Veritas Enterprise Vault™ Installing and Configuring

12.1

VERITAS™

Veritas Enterprise Vault: Installing and Configuring

Last updated: 2017-07-28.

Legal Notice

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Before you contact Technical Support, run the Veritas Quick Assist (VQA) tool to make sure that you have satisfied the system requirements that are listed in your product documentation. You can download VQA from the following article on the Veritas Support website:

http://www.veritas.com/docs/000095758

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

http://www.veritas.com/docs/000001907

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

evdocs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

http://www.veritas.com/community

Contents

Chapter 28   Managing metadata stores

Section 5   Clustering Enterprise Vault with VCS

Chapter 29   Introducing clustering with VCS

Chapter 30   Installing and configuring Storage Foundation HA for Windows

About this guide

This chapter includes the following topics:

- When to use this guide

- Introducing this guide

- Where to get more information about Enterprise Vault

When to use this guide

Work through this guide if you want to perform a new installation of Enterprise Vault.

To upgrade an existing installation of Enterprise Vault, see the *Upgrade Instructions* document.

If you want to install Enterprise Vault Reporting only, see the *Reporting* guide.

Introducing this guide

This manual provides detailed information on installing and configuring Enterprise Vault. Before you install Enterprise Vault, read the *Introduction and Planning* manual so that you have an understanding of the various components.

To install and configure Enterprise Vault, you need to know how to administer the following products:

- Microsoft Windows Server

- Microsoft SQL Server

- Microsoft Message Queue Server

- Microsoft Internet Information Services (IIS)

- Your archive storage hardware and software

To use Enterprise Vault with Domino Server, you also need administrative knowledge of Domino Server and the Notes client.

To use Enterprise Vault with Exchange Server, you also need administrative knowledge of Exchange Server and Outlook.

To use Enterprise Vault with Windows SharePoint Services and SharePoint Portal Server, you need administrative knowledge of these products.

To use Enterprise Vault Reporting, you need administrative knowledge of Microsoft SQL Server Reporting Services.

Where to get more information about Enterprise Vault

Table 1-1 lists the documentation that accompanies Enterprise Vault.

Table 1-1   Enterprise Vault documentation set

Document	Comments
Veritas Enterprise Vault Documentation Library	Includes all the following documents in Windows Help (`.chm`) format so that you can search across them all. It also includes links to the guides in Acrobat (`.pdf`) format.
	You can access the library in several ways, including the following:
	■ In Windows Explorer, browse to the `Documentation\`*`language`* subfolder of the Enterprise Vault installation folder, and then open the `EV_Help.chm` file.
	■ On the **Help** menu in the Administration Console, click **Help on Enterprise Vault**.
Introduction and Planning	Provides an overview of Enterprise Vault functionality.
Deployment Scanner	Describes how to check the required software and settings before you install Enterprise Vault.
Installing and Configuring	Provides detailed information on setting up Enterprise Vault.
Upgrade Instructions	Describes how to upgrade an existing Enterprise Vault installation to the latest version.
Setting up Domino Server Archiving	Describes how to archive items from Domino mail files and journal databases.

Table 1-1   Enterprise Vault documentation set *(continued)*

Document	Comments
Setting up Exchange Server Archiving	Describes how to archive items from Microsoft Exchange user mailboxes, journal mailboxes, and public folders.
Setting up File System Archiving	Describes how to archive the files that are held on network file servers.
Setting up IMAP	Describes how to configure IMAP client access to Exchange archives and Internet mail archives.
Setting up SMTP Archiving	Describes how to archive SMTP messages from other messaging servers.
Setting up SharePoint Server Archiving	Describes how to archive content from Microsoft SharePoint servers.
Administrator's Guide	Describes how to perform day-to-day administration procedures.
Backup and Recovery	Describes how to implement an effective backup strategy to prevent data loss, and how to provide a means for recovery in the event of a system failure.
Classification	Describes how to assign classification values to the metadata properties of all new and existing archived items. Users of applications such as Enterprise Vault Search and Compliance Accelerator can then use the classification values to filter the items when they conduct searches or reviews.
NSF Migration	Describes how to migrate content from Domino and Notes NSF files into Enterprise Vault archives.
PST Migration	Describes how to migrate content from Outlook PST files into Enterprise Vault archives.
Reporting	Describes how to implement Enterprise Vault Reporting, which provides reports on the status of Enterprise Vault servers, archives, and archived items. If you configure FSA Reporting, additional reports are available for file servers and their volumes.
Utilities	Describes the Enterprise Vault tools and utilities.
PowerShell Cmdlets	Describes how to perform various administrative tasks by running the Enterprise Vault PowerShell cmdlets.

Table 1-1   Enterprise Vault documentation set *(continued)*

Document	Comments
Registry Values	A reference document that lists the registry values with which you can modify many aspects of Enterprise Vault behavior.
Help for Administration Console	The online Help for the Enterprise Vault Administration Console.
Help for Enterprise Vault Operations Manager	The online Help for Enterprise Vault Operations Manager.

For the latest information on supported devices and versions of software, see the *Enterprise Vault Compatibility Charts* book, which is available from this address:

http://www.veritas.com/docs/000097605

Enterprise Vault training modules

The Enterprise Vault and eDiscovery Tech Center (http://www.veritas.com/elibrary) is an eLibrary of self-paced learning modules developed around key features, best practices, and common technical support questions.

More advanced instructor-led training, virtual training, and on-demand classes are also available. For information about them, see http://www.veritas.com/education-services/training-courses.

Section **1**

Enterprise Vault requirements

Enterprise Vault hardware requirements

This chapter includes the following topics:

- Hardware requirements for Enterprise Vault server
- Hardware requirements for SQL Server
- Network requirements for Enterprise Vault
- About the storage requirements for Enterprise Vault

Hardware requirements for Enterprise Vault server

Any computer on which you plan to install Enterprise Vault must be a member of a domain.

Table 2-1 shows the minimum and recommended specifications for a production Enterprise Vault system.

Table 2-1 Minimum and recommended specifications for an Enterprise Vault server

Item	Minimum and recommended specification
Number of processor cores	Minimum: 4 Recommended: 8 The total number of cores can be achieved by any combination of physical CPUs and their cores.
Power of CPUs	2 GHz

Table 2-1   Minimum and recommended specifications for an Enterprise Vault server *(continued)*

Item	Minimum and recommended specification
Memory	Minimum: 8 GB Recommended: 16 GB
Disk space	1 GB **Note:** Enterprise Vault prevents installation on a partition with less than 1 GB of free disk space.

In smaller Enterprise Vault environments, you can install all Enterprise Vault's core services on the same server. However, in larger environments you can consider deploying individual services, such as the Storage service and the Indexing service, on dedicated Enterprise Vault servers.

For more information about distributing Enterprise Vault services, see the *Introduction and Planning* manual.

Running Enterprise Vault on a virtual server

You can run Enterprise Vault on a virtual server. For more information about the virtualization technologies supported by Enterprise Vault, see the Enterprise Vault *Compatibility Charts* at http://www.veritas.com/docs/000097605.

If a virtual Enterprise Vault server hosts the Indexing service, we recommend that you use a virtual machine that supports eight processor cores. If the virtual machine does not support this many processor cores, we recommend that you deploy a dedicated virtual server to host only the Indexing service.

For more information about the performance of Enterprise Vault on a virtual server, see the Enterprise Vault *Performance Guide* at http://www.veritas.com/docs/000005725.

For more information about the deployment of Enterprise Vault on a virtual server, see the Enterprise Vault best practice articles at http://www.veritas.com/docs/000068528.

Additional processing capacity for initial archiving

If you have a large backlog of data that you want to archive quickly, when you first install Enterprise Vault, you may want to configure additional Enterprise Vault servers for the initial archiving run. When archiving reaches a steady state, the additional Enterprise Vault servers can be redeployed for other purposes.

Hardware requirements for SQL Server

Enterprise Vault requires a number of SQL databases:

- The Enterprise Vault Directory database holds the configuration information for an Enterprise Vault site.

- Each vault store has a vault store database, which holds configuration information for the vault store and details of the items stored in its archives.

- Each vault store group has a fingerprint database, which holds the fingerprints and other information related to the single instance storage parts that are created for Enterprise Vault single instance storage.

- The Monitoring database holds monitoring information for the Enterprise Vault site.

- If you configure FSA Reporting, Enterprise Vault creates an FSA Reporting database to hold the FSA Reporting data. You can configure additional FSA Reporting databases for scalability or to segregate information, if required.

The SQL Server that manages these databases will typically reside on a different computer from the Enterprise Vault server.

In general, the specification of the SQL Server computer should match that of the Enterprise Vault server. The amount of memory that the SQL Server can use depends on the Windows and SQL Server versions.

Table 2-2 shows the minimum and recommended specifications for a production SQL Server.

Table 2-2   Minimum and recommended specifications for SQL server

Item	Minimum and recommended specification
Number of processor cores	Minimum: 4 Recommended: 8 The total number of cores can be achieved by any combination of physical CPUs and their cores.
Power of CPUs	2 GHz
Memory	Minimum: 8 GB Recommended: 16 GB

You do not need a separate SQL Server for every Enterprise Vault server. As a general rule, one SQL Server can manage up to eight Enterprise Vault servers.

Network requirements for Enterprise Vault

Enterprise Vault can generate a considerable volume of network traffic. As a minimum we recommend an environment in which the connections support the expected response time of a 100 Mbps switched Ethernet LAN.

For guidelines on the network traffic you might expect between the various components under different conditions, see the *Enterprise Vault Performance Guide* at http://www.veritas.com/docs/000005725.

For more information about Enterprise Vault's interoperability with other products in an IPv6 environment, see the *Enterprise Vault Compatibility Charts* at http://www.veritas.com/docs/000097605.

When you configure sharing with Enterprise Vault single instance storage, Enterprise Vault provides a connectivity test to help you determine whether the network latency is acceptable across the relevant connections.

See "About Enterprise Vault single instance storage" on page 175.

About the storage requirements for Enterprise Vault

Storage is required for the following components of Enterprise Vault:

- Vault stores, where the archived items are held.

- Indexes.

- SQL Server databases:

    - Enterprise Vault Directory database

    - Vault store databases

    - Vault store group fingerprint databases

    - Monitoring database

    - One or more FSA Reporting databases, if FSA Reporting is configured

- Server cache for temporary files used by Enterprise Vault.

- Shopping baskets, which are used by Enterprise Vault for details of items that are to be restored.

In addition a small amount of local storage is needed on the Enterprise Vault server.

This section gives a basic guide to the Enterprise Vault storage requirements.

For full details of all the supported storage devices and software, see the Enterprise Vault *Compatibility Charts* at http://www.veritas.com/docs/000097605.

Storage for vault stores

The Enterprise Vault Storage service computer needs access to storage for the vault stores. Enterprise Vault is versatile in its use of storage for the vault stores, and it is designed to operate with various types of storage solution provided by third-party software and hardware products. Many storage solutions provide high performance archiving and retrieval. The types may be categorized as follows:

- Local storage
- NTFS (an NTFS volume or a network share that appears on the network as an NTFS volume)
- SAN
- NAS
- CAS (Centera)
- Storage device that supports the Enterprise Vault storage streamer API

The Write Once Read Many (WORM) feature is supported on several devices.

If you plan to create a vault store partition on a storage device that supports the Enterprise Vault storage streamer API, ensure that the appropriate storage device software is installed on the Enterprise Vault storage servers. Install the storage device software on all the Enterprise Vault storage servers that manage the partitions in the vault store group.

One of the most important factors that determines the performance of Enterprise Vault is the speed of the storage device.

Preparing WORM storage devices

The information in this section refers specifically to NetApp ONTAP devices with SnapLock. If you plan to use other WORM devices to hold vault store partitions, then we recommend that you configure them in a similar way, if possible.

For details of the required commands, refer to the API documentation for your storage system.

For a list of the WORM devices that can be used for vault store partitions, see the Enterprise Vault *Compatibility Charts* at http://www.veritas.com/docs/000097605.

On NetApp devices, you can set the default retention period and a maximum retention period for items stored on the device. To ensure that items with the

Enterprise Vault retention period of **Forever** remain locked, you need to configure the following settings explicitly on the storage device:

■ Set the default retention period to infinite.

■ Set the maximum retention period to infinite.

If either of these is not set, or set to a value other than infinite, then users or third party applications may be able to delete the items after the default or maximum retention period set on the device has expired.

Note: Enterprise Vault will not expire or delete the items.

Required amount of storage for vault stores

When an item is archived, it is first compressed and then metadata is added to it. As a general rule, the item is compressed to half its original size and the metadata comprises approximately 5 KB. When an item is shared, only the metadata is added.

The following general rules can be used for estimating the amount of storage needed:

■ Take the total size of items to be archived and halve it.

■ For email items, divide by the average number of recipients.

■ Add 5 KB multiplied by the total number of items.

The compression ratio may vary considerably. Office documents tend to compress well. Other document types, such as ZIP files or JPG files, are already compressed and cannot be compressed further. For this reason, you should always overestimate the amount of storage needed.

The above general rule applies to most types of archiving, but care needs to be taken with File System Archiving (FSA). For example, if ZIP files or JPG files are archived, there is no space saving.

For email archiving, growth in the number of mailboxes and the number and size of messages must also be taken into consideration. Because of these extra factors, a more conservative method of estimating storage is to assume that space used by archiving will equal the space used by Exchange Server or Domino Server in storing items.

Migration of archived data to secondary storage

You can migrate the data that you archive with Enterprise Vault to secondary storage systems. Table 2-3 describes the storage solutions that interoperate with Enterprise Vault to provide integrated data migration.

Table 2-3   Supported storage solutions

Storage solution	More information
Amazon Simple Storage Service	http://www.veritas.com/docs/000003245
AT&T Synaptic Storage as a Service	http://www.veritas.com/docs/000003246
Fujitsu ETERNUS Archive Storage	http://www.veritas.com/docs/000032560
IBM System Storage DR550	http://www.veritas.com/docs/000032561
Rackspace Cloud Files	http://www.veritas.com/docs/000003247
Simple Storage Service (S3) API	http://www.veritas.com/docs/000097850
Veritas Backup Exec	See the *Backup Exec Administrator's Guide*, which is available from the Veritas Support website: https://www.veritas.com/support/en_US/15047.html
Veritas NetBackup	http://www.veritas.com/docs/000070836

The Compatibility Charts provide the latest information on the secondary storage software that Enterprise Vault supports.

Caution: If you use secondary storage that is slow to respond, some Enterprise Vault operations that access this storage will take a long time. For example, both tape and cloud storage can be very slow.

Storage for Enterprise Vault indexes

The computer hosting the Enterprise Vault Indexing service requires access to adequate storage for the indexes.

Each indexing Service also requires disk space for indexing configuration and reporting data. This is set using **Index metadata location** in the Indexing service properties. If you install Enterprise Vault on a cluster, then the index metadata folder, `Enterprise Vault installation folder\EVIndexing\data\metadata`, must be moved to a shared drive. You will also need to update **Index metadata location** in the Indexing service properties.

Indexes may be placed on local storage, SAN, or NAS. If fast indexing is required or searches across a large number of archives, NAS devices may not be suitable.

File systems that use slow storage media as part of their solution, such as optical disk, are unsuitable for indexes.

If indexes are stored on NetApp devices, and possibly other NAS systems, opportunistic locking must be turned off for volumes that contain indexes. For more information, see the following article on the Veritas Enterprise Support site:

http://www.veritas.com/docs/000030672

As anti-virus software can potentially change data, it is important to exclude the index locations in your virus checking application. For more information, see the following article on the Veritas Enterprise Support site:

http://www.veritas.com/docs/000032085

Table 2-4 shows how to calculate the expected sizes of indexes.

Table 2-4   Index size compared to size of original data

Indexing type	Index size as a proportion of original data size
Brief	4%
Full	12%

The type of data being archived will also affect the size of indexes. Archiving a large number of text or HTML files will produce larger indexes. Archiving a large number of binary files, such as image files, will produce smaller indexes, as the content is not indexed.

There is no sharing of index files.

Storage requirements for SQL databases

Storage space is required for the following SQL databases:

- Enterprise Vault Directory database
- Vault store databases
- Vault store group fingerprint databases
- Monitoring database
- One or more FSA Reporting databases, if FSA Reporting is configured
- Audit database

Storage required for the Enterprise Vault Directory database

The directory database has an initial storage requirement of 10 MB for the data device and 25 MB for the transaction log device, making a total initial disk space requirement of 35 MB.

To allow for temporary growth and the transaction logs, it is suggested that you make 5 GB available for the directory database.

Storage required for the vault store databases

Each vault store database has an initial storage requirement of 100 MB for the data device and 80 MB for the transaction log device, making a total initial disk space requirement of 180 MB for each vault store database.

Ensure that there is adequate space for database devices to grow as data is added. Transaction logs should be limited to an appropriate size for your back-up and maintenance plan.

A basic sizing guide for each vault store database is 250 bytes for each item archived plus 5 GB for static data, transaction logs and temporary data fluctuations.

If you configure a vault store partition on an EMC Centera device, and the partition is enabled for collection, then an additional SQL index may be created for the Saveset table in the associated vault store database. The space required for this index on the SQL Server hosting the relevant vault store database is approximately 27 bytes per row in the Saveset table.

Storage required for the fingerprint databases

A vault store group's fingerprint database holds the fingerprint, the storage location, and sharing boundary information for each SIS part that is stored in the group's vault stores.

The fingerprint database has an initial storage requirement of 212 MB, made up as follows:

- 100 MB for the primary filegroup

- 1 MB for each of the 32 non-primary filegroups

- 80 MB for the transaction log device

The non-primary filegroups hold the SIS part fingerprints and other information about the SIS parts. If you share items using Enterprise Vault single instance storage, the non-primary filegroups may grow very rapidly in size. Ensure that there is adequate space for the non-primary filegroups to grow as data is added.

The New Vault Store Group wizard provides the following options for the initial configuration of the fingerprint database:

■ A default basic configuration, where Enterprise Vault locates the primary filegroup and all the non-primary filegroups on one device.

■ An advanced configuration option, where you can specify separate locations for the 32 non-primary SQL filegroups.

To ensure acceptable archiving and retrieval performance, it is important to configure the fingerprint database appropriately for the amount of sharing in the vault store group.

For optimal performance, do as follows:

■ Use the advanced configuration option to specify as many locations as possible on the SQL Server, up to the maximum of 32.

■ Use a separate device for each location. If you specify more than one location on the same device there is no performance benefit.

Note: To add or change locations after the fingerprint database is configured is a SQL Server administration task.

Limit transaction logs to an appropriate size for your back-up and maintenance plan.

Storage required for the Monitoring database

The Monitoring database has an initial storage requirement of 100 MB for the data device and 80MB for the transaction log device, making a total initial disk space requirement of 180 MB.

Ensure that there is adequate space for the database to grow as monitoring data is added.

Storage required for the FSA Reporting databases

If you configure FSA Reporting, Enterprise Vault creates an FSA Reporting database. This database contains the data that the Enterprise Vault File Collector service gathers. This data is used in FSA Reporting's data analysis reports.

You may want to create additional FSA Reporting databases, for example for scalability or to segregate the reporting data.

Each FSA Reporting database has an initial storage requirement of 100 MB for the data device and 80 MB for the transaction log device. The total initial disk space requirement is 180 MB.

Ensure that there is adequate space for each FSA Reporting database to grow as reporting data is added.

A batch file is provided to trim the FSA Reporting database history tables. The batch file retains recent and trend-related information.

See "Maintaining the FSA Reporting databases" in the *Reporting* guide.

Storage required for the audit database

The audit database is not created until you enable auditing. By default, auditing is disabled.

The initial storage requirement for the audit database is 100 MB for the database and 80 MB for the transaction log.

You can enable auditing for individual Enterprise Vault servers. The auditing events for several Enterprise Vault servers in a site can be written to a single auditing database.

The amount of space required will depend on the number and type of events logged and the level of detail required.

The *Utilities* manual describes how to set up auditing.

Limit transaction logs to an appropriate size for your back-up and maintenance plan. For instructions on how to roll over the audit database, see this Veritas Support document:

http://www.veritas.com/docs/000028295

Storage requirements for the Enterprise Vault cache folder

The cache provides space for the temporary files that Enterprise Vault uses. You must specify a cache location if any of the following are configured on this Enterprise Vault server:

- Indexing service
- PST migration
- File System Archiving with a Celerra/VNX file server target
- File System Archiving with a NetApp file server target, if pass-through recall is configured
- Vault Cache
- Classification

You must specify a location for the cache if any of these facilities is configured on the Enterprise Vault server. In the Administration Console, you configure the cache location on the **Cache** tab of the computer properties for the Enterprise Vault server.

Keep the following in mind when you configure the cache location:

- To ensure optimum performance, create the cache folder on fast, locally-attached storage.

- The Vault Service account must have read and write access to the cache folder.

- The major use for the cache is to provide temporary storage for Vault Cache clients. If only a few Enterprise Vault clients use Vault Cache, a location with a minimum of 20 GB of free space is probably sufficient. If many clients use Vault Cache, specify a location with far more free space.

- Anti-virus software can potentially change data in the cache, so it is important to exclude the cache location from virus checking.

- If you have clustered Enterprise Vault with Veritas Cluster Server or Windows Server Failover Clustering, the cache location should be a clustered resource.

Local storage requirements for temporary files

A small amount of local storage is needed for temporary files. For example, the local temporary area may be used by the Storage service when processing large files. Local storage is also required for MSMQ files and for Windows system files.

We recommend that you reassign the TEMP system variable to a drive other than the C: drive.

Slow local disks can seriously impact the performance of Enterprise Vault. You are recommended to allocate separate disks for MSMQ files. The disks need to be set up for maximum speed; for example using RAID 1+0 rather than RAID 5.

TEMP folder security requirements

To protect against unauthorized access to the TEMP folder, which can contain sensitive Enterprise Vault data, the Admin service checks access to the folder on startup, and periodically thereafter. If the Admin service finds unauthorized access permissions, it writes an error to the event log and terminates immediately.

Access to the TEMP folder must be granted using a SID that is authorized in one of the following ways:

- The SID identifies one of the following: local Administrators group, local Backup Operators group, Domain Admins group, local system, System Operators group.

- The SID identifies one of the accounts that is listed in the TempFolderExceptions registry value.

  See "Granting additional users and groups access to the TEMP folder" on page 34.

- Access is granted using the Creator Owner SID, and the current owner of the `TEMP` folder is allowed access under the previous conditions.

- The SID identifies a user, and it is the same as the SID of the user under which the Admin service is running.

The Enterprise Vault Admin service checks the folder's discretionary access control list (DACL). If there is no DACL, the check fails and the service terminates immediately. If the DACL is present, the Admin service checks the SID in each access control entry (ACE) and terminates immediately if access to the `TEMP` folder is granted using a SID that is not authorized correctly.

For more information about Enterprise Vault `TEMP` folder requirements, see the following technical note on the Veritas Support website:

http://www.veritas.com/docs/000023496

Granting additional users and groups access to the TEMP folder

You can specify additional users and groups that may access the `TEMP` folder by setting a registry entry that lists the authorized accounts.

To grant additional users and groups access to the TEMP folder

1 Open the Registry Editor.

2 Browse to the following subkey:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
```

3 Create a string entry called TempFolderExceptions and give it a value that lists the authorized accounts as a semicolon-separated list. For example:

