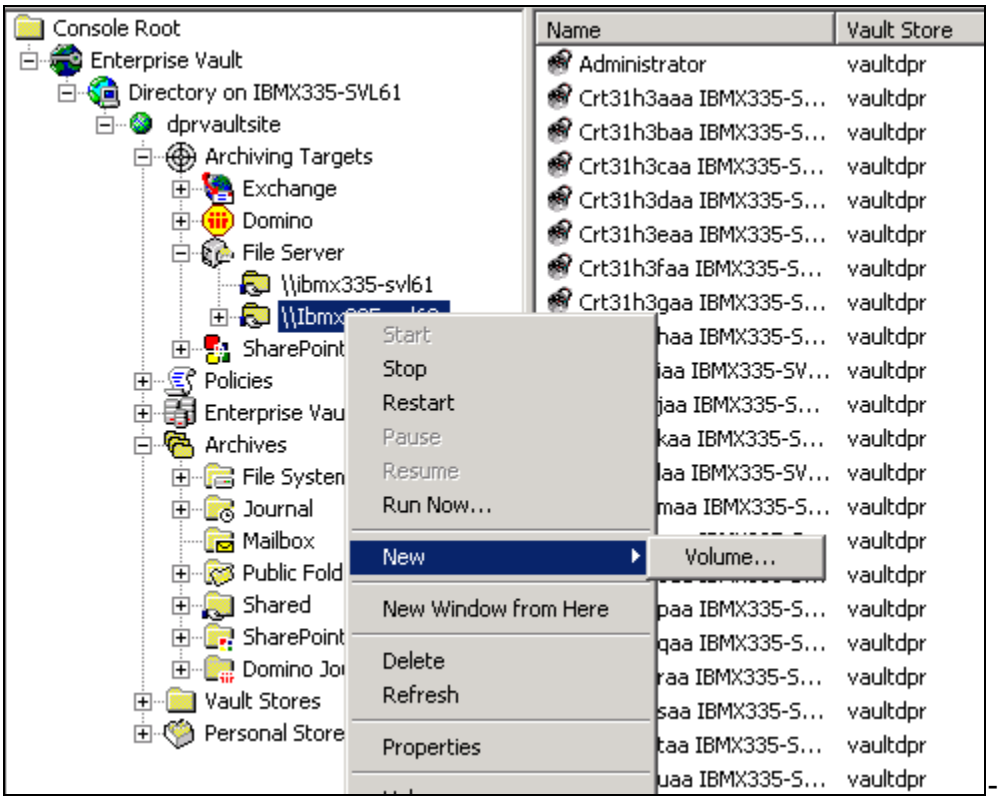


Figure 17. Creating a new volume for FSA targets.

Browsing the hidden type of share will display the directory path. Select a folder-archiving target. Apply the volume policy for the archiving target and select the required Vault Store on the processing computer. Figure 18 shows the information required to add the archiving volume.

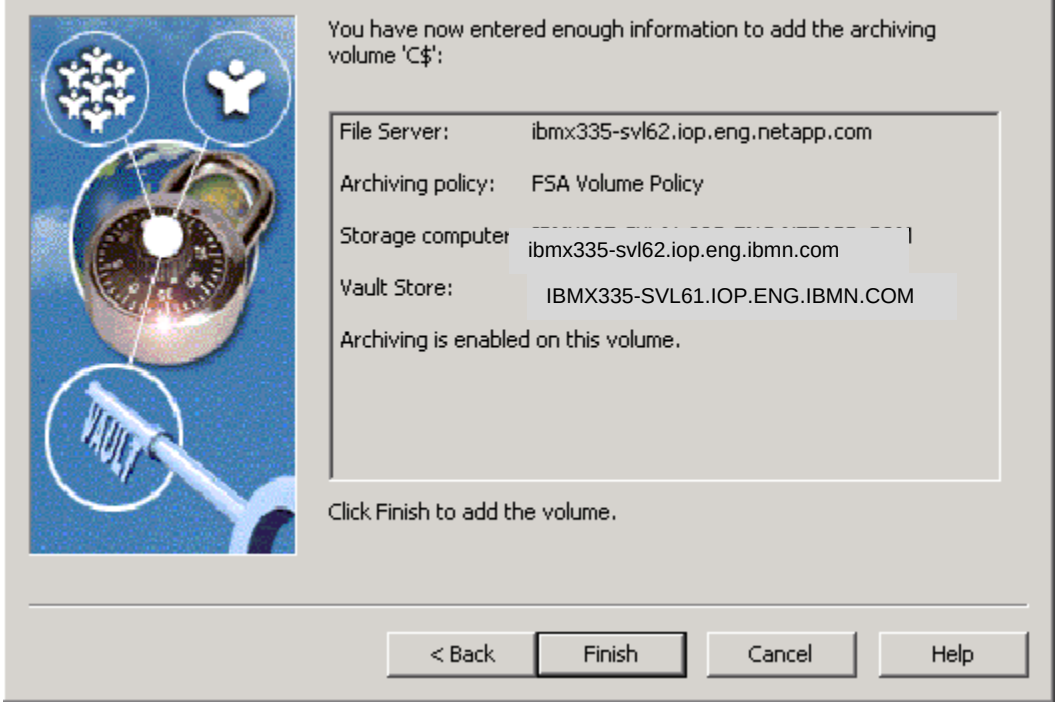


Figure 18. Creating new archiving volume for file server.