```
MyDomain\JohnDoe;builtin\JohnDoe
```

Note the use of `builtin` to identify local users and groups.

Enterprise Vault required software and settings

This chapter includes the following topics:

- About the Enterprise Vault required software and settings
- About valid computer names for Enterprise Vault servers
- About the Enterprise Vault Deployment Scanner
- Basic software requirements for Enterprise Vault
- Best practice settings for Enterprise Vault servers
- Preinstallation tasks for Enterprise Vault server

About the Enterprise Vault required software and settings

Read this chapter to find out the following:

- Software requirements for core Enterprise Vault components.
- Tasks that you need to perform before installing Enterprise Vault.

The Enterprise Vault *Compatibility Charts* at http://www.veritas.com/docs/000097605 contain details of the supported versions of required software.

There are additional requirements for other optional Enterprise Vault components and the different types of archiving. Ensure that you also review the additional requirement information for your planned installation, as outlined in later chapters.

There are also requirements if you are installing Enterprise Vault in a clustered environment.

About valid computer names for Enterprise Vault servers

An Enterprise Vault server that has Unicode characters in its computer name may not operate properly. We strongly recommend that the computer names of your Enterprise Vault servers contain ASCII characters only.

About the Enterprise Vault Deployment Scanner

Before installing Enterprise Vault, you can use Enterprise Vault Deployment Scanner to find out which requirements are missing. When you have finished preparing your servers for installation, it is advisable to run Deployment Scanner to check that all the requirements have been correctly installed. When you start the Enterprise Vault installer, you are given the option to run the Deployment Scanner before the installation begins.

Enterprise Vault Deployment Scanner is a separate wizard that is supplied on the Enterprise Vault media. When the tool runs, it creates a `Reports` folder in the folder in which it is run, and places a report file in the `Reports` folder.

You can find Deployment Scanner and accompanying documentation in the `Veritas Enterprise Vault\Deployment Scanner` folder on the Enterprise Vault media.

Basic software requirements for Enterprise Vault

This section describes the operating system and software requirements for the core Enterprise Vault services.

There may be additional requirements for the different types of archiving.

If required, the Enterprise Vault Administration Console can be installed on a separate computer.

See "About the requirements for a standalone Enterprise Vault Administration Console" on page 104.

Required operating system components for Enterprise Vault

Enterprise Vault requires a version of Windows Server to be installed on each Enterprise Vault server. Not all versions of Windows Server are supported, and for some versions you need a specific service pack or hotfix.

Caution: If you want to use the Classification feature in Enterprise Vault 12.1, we strongly recommend that you run Windows Server 2012 R2 on all Enterprise Vault servers. In some circumstances, performance issues can arise when you use the Classification feature with other versions of Windows Server.

For details of supported versions, see the Enterprise Vault *Compatibility Charts* at http://www.veritas.com/docs/000097605.

Install Windows with the following options and features:

- NTFS file system.

- Microsoft Message Queuing (MSMQ) services.
  See "Installing MSMQ" on page 37.

- Internet Information Services (IIS) 7.5 or later.
  See "Internet Information Services (IIS)" on page 38.

- .NET Framework 3.5 SP1, and .NET Framework 4.5.2.

- PowerShell 3.0 or later.
  See "PowerShell" on page 39.

- Internet Explorer 9 or later.

- MSXML.
  See "MSXML" on page 39.

- Windows TIFF IFilter
  See "Windows IFilter" on page 39.

Installing MSMQ

Enterprise Vault tasks use MSMQ to communicate with the Storage service. If you want to install Enterprise Vault services on more than one computer in the network, you must configure MSMQ on each computer.

Note the following when you install MSMQ:

- Active Directory Integration should not be enabled.

- We recommend that you place MSMQ storage folders on a drive other than the system drive.

To install MSMQ on Windows Server 2012

1   Open Server Manager.

2   Click **Add Roles and Features** in the **Quick Start** pane.

3   When the wizard opens, select **Role-based or feature-based installation** on the **Installation Type** screen, and then click **Next** until you see the **Select features** page.

4   Select **Message Queuing**. The only MSMQ feature that Enterprise Vault requires is **Message Queuing Server**.

5   Click **Next** and follow the remaining instructions to the end of the wizard.

Internet Information Services (IIS)

You need IIS 7.5 or later on each Enterprise Vault server.

In IIS, you can configure the level of isolation for particular web applications. For shopping baskets in the Enterprise Vault Web Access application to be created correctly, the application needs to run under the predefined Local System account.

The configuration wizard will automatically set the correct isolation and account settings. You do not need to configure this.

The configuration wizard will create a new Application Pool, EnterpriseVaultAppPool, for the Web Access application and assign the Local System account to that pool.

The Enterprise Vault Web Access application is configured in the Default Web Site in IIS. Although HTTP or HTTPS can be configured for Enterprise Vault client connections to the Web Access application, HTTPS is strongly recommended to ensure the security of transmitted data. To use HTTPS, you must first configure the Default Web Site in IIS for HTTPS, and install a valid SSL certificate.

Enterprise Vault requirements for IIS

There is a minimum set of role services that are related to IIS. The quickest way to ensure that these role services are present is to use the **Prepare my system** option that is in the Enterprise Vault Install Launcher. This option automatically installs all the Windows features and roles that are required by an Enterprise Vault server.

If you do not want to use **Prepare my system** you can add the features and roles manually.

See

Note: Windows Server Update Services role is not compatible with Enterprise Vault and should not be installed.

PowerShell

PowerShell is a Windows command-line shell that is designed for system administrators. You need Windows PowerShell 3.0 or later on each Enterprise Vault server. For help using PowerShell, see Microsoft's PowerShell documentation.

The Enterprise Vault PowerShell module also requires that the Server Graphical Shell feature is installed. You install this feature using **Add roles and features** in Server Manager. In Server Manager, navigate to **Features** > **User Interfaces and Infrastructure** and select **Server Graphical Shell**, if it is not already installed.

PowerShell includes native binary commands called *cmdlets*. Some Enterprise Vault administration tasks are managed using additional cmdlets that are provided in a PowerShell snap-in. To use these Enterprise Vault cmdlets, you must install PowerShell.

To run PowerShell and load the Enterprise Vault snap-in

◆   On the **Apps** screen, select **Enterprise Vault > Management Shell**.

The Enterprise Vault PowerShell snap-in is 32-bit and you must run it with the 32-bit version of PowerShell even on 64-bit servers. The **Management Shell** shortcut runs the 32-bit version of PowerShell automatically. However, if you run Enterprise Vault cmdlets directly from external scripts such as backup scripts, you must ensure that you call the 32-bit version of PowerShell.

MSXML

All Enterprise Vault server computers require MSXML. MSXML is installed automatically with Internet Explorer.

If MSXML 6.0 is not present when you install the Enterprise Vault Services component, the Enterprise Vault installer installs it without asking for confirmation.

Windows IFilter

The Storage service converts items to HTML or text, if possible, and this converted content is then used to index the item. Enterprise Vault Storage Service uses Outside In® Technology content converters from Oracle® Corporation to convert most file types. To provide Optical Character Recognition (OCR) conversion for image file types, Enterprise Vault uses Windows TIFF IFilter.

Windows TIFF IFilter is an optional Windows feature that the Enterprise Vault installer enables automatically, if it is not already enabled. You can install additional 64-bit IFilters to extend content conversion functionality, if required. For example, you can install IFilters to provide content conversion for file types that are not supported by the default content converters. Any IFilters that you add should be installed on each Enterprise Vault server that hosts a Storage service.

OCR and IFilter content conversion is also applied to files within archive and container files, such as zip, tar, and pst files.

You can modify the content conversion configuration using advanced site settings in the Enterprise Vault Administration Console. The setting, **File types for IFilter conversion**, lets you configure the file types that you want converted using IFilters that you add. The Content Conversion site settings are described in the *Administrator's Guide*.

SQL Server software

Enterprise Vault supports the following versions of SQL Server:

- SQL Server 2012 x64 Edition (Enterprise, Business Intelligence, and Standard)

- SQL Server 2014 x64 Edition (Enterprise, Business Intelligence, and Standard)

- SQL Server 2016 x64 Edition (Enterprise and Standard)

For the latest information on supported versions of SQL Server and required service packs, see the Enterprise Vault *Compatibility Charts* at http://www.veritas.com/docs/000097605.

Both Windows Authentication mode and Mixed Mode Authentication are supported.

The SQL installation must be case-insensitive, as case-sensitive installations are not supported.

Enterprise Vault requires that SQL has a uniform collation across the Master and all the Enterprise Vault databases. An inconsistent collation prevents you from installing Enterprise Vault, so you must ensure there is a uniform collation before you begin.

The Deployment Scanner performs checks to confirm that SQL Server meets all the requirements for Enterprise Vault.

SQLXML

SQLXML 4.0 SP1 is required on computers on which the Enterprise Vault Services component is installed.

If SQLXML 4.0 SP1 is not present when you install the Enterprise Vault Services component, the Enterprise Vault installer automatically installs it without asking for confirmation.

Net.Tcp port sharing on Index Servers

Enterprise Vault Indexing uses the Windows Net.Tcp Port Sharing Service. If the Net.Tcp Port Sharing Service startup type is set to 'Disabled' the Indexing service automatically changes the startup type to 'Manual' and starts the service.

Best practice settings for Enterprise Vault servers

The Enterprise Vault best practice settings help to ensure that an Enterprise Vault server performs as well as possible. Some of the settings prevent errors; others improve performance.

During the installation you have the option to set these best practice settings automatically. You do not need to modify these settings manually.

Message queue cleanup interval: MessageCleanupInterval

Name	MessageCleanupInterval

Location	`HKEY_LOCAL_MACHINE`
	`  \Software`
	`   \Microsoft`
	`    \MSMQ`
	`     \Parameters`

Type	DWORD
Best practice setting	1800000 (milliseconds = 30 minutes)
Description	MessageCleanupInterval controls the frequency with which Microsoft Message Queuing (MSMQ) removes old message files. The MSMQ default of 6 hours is too infrequent for Enterprise Vault. A build up of old messag files can eventually bring archiving services to a halt.

Message queue message storage limit: MachineQuota

Name	MachineQuota

Location	HKEY_LOCAL_MACHINE
	 \Software
	  \Microsoft
	   \MSMQ
	    \Parameters
	     \MachineCache

Type	DWORD
Best practice setting	8388608 (KB = 8 GB)
Description	The default disk quota that is allowed for Microsoft Message Queuing (MSMQ) messages is not sufficient for the Enterprise Vault archiving tasks. If all the space is used, the Enterprise Vault archiving tasks cannot archive items.

Disable opportunistic locking: OplocksDisabled

Name	OplocksDisabled

Location	HKEY_LOCAL_MACHINE
	 \System
	  \CurrentControlSet
	   \Services
	    \MRXSmb
	     \Parameters

Type	DWORD
Best practice setting	(Hex) 01
Description	Opportunistic locking can result in issues with 32-bit indexes, including index corruption.

Disable loopback check: DisableLoopbackCheck

Name	DisableLoopbackCheck

Location	HKEY_LOCAL_MACHINE
	 \System
	  \CurrentControlSet
	   \Control
	    \Lsa

Type	DWORD
Best practice setting	00000001 (Decimal)
Description	If DisableLoopbackCheck is not set you may get Access Denied errors in the Administration Console and in some configurations Enterprise Vault services may fail to start.

Disable strict name checking: DisableStrictNameChecking

Name	DisableStrictNameChecking
Location	HKEY_LOCAL_MACHINE 　\System 　　\CurrentControlSet 　　　\Services 　　　　\LanmanServer 　　　　　\Parameters
Type	DWORD
Best practice setting	00000001 (Decimal)
Description	Enterprise VaultVault uses DNS Aliases. When a client computer uses an alias name to connect to a Windows server, the client may receive an error message. This problem can occur when the client tries to connect by using a CNAME alias that is created in the DNS zone. The server is not listening on the alias, and so does not accept connections to that name. By disabling strict name checking, this issue is resolved.

Maximum Outlook attachments and recipients: AttachmentMax and RecipientMax

Names	AttachmentMax
	RecipientMax

Location	HKEY_CURRENT_USER
	 \Software
	  \Microsoft
	   \Office
	    version
	     \Outlook
	      \Options
	       \Mail

Type	DWORD
Best practice settings	AttachmentMax: (Hex) FFFFFFFF RecipientMax: (Hex) FFFFFFFF
Description	A Microsoft Outlook issue may cause errors when Outlook runs on the Enterprise Vault Storage service computer. The issue occurs when an archived item has either of the following: ■ At least 2048 recipients in any of the TO, CC or BCC fields. ■ At least 2048 attachments. The issue can cause errors whenever Enterprise Vault recalls an archived item. For example, when rebuilding an index. To resolve the issue, set the value of the RecipientMax and AttachmentMax registry entries to (Hex) FFFFFFFF.

TCP/IP maximum ports and TCP timed wait delay

Names	MaxUserPort TcpTimedWaitDelay

Location	HKEY_LOCAL_MACHINE
	 \System
	  \CurrentControlSet
	   \Services
	    \Tcpip
	     \Parameters

Type	DWORD
Best practice settings	MaxUserPort: (Hex) fffe TcpTimedWaitDelay: (Hex) 78

Description | The default number of ephemeral ports for TCP/IP client connections can be insufficient for Enterprise Vault archiving. If there are too few ports some items are not archived from the server and you may see error messages in Enterprise Vault.

For more information see the following Microsoft article:
http://msdn.microsoft.com/library/aa560610.aspx

Preinstallation tasks for Enterprise Vault server

You need to perform the tasks described in this section, irrespective of the types of archiving that you plan to implement.

Table 3-1   Preinstallation tasks for Enterprise Vault server

Step	Task	See this section for more details
Step 1	Create the Vault Service account.	See "Creating the Vault Service account" on page 45.
Step 2	Create a SQL login account.	See "Creating a SQL login account" on page 48.
Step 3	Assign the required permissions and roles in the SQL databases.	See "About assigning permissions and roles in SQL databases" on page 49.
Step 4	Create Enterprise Vault DNS aliases.	See "Creating Enterprise Vault DNS aliases" on page 50.
Step 5	Turn off or reconfigure Windows Firewall.	See "Turning off or reconfiguring Windows Firewall" on page 51.
Step 6	Secure the locations for Enterprise Vault index and vault store partition files.	See "Securing data locations" on page 51.
Step 7	Read about User Account Control (UAC).	See "About User Account Control (UAC)" on page 52.

Creating the Vault Service account

The Vault Service account is used by Enterprise Vault processes to access the Windows server operating system. The account is shared by all the Enterprise Vault computers in the Enterprise Vault directory. If you are managing multiple Enterprise Vault sites, you can use the same Vault Service account for more than one Enterprise Vault site.

The Vault Service account must be a member of the local Administrators group on each Enterprise Vault computer. The account must be a domain-based Windows security account that belongs to the local Administrators group on all servers in the Enterprise Vault directory. The account password must not be blank. If you create more than one Enterprise Vault site in the same Enterprise Vault directory you must use the same Vault Service account for all sites.

We recommend that you do not make this account a Domain Administrator. It is better to assign required permissions explicitly. This section describes the basic permissions that you need to set for this account. Different types of archiving require additional permissions for the Vault Service account. For details of these, see the section on the type of archiving that you are implementing.

If possible, create the account so that it is in the same domain as the Enterprise Vault computers. If it is necessary for the Vault Service account and the Enterprise Vault computers to be in different domains, create the account so that it is in a domain that is trusted by the Enterprise Vault computers' domain.

Ensure that the Microsoft Message Queue security has been set up to grant the Administrators group access to the Enterprise Vault queues.

You must be logged in to the Vault Service account when you install Enterprise Vault and when you run the Enterprise Vault Configuration wizard.

Some pages of the Configuration wizard require you to specify the locations for SQL Server database files. You can specify the locations explicitly, by entering the path from the perspective of the SQL Server computer. The wizard also provides Browse buttons to let you browse the SQL Server computer to select the locations. However, folder browsing is only available if the Vault Service account has access to the administrative shares on the SQL Server computer. Note that some wizards in the Administration Console provide similar Browse buttons. To use those Browse buttons, the account that you use to run the Administration Console also requires access to the SQL Server's administrative shares.

Unless you assign the SQL system administrator (sysadmin) role to the Vault Service account, you must perform some additional steps before you run the Enterprise Vault Configuration wizard for the first time.

See "About assigning permissions and roles in SQL databases" on page 49.

During configuration, you are asked to provide the name and password of the Vault Service account. Enterprise Vault automatically grants the account the following advanced user rights:

- Log On As a Service
- Debug programs
- Replace a process-level token

Note that you may need to wait for Active Directory replication to complete. The account cannot be used until the replication is complete.

To create the Vault Service account

1   On the domain controller, start **Active Directory Users and Computers**.

2   In the left-hand pane of **Active Directory Users and Computers**, double-click the **Domain** container.

3   Double-click the **Users** container.

4   On the **Action** menu, click **New** and then **User**. The **New Object — User** screen is displayed.

5   Complete the **New Object — User** screen and click **Next**. The next screen asks for password details.

6   Enter a password and confirm it. You must set a password; the Vault Service account password cannot be blank.

Note: If you ever change the password of the Vault Service account, and you have installed an Enterprise Vault add-on, you may also need to change the user account credentials of the Vault Service account in the add-on. See the documentation that accompanies the add-on for more information.

---

7   Select the **Password never expires** check box.

8   Leave the remaining check boxes clear:

   - **User must change password at logon**

   - **User cannot change password**

   - **Account is disabled**

9   Click **Next** to move to the summary screen.

10 Click **Finish** to create the new user.

To add the new Vault Service account to the local Administrators group

1   Log on to the Enterprise Vault computer as Administrator.

2   In Control Panel, open **Administrative Tools** and start the **Computer Management** console.

3   Expand **System Tools** and then **Local Users and Groups**.

4   Select **Groups**, and then double-click the **Administrators** group in the right-hand pane.

5   Use **Add** to add the Vault Service account to this group.

6   Click **OK**.

7   Repeat these steps on each computer which will have Enterprise Vault installed.

Creating a SQL login account

The Vault Service account must have a SQL login account for the SQL Server, with the required permissions.

To create a SQL login account

1   Start SQL Server Management Studio.

2   In the tree, select **Security**>**Logins**.

3   Right-click **Logins**, and select **New Login**.

4   Either type in the Vault Service account as *domain\username* or click **Search** and search for the account. In the search dialog box, ensure that the correct domain is entered in the **Locations** box.

5   Select **Windows authentication**.

6   In the tree, click **Server roles**.

7   Select the check box beside **dbcreator**.

8   Click **OK**.

9   In the toolbar, click **New Query**.

10   Enter the following script:

```
use Master
GRANT VIEW SERVER STATE TO "domain\vsa_account"
GRANT ALTER ANY LOGIN TO "domain\vsa_account"
GRANT VIEW ANY DEFINITION TO "domain\vsa_account"
GO
```

where *domain\vsa_account* is the domain and name of the Vault Service account.

11   Click **Execute**.

12   You can check that the Vault Service account has the **dbcreator** role as follows:

   ■   In the tree, select **Security** > **Server Roles**.

   ■   In the right-hand pane, double-click the **dbcreator** role.

   ■   The Vault Service account should be displayed in the membership list.

13   You can check that the Vault Service account has the correct permissions as follows:

- In the tree, right-click the top level SQL Server object and select **Properties**.

- Select the **Permissions** page.

- Under **Logins or roles**, select the Vault Service account and then click **Effective Permissions**. Check that **VIEW SERVER STATE**, **ALTER ANY LOGIN**, and **VIEW ANY DEFINITION** are included in the list of permissions.

About assigning permissions and roles in SQL databases

Unless you assign the SQL system administrator (sysadmin) role to the Vault Service account, you must perform the following additional steps before you run the Enterprise Vault Configuration wizard for the first time:

- Add the Vault Service account to the msdb system database.

- Grant the Vault Service account Select permissions on the msdb tables sysjobs, sysjobschedules, sysjobservers, and sysjobsteps.

- Assign the database role SQLAgentUserRole to the Vault Service account.

If you do not perform these steps, the following problems occur:

- Enterprise Vault fails to purge the history records from the Monitoring database, so these database records continue to grow.

- Upon completion, the Enterprise Vault Configuration wizard logs an error in the event log with the category 'Monitoring Configuration Utility' and Event ID 41123. The error description begins as follows and then lists the contents of a Purge Job SQL script file:

```
Monitoring Configuration Utility reported error: SQL Error at: --
```

If you run the Enterprise Vault Configuration wizard without performing these additional steps, see the following article on the Veritas Support website:

http://www.veritas.com/docs/000039201

Assigning permissions and roles in SQL Server databases

You must add the Vault Service account to the msdb system database, grant the required permissions to the account, and assign the database role SQLAgentUserRole to the account.

To add the Vault Service account to the msdb system database

1   On the SQL Server computer, start SQL Server Management Studio.

2   Select the required SQL Server.

3   Browse to **Databases** > **System Databases** > **msdb** > **Security** > **Users**.

4 Right-click **Users** and then click **New User**.

5 In the **User name** box, enter a new user name.

6 In the **Login name** box, enter the domain and the user name of the Vault Service account, in the form ***domain\user_name***.

7 Click **OK**.

To grant the permissions to the Vault Service account

1 Right-click the new user that you just created, and then click **Properties**.

2 Select the Securables page.

3 Add the following msdb tables to the list of securables, and then grant Select permission for them to the Vault Service account:

- sysjobs

- sysjobschedules

- sysjobservers

- sysjobsteps

To assign the SQLAgentUserRole to the Vault Service account

1 Browse to **Databases** > **System Databases** > **msdb** > **Security** > **Roles** > **Database Roles**.

2 Right-click **SQLAgentUserRole**, and then click **Properties**.

3 On the General page, click **Add**, and then specify the Vault Service account that you have just created.

Locking down Enterprise Vault SQL databases

By default, the Vault Service account owns all the Enterprise Vault SQL databases. This means that the Vault Service account has full access to all the objects in the databases.

Enterprise Vault databases contain a set of roles that let you revoke the Vault Service account's ownership of the databases, and assign only the minimum permissions it needs to run Enterprise Vault. For more information, see the following document on the Veritas Support website:

http://www.veritas.com/docs/000070503

Creating Enterprise Vault DNS aliases

It is good practice to create a DNS alias for each Enterprise Vault server computer. You are asked to enter the unqualified alias, for example "evserver1", when you

run the Enterprise Vault Configuration wizard. When you configure Enterprise Vault on the first computer in a site, Enterprise Vault automatically creates a vault site alias using the DNS alias entered for that computer. The vault site alias is used by the Enterprise Vault software to refer to the Enterprise Vault site.

The DNS alias must not contain special characters. As defined in RFC-1034, only the following characters are permitted: [a-z], [A-Z], [0-9], hyphen (-), and period (.). The last character must not be a hyphen or period.

Using an unqualified DNS alias allows future flexibility if you change the computer that is running the Enterprise Vault services.

Turning off or reconfiguring Windows Firewall

In Windows Server 2012, Windows Firewall is enabled by default. This prevents Distributed COM (DCOM) from working and therefore, because Enterprise Vault requires DCOM, you must either turn off Windows Firewall or configure it appropriately. Enterprise Vault requires dynamic TCP/IP ports for DCOM.

For guidelines on how to configure dynamic port ranges for TCP/IP, see the following article:

http://support.microsoft.com/kb/929851

In addition, you must open certain ports in Windows Firewall to allow Enterprise Vault to work. For information on these ports, see "Firewall settings for Enterprise Vault programs" in the *Administrator's Guide*.

Securing data locations

It is important to secure the locations that are to be used for Enterprise Vault data. Only authorized accounts should have access to the network shares and folders that are to be used for indexes and vault store partitions. Typically you implement access control on these locations using security ACLs.

If you use a network share for Enterprise Vault data, then you must ensure that the Vault Service account has full access to the network share on the remote server. A recommended way to manage access to Enterprise Vault data locations on network shares is to create a domain security group for this purpose. This approach avoids the need to propagate new permissions to all subfolders and files if you change the Vault Service account.

To secure data locations

1 Check the ACL on network shares and folders that you plan to use for index locations and vault store partition folders.

Accounts other than the Vault Service account and local administrators should not have, or inherit, access to these locations.

2 If you want to manage access to network shares using a group, create a domain security group in Active Directory, for example EVDataAccess.

3 Add the Vault Service account to the new group.

4 Grant the new group full access to the network shares and folders that you plan to use for index locations and vault store partitions.

About User Account Control (UAC)

Veritas recommends that you do not use mapped drives as storage locations. If you use mapped drives, Windows User Account Control (UAC) can prevent Enterprise Vault access to storage locations. We recommend that you use UNC paths instead of mapped drives.

Additional requirements for Operations Manager

This chapter includes the following topics:

- About additional requirements for Operations Manager

- Where and when to install Operations Manager

- Additional required software for Operations Manager

- Additional preinstallation tasks for Operations Manager

About additional requirements for Operations Manager

Enterprise Vault Operations Manager is a separately installable component. It is a web application that makes remote monitoring of Enterprise Vault possible from any computer on which Internet Explorer is installed.

Where and when to install Operations Manager

To use Operations Manager to monitor the Enterprise Vault servers in an Enterprise Vault site, Operations Manager must be installed on at least one Enterprise Vault server in that site.

Operations Manager requires Enterprise Vault Services on the same computer. You can install the Operations Manager component at the same time as installing the Enterprise Vault Services component, or at a later date. You must run the Enterprise Vault configuration wizard to configure the Enterprise Vault Services before you configure Operations Manager.

Additional required software for Operations Manager

The computer on which you install Operations Manager requires the following in addition to the core Enterprise Vault required software and settings:

■ Internet Information Services (IIS) must not be locked down.

Additional preinstallation tasks for Operations Manager

In the Active Directory domain, create a Windows user account named, say, "MonitoringUser", for Operations Manager to use when accessing the Enterprise Vault databases. This monitoring user account does not require an Exchange mailbox, and it need not be a member of the Windows Administrators group.

When you create the monitoring user account, note the following:

■ Select the **Password Never Expires** option.

■ Leave the remaining check boxes clear (**User Must Change Password At Logon**, **User Cannot Change Password**, and **Account Is Disabled**).

Additional requirements for classification

This chapter includes the following topics:

- Prerequisites for classification
- Roles-based administration (RBA) and the classification feature

Prerequisites for classification

To implement classification, you require all the following on all the Enterprise Vault storage servers in your site:

- Windows Server 2012 Original Release or R2.
  For performance reasons, we strongly recommend that you run Windows Server 2012 R2 on all Enterprise Vault servers, and not Windows Server 2012 Original Release.

- The File Server Resource Manager service and the associated tools feature (`fsrm.msc`).
  These components let you administer the Windows File Classification Infrastructure, so that you can create and edit classification rules and properties.
  In the Enterprise Vault Install Launcher, the **Prepare my system** option automatically enables the File Server Resource Manager service and tools.

- The Microsoft Data Classification Toolkit.
  To deploy the classification properties and rules across your Enterprise Vault site, you use Enterprise Vault PowerShell cmdlets, which work in combination with this toolkit. You can download it from the following page of the Microsoft website:
  https://msdn.microsoft.com/library/hh204743.aspx

You also require a license for the Enterprise Vault retention feature to manage classification. Classification operates in test mode if you have yet to install a license for the retention feature, or the existing license has expired.

Roles-based administration (RBA) and the classification feature

To administer the Enterprise Vault classification feature, you require one or more of the following RBA roles in the Vault Administration Console:

- Domino Administrator
- Exchange Administrator
- Extension Content Provider Administrator
- File Server Administrator
- NSF Administrator
- Power Administrator
- PST Administrator
- SharePoint Administrator
- SMTP Administrator

For more information on RBA, see the *Administrator's Guide*.

Additional requirements for Enterprise Vault Reporting

This chapter includes the following topics:

- About the requirements for Enterprise Vault Reporting

- Where and when to install Enterprise Vault Reporting

- Prerequisites for Enterprise Vault Reporting

- Enterprise Vault reports that require monitoring or auditing to be enabled

- Preparing for the installation of Enterprise Vault Reporting

About the requirements for Enterprise Vault Reporting

The Enterprise Vault Reporting feature provides enterprise-level reporting for Enterprise Vault servers, using Microsoft SQL Server Reporting Services as the reporting mechanism. Administrators manage report content and view reports using the Reporting Services Report Manager web application.

Enterprise Vault Reporting is required if you want to use FSA Reporting.

For more information on Enterprise Vault Reporting, see the *Reporting* guide.

Where and when to install Enterprise Vault Reporting

Typically, the Enterprise Vault Reporting component is installed without any other Enterprise Vault components on a server that runs Microsoft SQL Server Reporting

Services. However, you can include the Reporting component as part of an Enterprise Vault server installation, if the required prerequisites are met.

You can install the Enterprise Vault Reporting component at any time. However, you must not run the Reporting Configuration utility until after you have run the Enterprise Vault Configuration wizard successfully on at least one computer in the site on which Enterprise Vault services are installed.

Prerequisites for Enterprise Vault Reporting

You can install Enterprise Vault Reporting on a computer that has the following prerequisites:

- Microsoft .NET Framework 3.5 SP1

- One of the following versions of Microsoft SQL Server Reporting Services:

    - Microsoft SQL Server 2012 Reporting Services

    - Microsoft SQL Server 2014 Reporting Services

    - Microsoft SQL Server 2016 Reporting Services

- A network connection to the computer or computers that host the Enterprise Vault databases

If you intend to configure FSA Reporting, you must install the following software on the SQL Server computers that host FSA Reporting databases:

- Microsoft SQLXML 4.0 SP1

- Microsoft MSXML 6.0

Enterprise Vault reports that require monitoring or auditing to be enabled

Some of Enterprise Vault Reporting's reports rely on Enterprise Vault monitoring or Enterprise Vault auditing for source data.

The following reports require Enterprise Vault monitoring to be enabled:

- Enterprise Vault Server 24-hour Health Status

- Enterprise Vault Server Seven Day Health Status

- Exchange Server Journal Mailbox Archiving Health

- Exchange Server Journal Mailbox Archiving Trends

- Domino Server Journal Mailbox Archiving Health

- Domino Server Journal Mailbox Archiving Trends

The following reports require Enterprise Vault auditing to be enabled:

- Archived Item Access

- Archived Item Access Trends

If you want to use these reports, you must ensure that Enterprise Vault monitoring or auditing are set up, as required.

Note: You can set up monitoring and auditing before or after you install and configure Enterprise Vault Reporting. The affected reports do not contain any information until the Monitoring database or the Auditing database contains the relevant data.

You can enable monitoring from the Enterprise Vault Configuration wizard.

You can also enable monitoring from the Enterprise Vault Operations Manager web application, if you have installed the Operations Manager component.

See the section "Configuring the monitoring parameters" in the chapter "Monitoring with Enterprise Vault Operations Manager" in the *Administrator's Guide*.

To set up auditing, you must enable auditing and then configure auditing on the Enterprise Vault servers for which you want to gather information.

See "About auditing" in the *Administrator's Guide*.

Preparing for the installation of Enterprise Vault Reporting

Before you install the Enterprise Vault Reporting component, you must perform the following steps.

To prepare for the installation of Enterprise Vault Reporting

1 In the Active Directory domain, create a Windows user account named, say, "ReportingUser", for Enterprise Vault Reporting to use when accessing the Enterprise Vault databases. This reporting user account does not require a mailbox, and it need not be a member of the Windows Administrators group.

When you create the reporting user account:

- Select the **Password Never Expires** option.

- Leave the remaining check boxes clear (**User Must Change Password At Logon**, **User Cannot Change Password**, and **Account Is Disabled**).

2 Give the Vault Service account a "Content manager" role on the Microsoft SQL Server Reporting Services server. Refer to the Microsoft documentation for instructions on how to assign Microsoft SQL Server Reporting Services roles to user accounts.

3 Add the Vault Service account to the Local administrators group on the Microsoft SQL Server Reporting Services server computer.

Additional requirements for Exchange Server archiving

This chapter includes the following topics:

- About Exchange Server archiving

- Preinstallation tasks for Exchange server archiving

- Enterprise Vault client access with Exchange Server archiving

- Requirements for RPC over HTTP

About Exchange Server archiving

You can archive items from mailboxes and public folders on the following target Exchange servers:

- Exchange Server 2010 SP1 and later

- Exchange Server 2013

- Exchange Server 2016

Preinstallation tasks for Exchange server archiving

This section describes the preinstallation tasks that you must complete to support archiving from all versions of Exchange Server:

- Installing Outlook on the Enterprise Vault server

- Creating the Enterprise Vault system mailbox

- Removing the restriction on NSPI connections to a Windows Server domain controller
- Creating a user profile on the Enterprise Vault server
- Creating a mailbox for the Vault Service account
- Configuring the Exchange throttling policy on the Vault Service account
- Granting the Vault Service account Send As permission on the system mailboxes
- Assigning Exchange Server permissions to the Vault Service account

Installing Outlook on the Enterprise Vault server

To support Exchange Server archiving, you must install the 32-bit version of Outlook 2013 SP1 on the Enterprise Vault server.

For the latest information on the supported versions of Outlook, see the *Enterprise Vault Compatibility Charts* at http://www.veritas.com/docs/000097605.

Outlook must be the default mail client on the Enterprise Vault server. On startup, the Enterprise Vault Admin service checks that Outlook is configured as the default mail client and, if it is not, configures it as such.

Currently, Enterprise Vault supports MAPI over HTTP connections on Enterprise Vault client computers only. MAPI over HTTP connections to Exchange Server from the Enterprise Vault server are not supported. For instructions on how to disable MAPI over HTTP on the Enterprise Vault server, see the following article on the Veritas Support website:

http://www.veritas.com/docs/000004771

Creating the Enterprise Vault system mailbox

The Enterprise Vault system mailbox is a mailbox that is used by the Exchange Mailbox, Exchange Journaling, and Exchange Public Folder tasks when connecting to the Exchange Server.

You must create an Enterprise Vault system mailbox on each Exchange Server that you want Enterprise Vault to archive.

Note: If you use database availability groups (DAGs) in your Exchange environment, you must create each Enterprise Vault system mailbox in a database that is replicated across the DAG.

Note also the following requirements:

- The Enterprise Vault tasks require exclusive use of this mailbox, so the mailbox must not be used for any other purpose.

- The mailbox must not be hidden from address lists.

- The account that the Enterprise Vault system mailbox is associated with must not be disabled.

Enterprise Vault prompts you for the name of this mailbox whenever you create an Exchange Server archiving task.

After you create the Enterprise Vault system mailbox, it may take some time for the mailbox to be available. The mailbox must be available before you add an Exchange Server archiving task.

Removing the restriction on NSPI connections to a Windows Server domain controller

Windows Server domain controllers restrict NSPI connections to 50 concurrent connections per user. You must remove this restriction to prevent the failure of Enterprise Vault's Exchange archiving tasks.

To remove the restriction on concurrent NSPI connections to a Windows Server domain controller

1 On the Windows Server domain controller, create a new registry DWORD value called "NSPI max sessions per user" under the following registry key:

```
HKEY_LOCAL_MACHINE
\System
 \CurrentControlSet
  \Services
   \NTDS
    \Parameters
```

2 Set "NSPI max sessions per user" to 0xffffffff.

This sets "NSPI max sessions per user" to its maximum value, which removes the restriction on concurrent NSPI connections by each user. For more information about the restriction, see the following Microsoft Knowledge Base article:

https://support.microsoft.com/kb/949469

Creating a user profile on the Enterprise Vault server

Before you install Enterprise Vault, you must:

- Log in to the Enterprise Vault server using the Vault Service account, to create a Windows user profile

If you run Exchange archiving tasks under any other service accounts, you must also complete this action for each service account.

Creating a mailbox for the Vault Service account

Note: The information in this section describes the configuration of the Vault Service account. If you run Exchange archiving tasks under a service account other than the Vault Service account, the information applies to this other account.

During the preinstallation tasks for Exchange server archiving, you must run a PowerShell script to configure the Exchange throttling policy on the Vault Service account.

Before you can run the throttling policy script, you must create a mailbox for the Vault Service account.

If you run Exchange in a cross-forest environment, the Vault Service account must have a linked mailbox in the resource forest.

For example, Exchange might reside in a resource forest called "Resources", and user accounts in a user forest called "Users". In this case, the Vault Service account is in the Users forest, and you must ensure it has a linked mailbox in the Resources forest.

In a cross-forest environment such as this, run the PowerShell script against the disabled user account that owns the linked mailbox.

Configuring the Exchange throttling policy on the Vault Service account

Note: The following procedure describes the configuration of the Vault Service account. If you run Exchange archiving tasks under a service account other than the Vault Service account, run the procedure against this other account.

Exchange Server has a default throttling policy which restricts user accounts to no more than 20 open connections to the server. This restriction on the Vault Service account would cause failures of the Enterprise Vault tasks that run under the account.

You must remove the restriction from the Vault Service account, and Enterprise Vault includes a PowerShell script called `SetEVThrottlingPolicy.ps1` which

creates a new policy and assigns it to the Vault Service account to remove the restriction.

Note the following requirements for the throttling policy script:

- If you archive from both Exchange 2010, and Exchange 2013 or later in your environment, you must run the script in the Exchange Management Shell on an Exchange 2013 or later server.

- If both Exchange 2010, and Exchange 2013 or later are present in your environment, `SetEVThrottlingPolicy.ps1` automatically configures Exchange 2010 servers before later servers, which is mandatory. If you use the `-version` to configure Exchange throttling policies separately for each Exchange version, you must configure the Exchange 2010 throttling policy first.

The syntax for `SetEVThrottlingPolicy.ps1` is:

```
.\SetEVThrottlingPolicy.ps1 -user domain\user_name [-server
exchange_mailbox_server] [-version exchange_version]
[-DomainController domain_controller_name]
```

where:

- *domain\user_name* is the Vault Service account and the domain it belongs to. If *user_name* contains spaces, enclose the whole *domain\user_name* string in quotation marks.
  If you run Exchange in a cross-forest environment, run the PowerShell script against the disabled user account that owns the Vault Service account's linked mailbox.
  See "Creating a mailbox for the Vault Service account" on page 64.

- *exchange_mailbox_server* is the name of the Exchange mailbox server. You must specify an Exchange mailbox server if you run `SetEVThrottlingPolicy.ps1` on a computer other than the mailbox server.

- *exchange_version* is the Exchange server version whose throttling policy you want to configure.
  exchange_version can be `2010` or `2013AndLater`.

- *domain_controller_name* is the name of a domain controller in the domain of which the Vault Service account is a member. This parameter is optional but you should specify a domain controller in environments with multiple domain controllers, to ensure consistency across all the commands in the throttling policy script.

To configure the Exchange throttling policy on the Vault Service account

1   Log in to an Exchange server using an account that is assigned the following management roles:

- Mail Recipients
- Recipient Policies

By default, members of the "Organization Management" role group are assigned these roles.

2 Copy the script called `SetEVThrottlingPolicy.ps1` from the `\Veritas Enterprise Vault\PowerShell Scripts` folder on the Enterprise Vault media to the Exchange Server.

3 On the Exchange server, open the Exchange Management Shell.

4 If you moved an existing Vault Service account mailbox from Exchange 2007 or earlier, update the mailbox using the following command:

```
Set-Mailbox mailbox_name -ApplyMandatoryProperties
```

where:

mailbox_name is the name of the Vault Service account's mailbox. If *mailbox_name* contains spaces, enclose it in quotation marks.

5 Run `SetEVThrottlingPolicy.ps1`.

Note: In a cross-forest environment, you must specify the resource domain so that `SetEVThrottlingPolicy.ps1` runs against the Vault Service account's linked mailbox in the resource forest.

See "Creating a mailbox for the Vault Service account" on page 64.

---

6 When `SetEVThrottlingPolicy.ps1` finishes, close the Exchange Management Shell.

7 If you want to force these changes to take effect immediately, restart the Microsoft Exchange RPC Client Access service on each Exchange server where the service exists.

If you do not restart the service, the changes can take up to two hours to take effect by default.

You can also run `SetEVThrottlingPolicy.ps1` remotely from the Exchange server under PowerShell. When you run the script remotely, use the `-server` switch to specify the name of the Exchange mailbox server.

In this case, the full syntax for this script is:

```
.\SetEVThrottlingPolicy.ps1 -user domain\user_name -server
exchange_mailbox_server
```

Granting the Vault Service account Send As permission on the system mailboxes

The Vault Service account requires Send As permission on the Enterprise Vault system mailbox on each Exchange mailbox server. You can set this permission manually on each account, or use the following procedure.

To grant the Vault Service account Send As permission on a system mailbox

1   Log in to the Exchange Server using an account that is assigned the management role "Active Directory Permissions".

By default, members of the "Organization Management" role group are assigned this role.

2   Open the Exchange Management Shell.

3   Run the following command:

```
Add-ADPermission -Identity mailbox_name -User domain\user_name
-AccessRights ExtendedRight -ExtendedRights "send as"
```

where:

- *mailbox_name* is the Enterprise Vault system mailbox. If *mailbox_name* contains spaces, enclose it in quotation marks.

- *domain* is the Active Directory domain that the Vault Service account belongs to.

- *user_name* is the Vault Service account. If *user_name* contains spaces, enclose it in quotation marks.

Assigning Exchange Server permissions to the Vault Service account

Enterprise Vault includes a PowerShell script which assigns the necessary permissions to the Vault Service account.

To assign Exchange Server permissions to the Vault Service account

1   Log in to the Exchange Server using an account that is assigned the following management roles:

- Active Directory Permissions

- Exchange Servers

- Organization Configuration

By default, members of the "Organization Management" role group are assigned these roles.

2 Copy the script called `SetEVExchangePermissions.ps1` from the `\Veritas Enterprise Vault\PowerShell Scripts` folder on the Enterprise Vault media to the Exchange Server.

3 On the Exchange Server, open the Exchange Management Shell.

4 Run `SetEVExchangePermissions.ps1`.

The syntax for this script is:

```
.\SetEVExchangePermissions.ps1 -User domain\user_name [-Server
exchange_server] [-Action <String>] [-Level <String>] [-Verbose
<Boolean>]
```

The parameters are as follows:

`-User` (required)	*domain\user_name* is the Vault Service account and the domain that it belongs to. If *user_name* contains spaces, enclose the whole *domain\user_name* string in quotation marks.
`-Server`	*exchange_server* is the name of the Exchange Server. The default is the Exchange Server on which the script is running.
`-Action`	Add permissions (`Add`) or remove them (`Remove`). The default value is `Add`.
`-Level`	Apply permissions that are required by the mailbox and provisioning task (`All`), or apply read-only permissions that are required by the provisioning task (`Provisioning`). The default value is `All`. This parameter is ignored if the `Action` parameter is set to `Remove`.
`-Verbose`	Show all script output (`$True`) or minimal information (`$False`). The default value is `$False`.

5 If you want to force these changes to take effect immediately, restart the Microsoft Exchange Information Store service on each Exchange mailbox server.

Microsoft Exchange permissions assigned to the Vault Service account

Table 7-1 lists the permissions that `SetEVExchangePermissions.ps1` assigns to the Vault Service account.

Table 7-1 Permissions assigned to the Vault Service account

Path	Object	Permissions
CN=Configuration, CN=Services, CN=Microsoft Exchange, CN=*Organization*, CN=Administrative Groups, CN=*AdminGroup*	CN=Databases and descendant objects.	Read Administer information store Create named properties in the information store Receive as View information store status
	CN=Servers and descendant objects. `SetEVExchangePermissions.ps1` assigns these permissions if Exchange Server 2007 or earlier exists in your environment.	Read Administer information store Create named properties in the information store Receive as View information store status
CN=Configuration, CN=Services, CN=Microsoft Exchange	CN=*Organization*.	Read
CN=Configuration, CN=Services, CN=Microsoft Exchange, CN=*Organization*	CN=ELC Folders Container and descendant objects.	Read
	CN=Global Settings and descendant objects.	Read
	CN=Transport Settings.	Read
CN=Configuration, CN=Services, CN=Microsoft Exchange, CN=*Organization*, CN=Transport Settings	CN=Rules.	Read
CN=Configuration, CN=Services, CN=Microsoft Exchange, CN=*Organization*, CN=Transport Settings, CN=Rules	CN=Journaling and descendant objects.	Read
	CN=JournalingVersioned and descendant objects.	Read

Enterprise Vault client access with Exchange Server archiving

Users can access and manage items in archives using various client access methods, which include the following:

- Enterprise Vault Outlook Add-In

- Enterprise Vault Client for Mac OS X

- Enterprise Vault Office Mail App (for OWA 2013 and later, and Outlook 2013 and later)

- OWA clients (for OWA 2010)

- Enterprise Vault customized shortcuts

Requirements for the Enterprise Vault Outlook Add-In

The Enterprise Vault Outlook Add-In lets users carry out various activities in Outlook, including the following:

- Manually storing items in their Enterprise Vault archives.

- Viewing, copying, and deleting archived items.

- Conducting searches to find items that are stored in archives.

Before users can send items to an archive from within their Outlook client, the Outlook Add-In must be installed on their computers. Install the Outlook Add-In on users' computers after you have configured the Enterprise Vault server.

Users' computers must have the following:

- One of the following versions of Windows:

  - Windows 7

  - Windows 8

  - Windows 10

- Internet Explorer 9 or later, with JavaScripting enabled.
  This must be installed, even if it is not used.

- TCP/IP protocol.

- Outlook 2010 or later mail client.
  Install Internet Explorer before you install the mail client.

- Microsoft Visual C++ 2013 (x86) and (x64) redistributable packages. If these do not exist on the user's computer, they are installed automatically by the Enterprise Vault Outlook Add-In installer.

- If you plan to enable Vault Cache, Background Intelligent Transfer Service (BITS) 2.0 or later must be installed and enabled on users' computers. This service is used by Microsoft Windows Update and is included in all recent versions of Windows. If necessary, it can be downloaded from the Microsoft website.

- If you plan to enable Vault Cache, and you have disabled the expansion of PST files on users' computers by setting the registry entry, PstDisableGrow, then you need to request and install the appropriate Outlook hotfix from Microsoft. Note that the hotfix may already have been installed as part of a Microsoft Update.

  You will also need to configure the registry setting PSTDisableGrowAllowAuthenticodeOverrides on users' computers, as described in the *Setting up Exchange Server Archiving* guide.

- If you plan to enable the Windows Search plug-in, Windows Search 4.*x* or later must be available on the desktop computers.

  If necessary, you can download Windows Search from the following address: http://www.microsoft.com/windows/desktopsearch/downloads/default.mspx

Requirements for Enterprise Vault Client for Mac OS X

The Enterprise Vault Client for Mac OS X provides Enterprise Vault functionality to users of Microsoft Outlook for Mac 2011 or 2016. These users can archive, restore, and delete items, and conduct searches of the items in their archives.

You can install the Enterprise Vault Client for Mac OS X on any computer that meets the following requirements:

- Mac OS X version 10.9 (Mavericks) or later

- One of the following versions of Outlook for Mac:

  - Outlook for Mac 2011 version 14.0.0 or later

  - Outlook for Mac 2016 version 15.8.1 or later

- Safari version 7.0 or later

For the latest information on supported versions of software, see the Enterprise Vault *Compatibility Charts* at http://www.veritas.com/docs/000097605.

Requirements for the Enterprise Vault Office Mail App

The Enterprise Vault Office Mail App provides Enterprise Vault functionality to OWA 2013 and later users. You can also enable the Office Mail App for Outlook 2013 and later users, as an alternative to the Outlook Add-In or in addition to it.

The requirements for the Office Mail App are as follows:

- Internet Explorer 9 or later must be installed on users' computers. For the latest information on supported browsers, see the Enterprise Vault *Compatibility Charts* at http://www.veritas.com/docs/000097605.

- For the Office Mail App to work correctly on tablets or phones with Exchange Server 2013, you must install Cumulative Update 3 for Exchange Server 2013 (see https://support.microsoft.com/kb/2892464). Without Cumulative Update 3, you cannot restore or delete archived items with the Office Mail App.

For information about setting up the Office Mail App and the additional configuration required, see *Setting up Exchange Server Archiving*.

Requirements for OWA

You can configure OWA access to Enterprise Vault after you have set up your Enterprise Vault server for Exchange Server archiving. The instructions for configuring OWA access to Enterprise Vault assume that you have already configured OWA on Exchange Servers.

To provide Enterprise Vault access in OWA 2010 clients, the Enterprise Vault OWA 2010 Extensions are required on the Exchange Server 2010 CAS computers.

See "Requirements for Enterprise Vault OWA Extensions" on page 72.

Enterprise Vault OWA Extensions are not required for later OWA clients. Instead, the Enterprise Vault Office Mail App provides Enterprise Vault functionality in OWA 2013 and later clients.

See "Requirements for the Enterprise Vault Office Mail App" on page 72.

Requirements for Enterprise Vault OWA Extensions

All the Exchange Servers on which you install the Enterprise Vault OWA Extensions should be at the same Exchange Server service pack and hotfix level.

When you install the Enterprise Vault OWA Extensions on your Exchange Servers, ensure that you install the same Enterprise Vault release version of the extensions on all the Exchange Servers.

The following are required for accessing Enterprise Vault from OWA clients:

- Enterprise Vault OWA 2010 Extensions require Exchange Server 2010 SP1 or later. Install the Enterprise Vault OWA 2010 Extensions on the Exchange CAS computers.

- The following Role Services must be installed for the web server (IIS):

    - IIS Management Scripts and Tools

    - IP and Domain Restrictions

    In addition, the option **Address and Domain Restrictions** in Feature Delegation must be set to Read/Write. To find this option, open Internet Information Services (IIS) Manager and click the server object in the navigation pane. Open Feature Delegation and ensure that **Address and Domain Restrictions** is included in the listed options.

- MSXML is required on Exchange Servers. MSXML is installed automatically with Internet Explorer 7.0 and later.

Customized shortcuts

If you do not want to install the Enterprise Vault clients on desktop computers, you can configure Enterprise Vault customized shortcuts in the Exchange Mailbox Policy. These shortcuts let users view an HTML version of their archived items. In addition, the users can open the Enterprise Vault browse and search facilities in a browser window to access and manage the archived items.

On Windows computers, Internet Explorer 9 or later with JavaScripting enabled must be installed on each user's computer.

On Mac computers, the Safari browser and Outlook for Mac email client are supported. For details of supported versions, see the Enterprise Vault *Compatibility Charts* at http://www.veritas.com/docs/000097605.

Browser-based access to archives

Users can access the contents of their archives without installing the Enterprise Vault Outlook Add-In on their desktop computers. Instead, they can access their archives by opening the Enterprise Vault Search facilities in a web browser.

The Enterprise Vault Search URL is as follows:

http://*web_server_name*/EnterpriseVault/search/

Requirements for RPC over HTTP

This section describes the requirements to support RPC over HTTP access for Outlook Anywhere users.

Requirements for Outlook Anywhere access to Enterprise Vault

In Exchange Server 2010 environments, Outlook in RPC over HTTP mode is called Outlook Anywhere. To support Enterprise Vault requests from Outlook Anywhere clients, no Enterprise Vault extensions are required on the Exchange CAS computer. However, you need to configure RPC over HTTP access on the Enterprise Vault server.

Outlook on users' computers needs to be configured to use RPC over HTTP, and the Enterprise Vault Outlook Add-In needs to be installed on users' computers. See the *Setting up Exchange Server Archiving* manual for instructions.

Additional requirements for Domino Server archiving

This chapter includes the following topics:

- Domino Server archiving requirements for all Enterprise Vault servers
- Requirements for Domino mailbox archiving
- Requirements for Domino journaling archiving

Domino Server archiving requirements for all Enterprise Vault servers

For all Domino archiving, you must install the Notes client on every Enterprise Vault server.

Note: The Enterprise Vault Domino Gateway has different requirements from those of the Enterprise Vault servers.

See "Required software for Enterprise Vault Domino Gateway" on page 76.

Install Notes client on every Enterprise Vault server, as follows:

- Install Notes 8.5.3 or later client software. For details of the latest supported software versions, see the Enterprise Vault *Compatibility Charts* (http://www.veritas.com/docs/000097605).
- If you installed the Notes client with the Multi-User Install option, log on as the Windows account that the Enterprise Vault services will use. This is normally the Vault Service account.

- Start the Notes client and complete its configuration wizard. Use the ID file that you want to use for Domino archiving.
  See "About the user ID for Domino mailbox archiving" on page 83.

Requirements for Domino mailbox archiving

For Domino mailbox archiving, you need to configure the following:

- One or more Enterprise Vault Domino Gateways.
  The Enterprise Vault Domino Gateway is a Domino server that is customized by Enterprise Vault configuration. The Enterprise Vault Domino Gateway provides the interface between Notes clients and Enterprise Vault. All the major actions on archived data (opening, restoring, deleting and searching) are handled by the Enterprise Vault Domino Gateway.

- One or more Enterprise Vault servers. If necessary, you can use the Enterprise Vault Domino Gateway to run Enterprise Vault services and tasks.

- Target Domino mail servers.

- Enterprise Vault client extensions for Notes and Domino Web Access.

If you are going to install Enterprise Vault Administration Console on a remote computer, then you must also install Notes 8.5.3 or later on that computer to manage Domino user archives.

For details of the latest supported software versions, see the Enterprise Vault *Compatibility Charts* (http://www.veritas.com/docs/000097605).

Required software for Enterprise Vault Domino Gateway

The Enterprise Vault Domino Gateway must be a Windows server that is running Enterprise Vault 12.1 and one of the following:

- Version 8.5.3 or later service pack, of both Domino Server (64-bit version) and Notes Client

- Version 9.0.0 or later service pack, of both Domino Server (64-bit version) and Notes Client

It is best practice for the standard Domino mail templates to be present on the Enterprise Vault Domino Gateway. These templates are required by the Enterprise Vault `EVinstall.nsf` installer.

For details of all supported software versions and the required hotfixes, see the Enterprise Vault *Compatibility Charts* (http://www.veritas.com/docs/000097605).

You need at least a Domino Messaging server license for each Enterprise Vault Domino Gateway.

Required software for target Domino mail servers

Target Domino mail servers that you want to archive must be running Domino Server 8.0.0 or later.

For details of the latest supported software versions, see the Enterprise Vault *Compatibility Charts* (http://www.veritas.com/docs/000097605).

Requirements for Enterprise Vault extensions for Notes clients

Client access to archived items from Notes or Domino Web Access (DWA) clients is provided through changes to the Notes and DWA mail templates; no application needs to be installed on user workstations. You install the updated mail templates on target Domino mail servers and DWA servers throughout an organization.

Users who require Enterprise Vault functionality available in their Notes client must have Notes Client 8.0.0 or later installed on their workstations.

For details of the latest supported software versions, see the Enterprise Vault *Compatibility Charts* (http://www.veritas.com/docs/000097605).

To enable the use of Enterprise Vault Search from within Notes or DWA mail clients, users must have Internet Explorer 9 or later installed on their workstations, and it must be set as the default web browser in Notes. In addition, you need to configure Single Sign-On for the users on the Enterprise Vault Domino Gateway.

See "Configuring Single Sign-On on the Enterprise Vault Domino Gateway" on page 80.

Preinstallation tasks for Domino mailbox archiving

You should have already created the following:

- The Vault Service account

- A SQL login account for the Vault Service account

- DNS aliases for the Enterprise Vault server and site

See "Preinstallation tasks for Enterprise Vault server" on page 45.

You now need to perform the following tasks to set up Domino server and Notes on the Enterprise Vault Domino Gateway computer. The following steps must be completed before you install Enterprise Vault on the computer. This ensures that the Enterprise Vault installation program detects that this is a Domino server and will install the extension manager files and other database files.

- Use IBM Domino Administrator client to do the following:

- Register the Domino server that will run on the Enterprise Vault Domino Gateway computer, and set up the configuration for this server in the Domino Directory.
  See "Register the Enterprise Vault Domino Gateway" on page 78.

- Identify or create a user ID for the Domino mailbox archiving.
  See "About the user ID for Domino mailbox archiving" on page 83.

- Configure the server documents for the Domino mail servers from which Enterprise Vault will archive.
  See "Configuring the server document for each target Domino mail server" on page 85.

- On the computer that will host the Enterprise Vault Domino Gateway, do the following:

  - Install Domino server binaries and configure the Domino server.
    See "Install and configure Enterprise Vault Domino Gateway" on page 86.

  - Install Notes client binaries and hotfix, and configure the client. Use the ID file that you want to use for Domino archiving.
    See "Domino Server archiving requirements for all Enterprise Vault servers" on page 75.

After you have completed these tasks, you can install Enterprise Vault and perform the initial configuration.

See "Installing Enterprise Vault (wizard)" on page 112.

You can then complete the configuration of Domino mailbox archiving. See the *Setting up Domino Server Archiving* manual for instructions.

Register the Enterprise Vault Domino Gateway

There must be at least one Enterprise Vault Domino Gateway for each Domino domain to be archived. In a production environment, the Enterprise Vault Domino Gateway should not be used as a general mail server.

The Enterprise Vault Domino Gateway can be a partitioned Domino server.

Use the IBM Domino Administrator Client to register the Enterprise Vault Domino Gateway, and configure the server document, as described in this section. If you plan to have several Enterprise Vault Domino Gateway computers in your Domino domain, repeat the following tasks for each Enterprise Vault Domino Gateway:

- Configure the Internet port for HTTP on the Enterprise Vault Domino Gateway.

- Configure server security.

- Set up Single Sign-On on the Enterprise Vault Domino Gateway.

- Optionally, add the Enterprise Vault Domino Gateway servers to a Domino server cluster.
- Optionally, configure an alias URL for web connections to the Enterprise Vault Domino Gateway server.

Configuring the Internet port for HTTP on the Enterprise Vault Domino Gateway

Enterprise Vault requires the HTTP task to be configured on the Enterprise Vault Domino Gateway. As IIS and the Domino server HTTP task both use port 80, change the port used by the Domino server.

To configure the Internet port for HTTP on the Enterprise Vault Domino Gateway

1 In the IBM Domino Administrator Client, open the server document for the Enterprise Vault Domino Gateway.

2 Select the **Ports** tab and then the **Internet Ports** tab in the subdocument.

3 On the **Web** tab, set the TCP/IP port number to something other than 80; for example, 8080.

Configuring server security for the Enterprise Vault Domino Gateway

Use the IBM Domino Administrator Client to configure the server document. If you plan to have several Enterprise Vault Domino Gateway computers in your Domino domain, repeat the following procedure for each Enterprise Vault Domino Gateway.

To configure server security for the Enterprise Vault Domino Gateway

1 Open the **Security** page of the server document.

2 In the **Programmability restrictions Who can** section, ensure that the user who will sign the mail templates is displayed in the field **Sign agents or XPages to run on behalf of the invoker**.

3 Scroll down to **Server Access**.

4 Add the user who will create the Enterprise Vault Domino Gateway mail template to **Create master templates**.

5 Add the target Domino mail servers to **Trusted servers**.

6 Click **Save and Close**.

7 Repeat steps 1 through 6 for each Enterprise Vault Domino Gateway.

Configuring Single Sign-On on the Enterprise Vault Domino Gateway

To enable authentication for the archive search feature, you need to set up Single Sign-On on the Enterprise Vault Domino Gateway.

The following procedure assumes that you are not using Internet Sites documents, if you are then use the procedure outlined in the Domino documentation.

For more detail on how to configure Single Sign-On using Web Configuration, see the following IBM article:

https://publib.boulder.ibm.com/infocenter/iseries/v5r4/topic/rzatz/51/sec/secssdom.htm

To configure Single Sign-On on the Enterprise Vault Domino Gateway

1 In the IBM Domino Administrator Client, go to the **Configuration** tab and select **Server** > **All Server Documents** view. Select (but do not open) the server document for the Enterprise Vault Domino Gateway.

2 Click **Web**, and select **Create Web SSO Configuration** from the drop-down box.

   ■ In the **Configuration Name** field, change the default name to EVLtpaToken.

   ■ In the **DNS Domain** field, enter the DNS domain of the participating Domino servers.

   ■ In the **Domino Server Names** field, add all the Enterprise Vault Domino Gateways. If you want Single Sign-On to cover DWA users, then you also need to add the target Domino mail servers.

   ■ Click **Keys** and, in the drop-down menu, select **Create Domino SSO Key**. Click **OK**.

   ■ Save and close the Web SSO Configuration.

3 While the server document for the Enterprise Vault Domino Gateway is selected, click **Edit server**.

   ■ Click the **Internet Protocols** tab and then **Domino Web Engine** sub-tab.

   ■ Change the **Session Authentication** field to **Multiple Servers (SSO)** and click **OK**.

   ■ In the **Web SSO Configuration** field, select **EVLtpaToken**.

   ■ Save and close the server document.

Clustering Enterprise Vault Domino Gateway servers

In a Domino Server archiving environment, you can cluster Enterprise Vault services using, for example, Veritas Cluster Server (VCS) or Windows Server Failover Clustering. Use IBM Domino server clustering to cluster Enterprise Vault Domino Gateway servers.

Use the IBM Domino Administrator client to add all of the Enterprise Vault Domino Gateway servers to the same Domino cluster.

Configuring an alias URL for web connections to the Enterprise Vault Domino Gateway server

By default, the fully qualified Internet host name of the Enterprise Vault Domino Gateway server is used as the base URL for mail file extension operations in iNotes, and Enterprise Vault Search operations in Notes client and iNotes. The fully qualified Internet host name is set in the **Basics** subdocument of the server document, as shown in Figure 8-1.

Figure 8-1   Default value for base URL
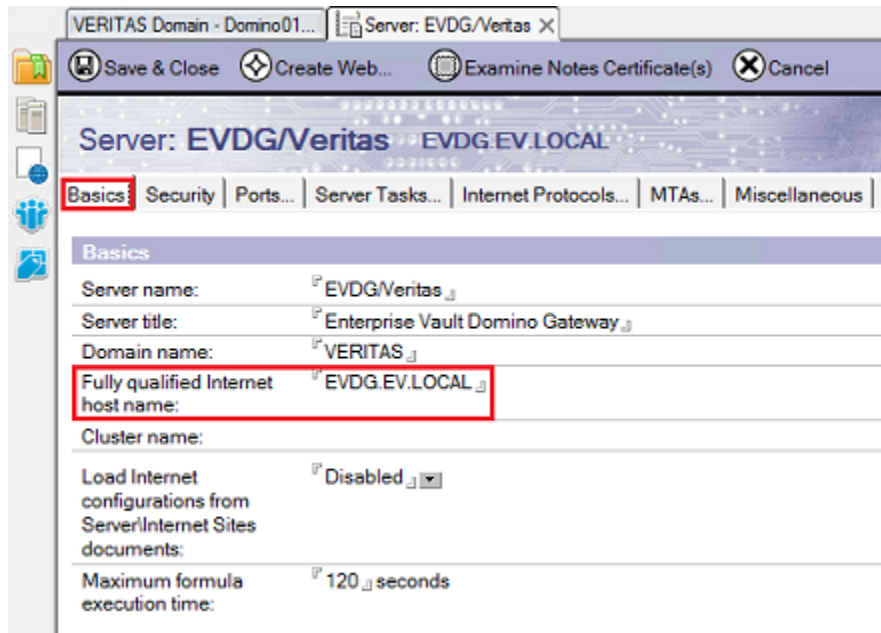
Optionally, you can configure an alias value to use as the base URL instead of the fully qualified host name. The instructions in this section describe how to configure the alias value.

Configuring an alias URL for web connections to the Enterprise Vault Domino Gateway server

1 In DNS, create an alias for each of the Enterprise Vault Domino Gateway servers that you want to make available. This alias address in DNS is used to configure the alias value for the base URL.

2 In the IBM Domino Administrator Client, open the server document for one of the Enterprise Vault Domino Gateway servers.

3 Select the **Internet Protocols** tab.

4 In the **Host name(s)** field on the **HTTP** subdocument, enter the DNS alias that you created earlier for this server. Figure 8-2 shows an example value in this field.

If there is a value in the **Host name(s)** field, then clients use this value as the base URL in web connections to this Enterprise Vault Domino Gateway server. If the field is empty, then clients use the fully qualified Internet host name as the base URL.

5 Restart the Enterprise Vault Domino Gateway server.

6 Repeat steps 2 to 5 for each Enterprise Vault Domino Gateway server.

In a cluster, repeat the steps for each Enterprise Vault Domino Gateway server in the cluster.

Figure 8-2   Alias value for base URL
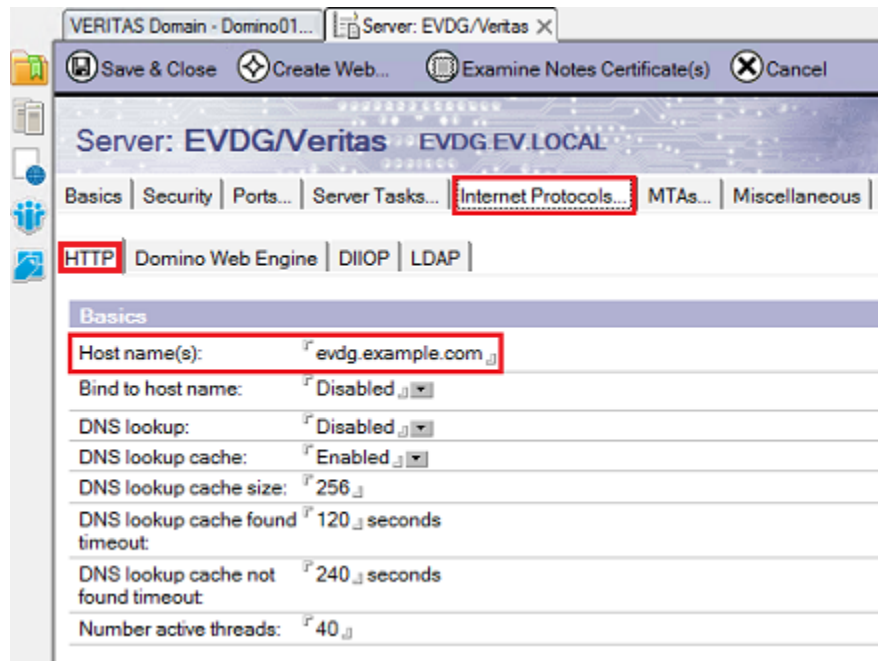
About the user ID for Domino mailbox archiving

The Domino provisioning and mailbox archiving tasks need to access the user's mail databases to do the following:

- Add hidden views.

- Add or update a hidden Enterprise Vault profile document.

- Change mail items into shortcuts.

To comply with the Domino security model, this access to Domino mail databases needs to be done by an authenticated user using a Notes ID file. When you configure the server document for target Domino mail servers, you will give this ID at least Editor access and Delete Documents and Create shared folders/views permissions on mail files to be archived.

See "Granting the Domino archiving user access to all mail files" on page 84.

Later, you specify this ID in the Enterprise Vault Administration Console when you are configuring Domino mailbox archiving. The ID details (including the password) are encrypted and stored in the Enterprise Vault directory database.

Although you can use any user ID file that has the correct level of access, we recommend that you create a generic user account and grant the user the access permissions required.

Creating the Domino archiving user

Use the user registration tool in the Domino Administrator client to create a generic user account. As the user's person document must contain the Domino domain name, the user must be a Notes mail user. It is advisable to give the user a sensible generic name, such as Enterprise Vault Domino Archiving.

You can prefix the last name with the special character '&' to ensure that the user is only displayed at the end of the address list; for example, Enterprise Vault Domino &Archiving/*organization*.

Note: Place the user's ID file and copy it to the Notes data folder on every Enterprise Vault server that will run the Domino archiving task. You must also copy the ID file to the Notes data folder on the Enterprise Vault Domino Gateway (for example `C:\Program Files\IBM\Notes\data`).

Granting the Domino archiving user access to all mail files

The Domino archiving user account needs permissions to all the mail files to be archived. We recommend that you provide **Manager** access to the mail files. The account requires a minimum of **Editor** access with **Delete Documents** and **Create shared folders/views**

Note: If you intend not to archive unread items then the Domino archiving user requires Manager access to the mail files. This is because Domino requires Manager access to determine which items are unread.

If Domino administrators have Manager access to all mail files, then you can use the Manage ACL tool in the Domino Administrator client to add the Domino archiving user to all mail databases.

Repeat the following steps for each target Domino mail server.

To grant the Domino archiving user access to all mail files

1   In the Domino Administrator client, navigate to the Domino mail server and click the **Files** tab.

2   In the tasks pane, click the **Mail** folder to display a list of all the mail databases in the results pane.

3 Select the first mail database, and then press Shift+End to select all the mail databases.

4 Right-click and select **Access Control** > **Manage**.

5 Click **Add** and then click the person icon to select the Domino archiving user from the Domino directory list. Click **OK**.

6 When the user is in the Access Control List dialog box, change the set **User Type** to **Person** and **Access** to **Manager**.

7 Select **Delete documents**.

8 Click **OK** to add the user to the ACL of all mail databases selected.

If no user has Manager access to every mail database, do the following:

■ Place the Domino server administrator's user name in the Full Access Administrators field in the server document.

■ Restart the Domino server.

■ In the Domino Administrator client, choose **Administration** > **Full Access Administration** and complete the procedure described above.

■ If necessary, the administrator can then be removed from the Full Access Administrators field.

Configuring the server document for each target Domino mail server

When configuring the server document for each of the target Domino mail servers, you will need to do the following:

■ The server document for each target Domino mail server must have Enterprise Vault Domino Gateways added as trusted servers.

■ The signing ID that will be used to sign the Enterprise Vault client templates also needs to be given the following permissions:

■ **Sign agents or XPages to run on behalf of the invoker**

■ Create master templates

■ The Domino archiving user needs to be given access to target user mail files.

■ Optionally, you may want to enable Single Sign-On for DWA users.
The main requirement for Single Sign-On is to enable users to use the Enterprise Vault search feature. However, if Single Sign-On is not configured, DWA users will need to re-enter authentication details when opening archived items. To avoid this, you may want to configure Single Sign-On on DWA servers, even if you do not plan to give users access to the Enterprise Vault search feature.

To configure the server document for each target Domino mail server

1   Open the **Security** page of the server document.

2   In the **Programmability restrictions Who can** section, ensure that the user who will sign the mail templates is displayed in the following field:

   ■   **Sign agents or XPages to run on behalf of the invoker**

3   Scroll down to **Server Access**, and add all the Enterprise Vault Domino Gateways in the domain as trusted servers.

4   Add the user who will create the Enterprise Vault mail template to **Create master templates**.

5   Click **Save and Close**.

6   Repeat the above steps for each Enterprise Vault target Domino mail server.

Install and configure Enterprise Vault Domino Gateway

Install Domino Server binaries on each Enterprise Vault Domino Gateway computer. Select the Messaging Server option when installing.

You must install the appropriate Domino hotfixes on the Enterprise Vault Domino Gateway.

You must make the Vault Service account into a local administrator on the Enterprise Vault Domino Gateway.

The Domino server on the Enterprise Vault Domino Gateway must run under the Vault Service account. It is best practice to run the Domino server as a service, but be aware that the server console is not displayed when running a service under an account other than the system account. This is a Microsoft Windows limitation. To see the console, you can connect to it remotely.

If you want to have the server console displayed locally while you are configuring Domino Mailbox archiving, you can run the Domino server as an application as follows:

■   Log on to the Enterprise Vault Domino Gateway computer using the Vault Service account.

■   In Windows Services console, if the Domino Server service is running, stop it.

■   Disable the Domino Server service.

- Start the Domino Server (by double-clicking the desktop icon or running `Domino program directory\nserver.exe`), and select the option to start the server as a regular application. The Domino server configuration starts.

During Domino server configuration, do the following:

- Supply the Domino Server ID that was created when you registered the Domino server on the Enterprise Vault Domino Gateway.

- Select the option **Web Browsers (HTTP Services)** on the Internet Services page to add the HTTP server task.

- For optimum performance, use the **Customize** button to remove all but the minimum server tasks. The following Domino server services are the minimum required on the Enterprise Vault Domino Gateway:

  - Indexer (Update)

  - Administration process (AdminP)

  - Domino web server (HTTP)

Note: In a production environment, start the Domino Server on the Enterprise Vault Domino Gateway as a service running under the Vault Service account.

To ensure that Enterprise Vault can configure user mail files for archiving, and subsequently update the users' mail files with any archiving policy changes, the Domino Directory should replicate frequently to the Enterprise Vault Domino Gateway.

To enable DWA users to open those archived MIME items that are signed or encrypted there must be an SSL connection to the Enterprise Vault Domino Gateway. In this case, you must configure the Enterprise Vault Domino Gateway for SSL. If you do not do this configuration, DWA users receive the following error message:

```
Unable to complete the current operation.
SSL is required for secure mail,
but is not enabled on Domino Server.
Please notify your administrator.
```

Requirements for Domino journaling archiving

This section describes the minimum requirements for Domino journaling archiving. For details of the latest supported software versions, see the Enterprise Vault *Compatibility Charts* (http://www.veritas.com/docs/000097605).

Requirements for Enterprise Vault archiving from Domino Journaling databases

Enterprise Vault will archive from any subfolder of the target Domino server's Data directory. Each subfolder, which must already exist, must be an immediate subfolder of the Data directory, and not lower down the folder structure. Otherwise, the Domino Journaling task fails to find any databases to archive.

By default, Enterprise Vault archives from all Domino Journaling databases that are in the subfolder and use the STDMailJournaling template. You can use a registry value to specify other templates to use. See the *Setting up Domino Server Archiving* manual for instructions.

The normal Enterprise Vault configuration is to retain the original item until the vault store that contains the archived item has been backed up. Enterprise Vault then deletes the original item. The Domino Database Management method must not interfere with this Enterprise Vault process, which means that the Purge and Compact method (specified in the Journaling section of the server configuration document) is unsuitable, because there is the potential to lose items that have, for some reason, not been archived.

Thus, the Domino Journaling database must have its Database Management method set to one of the following in the Journaling section of the server configuration document:

- Periodic Rollover or Size Rollover. The rollover databases must be in the same directory as the initial database in order for them to be archived.

- None. If you select this method the database will continue to grow, so we recommend that you compact the journal directory each night.

Configure Domino Journaling so that the Journaling database is in a subfolder of the server's Data directory. If Domino Journaling is already configured, you may need to move the Journaling database and update the server configuration document.

Support for Enterprise Vault archiving from clustered Domino journal databases

Enterprise Vault can archive from Domino journal databases on Domino Servers that are clustered using Domino application clustering.

To support clustered journal databases, the following requirements must be satisfied:

- Each Domino Server in the cluster should be independently journaling to a local database.

- Mail journaling databases should not be configured to replicate to other Domino servers in the cluster. This includes both cluster replication and scheduled replication.

- Enterprise Vault should be configured to archive from the Domino journal databases on each server in the cluster.

Configuring access for Enterprise Vault to Domino domain, server, and Journaling location

When you configure Enterprise Vault to archive a Domino Journaling location you must supply at least one Notes ID file. Enterprise Vault requires three levels of access, to domain, server, and journaling location. You can use a different ID file for each level or, for simplicity, a single ID file.

The access levels are as follows:

- Access to the Domino domain. This is provided by the ID file of a user who is enabled for Notes mail and whose account is in the same domain as the server. This account must have read access to the Domino Directory.

- Access to the Domino server. This is provided by the ID file of a user who has access to the Domino server and its directories.
  By default, Enterprise Vault will use the same ID file as is used to access the domain.

- Access to the Domino Journaling location. This is provided by the ID file of a user who has Editor, Designer, or Manager access to the journaling databases, and also has the Delete Documents permission. If the database is encrypted, this ID file must be the one that was used to encrypt the database.
  By default, Enterprise Vault will use the same ID file as is used to access the server. If you do not specify a file for server access, Enterprise Vault will use the same ID file as is used to access the domain.

To configure access for Enterprise Vault

- ◆ Place the user's ID file and copy it to the Notes data folder on every Enterprise Vault server that will run a Domino Journaling task (for example `C:\Program Files\IBM\Notes\data`).

Domino mailing list groups

To ensure the expansion of Domino mailing list groups when using Enterprise Vault Compliance Accelerator, set the Mail Domain field explicitly when you configure Domino mailing list groups.

Client access for Domino journal archiving

Client users can access Domino Server journal archives by using the browser-based search facilities in Enterprise Vault.

Additional requirements for File System Archiving (FSA)

This chapter includes the following topics:

- About the requirements for FSA

- Enterprise Vault server requirements for FSA

- About FSA shortcuts

- About the FSA Agent

- Preparing file servers for FSA

- Client requirements for FSA

About the requirements for FSA

For full details of all the supported versions of required products, see the Enterprise Vault Compatibility Charts. That document also provides full details of the target platforms, operating systems and protocols that Enterprise Vault supports for FSA, and lists the operating systems supported for client access of archived items, including opening Internet and placeholder shortcuts to archived items.

Enterprise Vault server requirements for FSA

An Enterprise Vault Storage service is required on the Enterprise Vault server that hosts FSA.

Internet Explorer 9 or later is required on the Enterprise Vault server computer that hosts FSA.

If you are implementing FSA but not Exchange Server archiving, you do not need to install Outlook on the Enterprise Vault server. However, Outlook is required on the Enterprise Vault server if you want to access any files that Enterprise Vault archived before Enterprise Vault 7.0.

Note also that if FSA archives `.MSG` files then Enterprise Vault indexing of these files is restricted unless Outlook is installed on the Enterprise Vault server that archives from the file server. For example, Enterprise Vault can index the content of Outlook messages, but not the message subjects or attachments. If you want the full indexing functionality, install Outlook on the Enterprise Vault server.

If you archive Outlook `.MSG` files from a file server and Outlook is not present on the Enterprise Vault server, Enterprise Vault generates a warning message in the Enterprise Vault event log. If you do not want to receive these warning messages you can prevent them by setting a registry value. To prevent the messages, add a DWORD registry value named WarnForMissingOutlook with a value of 0 to the following registry key on the Enterprise Vault server:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \Storage
```

About FSA shortcuts

When a file is archived, Enterprise Vault can optionally leave one of the following types of shortcut in its place:

- A placeholder shortcut. This is a special file that appears exactly as the original file but, when opened, forces Enterprise Vault to fetch the archived file. A Placeholder service needs to be configured to create these shortcuts.

- An internet (URL) shortcut. This is a `.url` text file containing a hypertext link to the archived file. The Placeholder service is not required to create these shortcuts.

Enterprise Vault cannot create placeholders for certain legacy files. This is particularly true of files that have extended attributes because they were previously stored in an HPFS (OS/2) file system.

Check in the Enterprise Vault Compatibility Charts that users' operating systems are supported for client access of archived items, including opening internet and placeholder shortcuts.

Placeholder shortcut requirements

Enterprise Vault supports the creation of placeholder shortcuts on the following file system types:

- NTFS.
  The FSA Agent must be installed on each Windows file server to provide the Enterprise Vault Placeholder service.
  See "About the FSA Agent" on page 93.
  Each disk on which placeholder shortcuts are required must be an NTFS device; it is not sufficient to use a non-NTFS device that appears on the network as an NTFS device.
  The Enterprise Vault server uses CIFS when accessing the file system, for example, to archive files.

- NetApp Filer.
  The FSA Agent is not required. The Enterprise Vault server runs an equivalent process to the Placeholder service, and accesses the NetApp Filer using CIFS.

- EMC Celerra/VNX.
  The FSA Agent is not required. The Enterprise Vault server runs an equivalent process to the Placeholder service, and accesses the EMC Celerra/VNX file system using CIFS.

Before installing and configuring FSA, ensure that the target file system that you want to archive is supported.

See the Enterprise Vault *Compatibility Charts* at
http://www.veritas.com/docs/000097605.

About the FSA Agent

For Windows file servers, the FSA Agent must be installed on a target file server if you want to do any of the following:

- Use placeholder shortcuts.

- Implement File Blocking.

- Gather data for FSA Reporting.

In an environment where Windows file servers are grouped in a cluster, the FSA Agent must be installed on each cluster node.

Requirements and instructions for installing the FSA Agent are included in *Setting up File System Archiving*.

For non-Windows file servers the FSA Agent is used only in the following circumstances:

■ To implement File Blocking on NetApp file servers you must configure a Windows server in the Administration Console as a file server, and install the FSA Agent on the Windows server to provide a File Blocking agent server for the NetApp file server.
See the *Setting up File System Archiving* guide.

■ To implement FSA Reporting on non-Windows file servers you must configure an FSA Reporting proxy server to gather the FSA Reporting data. If you configure an FSA Reporting proxy server that is not an Enterprise Vault server, the proxy server must have the FSA Agent installed.
See the *Reporting* guide.

Note: To use File Blocking and FSA Reporting on NetApp C-Mode filers, you must have the Enterprise Vault 11.0.1 or later FSA Agent installed.

Preparing file servers for FSA

You can configure and manage file servers in Enterprise Vault with the Vault Service account or an account that belongs to a suitable administrator role. The predefined administrator roles that permit FSA administration are the File Server Administrator and the Power Administrator.

See "Managing administrator security" in the *Administrator's Guide*.

The account that you use must have local administrator rights on the computer on which you run the Administration Console.

For Windows file servers, the account must also meet the following requirements:

■ To perform the following actions, the account must be a member of the local Administrators group on the file server:

  ■ Installation of the FSA Agent, from the Vault Administration Console or manually.

  ■ Configuring or reconfiguring the resource for a file server cluster. The account must be a member of the local Administrators group on each of the file server cluster nodes.

■ The account must have Full control on any share that is configured as a target volume. The account must also have NTFS read permission on the folder that the share maps to.

■ If you want to browse in the Administration Console when selecting folders as targets, the account must have Browse permissions on the target folders. Otherwise you must specify the folder path by typing it.

For Windows file server targets, if you do not want to add the Vault Service account as a member of the local Administrator's group on the file server, the account can run as a member of the built-in local Print Operators group, and with a set of minimum permissions and privileges. If you install the FSA Agent, the installer configures this set of minimum requirements for the account.

See "About the permissions required by the Vault Service account for FSA" in *Setting up File System Archiving*.

Before configuring a NetApp file server for archiving you must set up the required administrative permissions on the file server.

For instructions on how to prepare a NetApp file server or EMC Celerra/VNX device, see *Setting up File System Archiving*.

Client requirements for FSA

The following client access to archived items is available with FSA:

■ If shortcuts are created in the item's original location, users can access an archived item by double-clicking the shortcut on the file server.

■ If shortcuts are not created, users can access the archived items in the archives by using the Enterprise Vault Search facilities (requires Internet Explorer 9 or later with JavaScripting enabled).

Additional requirements for SharePoint Server archiving

This chapter includes the following topics:

- About the Enterprise Vault server requirements for SharePoint Server archiving

- Requirements for SharePoint Servers

About the Enterprise Vault server requirements for SharePoint Server archiving

Internet Explorer 9 or later is required on the server that hosts the Enterprise Vault Storage service.

If you are implementing SharePoint Server archiving but not Exchange Server archiving, you do not need to install Outlook on the Enterprise Vault server. However, Outlook is required on the Enterprise Vault server if you want to access any files that Enterprise Vault archived before Enterprise Vault 7.0.

Requirements for SharePoint Servers

The required software and settings for the SharePoint Servers are as follows:

- You must use a version of Microsoft SharePoint that Enterprise Vault supports. For more information see the Enterprise Vault *Compatibility Charts* at http://www.veritas.com/docs/000097605.

- Ensure that the Vault Service account has local administrator permissions on the SharePoint Server computer.

- The account under which the Enterprise Vault SharePoint task runs (typically the Vault Service account) must have full access to target site collections and their content.

- SharePoint Servers must be running Windows Server 2008 with Service Pack 1 or later. If Windows Server 2008 with Service Pack 1 is installed, you must also install the following mandatory hotfix for IIS:

  http://support.microsoft.com/kb/949516

  Note the following:

  - The hotfix that Microsoft provides for Windows Vista is the hotfix to use for Windows Server 2008.

  - By default, the Microsoft web page presents a hotfix download that matches the operating system of the computer that you are using. On the download page, choose the option to show hotfixes for all platforms and languages so that you can select the correct version of the hotfix.

- If you install in a server farm, you must install the Enterprise Vault components on all the front-end web servers.

- The Enterprise Vault SharePoint components require the Enterprise Vault SharePoint HttpModule. The Enterprise Vault Setup program automatically installs the Enterprise Vault HttpModule when you choose to install the Enterprise Vault SharePoint component.

- The DCOM port (135) must be open on the target SharePoint system.

- If Enterprise Vault and SharePoint run on separate computers, we recommend that you do not install Backup Exec on the same computer as the Enterprise Vault Microsoft SharePoint Components.

- You must use host names in the URL when adding SharePoint targets.

- To add a web application in SharePoint 2013 or later as an archiving target, you must ensure that the web application has the following authentication settings:

  - Integrated Windows authentication is enabled.

  - Trusted identity providers and forms-based authentication for all zones in the target web application are disabled.

  To add a web application in SharePoint 2010 as an archiving target, you must ensure that the web application has the classic mode authentication enabled.

> **Note:** Authentication settings are required not only for adding the web application as a target but also for archiving its content. Archiving stops if these settings are changed after adding the target.

- When a site in SharePoint 2013 or later uses claims authentication, the Claims to Windows Token Service (C2WTS) must be configured and running.
  For more information on how to configure C2WTS, see the following article:
  http://support.microsoft.com/kb/2722087

For full details of all the supported versions of required products, see the Enterprise Vault *Compatibility Charts* at http://www.veritas.com/docs/000097605.

About SharePoint security certificates

The certificate used by the SharePoint virtual server or web application must have the same name as the SharePoint URL. For example, if the SharePoint URL is `https://sharepoint`, then the name of the certificate used when issuing a certificate request must be `sharepoint`.

If the names do not match, Enterprise Vault will not be able to validate the SharePoint site when you try to configure it in the Administration Console.

Additional requirements for SMTP Archiving

This chapter includes the following topics:

■ Additional requirements for Enterprise Vault SMTP servers

Additional requirements for Enterprise Vault SMTP servers

The required software and settings for Enterprise Vault SMTP servers are as follows:

■ You must install the Enterprise Vault SMTP Archiving component on each Enterprise Vault server that is to perform SMTP archiving.
Make sure that the required port for SMTP is open on each Enterprise Vault SMTP server.

■ Administrators who are to manage SMTP Archiving using the Administration Console need the Enterprise Vault SMTP Administrator role. This role is included in the Enterprise Vault Messaging Administrator and Enterprise Vault Power Administrator roles.

■ If you intend to secure SMTP connections using SSL, you must obtain an SSL certificate to authenticate the Enterprise Vault servers to which MTAs will connect. You can use a single certificate that authenticates multiple servers, or use a separate certificate for each.
See the *Setting up SMTP Archiving* guide.

■ Local disk space is required on the Enterprise Vault SMTP server for the SMTP holding folder. The SMTP service accepts messages and places them as EML files in this folder. The SMTP Archiving task then processes the messages and archives those that contain SMTP target addresses. When you create the SMTP

Archiving task, you specify its SMTP holding folder. The holding folder location is displayed in the properties of the SMTP Archiving task.

The Vault Service account must have full access to the SMTP holding folder. For security, other accounts should not have access to this folder.

Ensure that virus scanning software excludes this folder. MTAs that send the messages to Enterprise Vault should perform virus scanning of the messages.

- To ensure that Enterprise Vault processes journal reports (P1 messages) correctly, these messages must comply with the format described in the following article:

  http://technet.microsoft.com/library/bb331962.aspx

  Note that SMTP Archiving does not currently process the journal report information in messages that are journaled by Domino Server.

- If you are implementing SMTP Archiving but not Exchange Server archiving, you do not need to install Outlook on the Enterprise Vault SMTP server. However, Outlook is required on the Enterprise Vault server if you plan to export archived items in MAPI format, for example, using the Export to PST feature in Discovery Accelerator. If the Storage service that manages the archived items is hosted on a separate Enterprise Vault server, then Outlook must be installed on that server.

The Enterprise Vault *Compatibility Charts* at http://www.veritas.com/docs/000097605 contain details of the supported versions of prerequisite software.

Additional requirements for Enterprise Vault Search

This chapter includes the following topics:

- Server requirements for Enterprise Vault Search
- Requirements for installing Enterprise Vault Search Mobile edition on a proxy server

Server requirements for Enterprise Vault Search

Each Enterprise Vault server requires the Net.Tcp Listener Adapter service (NetTcpActivator) for Enterprise Vault Search. This service requires the following Windows Communication Foundation (WCF) Activation features:

- HTTP Activation
- Non-HTTP Activation

The **Prepare my system** option in the Enterprise Vault Install Launcher automatically installs these features, if they are not already installed. However, if you do not want to use the **Prepare my system** option, you can manually install the WCF Activation features.

To add the requirements for Enterprise Vault Search manually

1 Click **Start** > **Control Panel** > **Turn Windows features on or off**.

The **Add Roles and Features** wizard starts.

2 Click **Next** until the **Features** page is shown.

3 Expand **.NET Framework 4.5 Features**.

4 Expand **WCF Services**.

5 Select **HTTP Activation** and then click **Install**.

6 Work through to the end of the wizard.

Requirements for installing Enterprise Vault Search Mobile edition on a proxy server

---

Caution: To maximize security, install Enterprise Vault Search on a reverse proxy server or protect the server with Microsoft Threat Management Gateway (TMG).

You can install Enterprise Vault Search Mobile edition on a proxy server on which you have also installed the following:

- One of the following versions of Windows:

  - Windows Server 2012

  - Windows Server 2012 R2

  The server must have an NTFS file system.

- The Enterprise Vault API Runtime. The process of installing Enterprise Vault Search Mobile edition on the proxy server automatically installs the API Runtime, if it is not already present.

- Internet Information Services (IIS) 7.5 or later.
  The following table lists the minimum set of role services that you must install for the Web Server (IIS) role.

Common HTTP Features	■ Static Content ■ Directory Browsing ■ HTTP Errors ■ HTTP Redirection
Application Development	■ ASP.NET ■ ISAPI Extensions ■ ISAPI Filters
Health and Diagnostics	■ HTTP Logging ■ Logging Tools
Security	■ Request Filtering
Performance	■ Static Content Compression
Management Tools	■ IIS Management Console

- Microsoft .NET Framework 4.5.2.

  The Windows Communication Foundation (WCF) HTTP Activation feature must be installed and enabled. You do not need to install and enable the non-HTTP Activation feature.

In addition, you must ensure the following:

- The proxy server is part of a Windows domain.

- Distributed COM (DCOM) is enabled.

- Port 135 is open on the firewall.

- None of the following is also installed on the proxy server:

  - The Enterprise Vault server software

  - Microsoft SQL Server

  - Microsoft Exchange Server (the target system for Enterprise Vault archiving)

Disabling unsafe cryptographic protocols and cipher suites

If you want to give your users Internet access to Enterprise Vault Search without exposing your proxy server to unnecessary security risks, you can disable unsafe cryptographic protocols and cipher suites on the server.

When a client device uses HTTPS to connect to Enterprise Vault Search on a proxy server, the client and server negotiate a common cryptographic protocol to help secure the channel. If the client and server have multiple protocols in common, Internet Information Services (IIS) tries to secure the channel with one of the protocols that IIS supports. However, some protocols are stronger than others; to maximize the security of your environment, you may therefore want to disable the weak protocols in favor of stronger, Veritas-approved alternatives.

You can comply with Veritas recommendations by configuring the cryptographic protocols and cipher suites on your proxy server as follows:

- Enable the TLS 1.1. and 1.2 protocols.

- Disable the SSL 2.0 protocol.

- Disable the RC2, RC4, and DES cipher suites.

The following articles in the Microsoft Knowledge Base provide guidelines on how to implement these changes:

- http://support.microsoft.com/kb/187498

- http://support.microsoft.com/kb/245030

Additional requirements for a standalone Enterprise Vault Administration Console

This chapter includes the following topics:

■ About the requirements for a standalone Enterprise Vault Administration Console

About the requirements for a standalone Enterprise Vault Administration Console

You can install the Enterprise Vault Administration Console on a separate computer that has the following required software:

■ One of the following versions of Windows:

■ Windows 7.
See Standalone Administration Console on Windows 7.

■ Windows 8.

■ Windows 8.1.

■ Windows 10.

■ Windows Server 2012.

■ .NET Framework 3.5 SP1, and .NET Framework 4.5.2.

■ Windows PowerShell 3.0 or later

If Enterprise Vault is configured to archive Exchange servers, you also require one of the following versions of Microsoft Outlook on the remote Administration Console computer:

- Outlook 2010

- Outlook 2013

- Outlook 2016

If Enterprise Vault is configured to archive Domino servers, you require the IBM Notes client on the remote Administration Console computer.

Standalone Administration Console on Windows 7

The standalone Administration Console on Windows 7 requires an activation configuration file. After installation and before using the Administration console, perform the following steps:

1. Create an activation configuration file containing the following lines:

```
<?xml version="1.0" encoding="utf-8" ?>
 <configuration>
   <startup useLegacyV2RuntimeActivationPolicy="true">
     <supportedRuntime version="v4.0"/>
   </startup>
 </configuration>
```

2. Save the configuration file with the name `mmc.exe.activation_config`.

3. Set the `COMPLUS_ApplicationMigrationRuntimeActivationConfigPath` environment variable to the full path of the folder containing the configuration file.

For more information about activation configuration files, see the following Microsoft article: https://msdn.microsoft.com/en-us/library/vstudio/ff361644(v=vs.100).aspx.

2

Installing Enterprise Vault

Licenses and license keys

This chapter includes the following topics:

- Overview of Enterprise Vault licensing

- Obtaining license keys for Enterprise Vault

- Installing Enterprise Vault license key files

- Replacing Enterprise Vault licenses and installing additional licenses

Overview of Enterprise Vault licensing

Enterprise Vault uses the Enterprise Licensing System (ELS). To run the associated Enterprise Vault services, you must install a license key file that covers the Enterprise Vault features that you want to implement.

The following types of Enterprise Vault license are available:

- Production license. This license comprises a product base license and any additional feature licenses. When the license file is installed, the functionality of Enterprise Vault depends on the feature licenses that you have purchased. Production licenses generally do not have an expiry date.

- Trialware license. With this 30 day license, the full functionality of Enterprise Vault is available, but the functionality is time-limited, as defined by the key. When the license expires, the software continues to run in restricted, read-only mode, which allows archived items to be viewed and retrieved, but no items can be archived. Enterprise Vault tasks will not start, and you cannot migrate the contents of personal folder (PST) files to Enterprise Vault.

- Temporary licenses. Temporary licenses are available for 10 day to 90 day duration.
  When the license expires, the software continues to run in restricted, read-only mode, which allows archived items to be viewed and retrieved, but no items can

be archived. Enterprise Vault tasks will not start, and you cannot migrate the contents of personal folder (PST) files to Enterprise Vault.

In an existing Enterprise Vault environment, you can use the Enterprise Vault report, "Content Provider Licensing and Usage Summary", to assist with licensing true-up. See the *Reporting* guide for information on the report.

Obtaining license keys for Enterprise Vault

For information on how to purchase Enterprise Vault licenses, see Veritas Enterprise Vault Licensing Information at the following address on the Veritas website:

https://www.veritas.com/licensing/process

The Enterprise Vault features for which you require licenses include the following:

- Enterprise Vault core services
- Exchange Server mailbox archiving
- Exchange Server journal archiving
- Domino Server mailbox archiving
- Domino Server journal archiving
- Exchange Server public folder archiving
- Migrating PST files
- NSF migration wizard
- SharePoint Server archiving
- IMAP client access

- Vault Cache
- File System Archiving (FSA)
- SMTP archiving
- Policy Manager (EVPM)
- Custom filters and properties
- Migrating collected Enterprise Vault files
- Compliance Accelerator
- Discovery Accelerator
- Data Classification Services
- Retention

After you have purchased licenses and received your License Certificate, Voucher Document, or Upgrade Notification, you need go to the Veritas Licensing Portal at the following address to register and generate your license key file.

https://www.veritas.com/licensing/process/activate

You will need the serial number on the license document or notification in order to generate a Veritas Licensing Portal account.

When you have generated a license key file, you download a zipped and digitally-signed ELS license file. The ELS license file has a unique name and the extension `.slf`. Each license file can contain the license keys for several Enterprise Vault features.

Installing Enterprise Vault license key files

Save this file in a temporary location on each Enterprise Vault server computer.

The Enterprise Vault installation wizard prompts for the location of your ELS license file, and copies the file to the top-level Enterprise Vault folder (for example `C:\Program Files (x86)\Enterprise Vault`). When the Enterprise Vault Admin service is started, it installs the licenses and writes a license information report message to the event log.

You can continue Enterprise Vault installation without an ELS license file, but Enterprise Vault will operate in restricted, read-only mode until you obtain and install a new ELS license.

Replacing Enterprise Vault licenses and installing additional licenses

You can use the Enterprise Vault report, "Content Provider Licensing and Usage Summary", to assist with licensing true-up. More information on this report is given in the *Reporting* guide.

Follow the instructions in this section if you have already installed Enterprise Vault and subsequently want to install additional license files or replace existing license files.

To replace a license or install an additional license

1   Place the new `.slf` license file in the Enterprise Vault folder (for example `C:\Program Files (x86)\Enterprise Vault`).