Continue to create necessary archiving targets for all the folders that require file system archiving. Figure 19 shows the available file server archiving targets on our test setup.

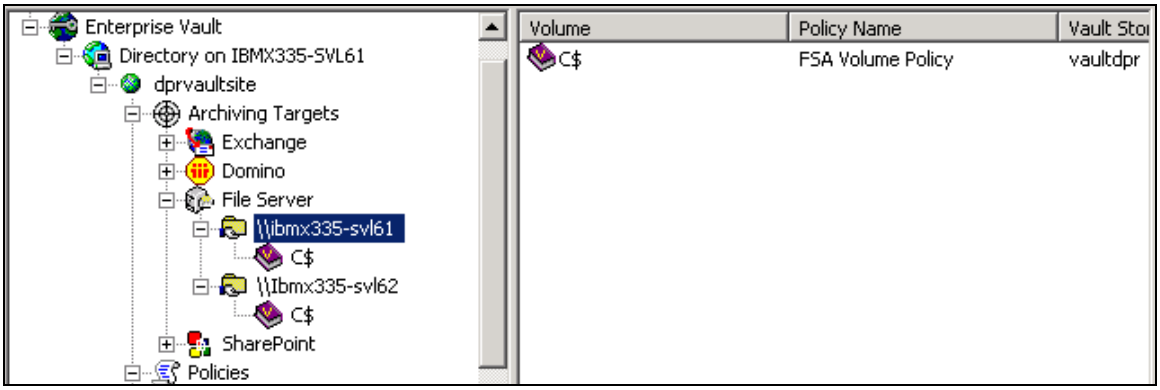


Figure 19) Available archiving targets on file servers (FSA).

Summary

Enterprise Vault supports archiving messages from Microsoft Exchange Server. It can archive Lotus Domino servers for the journaling feature, in addition to the ability of archiving file system and Sharepoint Portal data. When using IBM N series storage systems, data can be archived on to a network share or on configured local disks. Using IBM N series with SnapLock software, data archived by Enterprise Vault achieves compliance goals. This paper discussed the procedure to integrate Enterprise Vault with IBM N series storage systems. This paper covered the topics related to configuring a storage area network as well as NTFS file systems.

In our test setup, storage systems were configured as virtual local disks and were used to install and configure Microsoft Exchange Server, Microsoft SQL Server, and Enterprise Vault Server. Enterprise Vault used IBM N series 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 has to be recovered from the backup copy without losing all the recently archived items. Data replication could take a significant amount of time and resources. The creation of HTML files is archived, reducing the space savings from archiving and compression. Restoring a corrupted database could be disastrous in an enterprise environment.

IBM N series storage solutions effectively address the possible shortcomings. The integrated design of Symantec Enterprise Vault and IBM N series products offers highly available and exceptional performance with a lower total cost of ownership.

IBM N series and Symantec provide Enterprise Vault users with superior solutions designed to meet business objectives. IBM N series storage system solutions ensure protection of Enterprise Vault data as well as its availability 24x7.

IBM N series offers a complete solution for the Enterprise Vault Server environment. SnapManager for Exchange is ideal for Exchange Server data management processes, such as backup and recovery. SnapManager for SQL supports consistent, quick backup copying. The same also lets you restore the database backup from Snapshot files taken with SnapManager for SQL Server. SnapDrive for Windows provides an efficient and easy way of accomplishing data storage management on Windows server.

The recommendations made in this paper are intended to be an overview of the best practices for most environments. This paper serves as a starting guide when designing and deploying Symantec Enterprise Vault. To ensure a supported and stable environment, familiarize yourself with the products. During the design phase, involve the Microsoft Exchange and SQL Server specialists and Enterprise Vault experts.

Caveat

All possible combinations of hardware, storage architecture and software solutions have not been tested. If you use a different Windows Server operating system or a different version of Enterprise Vault, then significant differences in your configuration could exist. These differences could alter the procedures necessary to achieve the objectives outlined in this document.

Trademarks and special notices

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.

Network Appliance, the Network Appliance logo, Data ONTAP, SnapDrive, SnapManager and SnapLock are trademarks or registered trademarks of Network Appliance, Inc., in the U.S. and other countries.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Information is provided "AS IS" without warranty of any kind.

All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.