2   Restart the Enterprise Vault Admin service to install the licenses. The Admin service writes a license information report message to the event log.

3   For a multi-server Enterprise Vault deployment, you must repeat the steps on each Enterprise Vault server.

Installing Enterprise Vault

This chapter includes the following topics:

- About installing Enterprise Vault
- Installing Enterprise Vault (wizard)
- Installing Enterprise Vault (command line)

About installing Enterprise Vault

Before you install Enterprise Vault, do the following:

- Ensure that the computers on which you plan to install Enterprise Vault do not have Unicode characters in their names, as this may prevent Enterprise Vault from operating properly. We strongly recommend that the computer names contain ASCII characters only.
- Check that all the prerequisites for your planned installation have been fulfilled. Run the Deployment Scanner on the computers on which you plan to install Enterprise Vault.
  See "About the Enterprise Vault Deployment Scanner" on page 36.

Enterprise Vault provides both a wizard-based installer and a command line installer. Both installers enable you do to the following:

- Install Enterprise Vault
- Repair an existing Enterprise Vault installation
- Add Enterprise Vault components to an existing installation
- Uninstall Enterprise Vault

Software that is automatically installed

The Enterprise Vault installers automatically install the following software if required:

- Microsoft Visual C++ 2005 SP1 (x86) redistributable package

- Microsoft Visual C++ 2008 SP1 (x86) redistributable package

- Microsoft Visual C++ 2008 SP1 (x64) redistributable package

- Microsoft Visual C++ 2010 SP1 (x86) redistributable package

- Microsoft Visual C++ 2010 SP1 (x64) redistributable package

- Microsoft Visual C++ 2013 (x86) redistributable package

- Microsoft Visual C++ 2013 (x64) redistributable package

- SQLXML 4.0 SP1, if you install the Enterprise Vault Services feature

Core features for an Enterprise Vault server

The installation enables you to install the core Enterprise Vault server features, as follows:

- **Enterprise Vault Services**. All the core Enterprise Vault services. After the installation, you must configure the services before using them. This is done when you run the Enterprise Vault configuration wizard.
  See "About configuring Enterprise Vault" on page 133.

- **Administration Console**. The Enterprise Vault Administration Console. This is a snap-in to the Microsoft Management Console (MMC) that enables you to manage Enterprise Vault. This feature also installs the Enterprise Vault configuration wizard, and the PST Migrator and NSF Migrator wizards.
  If you want to install a standalone Administration Console on a remote system, select this feature only.

- **Search Access Components**. This feature enables users with mobile devices to search for and open the items in their archives.

Additional features

You can install a number of other features as required. The installer always checks that the prerequisites are met before it installs any feature.

The additional features are as follows:

- **Enterprise Vault Lotus Domino Gateway**. This feature provides the interface between Notes and Enterprise Vault. All the major actions on archived data (opening, restoring, deleting and searching) are handled by the Enterprise Vault Domino Gateway.

- **SMTP Archiving Components**. Install the Enterprise Vault SMTP Archiving component on each Enterprise Vault server that is to perform SMTP archiving.
  See "Additional requirements for Enterprise Vault SMTP servers" on page 99.

- **Microsoft SharePoint components**. These components are usually installed on computers other than the Enterprise Vault server.
  See "Requirements for SharePoint Servers" on page 96.

- **Operations Manager**. This feature is a web application that enables you to monitor Enterprise Vault servers remotely from a computer on which Internet Explorer is installed.
  Enterprise Vault Operations Manager must be installed on at least one Enterprise Vault server in a site if you want to monitor the Enterprise Vault servers in that site.

- **Enterprise Vault Reporting**. This feature provides enterprise-level reporting for Enterprise Vault servers, using Microsoft SQL Server Reporting Services as the reporting mechanism. Administrators manage report content and view reports using the Reporting Services Report Manager web application.
  Enterprise Vault Reporting is required if you want to use FSA Reporting.
  Enterprise Vault Reporting requires Microsoft SQL Server Reporting Services (SSRS).
  Enterprise Vault Reporting can be installed on an Enterprise Vault server, but is more typically installed on a separate server that is running SSRS. For more information about installing and configuring Enterprise Vault Reporting, see the *Reporting* guide.

Installing Enterprise Vault (wizard)

The wizard installation enables you to choose the installation options interactively.

To install Enterprise Vault

1. Log in to the Vault Service account.

2. Load the Enterprise Vault media.

3. If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Click **Run Setup.exe**.

   If AutoPlay is not enabled, use Windows Explorer to open the root folder of the installation media and then double-click the file Setup.exe.

4. In the right pane of the Install Launcher click **View ReadMeFirst** under Enterprise Vault. Read the ReadMeFirst before you continue with the installation.

5. In the list in the left pane of the **Veritas Enterprise Vault Install Launcher** window, click **Enterprise Vault**.

6. Click **Server Installation**.

7 In the right pane, click **Installation on first server in new site**.

8 Click **Install**. The Enterprise Vault installation wizard starts.

9 Install the required Enterprise Vault features for this computer.

10 If Domino is installed, the installation lists the Domino partitions that are available. The installation installs the Enterprise Vault Domino Gateway software in each partition that you select.

11 Setup automatically scans the computer to determine whether it meets the Enterprise Vault prerequisites and generates a report. If the computer does not meet all the requirements, the wizard gives you the option to view a report of the findings.

12 Setup checks that the computer is configured to use Enterprise Vault best practice settings.

13 At the end of installation, you may be instructed to restart your computer. The installation continues after you have restarted the computer. There is a confirmation message that informs you that the installation is complete.

Installing Enterprise Vault (command line)

The command line installation enables you do the following:

- Perform a silent installation of Enterprise Vault.

- Run the installation wizard with pre-populated default values.

- Repair, modify, or remove an existing installation.

To install Enterprise Vault

1 Log in to the Vault Service account.

2 Load the Enterprise Vault media.

3 Open a command prompt window and navigate to the following folder on the Enterprise Vault media:

`\Veritas Enterprise Vault\Server`

4 Run `setup (x64).exe` with the required parameters. See below for details of the parameters.

Syntax

`"setup (x64).exe" [/s] /v"COMPONENTS=`*Option*`[|`*Option*`][...]"`

Parameters

`/s`   Optional. Silent installation. Install Enterprise Vault with the default options. You can use other command line options to override the default values.

              If you omit this parameter, the installation wizard starts. You can use other command line options to override the wizard's defaults. By overriding the default values you can click through the wizard without the need to select different options.

`/v`   Mandatory. Introduces command options. Use double quotes around the complete option string. For individual options, use a backslash followed by a double quote to delimit any option that contains a space or a backslash. For example:

```
LOGFILE=\"C:\EV.log\"

LOGFILE=\"C:\My Logs\EV.log\"
```

Options

Use a vertical bar (|) to separate multiple options. For example:

```
/v"COMPONENTS=VAULT|SMTP"
```

The options can be any of the following:

`BESTPRACTICE`   Controls whether to use best practice settings. Possible values are as follows:

              `BESTPRACTICE=0`. Do not use best practice settings

              `BESTPRACTICE=1` (default). Use best practice settings

              See "Best practice settings for Enterprise Vault servers" on page 41.

`DOMINOPARTITIONS`   Specifies the Domino partitions in which you want to install the Enterprise Vault Domino Gateway software.

              Use a vertical bar to separate multiple partitions. For example, to install into Domino partitions 1 and 2:

              `DOMINOPARTITIONS=1|2`

`ENABLEFEATURES`   Controls whether the installer automatically installs all the Windows features and roles that are required by an Enterprise Vault server. Possible values are as follows:

              `ENABLEFEATURES=0` (default). The installer does not install Windows features and roles.

              `ENABLEFEATURES=1`.The installer automatically installs all the required Windows features and roles.

              See "Windows features enabled automatically by the 'Prepare my system' option" on page 301.

`INSTALLDIR`	The folder in which to install. The default folder is `C:\Program Files (x86)\Enterprise Vault`.
`LOGFILE`	The path to the installation log file. The default path is `%temp%\EVInstall.log`
`COMPONENTS`	This is a mandatory option when you install. The components can be any of the following:

- `VAULT`. Installs all Enterprise Vault server components and also `VAC` and `EVSEARCH`.
- `VAC`. Installs the Administration Console. This option is also installed automatically when you specify `VAULT`
- `EVSEARCH`. Installs Enterprise Vault search. This option is also installed automatically when you specify `VAULT`.
- `DOMINO`. Installs Domino archiving and the `VAULT` component.
- `SMTP`. Installs SMTP archiving and the `VAULT` component.
- `SHAREPOINT`. Installs SharePoint archiving.
- `EVOMREPORTING`. Installs Enterprise Vault Reporting.
- `EVOMMONITORINGWEBAPP`. Installs the Enterprise Vault Operations Manager web application and the `VAULT` component.

See

Default options

You can override any of the default options. If you omit the `/s` parameter you can override the options within the installation wizard.

The default options are as follows

- **Installation location:** `C:\Program Files (x86)\Enterprise Vault`
- Domino Partitions: No partitions
- Best practice settings: Use best practice settings
- **Installation log location:** `%temp%\EVInstall.log`

Example commands

- To install the VAULT component with the default options:

  `"setup (x64).exe" /s /v"COMPONENTS=VAULT"`

- To start the installation wizard with the default options, but with the installation log file in `D:\Logs\EVinstall.log`:

  `"setup (x64).exe" /v"LOGFILE=\"D:\Logs\EVinstall.log\""`

- To install the VAULT component in folder `D:\myVault`:

  `"setup (x64).exe" /s /v"INSTALLDIR=\"D:\myVault\" COMPONENTS=VAULT"`

■ To install the VAULT component with the default options but with the installation
   log file in `D:\Logs\EVinstall.log`:

```
"setup (x64).exe" /s /v"LOGFILE=\"D:\Logs\EVinstall.log\"
COMPONENTS=VAULT"
```

Postinstallation tasks

This chapter includes the following topics:

- Default security for the Enterprise Vault Web Access components

- Customizing security for the Enterprise Vault Web Access components

- Customizing security for the Web Access components on client computers

Default security for the Enterprise Vault Web Access components

The Web Access components provide Enterprise Vault users with browser-based access to their archives using the Enterprise Vault Search application.

The Enterprise Vault Web Access components are located in the IIS virtual directory **EnterpriseVault** in the Default Web Site. Although HTTP over TCP port 80 is the default setting for Enterprise Vault client connections to the Web Access components, HTTPS is recommended to ensure the security of transmitted data.

Warning: If you use HTTP, ensure that your network is secure. HTTP communication between Enterprise Vault clients and the Enterprise Vault Web Access components is unencrypted, and therefore vulnerable to interception on the network.

Both Basic authentication and Integrated Windows authentication are configured automatically.

The authentication that is automatically set up affects users when they log in, as follows:

- A user logging in with a browser that supports Integrated Windows Authentication, such as Internet Explorer, must supply domain name and username separately:

Username: *username*

Password: *password*

Domain: *domain*

This domain can never be defaulted.

An Internet Explorer user with suitably-customized browser settings does not need to supply logon details manually because the logon is automatic; Internet Explorer automatically uses the details of the account to which the user is currently logged on.

See "Customizing security for the Web Access components on client computers" on page 121.

- A user logging in to the Web Access components with a browser that does not support Integrated Windows Authentication must supply both domain name and username in response to a single username prompt:

  Username: *domain\username*

  Password: *password*

  It is possible for you to set up a default domain.

  See "Customizing authentication for the Enterprise Vault Web Access components" on page 119.

Customizing security for the Enterprise Vault Web Access components

You can change the port or protocol that is used to access the Web Access components. For example, it is recommended that connections to the application use HTTPS.

See "Customizing the port or protocol for the Enterprise Vault Web Access components" on page 118.

You can also customize the amount of information that users need to provide when logging in to the Web Access components.

See "Customizing authentication for the Enterprise Vault Web Access components" on page 119.

Customizing the port or protocol for the Enterprise Vault Web Access components

You can change the port or protocol that is used to access the Enterprise Vault Web Access components. For example, it is recommended that you configure HTTPS for client connections. If you are configuring HTTPS for access to the

Enterprise Vault Web Access components, you must first configure the Default Web Site in IIS for HTTPS, and install a valid SSL certificate.

If you change the port after items have been archived, existing shortcuts will no longer work. Shortcuts in Outlook and Notes can be updated with the new protocol or port information using Synchronize mailboxes in the Enterprise Vault Administration Console, but customized shortcuts, FSA shortcuts and SharePoint shortcuts cannot be updated.

Before you change the Web Access port or protocol in Enterprise Vault, you must first make the required changes to the Default Web Site in IIS for each server in the Enterprise Vault site. Bear in mind that changing the protocol or port for the Default Web Site will affect all virtual directories in the website, including the FSAReporting virtual directory.

When you have made the necessary changes in IIS, change the Web Access port or protocol settings on the **General** tab of the Site properties in the Administration Console.

If the Enterprise Vault site uses FSA Reporting, you must then perform some additional steps. Otherwise the status of FSA Reporting is shown as Off in the Administration Console. Perform the following steps on each Enterprise Vault server and on each file server in the Site.

Additional steps for FSA Reporting after you change the port or protocol

1   Log on as the FSA Reporting user. The FSA Reporting user is the Windows user account that you specified for FSA Reporting to use when you ran the FSA Reporting Configuration wizard.

2   Open Internet Explorer and select **Tools** > **Internet Options**.

3   If you chose to use an SSL port, click the **Advanced** tab and under **Security** make sure that **Check for server certificate revocation** is not selected.

4   Click the **Security** tab and select the **Local intranet** zone. Then click **Custom Level** to display the Security Settings. Under **User Authentication**, make sure that **Prompt for user name and password** is not selected.

5   Repeat steps 1 to 4 on each Enterprise Vault server and on each file server in the Site.

Customizing authentication for the Enterprise Vault Web Access components

The standard security for the Web Access components means that users must provide domain name, user name, and password whenever they start the components.

You can set up various levels of automatic authentication for the users. If none of these methods is acceptable to you, the default authentication enables users to log on by supplying domain, username, and password.

Using a default domain with Basic authentication

With only Basic authentication configured, users must provide a domain name when logging on to the Web Access components. For example, a user in domain myDomain with a username of Rogers must specify myDomain\Rogers.

It is possible for IIS and Enterprise Vault to use a default domain for Basic authentication. In this case, users in the default domain do not need to specify a domain name when starting the Web Access components. Users in other domains must still specify a domain name.

Setting up a default domain in IIS

You can set up IIS so that it uses a default domain for Basic authentication. How you do this depends on the version of IIS that you have installed.

Note that the default domain does not work unless you also define it for the Web Access components.

To set up a default domain in IIS 7

1 Start Internet Information Services (IIS) Manager.

2 Expand the Sites container for the Enterprise Vault Web Access computer.

3 Click the **EnterpriseVault** folder.

4 Double-click **Authentication** in the **IIS** area at the right.

5 Ensure that **Anonymous Authentication** is disabled and **Basic Authentication** is enabled.

6 To set the default domain, do the following:

- Right-click **Basic Authentication**, and then click **Edit**.

- Enter the name of the domain that contains the majority of the user accounts that will be using the Web Access components.

- Click **OK**.

Setting up a default domain in the Web Access components

Note that the default domain does not work unless you also define it in IIS.

To set up the Web Access components so that they use the same default authorization domain as you have set up in IIS

1   Use a text editor to create an initialization file called `WebApp.ini`, containing the following line:

```
Domain=DomainName
```

where *DomainName* is the name of the domain that you have specified in IIS for Basic authentication. Note that entries in this file are case-sensitive.

For example, to use a domain called "myDomain", the line to use is as follows:

```
Domain=myDomain
```

2   Save the file in the Enterprise Vault program folder, for example `C:\Program Files (x86)\Enterprise Vault`, on the computer that runs the Web Access components.

Customizing security for the Web Access components on client computers

On user computers, you can configure Internet Explorer so that users are automatically logged on to the Web Access components, without receiving a logon prompt. Essentially, you must configure Internet Explorer so that it trusts the Web Access computer.

For this to work, you must also be using the Integrated Windows Authentication.

To make Internet Explorer log on automatically, you may need to modify the Internet Explorer Internet Options on each client computer. The settings are saved in the Windows registry, so you can save them for rollout to many client computers.

There are many possible ways for you to configure Internet Explorer security, some of which may not be acceptable to you. The following methods are described here:

■   Using the proxy bypass list

■   Explicitly naming the Web Access computer

See the Internet Explorer Help if you need more information on configuring browser security.

On Windows computers that comply with the United States Government Configuration Baseline (USGCB), you cannot change local intranet zone settings in Internet Explorer. However, you can publish the Enterprise Vault server details to users' computers by modifying the relevant USGCB group policy object. Users

can then perform Enterprise Vault operations without being prompted for authentication each time.

See "Publishing Enterprise Vault server details to USGCB-compliant computers" on page 123.

Configuring Internet Explorer to use the proxy bypass list

Note that you must be using a proxy server before you can use the proxy bypass list.

To configure Internet Explorer to use the proxy bypass list

1   In Internet Explorer, click **Tools** and then **Internet Options**.

2   Click the **Security** tab and then click the **Local Intranet** zone.

3   Click **Sites** and then select **Include all sites that bypass the proxy server**.

4   Click **OK**.

5   Click **Custom Level**.

6   Under **Logon**, select **Automatic logon only in Intranet zone**.

7   Click **OK**.

8   Click the **Connections** tab, and click **LAN Settings**.

9   Check that a proxy server is being used.

10   If either of the **Automatic configuration** settings is selected, you must make sure that the Web Access computer is in the automatic configuration exceptions list.

11   If neither of the **Automatic configuration** settings is selected, click **Use a proxy server** and then **Advanced**. If there is no existing entry that includes the Web Access computer, specify the computer in the **Exceptions** list.

Configuring a web browser to trust the Enterprise Vault Web Access components

By configuring the user's web browser to trust the Enterprise Vault Web Access components, you can save the user from having to log on to search archives or view and restore archived items. As an illustration, the following procedure describes how to configure Internet Explorer appropriately.

It is possible to configure users' desktops so that they automatically add the Web Access computer to the local intranet zone. You configure this using the advanced Outlook settings in the Exchange Desktop policy. See the *Administrator's Guide* for more details.

To configure Internet Explorer to trust the Enterprise Vault Web Access components

1 In Internet Explorer, click **Tools** and then click **Internet Options**.

2 Click the **Security** tab and then click the **Local Intranet** zone.

3 Click **Custom Level**.

4 Under **Logon**, select **Automatic logon only in Intranet zone** and then click **OK**.

5 Click **Sites** and then **Advanced**.

6 In the **Add this Web site to the zone** box, enter the fully-qualified domain name of the Web Access computer and then click **Add**. For example, **vault.company.com**.

7 In the **Add this Web site to the zone** box, enter the computer name, without the DNS domain, of the Web Access computer, and then click **Add**.

8 Click **OK**.

Publishing Enterprise Vault server details to USGCB-compliant computers

The United States Government Configuration Baseline (USGCB), formerly known as the Federal Desktop Core Configuration (FDCC), is a list of recommended security settings for general-purpose microcomputers that are connected directly to the network of a United States government agency. If you have applied USGCB group policy objects (GPO) to Windows computers, users cannot change local intranet zone settings in Internet Explorer. As a result, users need to enter authentication credentials each time they access Enterprise Vault. For example, users would be prompted for credentials when they archive or retrieve an item.

This section describes how to add the Enterprise Vault server details to the USGCB Internet Explorer GPO. When the GPO is refreshed, the Enterprise Vault server details are added to the local intranet zone on users' computers. You must ensure that the Enterprise Vault server details are correct, because settings in the GPO take precedence over user settings.

To publish Enterprise Vault server details to USGCB-compliant computers

1 Log on to the domain controller computer using an administrator account with permission to modify and publish GPOs.

2 Open the Group Policy Object Editor.

3 Select the USGCB group policy object that applies Internet Explorer settings to the Windows computers.

4 In the Group Policy Object Editor, navigate to the following section:

Computer Configuration > **Administrative Templates** > **Windows Components** > **Internet Explorer** > **Internet Control Panel** > **Security Page**

5 Right-click **Site to Zone Assignment List**, and select **Properties**.

6 Select **Enabled**, if it is not already selected, and then click **Show** to enter the required zone assignments.

7 Click **Add**.

8 In the box **Enter the name of the item to be added**, type the name of the Enterprise Vault server.

In the box **Enter the value of the item to be added**, type **1**.

This maps the server name to the intranet zone.

In the same way, add all the Enterprise Vault server names to the list and map them to the intranet zone. The list should include all the Enterprise Vault server aliases. For an Enterprise Vault server that has the name SRV1 and the alias EVSERVER1, you would add the following to the Site to Zone Assignment List:

```
Value Name: evserver1.mycorp.local
Value: 1
Value Name: srv1
Value: 1
```

9 When you have finished adding Enterprise Vault server names to the list, click **OK**.

10 On the Site to Zone Assignment List Properties page, click **Apply**.

11 When the policy is next refreshed, the changes to the GPO are applied to the Windows computers.

12 On one of the users' computers, you can verify that the Enterprise Vault server names have been added to the local intranet sites:

- Log on to the computer as a standard user.

- Open Internet Explorer.

- Click **Tools** > **Internet options** > **Security** > **Local Intranet > Sites** > **Advanced**.

- The Enterprise Vault server names should be listed in the websites.

Enabling remote access to the Enterprise Vault Web Access computer

You may need to grant users of the Enterprise Vault Web Access components access to the IIS computer, using the local IIS computer accounts database, not the domain accounts database.

Note: If the IIS computer is a domain controller, there is no local accounts database, only a domain accounts database. If you continue with these instructions when the IIS computer is a domain controller, you will make changes to the security access of the domain accounts database. This will affect all computers within the domain, not just the IIS computer. If you do not want to affect the whole domain, you should ensure that you run IIS on a non-domain controller.

To enable remote access to the Enterprise Vault Web Access computer

1   Start the **Local Security Policy** administrative tool.

2   In the Local Security Policy window, expand the **Local Policies** container.

3   Click **User Rights Assignment**.

4   Set up Basic authentication access by following the steps below in the order listed:

  ■ In the right-hand pane, right-click **Allow log on locally** and then, on the shortcut menu, click **Properties**.

  ■ Check that the **Users** group appears in the **Local Security Setting** list.

5   Set up Integrated Windows Authentication access by following the steps below in the order listed:

  ■ With **User Rights Assignment** still selected in the left pane of the Local Security Policy window, right-click **Access this computer from the network** in the right pane and then, on the shortcut menu, click **Properties**.

  ■ Check that the **Users** group appears in the **Local Security Setting** list. If you do not want to add the **Users** group, see the other options below.

  By default, the Users group includes Domain Users. If the Users group does not include Domain Users, or if some Web Access users are in a different domain, you must do one of the following:

  ■ Add the Web Access users to the **Users** group.

  ■ Add the Web Access users to some other group and then grant the access right to that group.

  ■ Grant the access right to each Web Access user's account.

The Enterprise Vault Web Access components are now set up and ready to be used by users in the same domain as IIS.

Repairing, modifying, or uninstalling Enterprise Vault

This chapter includes the following topics:

- About repairing, modifying, or uninstalling Enterprise Vault

- Modifying Enterprise Vault

- Repairing Enterprise Vault

- Uninstalling Enterprise Vault

About repairing, modifying, or uninstalling Enterprise Vault

Enterprise Vault provides both a wizard-based installer and a command line installer. Both installers enable you do to the following:

- Install Enterprise Vault

- Repair an existing Enterprise Vault installation

- Add Enterprise Vault features to an existing installation

- Uninstall Enterprise Vault

Modifying Enterprise Vault

Modifying Enterprise Vault with the wizard

You can use the wizard to add new features to Enterprise Vault as required. Run the wizard in the same way as when you installed Enterprise Vault.

See "Installing Enterprise Vault (wizard)" on page 112.

Modifying Enterprise Vault from the command line

You can use the command line to add new features to Enterprise Vault as required. The command line options are the same as the one that you use to install Enterprise Vault.

See "Installing Enterprise Vault (command line)" on page 113.

Repairing Enterprise Vault

You can use the wizard or the command line to repair Enterprise Vault.

Repairing from Programs and Features

To repair Enterprise Vault from Programs and Features

1   Open Windows **Control Panel** and under **Programs** click **Uninstall a program**.

2   In **Programs and Features**, right-click **Veritas Enterprise Vault** and on the shortcut menu click **Change**.

3   In the **InstallShield Wizard**, select **Repair** and click **Next**.

4   Work through the wizard to repair the installation.

Repairing from the command line when SMTP is not installed

To repair Enterprise Vault silently from the command line when SMTP is not installed

1   Load the Enterprise Vault media.

2   Open a Command Prompt window with administrator privileges.

3 In the Command Prompt window, change to the following folder on the Enterprise Vault media:

```
\Veritas Enterprise Vault\Server
```

4 Enter the following command:

```
"setup (x64).exe" /s /v"REINSTALL=ALL"
```

The default location for the log file is as follows:

```
%temp%\EVInstall.log
```

Optionally, you can specify a log file location, as in the following example:

```
"setup (x64).exe" /v"REINSTALL=ALL
LOGFILE=\"C:\logs\EVreinstall.log\""
```

Repairing from the command line when SMTP is installed

If the SMTP component is installed you must specify whether or not to repair SMTP.

Note: If you choose to repair SMTP and the Enterprise Vault SMTP service is running, then the installation stops that service before the repair and then restarts it afterwards. The SMTP service is unavailable until the restart.

To repair Enterprise Vault silently from the command line when SMTP is installed

1 Load the Enterprise Vault media.

2 Open a Command Prompt window with administrator privileges.

3 In the Command Prompt window, change to the following folder on the Enterprise Vault media:

```
\Veritas Enterprise Vault\Server
```

4 Enter the appropriate command, as follows:

- To repair all components except SMTP, enter the following. This option does not stop the Enterprise Vault SMTP service.

  ```
  "setup (x64).exe" /s /v"REINSTALL=ALL SMTPSERVICE=0"
  ```

- To repair all components and SMTP, enter the following. This option does stop and restart the SMTP service if it is running.

  ```
  "setup (x64).exe" /s /v"REINSTALL=ALL SMTPSERVICE=1"
  ```

The default location for the log file is as follows:

```
%temp%\EVInstall.log
```

Optionally, you can specify a log file location, as in the following example:

```
"setup (x64).exe" /v"REINSTALL=ALL SMTPSERVICE=1
LOGFILE=\"C:\logs\EVreinstall.log\""
```

Uninstalling Enterprise Vault

Note the following before you proceed:

- Before you uninstall Enterprise Vault, back up the Enterprise Vault system databases as described in the *Backup and Recovery* guide.

- The uninstaller does not remove files that have been created or changed since the installation. For example, the uninstaller does not remove report files from the Enterprise Vault Reports folder.

- If an Enterprise Vault service has data associated with it, you cannot use the Enterprise Vault Administration Console to remove that service.

- The uninstaller does not remove the following software components, which are automatically installed as part of the Enterprise Vault installation process:

  - Microsoft Visual C++ Redistributable Packages

  - SQLXML 4.0 SP1

Using the wizard to uninstall Enterprise Vault

To use the wizard to uninstall Enterprise Vault

1   Open Windows **Control Panel** and under **Programs** click **Uninstall a program**.

2   From the list of programs, select **Enterprise Vault**, and then click **Uninstall**.

    The wizard asks you to confirm that you want to remove Enterprise Vault and all its features from your system.

3   Click **Yes**.

    The uninstaller stops Enterprise Vault services that are still running. It then removes all Enterprise Vault Services and Enterprise Vault software from your system. The uninstaller does not delete data. If you do not want to reinstall Enterprise Vault, delete the Enterprise Vault data manually.

Using the command line to uninstall Enterprise Vault

To use the command line to uninstall Enterprise Vault silently

1   Open a Command Prompt window with administrator privileges.

2   In the Command Prompt window, change to the following folder on the Enterprise Vault media:

3   Enter the following command:

```
"setup (x64).exe" /s /uninst
```

Optionally, you can specify a log file location, as in the following example:

```
"setup (x64).exe" /s /uninst
/V"LOGFILE=\"C:\logs\EVuninstall.log\""
```

The uninstaller stops Enterprise Vault services that are still running. It then removes all Enterprise Vault Services and Enterprise Vault software from your system. The uninstaller does not delete data. If you do not want to reinstall Enterprise Vault, delete the Enterprise Vault data manually.

Configuring Enterprise Vault

About configuring Enterprise Vault

This chapter includes the following topics:

■ About configuring Enterprise Vault

About configuring Enterprise Vault

On completion of the Enterprise Vault installation program, you may need to run one or more configuration programs, depending on which Enterprise Vault components you installed.

If you have upgraded from an earlier version of Enterprise Vault, follow the Enterprise Vault upgrade instructions for your new version.

For a new Enterprise Vault installation, do as follows:

■ If you installed the Enterprise Vault Services component, run the Enterprise Vault configuration wizard before you run any other configuration programs.
See "When to run the Enterprise Vault configuration wizard" on page 135.

■ If you installed the Enterprise Vault Operations Manager component, configure Enterprise Vault Operations Manager.
See "When to run the Enterprise Vault Operations Manager Configuration utility" on page 159.

■ If you installed the Enterprise Vault Reporting component, configure Enterprise Vault Reporting.
See the chapter "Configuring Enterprise Vault Reporting" in the *Reporting* guide.

■ If you installed only the Administration Console component, you do not need to run any configuration program.

- If you installed components for specific archiving implementations such as Exchange, Domino, SharePoint, or SMTP, you may need to perform separate configuration steps for those components. See the relevant section elsewhere in this manual.

Running the Enterprise Vault configuration wizard

This chapter includes the following topics:

- When to run the Enterprise Vault configuration wizard
- What the Enterprise Vault configuration wizard does
- Running the Enterprise Vault configuration wizard
- Troubleshooting configuration of the Enterprise Vault Monitoring database

When to run the Enterprise Vault configuration wizard

Run the Enterprise Vault configuration wizard either immediately after installation (after restarting your computer if prompted), or after performing the postinstallation tasks for the Web Access components.

Note the following:

- If you run the configuration wizard immediately after the installation, remember that there are some additional tasks that you need to do before users can use Enterprise Vault.
  See "About configuring Enterprise Vault" on page 133.

- If you exit from the configuration wizard before configuration is complete, you can run the configuration wizard again and have the option to delete the Directory database. Once you have successfully completed the configuration wizard, you cannot run it again on the same computer.

What the Enterprise Vault configuration wizard does

The configuration wizard lets you do the following:

- Select which SQL Server you want to use for the Enterprise Vault Directory database

- Create the Enterprise Vault Directory database

- Create the Enterprise Vault Monitoring database

- Create an Enterprise Vault site

- Add the computer to the site

- Select the Enterprise Vault services you want to run on the computer

- Choose the storage areas to use for Enterprise Vault data

Some tasks, such as adding a service or assigning storage areas for the data, can also be done using the Enterprise Vault Administration Console. However, the following tasks can only be done using the configuration wizard:

- Creating a new Enterprise Vault Directory

- Creating a new Enterprise Vault site

- Adding a new Enterprise Vault server

Running the Enterprise Vault configuration wizard

Note: These instructions apply to a non-clustered environment. If you are configuring Enterprise Vault in a Veritas Cluster Server or Windows Server Failover Clustering environment, see instead the appropriate clustering section in this guide.

You may be starting the configuration wizard after restarting your computer or after completing the installation program.

Follow the instructions below to run the configuration wizard on the first Enterprise Vault server in your site. When you are using the configuration wizard to configure Enterprise Vault on subsequent computers, refer to the online Help if you are unsure about how to proceed.

Before you run the configuration wizard, make sure that you have assigned the required SQL Server permissions and roles to the Vault Service account.

See "About assigning permissions and roles in SQL databases" on page 49.

If during the running of the configuration wizard you receive an error related to the configuring of the Enterprise Vault Monitoring database, complete the configuration wizard and then refer to the troubleshooting information for the Monitoring database.

See "Troubleshooting configuration of the Enterprise Vault Monitoring database" on page 139.

To run the Enterprise Vault configuration wizard

1   On the **Apps** screen, select **Enterprise Vault > Configuration**.

   The Configuration wizard starts. The first screen asks whether you want to create a new Enterprise Vault Directory database.

2   Click **Yes** and then **Next**.

   The wizard asks you to select the language you want Enterprise Vault to use when populating the default settings in the Administration Console.

3   Select the required language and then **Next**.

   The wizard asks for details of an account for Enterprise Vault services to use.

4   Enter the details of the Vault Service account that you created earlier.

   See "Creating the Vault Service account" on page 45.

   You must use the format *domain_name\username* when you specify the account. Alternatively, browse for the Vault Service account.

   Enter the password for the Vault Service account and confirm it.

5   Click **Next**.

   A warning message is displayed if the account you are using does not have sufficient privileges to validate the password to the Vault Service account. Click **Yes** to continue.

   A message tells you that the Vault Service account has been added to the local Administrators group. Click **OK** to close the message.

   A second message notifies you that the account will be given the advanced user rights, **Log On As a Service**, **Debug programs**, and **Replace a process-level token**. Click **OK** to close the message.

   The configuration wizard creates the Directory service and then the next screen asks for the location of the SQL Server that you want to use for the Directory database.

6   Enter the location of the SQL Server that you want to use. Alternatively, click **Browse** to browse for the SQL Server. You can specify a SQL Server instance if required.

7   Click **Next**.

The wizard shows the default locations for the Directory database files and transaction log.

8   Change the locations if necessary.

If you have specified that SQL Server is on a remote computer, the paths for the data file and transaction log file must be valid on that remote computer.

9   Click **Next**.

The wizard creates the Directory database. The next screen asks for the location of the SQL Server that you want to use for the Monitoring database.

10 Enter the location of the SQL Server that you want to use. You can specify a SQL Server instance if required.

11 Click **Next**.

The next screen shows default locations on the SQL server for the Monitoring database files and transaction log.

12 Change the locations if necessary.

If you have specified that SQL Server is on a remote computer, the paths for the data file and transaction log file must be valid on that remote computer.

Do not specify paths that are on the root of a file system, such as `c:` or `c:\`.

13 Click **Next**.

The wizard creates the Monitoring database.

The next screen asks for details of the new Enterprise Vault site.

14 Enter a name and description for the new Enterprise Vault site.

15 Click **Next**.

The next screen asks for a DNS alias for current computer.

The value you enter must be an unqualified DNS alias for this computer, for example, "evserver1". A fully-qualified DNS name (for example, "evserver1.mycompany.local") is not permitted.

If this is the first computer added to the site, the DNS alias entered will automatically be used as the vault site alias.

See "Creating Enterprise Vault DNS aliases" on page 50.

16 Enter a DNS alias for the current computer and click **Next**.

17 Click **Next** to add the computer to the Enterprise Vault site.

An information screen lists software that is installed on your computer. Based on this list, the wizard automatically selects Enterprise Vault services to add to your computer.

18 Click **Next**. The list shows the services that will be added to your computer.

19 Check the list of services. You can add or remove services as required, as follows:

- To remove a service, click the service to select it and then click **Remove**.

- To add a service, click **Add** and then select the service you require.

20 Click **Next**. An information page lists the services that the wizard will create.

21 Click **Next** to create the services.

22 The final screen of the wizard gives you the following options:

- **Run the Enterprise Vault Getting Started Wizard**. Choose this option to set up archiving as quickly as possible. The wizard provides both express and custom options for maximum flexibility.

- **Run the Enterprise Vault Administration Console**. Choose this option if you are already familiar with the Administration Console and familiar with setting up archiving.

- **Just close this wizard**. Choose this option to close the Configuration Wizard. You can then click the desktop shortcuts to run the Enterprise Vault Getting Started Wizard or the Administration Console.

23 Click **Finish** to exit from the configuration wizard.

Note: Remember that you can run the configuration wizard successfully only once on a computer. If you exit the configuration wizard after successfully configuring Enterprise Vault, you cannot run the wizard again. To do any further setup or management of the Enterprise Vault components, other than that related to Enterprise Vault Operations Manager or Enterprise Vault Reporting, you must use the Administration Console.

Troubleshooting configuration of the Enterprise Vault Monitoring database

If while running the configuration wizard you receive errors indicating that the configuration of the Enterprise Vault Monitoring database has failed, complete the

configuration wizard and then run the Monitoring Configuration utility to configure the Monitoring database and the Monitoring agents manually.

For information on how to do this, see the following technical note on the Veritas Support website:

http://www.veritas.com/docs/000033005

The technical note also describes how to troubleshoot issues with Monitoring agents.

Running the Enterprise Vault Getting Started wizard

This chapter includes the following topics:

- What the Enterprise Vault Getting Started wizard does
- Preparing to run the Enterprise Vault Getting Started wizard
- Running the Enterprise Vault Getting Started wizard
- About the express and custom modes of the Enterprise Vault Getting Started wizard
- Planning for the Enterprise Vault Getting Started wizard

What the Enterprise Vault Getting Started wizard does

The Enterprise Vault Getting Started Wizard enables you to configure archiving as quickly as possible.

The wizard helps you do the following, as appropriate:

- Create archiving policies for Exchange Server, Domino, and File System Archiving.
- Set up storage locations.
- Configure indexing.
- Create retention categories.

You can choose to run sections of the wizard in express mode or in custom mode, as follows:

- In express mode, the wizard does not ask many questions. Instead, it applies as many default settings as possible. Later, you can use the Administration Console to make changes to the settings, if required.

- In custom mode, you have the flexibility to change the default settings.

Note: In express mode, the Getting Started wizard asks you to specify a local disk. The wizard then configures Enterprise Vault to use that disk for all storage. If you want to configure remote storage or a different local storage configuration, you must select custom mode for storage configuration.

Preparing to run the Enterprise Vault Getting Started wizard

The Getting Started wizard checks the Enterprise Vault license keys to determine which options to present to you. Before you run the Getting Started wizard you must have installed your license keys.

See "Overview of Enterprise Vault licensing" on page 107.

You can run the Enterprise Vault Deployment Scanner to create a report that shows whether the Enterprise Vault configuration is correct.

See the *Deployment Scanner* manual in the `Documentation` folder of the Enterprise Vault media.

To run the Deployment Scanner from within the Enterprise Vault Getting Started wizard

◆ On the **Before You Begin** page, click **Run Deployment Scanner**.

Running the Enterprise Vault Getting Started wizard

You can run the Getting Started wizard immediately after you complete the Configuration wizard as part of a new installation of Enterprise Vault.

If you exit from the Getting Started wizard before the end of the wizard, you can run the wizard again. When you have successfully completed the Getting Started wizard, you can run it again later on the same computer but some options may not

be available. You can also run the Getting Started wizard on other computers in the site.

To run the Enterprise Vault Getting Started wizard

◆ Do one of the following:

- Select the **Run the Enterprise Vault Getting Started Wizard** option on the last page of the Configuration wizard.

- On the **Apps** screen, select **Enterprise Vault > Getting Started Wizard**.

About the express and custom modes of the Enterprise Vault Getting Started wizard

The Getting Started wizard enables you to select express mode or custom mode to perform the following:

- Indexing configuration

- Storage configuration

- Policy definition

- Exchange target configuration

- Domino target configuration

- File Server target configuration

In express mode, the wizard does not ask many questions. Instead, the wizard applies default settings so that you can configure Enterprise Vault as quickly as possible. Later, you can use the Administration Console to make changes to the settings, if required.

In custom mode, you can make any changes you require but it can take a long time to go through all the options. You may prefer to accept the default options and then make changes in the Administration Console.

There is a planning sheet that lists the Getting Started wizard's express-mode choices. You can use the sheet to record your own requirements and then later use the Administration Console to make the required changes.

See "Planning for the Enterprise Vault Getting Started wizard" on page 151.

About indexing configuration with the Enterprise Vault Getting Started wizard

In express mode the Enterprise Vault Getting Started wizard automatically configures Indexing services to use local Storage services. The Getting Started wizard does not create an Index Server group and does not add the current server to any existing Index Server group.

If you want to add the current server to an Index Server group, select **Custom** mode for **Indexing Configuration**. Custom mode enables you to create an Index Server group and to add the server to the Index Server group.

Automatic indexing configuration in express mode

This section lists the settings that the Enterprise Vault Getting Started wizard automatically configures when you choose express mode for Indexing Configuration.

Table 20-1 shows the Vault Store Group settings that the wizard creates in express mode.

Table 20-1   Indexing settings in express mode

Item	Description
Indexing level	'Full'. Indexes the metadata and content of archived items.
Preview length	'128 characters'.
Create previews of attachments	'Off'. Enterprise Vault does not create previews of attachments. These previews cannot be viewed in this release of Enterprise Vault.
Delete indexing subtasks after	'7 days'. Enterprise Vault deletes indexing subtasks after this amount of time has elapsed since the tasks finished. If all of a task's subtasks are deleted, the task is itself deleted.
Index server location in Administration Console	The Administration Console shows the new Index server under **Indexing**, in the **Ungrouped Servers** container.

About storage configuration with the Enterprise Vault Getting Started wizard

In express mode, the Enterprise Vault Getting Started wizard configures all storage locally on the server.

See "About setting up storage for Enterprise Vault archives" on page 174.

The wizard sets up the following:

- A vault store group
- A vault store
- A vault store partition
- The Enterprise Vault server cache
- Indexes
- Shopping baskets (if a Shopping service is present)

Select the custom option for storage configuration if you want to do any of the following:

- Configure remote storage.
- Use a different SQL Server for vault stores from the one that you specified in the configuration program.
- Configure the structure of the vault store group's fingerprint database.

If you create an open vault store partition on the first server in the site, storage configuration may appear to be optional when you run the Enterprise Vault Getting Started wizard on subsequent servers in the site. However, you must configure an Enterprise Vault server cache on each Enterprise Vault server that has an Indexing service. Similarly, you must configure a shopping basket area on each server that has a Shopping service.

When a vault store partition is configured on another server, you can configure the Enterprise Vault server cache or shopping location in one of the following ways:

- Select **Indexing Configuration** and **Express** mode. This lets you set the location for both the Enterprise Vault server cache and the shopping location.
- Select **Storage Configuration** and **Custom** mode. This lets you set the server cache location.

Storage configuration information you must supply in express mode

For the express storage configuration, you must specify which volume to use to store Enterprise Vault data. This information is used when Enterprise Vault creates the following storage locations:

- Cache location: `<volume>\EVStorage\Cache`

- Index locations: `<volume>\EVStorage\Index`

- Shopping location: `<volume>\EVStorage\Cache\Shopping`

Note: As antivirus software can potentially change data, it is important to exclude the cache and index locations in your virus checking application.

Automatic storage configuration in express mode

This section lists the settings that the Enterprise Vault Getting Started wizard automatically configures when you choose express mode for Storage Configuration.

Table 20-2 shows the Vault Store Group settings that the wizard creates in express mode.

Table 20-2   Vault Store Group settings in express mode

Item	Description
Name	"Express Vault Store Group". If the name already exists a number is appended to make the name unique. For example, "Express Vault Store Group_1".
Description	The same as the Vault Store Group name.
SQL Server name for fingerprint database	The same SQL Server as was specified in the Configuration program for the Enterprise Vault Directory database.
Folder for all fingerprint database filegroups.	The default database folder for the Enterprise Vault Directory computer.
Folder for fingerprint database log	The default log folder for the Enterprise Vault Directory computer.

Table 20-3 shows the Vault Store settings that the wizard creates in express mode.

Table 20-3   Vault Store settings in express mode

Item	Description
Name	"Express Vault Store". If the name already exists a number is appended to make the name unique. For example, "Express Vault Store_1".
Description	The same as the vault store name.
SQL Server	The same SQL Server as was specified in the Configuration program for the Enterprise Vault Directory database.
Sharing	Set to 'Share within Vault Store'.
Safety Copies	'Remove original items' is enabled. Default behavior is set to 'Yes, in the original location'. For journal archive is set to 'No, remove immediately after archiving'.
Limit archive usage	Set to 'Use Site setting'.

Table 20-4 shows the Vault Store partition settings that the wizard creates in express mode.

Table 20-4   Vault Store partition settings in express mode

Item	Description
Name	"Express Vault Store Ptn1". If the name already exists a number is appended to make the name unique. For example, "Express Vault Ptn2".
Description	Partition of Vault Store [*Vault_store_name*]
State	Open.
Device type	NTFS volume.
Data deduplication	Destination device does not perform data deduplication.
Data compression	Destination device does not perform data compression.

Table 20-4   Vault Store partition settings in express mode *(continued)*

Item	Description
Partition rollover	Not enabled.
How to check that items have been secured	Use the archive attribute.
Use collection files	Not enabled.
Migrate files	Not enabled.

About policy definition with the Enterprise Vault Getting Started wizard

A policy defines which documents are to be archived and how they are to be archived.

Enterprise Vault creates policies automatically. The Getting Started wizard uses the default Enterprise Vault policies. The default policies in express mode and custom mode are the same.

You can use the Administration Console to modify all policy settings later, if required.

About Exchange target configuration with the Enterprise Vault Getting Started wizard

If you choose to configure Exchange Server targets, the Getting Started wizard searches the network for instances of Exchange Server. You can then select the Exchange Server computers for which you want to configure archiving.

For the Exchange Server that you select you must do the following:

- Specify whether to configure mailbox archiving or journal archiving, or both.

- If you choose to configure mailbox archiving you must specify a system mailbox on that server that Enterprise Vault can use to log on.

- If you choose to configure journal archiving you must specify which journal mailboxes to archive and specify the journal archive to use for each mailbox. The wizard enables you to create new archives, if required.

Table 20-5 shows the Exchange provisioning group settings that the wizard creates in express mode.

Table 20-5   Exchange provisioning group settings in express mode

Item	Description
Provisioning group name	'Express Provisioning Group'. If you have selected 'Storage configuration' the provisioning group uses a new vault store that the wizard creates. If you have not selected 'Storage configuration', the wizard uses an existing vault store.
Provisioning group scope	'Whole Exchange Server organization'
Desktop policy	'Default Exchange Desktop Policy'
Mailbox policy	'Default Exchange Mailbox Policy'
PST migration policy	'Default Exchange PST migration Policy'
Default retention category	'Default Retention Category'

About Domino target configuration with the Enterprise Vault Getting Started wizard

If you choose to configure Domino targets, the Getting Started wizard searches the network for Domino servers. You can then select the Domino servers for which you want to configure archiving. For each Domino server you can specify whether to configure mailbox archiving or journal archiving, or both. The Getting Started wizard then configures archiving appropriately.

For the express Domino configuration you must provide the following:

- ID file name. Enterprise Vault uses the ID file as the default ID file for all Enterprise Vault operations that require an ID file. The wizard lists Domino ID files that are in the Notes data folder (for example `C:\Program Files\IBM\Notes\data`).
  You must place the ID file that you want to use in the data folder so that you can select it in the wizard.

- ID file password. The password for the ID file.

- The names of the Domino servers for which you want to configure mailbox archiving.

- The names of the Domino servers for which you want to configure journal archiving.

- The retention category to use when archiving from a Domino target.

Table 20-6 shows the Domino provisioning group settings that the wizard creates in express mode.

Table 20-6   Domino provisioning group settings in express mode

Item	Description
Provisioning group name	'Express Provisioning Group'. If the name already exists a number is appended to make the name unique. For example, "Express Provisioning Group_1".
Vault store	If you have selected 'Storage configuration' the provisioning group uses a new vault store that the wizard creates. If you have not selected 'Storage configuration', the wizard selects an existing vault store.
Provisioning group scope	'All Organizational Units'
Desktop policy	'Default Domino Desktop Policy' If this policy is not available the wizard selects the first policy that is available, alphabetically.
Mailbox policy	'Default Domino Mailbox Policy'. If this policy is not available the wizard selects the first policy that is available, alphabetically.
Default retention category	'Default Retention Category'

Table 20-7   Vault Store settings in express mode

Item	Description
Name	The Vault store that was created in the current run of the wizard, if any. If the wizard did not create a vault store the first vault store with an open partition is used.
Description	The same description as for the vault store name.
SQL Server	The same SQL Server as was specified in the Configuration program for the Enterprise Vault Directory database.
Sharing	Set to 'Share within Vault Store'.

Table 20-7   Vault Store settings in express mode *(continued)*

Item	Description
Safety Copies	'Remove original items' is enabled.
	Default behavior is set to 'Yes, in the original location'.
	For journal archive is set to 'No, remove immediately after archiving'.
Limit archive usage	Set to 'Use Site setting'.

About file target configuration with the Enterprise Vault Getting Started wizard

The Getting Started wizard enables you to configure archiving for the file servers that you specify.

You can install the Enterprise Vault FSA Agent on each Windows file server if required. You need to install the FSA agent if you require placeholder shortcuts, File Blocking, or need to obtain data for FSA Reporting.

Planning for the Enterprise Vault Getting Started wizard

This section lists the choices that the Getting Started wizard makes automatically when you run it in Express mode. In Express mode, the Getting Started wizard does not ask many questions. Instead, the wizard applies as many default settings as possible. Later, you can use the Administration Console to make changes to the settings, if required.

Table 20-8 shows the Indexing settings that the wizard creates in Express mode.

Table 20-8   Indexing settings in Express mode

Item	Wizard's value	Administration Console possible values	Your choice
Indexing level	Full	Brief or Full	
Preview length	128 characters	128 or 1000	
Create previews of attachments	Off	Off or On	

Table 20-8   Indexing settings in Express mode *(continued)*

Item	Wizard's value	Administration Console possible values	Your choice
Delete indexing subtasks after	7 days	Edit as required	

Table 20-9 shows the Vault Store Group settings that the wizard creates in Express mode.

Table 20-9   Vault Store Group settings in Express mode

Item	Wizard's value	Administration Console possible values	Your choice
Name	"Express Vault Store Group". If the name already exists a number is appended to make the name unique. For example, "Express Vault Store Group_1".	Edit as required.	
Description	The same as the Vault Store Group name.	Edit as required.	
SQL Server for fingerprint database	The same SQL Server as was specified in the Configuration program for the Enterprise Vault Directory database.	Cannot change.	
Folder for all fingerprint database filegroups	The default database folder for the Enterprise Vault Directory computer.	Cannot change.	
Folder for fingerprint database log	The default log folder for the Enterprise Vault Directory computer.	Cannot be changed.	

Table 20-10 shows the Vault Store settings that the wizard creates in Express mode.

Table 20-10   Vault Store settings in Express mode

Item	Wizard's value	Administration Console possible values	Your choice
Name	"Express Vault Store". If the name already exists a number is appended to make the name unique. For example, "Express Vault Store_1".	Edit as required.	
Description	The same as the vault store name.	Edit as required.	
SQL Server	The same SQL Server as was specified in the Configuration program for the Enterprise Vault Directory database.	Can be changed to another SQL Server.	
Sharing	'Share within Vault Store'.	'No sharing'; 'Share within Vault Store'; 'Share within group'.	

Table 20-10 Vault Store settings in Express mode *(continued)*

Item	Wizard's value	Administration Console possible values	Your choice
Safety Copies	Controls the location and deletion of safety copies. **Remove original items** is enabled. **Default behavior** is set to 'Yes, in the original location'. **For journal archive** is set to 'No, remove immediately after archiving'.	**Remove original items** can be enabled or disabled. **Default behavior** can be: ■ 'No, remove immediately after archiving' ■ 'Yes, in the original location' ■ 'Yes, in the storage queue' **For journal archives** can be: ■ 'No, remove immediately after archiving' ■ 'Yes, in the original location' ■ 'Yes, in the storage queue'	
Limit archive usage	'Use Site setting'.	'Disabled'; 'Enabled'; 'Use Site setting'.	

Table 20-11 shows the Vault Store partition settings that the wizard creates in Express mode.

Table 20-11 Vault Store partition settings in Express mode

Item	Wizard's value	Administration Console possible values	Your choice
Name	"Express Vault Store Ptn1". If the name already exists a number is appended to make the name unique. For example, "Express Vault Ptn2".	Edit as required.	
Description	Partition of Vault Store [*Vault_store_name*]	Edit as required.	
State	Open.	'Closed'; 'Open'; 'Ready'.	
Device type	NTFS volume.	Cannot change.	
Data deduplication	Destination device does not perform data deduplication.	Device performs data deduplication; Device does not perform data deduplication.	
Data compression	Destination device does not perform data compression.	Device performs data compression; Device does not perform data compression.	
Partition rollover	Not enabled.	'Not Enabled'; 'Enabled based on volume'; 'Enabled based on time'; 'Enabled based on time or volume'.	
How to check that items have been secured	Use the archive attribute.	'Use the archive attribute'; 'Check for a trigger file'.	
Use collection files	Not enabled.	Use collection files; Do not use collection files.	

Table 20-11   Vault Store partition settings in Express mode *(continued)*

Item	Wizard's value	Administration Console possible values	Your choice
Migrate files	Not enabled.	Enabled; Not enabled.	

Table 20-12 shows the Exchange provisioning group settings that the wizard creates in Express mode.

Table 20-12   Exchange provisioning group settings in Express mode

Item	Wizard's value	Administration Console possible values	Your choice
Provisioning group name	'Express Provisioning Group'. If you have selected 'Storage configuration' the provisioning group uses a new vault store that the wizard creates. If you have not selected 'Storage configuration', the wizard uses an existing vault store.	Edit as required.	
Provisioning group scope	'Whole Exchange Organization'	'Windows group'; 'Windows user'; 'Distribution group'; 'Organizational Unit'; 'LDAP query'; 'Whole Exchange Organization'.	
Desktop policy	'Default Exchange Desktop Policy'	Edit as required.	
Mailbox policy	'Default Exchange Mailbox Policy'	Edit as required.	
PST migration policy	'Default Exchange PST migration Policy'	Edit as required.	

Table 20-12   Exchange provisioning group settings in Express mode
(continued)

Item	Wizard's value	Administration Console possible values	Your choice
Default retention category	'Default Retention Category'	Edit as required.	

Table 20-13 shows the Domino provisioning group settings that the wizard creates in Express mode.

Table 20-13   Domino provisioning group settings in Express mode

Item	Wizard's value	Administration Console possible values	Your choice
Provisioning group name	'Express Provisioning Group'. If the name already exists a number is appended to make the name unique. For example, "Express Provisioning Group_1".	Edit as required.	
Vault store	If you have selected 'Storage configuration' the provisioning group uses a new vault store that the wizard creates. If you have not selected 'Storage configuration', the wizard selects an existing vault store.	Edit as required.	
Provisioning group scope	'All Organizational Units'	'Directory Group'; 'Mailbox'; 'Organizational Unit'; 'Corporate Hierarchy'.	

Table 20-13   Domino provisioning group settings in Express mode *(continued)*

Item	Wizard's value	Administration Console possible values	Your choice
Desktop policy	'Default Domino Desktop Policy'. If this policy is not available the wizard selects the first policy that is available, alphabetically.	Edit as required.	
Mailbox policy	'Default Domino Mailbox Policy'. If this policy is not available the wizard selects the first policy that is available, alphabetically.	Edit as required.	
Default retention category	'Default Retention Category'	Edit as required.	

Configuring Enterprise Vault Operations Manager

This chapter includes the following topics:

- When to run the Enterprise Vault Operations Manager Configuration utility
- Running the Enterprise Vault Operations Manager Configuration utility
- Accessing Enterprise Vault Operations Manager
- Troubleshooting Enterprise Vault Operations Manager

When to run the Enterprise Vault Operations Manager Configuration utility

Run the Enterprise Vault Operations Manager Configuration utility after installing Operations Manager on a server, but only after the server has been successfully configured using the Enterprise Vault configuration wizard.

You can rerun the Operations Manager Configuration utility if the configuration fails for some reason and you need to repeat it.

You can also rerun the utility if you need to change the details of the monitoring user account. In this case, be sure to rerun the utility on all servers on which Operations Manager is installed.

Note: You must also re-run the Operations Manager Configuration utility after you enable or disable the Windows policy setting for FIPS-compliant algorithms on a server on which the Operations Manager is configured.

Running the Enterprise Vault Operations Manager Configuration utility

Run the Operations Manager Configuration utility to configure the Operations Manager for the first time or to update the configuration, for example to change the details of the monitoring user account.

To run the Enterprise Vault Operations Manager Configuration utility

1   Ensure you are logged in under the Vault Service account.

2   Start the Operations Manager Configuration utility.

3   Provide the details of the monitoring user account you have created for Operations Manager to run under.

    Enter the Active Directory domain, the user name, and the password for the monitoring user account.

4   Click **Configure** to run the utility.

    The utility gives the account the required permissions, and adds the user to the Enterprise Vault Directory database as the monitoring user.

5   When the utility has finished, click **OK** on the displayed dialog to quit the utility.

Note: If you ran this utility to update the details of the monitoring user account, remember to rerun the utility on any other Enterprise Vault server with Operations Manager installed.

You can now try accessing Operations Manager to confirm that it has been successfully configured.

Accessing Enterprise Vault Operations Manager

If you have installed the Enterprise Vault Operations Manager web application on at least one Enterprise Vault server in an Enterprise Vault site, you can use it to monitor the site's Enterprise Vault servers.

After configuring Operations Manager, try accessing it to confirm the configuration has been successful.

To access Enterprise Vault Operations Manager

1   Enter the following URL in Internet Explorer:

http://*host_ipaddress*/MonitoringWebApp/default.aspx

where *host_ipaddress* is the IP address of the computer hosting an Enterprise Vault server on which the Enterprise Vault Operations Manager web application feature is installed.

Alternatively, if you are accessing Operations Manager from the computer on which it is installed, you can use the following URL, which does not require the next step:

http://localhost/MonitoringWebApp/default.aspx

2   In the **Connect to <IP Address>** dialog box, enter the user name and password of an account in the host computer's domain (use the format *domain\account*). Then click **OK**.

Note: Any user other than the Vault Service account must be assigned to a suitable role to access Operations Manager. Users can view only the tabs and tables in Operations Manager that are applicable to the role to which they are assigned.

See "Roles-based administration" in the *Administrator's Guide*.

If the user credentials are valid, Operations Manager displays its Site Summary page.

Troubleshooting Enterprise Vault Operations Manager

If you see an error page when attempting to access Enterprise Vault Operations Manager, ensure that you have done the following and then try to access the application again:

- Confirm that you have satisfied all the preinstallation steps.
  See "About additional requirements for Operations Manager" on page 53.

- Check that IIS is not locked down.

- Ensure that Integrated Windows Authentication is enabled for the Default Web Site in IIS, and then restart IIS.

If this does not solve the problem, see the following technical note on the Veritas Support website:

http://www.veritas.com/docs/000033198

The technical note provides detailed troubleshooting information related to installing and using Operations Manager.

Section **4**

Initial Enterprise Vault setup

Initial Enterprise Vault setup

This chapter includes the following topics:

- License keys

- Using the Enterprise Vault Administration Console

- Adding core Enterprise Vault services with the Administration Console

- Creating Enterprise Vault retention categories

- Performance issues when Enterprise Vault has limited or no access to the Internet

License keys

At the end of the configuration wizard you were asked to start the Enterprise Vault services. These services will not start until you have installed the appropriate license keys.

Using the Enterprise Vault Administration Console

The Enterprise Vault Administration Console is a snap-in for Microsoft Management Console (MMC). MMC provides a common framework for administrative tools that gives them all a similar look and feel. It is possible to customize an MMC snap-in so that it includes the exact functionality needed by a particular administrator.

The Administration Console enables you to manage the Enterprise Vault sites, services, archiving tasks, policies and targets.

If people are using separate administration consoles at the same time to make changes to Enterprise Vault, the changes made by one person are not necessarily shown in the other consoles. You are recommended to avoid using multiple consoles simultaneously when managing Enterprise Vault. If you do use multiple consoles, press F5 to refresh the Administration Console display before you make any changes.

Starting the Enterprise Vault Administration Console

To use the Administration Console initially, log in as the Vault Service account. You can then assign roles to other administrators so that they can perform the required Enterprise Vault management tasks using the Administration Console.

To start the Enterprise Vault Administration Console

1   On the **Apps** screen, select **Enterprise Vault > Administration Console**.

2   In the **Connect** dialog box, type the name or IP address of any server in the Enterprise Vault site that is running the Directory service. You can type the IP address in IPv4 or IPv6 format.

On the first occasion that you open the Administration Console, a dialog box describing the new features in this release appears. You may also see an invitation to opt in to Enterprise Vault Product Improvement. This feature helps Veritas to improve the quality of Enterprise Vault.

The left pane of the Administration Console shows the hierarchy of components that make up your Enterprise Vault site. The right pane shows you the contents of whatever you select in the hierarchy.

To get Help

◆   Do one of the following:

- To access online Help for Enterprise Vault, click **Help > Help on Enterprise Vault**. This online Help includes Enterprise Vault manuals.

- To find out more about MMC, click **Help > Help on MMC** in the **MMC** window. The MMC Help appears.

To refresh the screen

◆   Press F5 to force a refresh at any time.

About administration roles in the Enterprise Vault Administration Console

Enterprise Vault provides the following mechanisms that you can use to control the access administrators have to the Administration Console:

- Roles-based administration. Many administrative tasks do not require all the permissions that are associated with the Vault Service account. Roles-based administration enables you to provide individual Enterprise Vault administrators with exactly the permissions required to perform their individual administrative tasks.

  You can assign individuals or groups to roles that match their responsibilities and they are then able to perform the tasks that are included in those roles. Because the permissions are associated with roles, rather than with individual administrators, you can control the role permissions without having to edit the permissions for each administrator.

- Admin permissions. You can grant or deny access to the following containers in the Administration Console tree:

  - File Server

  - Exchange Server

  - SharePoint Virtual Server

  - Enterprise Vault Server

You can control access by assigning roles, or by using admin permissions, or both.

When you install Enterprise Vault for the first time, only the Vault Service account can access the Administration Console. You can restrict the tasks administrators can perform by assigning roles and you can further restrict access by using admin permissions to restrict administrators to managing specific Administration Console containers.

For instructions on setting up roles-based administration, see the *Administrator's Guide*.

Adding core Enterprise Vault services with the Administration Console

Use the Administration Console to add the following core Enterprise Vault services:

- Indexing service

- Storage service

- Shopping service

- Task Controller service

When creating services, you may be prompted for the password of the Vault Service account.

Ensure that the index storage location is on an accessible device to which the Vault Service account has write access.

When you add archiving tasks, such as Exchange Mailbox or File System archiving tasks, they run under the control of the Task Controller service. If you stop the Task Controller service, all tasks running under the control of this service also stop.

The same instructions can be repeated to add each of these services.

To add a core Enterprise Vault service with the Administration Console

1   In the left pane, expand the Enterprise Vault site hierarchy until the **Enterprise Vault Servers** container is visible.

2   Expand the **Enterprise Vault Servers** container.

3   Expand the computer to which you want to add a service.

4   Right-click **Services** and, on the shortcut menu, click **New** and then **Service**.

    The **Add Service** dialog box appears, listing the services you can add.

5   Click the service that you want to add.

6   Click **Add**.

Creating Enterprise Vault retention categories

You may have decided during planning that you wanted more retention categories than the ones predefined in Enterprise Vault. If this is the case, you must create your own retention categories. Alternatively, you can edit the predefined retention categories to suit your needs.

If you configure Enterprise Vault to archive from Exchange managed folders, it can automatically synchronize managed content settings to managed folder retention categories. Enterprise Vault creates managed folder retention categories automatically. For more information, see the *Administrator's Guide*.

To create a new retention category

1   In the left pane of the Administration Console, expand the vault site hierarchy until **Policies** is visible.

2   Expand **Policies** and then expand **Retention & Classification**.

3   Right-click **Categories** and then, on the shortcut menu, click **New** > **Retention Category**.

    The New Retention Category wizard starts.

4   Work through the wizard.

About the properties of Enterprise Vault retention categories

By assigning an Enterprise Vault retention category to items at the time they are archived, it is possible to categorize stored items. This categorization makes it easier to retrieve items because it is possible to search by category.

A retention category also specifies the minimum amount of time after its last modification date that an item must be retained. This length of time is the retention period. For mail messages, the retention period is the time since the message was received. For documents, it is the time since the document was last modified.

With Exchange Server archiving, users can select retention categories for mailbox folders or items so that, when archiving occurs, items are stored with the appropriate retention category.

If you later modify a retention category, the changes are retrospective. For example, if you have a retention category called Customer Accounts with a retention period of 5 years and you change the retention period to 10 years, items that have been already archived with the Customer Accounts retention category are retained for a minimum of 10 years.

Enterprise Vault can automatically delete expired items. See the *Administrator's Guide* for more details.

Note: You cannot delete retention categories. You can rename them as required and you can hide them from users.

A retention category has the following properties:

Name	You can modify the retention category name as needed. The new name is used immediately.
Description	(Required) This is a description of the retention category. Make sure that the description you give here is meaningful to users.

Retention period	This is the minimum amount of time to retain an item that has been archived using this retention category.
	You can choose whether the period runs from the date the item was last modified or from the date that the item was archived.
	If you choose to archive by last modified date, Enterprise Vault calculates the date as follows:
	■ For mail messages, the date is the date that the message was received.
	■ For documents, the date is the date the document was last modified.
Retain items forever	Select this option if you want items never to expire.
	If you plan to store items indefinitely on a WORM storage device, then ensure that the retention settings on the device are correctly configured.
	See "Preparing WORM storage devices" on page 26.
Prevent automatic deletion of expired items with this category	Select this option to prevent automatic deletion of items with this retention category when the retention period expires.
	This setting affects only those items that are stored in archives. It does not affect items that are still on archiving target servers.
Prevent user deletion of items with this category	Select this option to prevent users from deleting items with this retention category.
	This setting affects only those items that are stored in archives. It does not affect items that are still on archiving target servers.
	This setting does not prevent applications that use the Enterprise Content Management API from deleting items with this retention category.
Hide this category from users	Select this option to prevent users from using this category when archiving new items. The category is still available to users when they are searching for items that have already been archived.
	Enterprise Vault does not allow the site default retention category to be hidden from users. If you hide the site default retention category, Enterprise Vault automatically chooses another retention category and makes it the site default.

Lock this Retention Category	To prevent unintentional changes, select this option to lock all the retention category settings.
Base expiry on	Select one of the following: ■ Inherit from Site settings. The retention period is inherited from the Site default retention category settings. ■ Modified date. The retention period is based on the date when the item was last modified. For mail messages, a retention period that is based on the modified date is the time since the message was sent or received. For documents, it is the time since the document was last modified. ■ Archived date. The retention period is the time since the item was archived.
Administrative note	For your notes. Edit this text as necessary. This text is visible only to Enterprise Vault administrators.

About retention plans

With a retention plan, you can associate a retention category with a number of other settings, such as a classification policy and the criteria for discarding expired items, and apply them all to one or more archives. If you choose to set a classification policy with a retention plan then, for the archives to which you assign the retention plan, the classification policy determines the following:

■ Whether to classify items at the same time that Enterprise Vault indexes and archives them. After Enterprise Vault has applied the classification tags, users of applications like Compliance Accelerator and Discovery Accelerator can use them to filter items when they conduct searches and reviews.

■ Whether to classify items when users manually delete them or Enterprise Vault automatically expires them.

For more information on the classification feature, see the *Classification* guide.

Applying a retention plan to an archive gives you greater control over the retention periods of the items in the archive. In particular, a retention plan lets you dispose of already-archived items by giving them a different retention period than the one that Enterprise Vault first gave them when it archived the items. For example, you can configure a retention plan so Enterprise Vault expires the affected items according to the retention category that you have associated with the retention plan, and not the retention categories with which Enterprise Vault originally stamped them.

Creating a retention plan

We recommend that you only create retention plans after you have defined the retention categories and classification policies that you want to assign with those plans.

You can modify a retention plan after you have created it and applied it to one or more archives. You can also dissociate the plan from those archives and assign a different plan to them.

To create a retention plan

1   In the left pane of the Enterprise Vault Administration Console, expand the tree view until the **Policies** container is visible.

2   Expand the **Policies** container and then expand the **Retention & Classification** container.

3   Right-click **Plans** and then point to **New** and click **Retention Plan**.

The New Retention Plan wizard appears.

4   Work through the pages of the wizard, which prompt you to enter the following:

  ■   A name for the new retention plan. The name must be unique, and it can contain up to 40 alphanumeric or space characters.

  ■   A description of the plan. The description can contain up to 127 alphanumeric, space, or special characters.

  ■   A retention category to associate with the retention plan. If no suitable retention category exists, the wizard provides the option to create one.

  ■   Optionally, whether to allow the Enterprise Vault classification feature to classify the items that the retention plan handles. If you choose to classify the items, you must also select the required classification policy.

  ■   The expiry settings to assign to the affected items.

Performance issues when Enterprise Vault has limited or no access to the Internet

Enterprise Vault files are digitally signed with a Veritas SSL certificate. By default, when these files are accessed, Windows checks online to determine whether their digital certificate has been revoked. If Enterprise Vault does not have an Internet connection, or connectivity is slow, delays can occur at the following times:

■   When you install Enterprise Vault

■   When you start the Administration Console

■ When users browse and search archives through a web browser

If you experience these delays, you can stop Windows from checking for digital certificates that have been revoked. You can do this on a per-process basis or for all processes that run under a particular user account.

Turning off certificate revocation checking for individual processes

Note that if the Enterprise Vault server gains Internet access in the future, you can turn certificate revocation checking back on by deleting the configuration files that you create below.

To turn off certificate revocation checking for individual processes

1   Use a plain-text editor such as Windows Notepad to create a configuration file that contains the following lines:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <runtime>
    <generatePublisherEvidence enabled="false"/>
  </runtime>
</configuration>
```

For more information on the generatePublisherEvidence element, see the following article on the Microsoft website:

http://msdn.microsoft.com/library/bb629393.aspx

2   Do one or more of the following:

■ To turn off checks by the self-installation routines in the Enterprise Vault installer, save the configuration file as `InstallUtil.exe.config` in the same folder as `InstallUtil.exe` (typically `%windir%\Microsoft.NET\Framework\v4.`*n.n.n*`).

■ To turn off checks by the self-registration routines in the Enterprise Vault installer, save the configuration file as `RegAsm.exe.config` in the same folder as `RegAsm.exe` (typically `%windir%\Microsoft.NET\Framework\v4.`*n.n.n*`).

■ To turn off checks by the Enterprise Vault System Status MMC snapin, save the configuration file as `mmc.exe.config` in the same folders as `mmc.exe` (typically `%windir%\SysWOW64` and `%windir%\system32`).

■ To turn off checks by all web applications on the server, save the configuration file as `w3wp.exe.config` in the same folders as `w3wp.exe` (typically `%windir%\SysWOW64\inetsrv` and `%windir%\system32\inetsrv`).

Turning off certificate revocation checking for all processes that run under a particular user account

If you use this method, you must change the settings on each Enterprise Vault server for every account that runs an Enterprise Vault service.

To turn off certificate revocation checking for all processes that run under a particular user account

1   Log on to the Enterprise Vault server as an account that runs Enterprise Vault services on that server. This account is typically the Vault Service account.

2   In Windows Control Panel, double-click **Internet Options**.

3   In the **Internet Properties** dialog box, click the **Advanced** tab.

4   In the **Security** section, uncheck **Check for publisher's certificate revocation**.

5   Click **OK**.

Setting up storage

This chapter includes the following topics:

About setting up storage for Enterprise Vault archives

Before you set up storage for your archives, consider whether you want to use Enterprise Vault's optimized single instance storage. Single instance storage can greatly reduce your storage requirements by sharing the common parts of archived items. However, it can increase the network traffic between the Enterprise Vault servers and the storage devices that host the partitions.

If you intend to use single instance storage, you need to decide on a sharing regime that is appropriate for your requirements and compatible with your network connection speeds.

Note: A new vault store group is configured by default to use Enterprise Vault single instance storage. The only exception is the Default Upgrade Group that Enterprise Vault created if you previously upgraded to Enterprise Vault 8.0.

For Enterprise Vault to be able to create archives, you must create a vault store group that contains a vault store and at least one vault store partition:

- A vault store group is a container for vault stores. It defines the outer boundary for sharing items in Enterprise Vault single instance storage.
  See "Creating vault store groups" on page 183.

- A vault store is a logical entity to which an Enterprise Vault Storage service archives items. Each vault store has its own vault store database. The vault store database holds information about the archives in the vault store and all the items that are stored in each archive.
  See "About creating vault stores" on page 184.

- A vault store partition is a physical location where Enterprise Vault stores archived data. Each vault store must contain at least one partition. Partitions can be placed on different physical disks and on various types of storage medium. As the data in a vault store grows, you can create more partitions to provide additional capacity. You can configure the partitions so that archiving rolls over from one partition to another when certain criteria are met.
  See "Creating vault store partitions" on page 189.

To configure Enterprise Vault single instance storage for a vault store group, you must run the Configure Sharing wizard on the group.

See "Configuring sharing for a vault store group" on page 195.

About Enterprise Vault single instance storage

Enterprise Vault's optimized single instance storage can provide a significant reduction in the storage space that is required for archived items. Enterprise Vault identifies the shareable parts (SIS parts) of an item, such as a message attachment or the contents of a document. It stores each SIS part separately, and only once within a sharing boundary. A sharing boundary can include one or more vault stores within a vault store group. When Enterprise Vault identifies a SIS part that it has already stored in the target vault store's sharing boundary, it references the stored SIS part file instead of archiving the SIS part again.

Enterprise Vault applies a minimum size threshold for SIS parts. The size threshold enables Enterprise Vault to balance the likely storage savings against the resources that are required to create, archive, and retrieve the SIS parts.

Enterprise Vault single instance storage can save storage space in a number of ways:

- Enterprise Vault shares the SIS parts between all the vault stores within a sharing boundary. For example, if you use separate vault stores for journaling and mailbox archiving, Enterprise Vault can share the SIS parts between the vault stores.

- If a number of separate messages with the same attachment are sent to multiple recipients, Enterprise Vault stores the attachment only once within a sharing boundary.

- Enterprise Vault identifies a SIS part from the content, not the file name. If two messages both have the same file attachment, Enterprise Vault can share the attachments, even if they have different file names.

- Enterprise Vault can share the identical SIS parts that result from different types of archiving, such as an Exchange message attachment that is also stored as a file on a file server.

A new vault store uses single instance storage by default, and shares only the SIS parts of items that are archived within itself. You can run the Configure Sharing wizard on a vault store group to extend sharing between vault stores, or to turn off Enterprise Vault single instance storage if you want.

Note: Enterprise Vault single instance storage is not performed when items are stored to partitions that are hosted on EMC Centera devices. Enterprise Vault provides a separate device-level sharing option to take advantage of the sharing capabilities of EMC Centera devices.

See "About EMC Centera device-level sharing" on page 181.

About sharing levels and sharing boundaries

When you configure sharing for a vault store group, you set a sharing level for each vault store in the group. The sharing levels determine the boundaries for single instance storage sharing in the group.

Table 23-1 Vault store sharing levels

Vault store's sharing level	Effect on sharing
Share within group	The vault store shares SIS parts with all the other vault stores in the vault store group that have this sharing level.
Share within vault store	The vault store shares SIS parts only within itself.

Table 23-1   Vault store sharing levels *(continued)*

Vault store's sharing level	Effect on sharing
No sharing	Enterprise Vault does not perform single instance storage for this vault store.

A vault store group can therefore contain one or more sharing boundaries. Each sharing boundary contains one or more vault stores that share the SIS parts that result from Enterprise Vault single instance storage.

Figure 23-1 shows an example vault store group that contains five vault stores:

Figure 23-1   Sharing boundaries in a vault store group
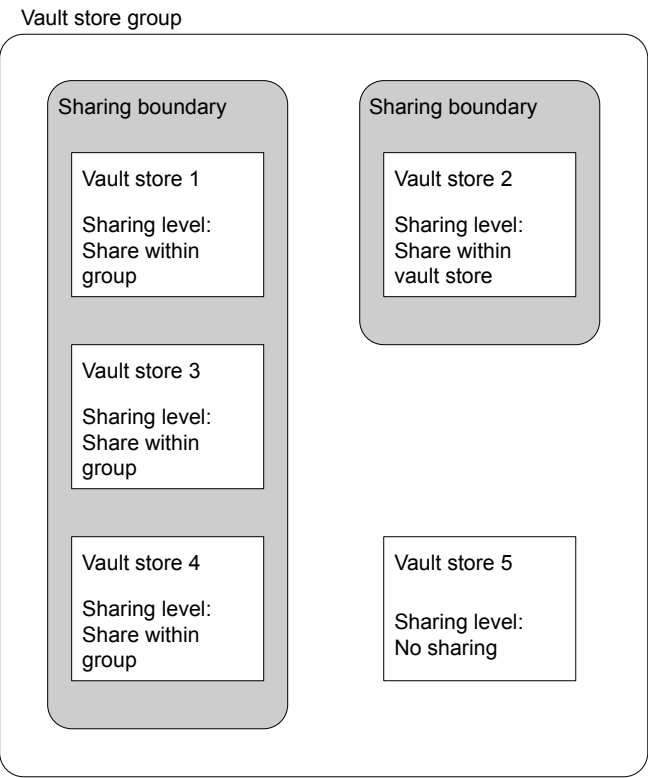
- Vault stores 1, 3, and 4 all have the sharing level "Share within group". These vault stores are within the same sharing boundary. Enterprise Vault shares SIS parts across the three vault stores for the items that it archives to these vault stores.

- Vault store 2 has the sharing level "Share within vault store", so it has its own sharing boundary. Enterprise Vault shares SIS parts within the vault store for the items that it archives to this vault store.

- Vault store 5 has the sharing level "No sharing". The vault store is not included in any sharing boundary. Enterprise Vault does not perform Enterprise Vault single instance storage on the items that it archives to this vault store.

Note that a vault store group can have only one sharing boundary that contains multiple vault stores. For example, in Figure 23-1, you cannot configure two new vault stores to share SIS parts across each other and not with the existing vault stores. You can instead create the new vault stores in another vault store group.

Enterprise Vault assigns a sharing level of "Share within vault store" to new vault stores.

To change the sharing level for a vault store, run the Configure Sharing wizard on the vault store group after you have created a partition for the vault store.

How Enterprise Vault single instance storage works

Enterprise Vault archives an item using single instance storage if both of the following conditions apply:

- The target vault store has a sharing level of "Share within vault store" or "Share within group".

- The current open partition is not hosted on an EMC Centera device.

Enterprise Vault archives an item for single instance storage as follows:

- It identifies the parts of an item that are suitable for sharing, such as large message attachments. These parts are referred to as SIS parts. Enterprise Vault uses a minimum size threshold for SIS parts, to balance the likely storage savings against the resources that are required to create, archive, and retrieve them.

- It generates a digital fingerprint to each SIS part. The fingerprint is a cryptographic, hash-based identifier that is determined by the contents of the SIS part.

- For each SIS part, Enterprise Vault accesses the vault store group's fingerprint database to determine whether a SIS part with the same fingerprint is already stored within the vault store's sharing boundary. A SIS part with the same fingerprint indicates an identical SIS part.

  - If an identical SIS part is not already stored within the sharing boundary, Enterprise Vault stores the SIS part and saves the SIS part's fingerprint information in the fingerprint database.

- If an identical SIS part is already stored within the sharing boundary, Enterprise Vault references the stored SIS part. It does not store the SIS part again.

- It stores the remainder of the item (the item minus any SIS parts) as the residual saveset file. The residual saveset file holds Enterprise Vault metadata about the item and unique information about it, such as the file name if it is a document or attachment, and follow up flags if it is a message.

When Enterprise Vault receives a request to restore an archived item, it reconstitutes the item from the item's residual saveset file and SIS part files.

If an item's target vault store has a sharing level of "no sharing" or the target partition is hosted on an EMC Centera device, then Enterprise Vault does not use single instance storage. It archives the item with its Enterprise Vault metadata as a single saveset file.

About the fingerprint database

A vault store group's fingerprint database holds information about each SIS part that is stored in the vault store group. The information includes the SIS part's digital fingerprint, the name of the partition in which the SIS part is stored, and in which sharing boundary the SIS part is shared.

When you create a vault store group, Enterprise Vault creates a fingerprint database for that vault store group.

Note: To add or change locations after the fingerprint database is configured is a SQL Server administration task. See your Microsoft SQL Server documentation for details.

The New Vault Store Group wizard provides the following options for configuring the fingerprint database's SQL filegroups:

- A basic configuration, where Enterprise Vault locates the primary filegroup and all the non-primary filegroups on one device.

- An option to configure additional locations for the 32 non-primary filegroups. The non-primary filegroups store fingerprint information for archived items and so they can grow rapidly when you use single instance storage. For best performance you need to spread the non-primary filegroups across multiple locations.

For optimal performance, do as follows:

- Select the option to configure additional locations for the non-primary filegroups.

- Specify as many locations as possible for the non-primary filegroups on the SQL Server, up to the maximum of 32.

- Specify a separate device for each location. If you specify more than one location on the same device there is no performance benefit.

Deletion of SIS parts

The fingerprint database for each vault store group records the number of references to each SIS part that are present in the group's vault stores.

As users delete archived items, the number of references to a SIS part decreases. On the deletion of an item, if the number of references to a SIS part falls to 0 then Enterprise Vault checks whether the group's vault stores contain any references to the SIS part. Provided that no references remain, Enterprise Vault deletes the SIS part. If any references remain, Enterprise Vault retains the SIS part and generates an error in the Enterprise Vault event log.

Note: If you use collections, unreferenced SIS parts may remain in a CAB file for some time before they are deleted.

See "About collections and migration" on page 191.

Requirements for Enterprise Vault single instance storage

Enterprise Vault single instance storage places some additional requirements on a system, as follows:

- Storage space for the fingerprint database. When you use Enterprise Vault single instance storage the fingerprint database may grow very rapidly. To ensure acceptable archiving and retrieval performance, it is important to configure the fingerprint database appropriately for the amount of sharing in the vault store group.
  See "Creating vault store groups" on page 183.

- Network connectivity requirements. An Enterprise Vault server communicates with the following computers when it stores or retrieves items using Enterprise Vault single instance storage:

  - The computers that host the vault store partitions for the vault stores that are within the vault store's sharing boundary.

  - The computer that hosts the vault store group's fingerprint database.
  Network connection speeds must be fast enough across these connections to provide acceptable storage and retrieval times.

About EMC Centera device-level sharing

You can configure a partition for an EMC Centera device to take advantage of the Centera's device-level sharing, if required. Enterprise Vault then stores the shareable parts of a saveset as separate data blobs, so that the Centera device is able to share them.

The New Partition wizard includes an option to enable device-level sharing when you create a partition and specify an EMC Centera device.

See "Creating vault store partitions" on page 189.

You can also enable device-level sharing from the General tab of the partition properties.

Partitions for EMC Centera do not take part in Enterprise Vault single instance storage sharing. If you create a partition for EMC Centera in a vault store that is configured for sharing, the partition is ignored for the purposes of Enterprise Vault single instance storage sharing.

About sharing partitions on storage devices that support the Enterprise Vault storage streamer API

You can create vault store partitions on storage devices that support the Enterprise Vault storage streamer API. The appropriate storage device software must be installed on the Enterprise Vault server that hosts the Enterprise Vault Storage service for the partition.

To support sharing within the vault store group, the storage device software must also be installed on each Enterprise Vault storage server that manages a partition in the same vault store group.

Developing a suitable sharing regime for Enterprise Vault single instance storage

If you use Enterprise Vault single instance storage, you need to create a sharing regime that meets your organization's data sharing requirements and which is appropriate for your network connection speeds.

Consider what sort of sharing regime you require before you start archiving. There are limits to what you can change:

- You can change a vault store's sharing level, but the change does not act retrospectively. For example, if you change a vault store's sharing level from 'share within group' to 'share within vault store', any items already shared within the vault store group remain so.

- You cannot move a vault store to another vault store group unless all of the following circumstances apply:

  - You previously upgraded to Enterprise Vault 8.0.

  - The vault store is one that Enterprise Vault upgraded to Enterprise Vault 8.0, or one that you created in the Default Upgrade Group.

  - The vault store's sharing level is "No sharing" and has never been changed.

When deciding how to set up single instance storage, consider the following:

- You may need to keep parts of your organization separated with information barriers, also known as "Chinese walls". For example, a datacenter may be required by law or by company policy to keep information separate between its investment, retail, and mergers and acquisitions groups, to avoid conflicts of interest.

  You may want to create a separate vault store group for each organizational group in which information must be isolated.

- Network connectivity between the appropriate computers must be sufficient to provide acceptable storage and retrieval times. As a minimum we recommend that you limit single instance storage to an environment in which the connections support the expected response time of a 100 Mbps switched Ethernet LAN.

  The Enterprise Vault server whose Storage service manages a vault store must have adequate connectivity with the following:

  - The computers that host the vault store partitions for the vault stores that are within the vault store's sharing boundary.

  - The computer that hosts the vault store group's fingerprint database.

  The slower the connection speeds between these computers, the longer it takes Enterprise Vault to archive and retrieve the shared items.

  If your organization spans several widely-dispersed geographical locations it may be appropriate to create separate vault store groups for each location. Remember to locate the fingerprint databases locally.

  Enterprise Vault provides a connectivity test to estimate connection speeds across sample network connections. The relevant wizards prompt you to run the connectivity test when you create a new vault store group or partition, or when you configure sharing. The connectivity test can help you create a sharing regime with an acceptable level of performance. To assess performance, the connectivity test measures the average round-trip time for a number of `ping` requests. If you have disabled `ping` in your environment, use your own tools to

decide if the performance is acceptable. We recommend a round-trip time of one millisecond or less.

If the test results indicate poor connectivity, consider modifying the sharing boundaries or changing the location of your computers to improve connection speeds. If you are willing to accept poorer performance, you can choose to accept poor connectivity test results.

- When you create a vault store group, configure its fingerprint database appropriately for the projected sharing requirements.
  See "Creating vault store groups" on page 183.

Creating vault store groups

Vault stores are grouped within vault store groups. If you use Enterprise Vault single instance storage, a vault store group forms an outer boundary for the sharing of SIS parts.

Before you start creating vault store groups and vault stores, consider what sort of sharing regime is compatible with your organization's structure and network connection speeds.

See "Developing a suitable sharing regime for Enterprise Vault single instance storage" on page 181.

You can create a vault store group using the New Vault Store Group wizard, as follows.

To create a vault store group

1   In the left pane of the Administration Console, expand the Enterprise Vault site hierarchy until **Vault Store Groups** is visible.

2   Right-click **Vault Store Groups** and then click **New** > **Vault Store Group**.

     The New Vault Store Group wizard starts.

3   Work through the wizard. You need to provide the following information:

     - A name for the Vault Store Group.

     - The SQL server that is to host and manage the group's fingerprint database.

     - The locations for the fingerprint database's SQL filegroups.

     The New Vault Store Group wizard provides the following options for configuring the filegroups:

     - A basic configuration, where Enterprise Vault locates the primary filegroup and all the non-primary filegroups on one device.

- An option to configure additional locations for the 32 non-primary filegroups. The non-primary filegroups can grow rapidly in size when you use single instance storage. For best performance, spread the non-primary filegroups across multiple locations.

For optimal performance do as follows:

- Select the option **Configure additional locations for non-primary filegroups**.

- Specify as many locations as possible for the non-primary filegroups on the SQL Server, up to the maximum of 32.

- Specify a separate device for each location. If you specify more than one location on the same device there is no performance benefit.

Note: To add or change locations after the fingerprint database is configured is a SQL Server administration task. See your Microsoft SQL Server documentation for details.

When the vault store group has been created, the New Vault Store wizard takes you through the steps to create a vault store.

See "About creating vault stores" on page 184.

About creating vault stores

When you create a vault store, you must specify an Enterprise Vault Storage service to manage it, and a location for the SQL vault store database.

The vault store database holds information about the archives in the vault store and all the items that are stored in each archive. For example, when an archived item has been backed up, this fact is reflected in the information that is held in the vault store database.

About Enterprise Vault safety copies

Enterprise Vault can be configured to retain archived items until the vault store partition in which they are archived has been backed up. During the time between archiving and removal, the original items are treated as safety copies by Enterprise Vault. When the vault store partition has been backed up, Enterprise Vault can remove the safety copies.

The removal of safety copies takes place when the storage service is started, or when backup mode is cleared from the vault store. Enterprise Vault also creates shortcuts and placeholders at this time if it is configured to do so.

Choosing when to remove Enterprise Vault safety copies

During the creation of each vault store, you must choose from the following settings to control how Enterprise Vault manages safety copies:

- **No, remove immediately after archiving**. All safety copies are removed immediately after the items have been archived.

- **Yes, in the original location**. Enterprise Vault keeps the original items until the partition that contains the archived items has been backed up.

- **Yes, in the storage queue**. Enterprise Vault keeps safety copies in the storage queue until the partition that contains the archived items has been backed up.

You can specify the default settings for all vault stores and you have the option to specify different settings for journal vault stores.

Checking that the partition has been backed up before Enterprise Vault removes safety copies

If you choose to keep safety copies Enterprise Vault must check that the partition has been backed up before it removes those safety copies.

Enterprise Vault checks that each partition has been backed up based on one of the following:

- The archive attribute of the files on the partition. You can use archive attributes to determine whether a partition has been backed up only if your backup software resets the archive attributes after backup.

- A trigger file mechanism. If you backup software does not reset the archive attribute on the files it backs up, you must use this mechanism.

You must choose which method to use for each partition when you create it using the **New Partition** wizard.

Using the archive attribute to determine whether a partition has been backed up

The **Use the archive attribute** option requires your backup software to reset the archive attribute on the files in vault store partitions after they have been secured. If your backup software does not reset the archive attribute, you must use the trigger file mechanism.

When Enterprise Vault creates a file in a vault store partition, the file's archive attribute is set. Until the archive attribute is cleared, Enterprise Vault considers that the file is not backed up, and the corresponding safety copies are not removed. However, when your backup software clears the archive attribute, Enterprise Vault considers that the file is backed up, and is free to remove the safety copy. If

appropriate, shortcuts to the archived items are created at the same time the safety copy is removed.

Note: Some WORM devices do not allow the archive attribute to be changed. These devices are incompatible with the **Use the archive attribute** option.

Using the trigger file mechanism to determine whether a partition has been backed up

Some backup software clears the archive bit on files after backing them up. This attribute is visible as the **File is ready for archiving** option in each file's properties.

However, some backup software and other methods of securing data do not clear this attribute. In this case you must use the trigger file mechanism to indicate that data on each partition is secure.

The use of trigger file mechanism would be necessary in the following examples:

- You take snapshots of the partition to secure its data.

- You use backup software that does not clear the archive bit, such as Tivoli Storage Manager (TSM).

- You take differential backups, which clear the archive bit only when a full backup occurs.

Note: You must ensure that your backup scripts do not create a trigger file unless the backup has completed successfully.

The **Check for a trigger file** option determines whether the files in a vault store partition have been secured by checking for a trigger file called `IgnoreArchiveBitTrigger.txt`. At each backup, your backup software or script must place a newly created `IgnoreArchiveBitTrigger.txt` in the root of the partition to show that a backup has taken place.

For example, if you have a vault store called "Sales", and you have placed its partitions in `E:\EVStorage`, you might have a partition folder called `E:\EVStorage\Sales Ptn1`. In this case, your backup software or script must place `IgnoreArchiveBitTrigger.txt` in `E:\EVStorage\Sales Ptn1` to indicate that it has backed up the partition.

Note: It is essential that your backup script creates a new
`IgnoreArchiveBitTrigger.txt` file when it backs up a partition. It is not sufficient
to rename another file because its file creation date does not match the time of the
backup.

For example, you can use the following command in your backup script to create
a new file:

```
echo "Enterprise Vault trigger file" > "E:\EVStorage\Sales
Ptn1\IgnoreArchiveBitTrigger.txt"
```

When Enterprise Vault finds `IgnoreArchiveBitTrigger.txt`, all the partition's
saveset files that were created before the creation of
`IgnoreArchiveBitTrigger.txt` are considered backed up. Enterprise Vault is
then free to remove the safety copies that correspond with the secured saveset
files, and to create shortcuts if appropriate.

If Enterprise Vault does not find `IgnoreArchiveBitTrigger.txt`, it considers that
the partition is not backed up, and safety copies are not removed.

When Enterprise Vault has completed the removal of safety copies, it renames
`IgnoreArchiveBitTrigger.txt` with a `.old` extension to show that the file has
been processed and that the relevant files on the partition are secure.

At the next backup, your backup software creates a new
`IgnoreArchiveBitTrigger.txt`.

Enterprise Vault checks partitions for a trigger file when the storage service starts
and when backup mode is cleared from a vault store. Additionally, if you set a scan
interval for the partition, Enterprise Vault checks the partition at intervals determined
by the value you set.

Although you cannot use the trigger file mechanism on Centera partitions, Enterprise
Vault queries the Centera API to determine whether or not a partition has been
replicated. Enterprise Vault checks Centera partitions when the storage service
starts, and when backup mode is cleared from a vault store.

Additionally, if you set a scan interval for the Centera partition, Enterprise Vault
checks the partition at intervals determined by the value you set.

Creating a vault store

You can create a vault store using the New Vault Store wizard.

To create a vault store

1   If you created a vault store group using the New Vault Store Group wizard, the New Vault Store wizard starts automatically. Go to step 5.

2   In the left pane of the Administration Console, expand the Enterprise Vault site hierarchy until **Vault Store Groups** is visible.

3   Expand the **Vault Store Groups** container to show the existing vault store groups.

4   Right-click the vault store group in which you want to create the vault store, and then click **New > Vault Store**.

    The New Vault Store wizard starts.

5   The New Vault Store wizard takes you through the steps to create a vault store.

    You need to provide the following information:

- The name of the computer that hosts the Storage Service that the vault store is to use. The wizard requests this information only if the Enterprise Vault site contains more than one computer with a Storage Service.

- The name of the vault store. The name can contain letters, numbers, and spaces.

- The SQL server that is to create and manage the vault store database, and the locations for the database files.

- The location for safety copies. Enterprise Vault can keep safety copies in the original location or on the storage queue. If you choose the storage queue location Enterprise Vault can remove the original items as soon as they have been archived. The storage space in the original location is recovered quickly.

- When safety copies of items are to be removed, and how Enterprise Vault checks that partitions have been backed up.
  See "About Enterprise Vault safety copies" on page 184.

Note: Enterprise Vault assigns a sharing level of "Share within vault store" to new vault stores. An exception to this rule applies to the Default Upgrade Group, which Enterprise Vault created if you previously upgraded to Enterprise Vault 8.0. If you do not configure sharing for the Default Upgrade Group, Enterprise Vault assigns a sharing level of "No sharing" to new vault stores in that group.

To change the sharing level for a vault store, run the Configure Sharing wizard on the vault store group after you have created a partition for the vault store.

When the vault store has been created, the New Partition wizard takes you through the steps to create a partition for the vault store.

Creating vault store partitions

Vault store partitions can be placed on different physical disks and on various types of storage medium. For example, you can create partitions on local NTFS volumes, NetApp filers, EMC Centera devices, or streamer storage devices. For a full list of supported devices, see the Enterprise Vault *Compatibility Charts* at http://www.veritas.com/docs/000097605.

When deciding on the location for a partition, do not choose the location of an existing partition, or a location that includes any folders that are associated with an existing partition. Take particular care to avoid the overlap of partition folders when using network shares or mount points. You may suffer data loss if a folder is associated with more than one partition.

Note: You are recommended not to use disk quota and File Server Resource Manager quotas for vault store partitions.

Enterprise Vault assumes that the partition root path is empty. Do not use the root path to hold files or folders other than those that Enterprise Vault creates.

If you plan to store items indefinitely on a WORM storage device, then ensure that the retention settings on the device are correctly configured.

See "Preparing WORM storage devices" on page 26.

If you plan to create a vault store partition on a storage device that supports the Enterprise Vault storage streamer API, then ensure that the appropriate storage device software is installed on the Enterprise Vault storage servers. Install the storage device software on all the Enterprise Vault storage servers that manage the partitions in the vault store group.

Initial states of vault store partitions

As the data in a vault store grows, you can create more partitions to provide additional capacity. Each vault store can contain only one open partition and Enterprise Vault archives data into this partition while it remains open.

There are two approaches to the management of open vault store partitions:

- You can manually change the open partition in a vault store. For example, when the disk that hosts the open partition reaches capacity, you can close the partition and open a partition on another disk.

- The automatic partition rollover feature which lets you configure partitions such that archiving rolls over from one partition to another when certain criteria are met. For example, you can configure a partition to roll over when the disk that hosts the open partition has only 5% free space. You can also configure partitions to roll over on a date that you set. For more information, see the *Administrator's Guide*.

To support both these features, during the creation of partitions, you can choose any one of these initial states:

- Select **Closed** to create a closed partition. If there is an existing open partition, it is not affected by this choice. You can open the new partition at any time by editing its properties.
  See

- Select **Open** to create an open partition. Each vault store can have only one open partition. If there is an existing open partition in the vault store, it is automatically closed and items are archived to this new partition.

- Select **Ready** to create a new partition that is available for partition rollover.

About closed Enterprise Vault partitions

When a partition is closed, Enterprise Vault stops writing new information to it. Enterprise Vault may still modify the items that are on the closed partition.

Note: A closed partition can increase in size and needs to be backed up.

Enterprise Vault modifies a closed partition for the following reasons:

- Deletion. Enterprise Vault modifies the partition if users delete items from their archives.

- Storage Expiry. Enterprise Vault deletes items from archives when their Retention Periods expire.

- Collections. The Enterprise Vault Collector continues to run on a closed partition. Collections are required on closed partitions because the collection process removes the temporary files that are created when users view archived items.

- Pending Items. Items that are in a pending state before the partition is closed result in writes to the closed partition.

If a closed partition is likely to be modified, we recommend that you continue to perform regular backups of the closed partition

If a closed partition is never modified, you do not need to perform regular backups. You can perform a final backup of the partition and then remove the partition from your backup routine.

About collections and migration

Where vault store partitions are held on non-WORM devices other than EMC Centera, you can configure and schedule the collection and migration of the files that are stored in the partition.

Collection involves collecting multiple small files into much larger collection files (`.cab` files). Collection may give you a significant improvement in backup times. Collection is not recommended on devices that perform deduplication, as it causes loss of deduplication.

Migration involves moving the collection files onto longer term storage devices. For example, you may want to migrate older collections to cheaper, slower storage.

If you choose to use collection files you can configure the collection criteria, and optionally provide details of how and when to migrate the collection files to secondary storage. See the Administration Console help for details on setting these options.

Note: When you use collections, an unreferenced item may remain in a `.cab` file for some time before it is deleted. Enterprise Vault compacts a `.cab` file and deletes the unreferenced items when the ratio of unreferenced items reaches a fixed level.

Other storage devices have been integrated with Enterprise Vault to enable the migration of data files. Supported devices are listed in the Enterprise Vault *Compatibility Charts* (http://www.veritas.com/docs/000097605).

For instructions on how to configure migration to the supported storage devices, see the migration articles on the Veritas support knowledge base.

Collections on EMC Centera devices

Collections are handled differently on EMC Centera devices, as follows:

- Centera collection clips are used instead of CAB files.

- Savesets are collected as soon as they are archived, and not according to a schedule.

- A collection clip and the savesets that it contains are not deleted until there are no references to any of the savesets in the clip.

To ensure optimal archiving performance when vault store partitions on Centera devices are enabled for collection, an additional index, IX_Collection_Saveset_Partition, can be created for the Saveset table in the associated vault store database. If the index does not exist, Enterprise Vault creates it automatically when the Storage service starts, provided that the following conditions are satisfied:

- At least one Centera vault store partition is open and enabled for collection.

- The number of records in the Saveset table is less than or equal to 1,000,000.

The space required for this index on the SQL Server hosting the relevant vault store database is approximately 27 bytes per row in the Saveset table.

Creating a vault store partition

You can create a vault store partition using the New Partition wizard.

In an environment that uses Enterprise Vault single instance storage, the network connection speeds must be adequate to support sharing. If you intend to use single instance storage in the vault store, run the connectivity test when the New Partition wizard prompts you. The connectivity test helps to determine whether the connection speeds are adequate for sharing.

See "Developing a suitable sharing regime for Enterprise Vault single instance storage" on page 181.

Note: You are recommended not to use disk quota and File Server Resource Manager quotas for vault store partitions.

To create a vault store partition

1   If you created a vault store using the New Vault Store wizard, the New Partition wizard starts automatically. Go to step 6.

2   In the left pane of the Administration Console, expand the Enterprise Vault site hierarchy until **Vault Store Groups** is visible.

3   Expand the **Vault Store Groups** container to show the existing vault store groups.

4   Expand the vault store group that contains the vault store for which you want to create the partition.

5 Right-click the vault store in which you want to create the partition, and then click **New** > **Partition**.

The New Partition wizard starts.

6 The New Partition wizard takes you through the steps to create a partition.

You need to provide the following information:

- The partition name and description.

- Whether the new partition should be created closed, open or ready. There can only be one open partition. If you create an open partition, any existing open partition is closed.

- The type of device on which the partition is to be created. Select the required type of storage device from the drop-down list. The additional information that you need to provide depends on which device type you select. For help with the options, see the Administration Console help for the wizard pages.

- The location on the device for the new partition. The location can be entered as a UNC path or a path that starts with a drive letter. For a network location, enter the full UNC path rather than a mapped network drive path.

Note: Do not specify the location of an existing partition, or a location that includes any folders that are associated with an existing partition. Take particular care to avoid the overlap of partition folders when using network shares or mount points. You may suffer data loss if any folder is associated with more than one partition.

The Storage service does not start if it detects that two partitions share the same path.

Enterprise Vault assumes that the partition root path is empty. Do not use the root path to hold files or folders other than those that Enterprise Vault creates.

The Storage service creates a network share for a partition if you specify the storage type as **NTFS Volume** and you specify a local path such as `H:\...` as the location. The Storage services on remote Enterprise Vault servers use the partition network share when they require access to the data on the partition.

See "Partition network shares for NTFS partitions with local paths" on page 194.

If you specify a UNC path that includes an administrative share, such as `\\server\H$\partitionlocation`, then administrative shares must always

be enabled. If you disable the server's administrative shares, Enterprise Vault is unable to access the partition.

- The storage settings that are used by the storage device. Enterprise Vault uses this information to help optimize data storage. For more details, see the Administration Console help for the wizard pages.
  With the exception of the storage mode, you can change the storage settings later from the Volume tab of the partition's properties.
  If you change the storage settings on the device at a later date, you must update the related storage settings on the **Volume** tab of the partition's properties to reflect the new behavior.

- For partitions on EMC Centera devices, whether to enable device-level sharing.

- Partition rollover criteria if you choose to enable the feature for this partition. Although you can create ready partitions on EMC Centera devices, you cannot enable onward rollover from a Centera-hosted partition.

- Whether to use Security ACLs. This option does not apply to Centera devices. It is usual to create a vault store partition with security ACLs on the folders in the partition. Some optical devices, however, do not allow Enterprise Vault to add the ACLs.
  See "Securing data locations" on page 51.

- How to check whether items have been secured.

- Whether to use file collection software. If you choose to use collection files you can configure the collection criteria, and optionally provide details of how and when to migrate the collection files to secondary storage.

Partition network shares for NTFS partitions with local paths

The Storage service creates a network share for a partition if you specify the storage type as **NTFS Volume** and you specify a local path; for example a path that begins `C:\...` or `H:\...`. The Storage services on remote Enterprise Vault servers use the partition network share when they require access to the data on the partition.

Note: Enterprise Vault does not create a partition network share if you specify the partition's location with a UNC path.

A benefit of using partition network shares is that, each time a Storage service starts, it verifies its local partition network shares. If the verification of a share fails, the Storage service attempts to create a new partition network share.

A partition network share has a UNC path with the following format:

```
\\server\EVPartitionnumber$
```

where *server* is the Enterprise Vault server on which the partition is located, and *number* is a unique hexadecimal number.

The Storage service creates the partition network share regardless of the vault store's sharing level. The Storage service grants access only to the Vault Service account, which has full access rights.

If the Storage service cannot create a partition network share, either for the first time or when verification fails, the Storage service does not start. Enterprise Vault logs an error in the event log with the following description:

```
The verification of a Partition Network Share failed.
```

The most likely cause is that Enterprise Vault cannot access the root path of the partition for one of the following reasons:

- A drive is offline.

- A disk is corrupt.

- The computer's name has changed.

- In a cluster environment, a shared drive was not configured properly.

If you see this error event, use Windows Explorer to check whether you can access the local paths to the local NTFS partitions.

Configuring sharing for a vault store group

To change the sharing levels for the vault stores in a vault store group, you must run the Configure Sharing wizard on the vault store group.

Note: You can rerun the Configure Sharing wizard at any time, but changes you make to the vault store sharing levels do not act retrospectively.

See "Developing a suitable sharing regime for Enterprise Vault single instance storage" on page 181.

To configure sharing for a vault store group

1   In the left pane of the Administration Console, expand the Enterprise Vault site hierarchy until **Vault Store Groups** is visible.

2   Expand the **Vault Store Groups** container to show the existing vault store groups.

3   Right-click the vault store group for which you want to configure sharing, and on the shortcut menu click **Properties**.

4   Click the **Sharing** tab.

The Sharing tab lists the vault stores in the vault store group, and their current sharing levels.

5   Click **Configure Sharing**.

The Configure Sharing wizard starts.

6   In the special case of the Default Upgrade Group, Enterprise Vault helps you to configure a fingerprint database for the group, if one does not exist already.

7   The Configure Sharing wizard takes you through the steps to configure the sharing levels for the vault stores in the vault store group.

If you change one or more vault store sharing levels to **Share within vault store** or **Share within group**, the wizard prompts you to run a connectivity test before the wizard makes any changes. The connectivity test helps to determine whether the network connectivity is sufficient to support the sharing configuration you have selected.

The wizard makes no changes until you click **Finish** on the final page of the wizard.

If the connectivity test shows poor results you may want to do one of the following:

- Click **Back**, modify the vault store sharing levels and rerun the connectivity test.

- Click **Cancel** to discard your changes.

For more information on the connectivity test, see the Administration Console help for the Configure Sharing wizard.

Adding index locations

This chapter includes the following topics:

- About Enterprise Vault index locations

- Creating an Enterprise Vault index location

About Enterprise Vault index locations

Enterprise Vault automatically creates an index for each archive. The size of an index depends on the amount of data that has been indexed and the level of indexing that you choose. Full indexing requires approximately 12% of the space that the original data uses. To store indexes, you must create one or more index locations for Enterprise Vault to use.

See the following article on the Veritas Support website for information on how to configure and administer Enterprise Vault indexing, as well as best practices:

http://www.veritas.com/docs/000064680

Note the following:

- If you ran the Getting Started Wizard, you have already created some index locations. You can create more index locations as necessary.

- Antivirus software can potentially change data, so it is important to exclude the index locations in your virus-checking application.

Creating an Enterprise Vault index location

The local Administrators group must have full access to the folders that you use for index locations and the files in them. Unless your policies dictate otherwise, these files and folders should not be accessible by anyone else.

See "Securing data locations" on page 51.

To create an index location

1   In the left pane of the Administration Console, expand the Enterprise Vault site
    hierarchy until the **Enterprise Vault Servers** container is visible.

2   Expand the **Enterprise Vault Servers** container.

3   Expand the server that runs the Indexing service for which you want to add an
    index location.

4   Click **Services**.

5   In the right pane, right-click the Indexing service and, on the shortcut menu,
    click **Properties**.

6   Click the **Index Locations** tab.

7   Click **Add**. Enter the password to the Vault Service account if you are prompted
    to do so.

8   In the **Choose Folder** dialog, select the folder that you want to use as an index
    location.

    Click **Help** if you need help to select or create the location.

When you create a new index location, Enterprise Vault creates eight new subfolders
in the folder you select. These subfolders are called `index1`, `index2`, and so on.
Enterprise Vault uses these subfolders to store the indexes.

Setting up Index Server groups

This chapter includes the following topics:

About Index Server groups

An Index Server is an Enterprise Vault server that has the Enterprise Vault Indexing service installed. An Index Server can be a member of an Index Server group, or it can be ungrouped.

The Index Servers in an Index Server group do the following:

- Index the vault stores that are associated with the Index Server group.

- Respond to search queries.

An Index Server group allocates new index volumes to different servers in the group. Index volumes that belong to journal archives are allocated to different servers in the group.

By default, Enterprise Vault attempts to allocate mailbox index volumes to the server in the Index Server group that has the Storage service that hosts the mailbox archive. If the mailbox is not hosted on an Index Server that is in the Index Server group then any Index Server in the Index Server group may be used.

- When you place the Storage service and Indexing service on separate servers the communication between these services results in an increase in network traffic.

Note: If the network cannot cope with the extra demands there is no benefit from Index Server groups.

- Index Server groups provide Indexing services for large or distributed Enterprise Vault environments. In a distributed environment, some Enterprise Vault servers may host Storage services, while others host Indexing services.

See the section "About Enterprise Vault indexing" in the *Introduction and Planning* manual.

There is a best practices white paper for Enterprise Vault indexing. See http://www.veritas.com/docs/000002688.

Do I need to create Index Server groups?

Table 25-1 lists various the considerations that determine whether you would benefit from Index Server groups:

Table 25-1   Index Server group considerations

In your Enterprise Vault environment	For details
Do you have more than one Enterprise Vault server?	See "Do you have more than one Enterprise Vault server?" on page 201.
Do you use or plan to use journal archiving or File System Archiving?	See "Do you use or plan to use journal archiving or File System Archiving?" on page 201.
Do you use or plan to use Compliance Accelerator or Discovery Accelerator?	See "Do you use or plan to use Compliance Accelerator or Discovery Accelerator?" on page 202.
If you currently use Enterprise Vault is the distribution of server loads uneven?	See "Is the server loading evenly distributed across existing Enterprise Vault servers?" on page 202.

Table 25-1 Index Server group considerations *(continued)*

In your Enterprise Vault environment	For details
Are there more than approximately 5,000 mailbox archives per Enterprise Vault server?	See "Are there more than approximately 5,000 mailbox archives per Enterprise Vault server?" on page 203.

If you answer "No" to all or most of the questions, it is unlikely that your environment can benefit from Index Server groups.

Do you have more than one Enterprise Vault server?

If you have a single Enterprise Vault server that has acceptable performance there is no benefit from Index Server groups. If you intend to add other servers then you may benefit from Index Server groups.

If you have several Enterprise Vault servers you can group some servers with Indexing services into one or more Index Server groups.

The benefit depends on whether you have some servers that are underused and others that cannot cope with the indexing demand or the archiving demand.

For example, suppose you have three servers, one dedicated to Exchange Journal archives and two dedicated to mailbox archives. In this case it can be beneficial to put all the servers into an Index Server group. The grouping enables you to distribute journal archive index volumes between all three servers. The effect of this distribution is to increase search performance for Discovery Accelerator applications.

Do you use or plan to use journal archiving or File System Archiving?

If you use journal archiving or FSA archiving, it can be beneficial to do either or both of the following:

- Group some servers with Indexing services into Index Server groups to distribute the indexing load.

- Add new servers to an Index Server group that is dedicated to indexing the vault stores that contain the Journal archives and FSA archives.

This configuration would also improve search performance because it distributes the large index volumes between servers.

Do you use or plan to use Compliance Accelerator or Discovery Accelerator?

If you use Compliance Accelerator or Discovery Accelerator, it can be beneficial to do the following:

■ Group some servers with Indexing services into Index Server groups to distribute the search load.

■ Arrange the vault stores so that the archives are split by archive type. For example, use specific vault stores for journal archives. You can then assign a vault store that contains a specific archive type to an Index Server group.

■ Add new servers to an Index Server group that is dedicated to indexing the vault stores that contain those archives that Compliance Accelerator or Discovery Accelerator search.

This configuration distributes large index volumes between separate servers. Search performance is improved because there is now parallel execution of queries across multiple servers.

Is the server loading evenly distributed across existing Enterprise Vault servers?

An Enterprise Vault server can be overloaded because both the Archiving tasks and Indexing tasks and Storage services all share resources. You may have some servers that are underused while others are short of memory and of CPU capacity.

It can be beneficial to do the following:

■ Add new servers to an Index Server group that is dedicated to indexing and searching some or all vault stores.

■ Arrange the vault stores so that archives are split by type. For example, use specific vault stores for journal archives. You can then assign a vault store that contains a specific archive type to an Index Server group.

This change has the following advantages:

■ Indexing CPU and memory requirements are shared between Index Servers.

■ The indexing load is removed from the servers that run the Archiving tasks and Storage tasks.

■ The performance of indexing and searching are improved because there are dedicated resources on separate servers.

Are there more than approximately 5,000 mailbox archives per Enterprise Vault server?

Indexing and searching may overload an Enterprise Vault server that has a large number of mailbox archives.

It can be beneficial to add new servers to an Index Server group that is dedicated to indexing those vault stores that contain mailbox archives.

This configuration distributes those index volumes that are associated with new mailbox archives between the servers in the Index Server group. This distribution enables separate servers to process concurrent queries of many archives.

An Enterprise Vault server can be overloaded by searching too many index volumes. If users find that many searches timeout, an index group may improve the search times. If some other problem is the cause of the unsatisfactory search performance, Index Server groups are unlikely to improve performance. For example, Index Server groups cannot improve performance if IIS is overloaded.

You can add new servers to an Index Server group that is dedicated to indexing and searching those vault stores that contain mailbox archives.

This change has the following advantages:

- Improved indexing performance because the index volumes are distributed between several servers.

- Improved search performance because concurrent queries to many archives are distributed between several servers.

Creating an Index Server group

Do not create the first Index Server group before you are sure that Index Server groups will benefit your Enterprise Vault site.

See "About Index Server groups" on page 199.

See "Do I need to create Index Server groups?" on page 200.

To create an Index Server group

1   In the Administration Console expand the Enterprise Vault container.

2   Expand the **Directory** container.

3   Expand the Enterprise Vault site.

4   Expand the **Indexing** container.

5   Right-click **Index Server Groups** and on the shortcut menu click **New** and then **Index Server Group**.

The **New Index Server Group** wizard starts. If there is only one Index Server in the Site there is a message that explains that there may be no benefit from an Index Server group. Click **Continue** if you are sure that you want to create an Index Server group.

6   The wizard introduction page refers you to documentation for information about Index Server groups.

See the section "About Index Server groups" in the *Introduction and Planning* manual.

Click **Next** to go the **Name and Description** page.

7   Enter a **Name** for the Index Server group and optionally a **Description**. You can change the **Name** and **Description** at any time.

Click **Next**

8   Select the Index Servers that you want to add to the new Index Server group. There is no requirement for you to add the Index Servers now. You can add Index Servers later, as required.

Click **Next**.

9   If you have chosen to add Index Servers to the new Index Server group you can now choose to associate vault stores with the new Index Server group.

When you add an Index Server to an Index Server group, its associated vault stores are not included automatically. Enterprise Vault does not index those vault stores unless you associate them with an Index Server group. If you want those vault stores to be indexed by the new Index Server group, select **All Vault Stores that are currently indexed by the servers you have chosen to add to the new index server**.

Click **Next**.

10   Click **Next**. The page shows the details that you have entered.

11   Click **Create Index Server Group**. The wizard creates the new Index Server group and shows a summary page.

12   Click **Close** to close the wizard.

If you did not add an Index Server to the new Index Server group you can edit the properties of the Index Server group to do so.

See "Adding an Index Server to an Index Server group" on page 205.

Adding an Index Server to an Index Server group

You can add an Index Server to an Index Server group at any time. You cannot remove the Index Server from the Index Server group once it has indexed data as a member of the Index Server group.

Note: When you add an Index Server to an Index Server group, its associated vault stores are not included automatically. Use the Vault Stores tab in an Index Server group's properties to associate those vault stores with that Index Server group.

To add an Index Server to an Index Server group

1   In the Administration Console expand the Enterprise Vault container.

2   Expand the **Directory** container.

3   Expand the Enterprise Vault site.

4   Expand the **Indexing** container.

5   Expand **Index Server Groups**.

6   Right-click the group to which you want to add an Index Server and click **Properties**.

7   In the Index Server group properties, click the **Index Servers** tab. The list shows the Index Servers that are already in the group.

8   Click **Add**. The list shows the Index Servers that can be added to an Index Server group.

9   Click the Index Server that you want to add to the Index Server group.

    You can run a connectivity test to check network performance. The test helps you to determine whether the network provides acceptable performance within the Index Server group. The test determines the response time for ping requests between the Index Server and a vault store that is associated with the Index Server group.

    To run the connectivity test:

    ■   Click **Connectivity Test**. The dialog expands to show the **Connectivity Test** section.

    ■   Click **Run Test**.

The test may take a few seconds to run. The list shows a summary of the results. To see the complete details, click **Report**.

10 When you have selected the Index Servers that you want to add, click **OK**. A prompt asks whether you are sure that you want to continue. You cannot remove the Index Server from the Index Server group once it has indexed data as a member of the Index Server group. Click **Yes** to continue.

You can also remove an Index Server from an Index Server group.

See

Removing an Index Server from an Index Server group

You can remove an Index Server from an Index Server group subject to the following limitations:

- You cannot remove an Index Server from an Index Server group once it has indexed data as a member of the Index Server group

- You cannot remove an Index Server that is associated with an incomplete indexing task.

To remove an Index Server from an Index Server group

1 In the Administration Console expand the Enterprise Vault container.

2 Expand the **Directory** container.

3 Expand the Enterprise Vault site.

4 Expand the **Indexing** container.

5 Expand **Index Server Groups**.

6 Right-click the group from which you want to remove an Index Server and click **Properties**.

7 In the Index Server group properties, click the **Index Servers** tab. The list shows the Index Servers that are already in the group.

8 Click the Index Server that you want to remove from the Index Server group.

9 Click **Remove**.

In response to the confirmation prompt, click **Yes**.

Assigning a vault store to an Index Server group

When you add an Index Server to an Index Server group, its associated vault stores are not included automatically. Enterprise Vault does not index those vault stores until you assign them to an Index Server or Index Server group.

To add a vault store to an Index Server group

1   In the Administration Console expand the Enterprise Vault container.

2   Expand the **Directory** container.

3   Expand the Enterprise Vault site.

4   Expand the **Indexing** container.

5   Expand **Index Server Groups**.

6   Right-click the group to which you want to add an Index Server and click **Properties**.

7   In the Index Server group properties, click the **Vault Stores** tab. The list shows the vault stores that are already assigned to the Index Server group.

8   Click **Add**. The list shows the vault stores that can be added to an Index Server group as follows:

   ■   Vault stores that Enterprise Vault does not index. These are likely to be vault stores that were associated with an Index Server that has been added to an Index Server group.

   ■   Vault stores that are currently indexed by an Index Server that is not in an Index Server group.

9   Select the vault stores that you to associate with the Index Server group.

10 You can run a connectivity test to check network performance. The test helps you to determine whether the network provides acceptable performance within the Index Server group. The test determines the response time for ping requests between a vault store and an Index Server that is in the Index Server group.

   To run the connectivity test:

   ■   Click **Connectivity Test**. The dialog expands to show the **Connectivity Test** section.

   ■   Click **Run Test**.
       The test may take a few seconds to run. The list shows a summary of the results. To see the complete details, click **Report**.

11 When you have selected the Index Servers that you want to add, click **OK**

You can also unassign a vault store from an Index Server group.

Unassigning a vault store from an Index Server group

You can unassign a vault store from an Index Server group subject to the following limitations:

■ You cannot unassign a vault store from Index Server group once data in the vault store has been indexed by a member of the Index Server group

■ You cannot unassign a vault store that is associated with an incomplete indexing task.

To unassign a vault store from an Index Server group

1 In the Administration Console expand the Enterprise Vault container.

2 Expand the **Directory** container.

3 Expand the Enterprise Vault site.

4 Expand the **Indexing** container.

5 Expand **Index Server Groups**.

6 Right-click the group to which you want to add an Index Server and click **Properties**.

7 In the Index Server group properties, click the **Vault Stores** tab. The list shows the vault stores that are assigned to the Index Server group.

8 Click the vault store that you want to unassign from the Index Server group.

9 Click **Remove**.

10 Click **Yes**.

Assigning a vault store to a different indexer

You can reassign a vault store to a different indexer as follows:

■ You can reassign to an Index Server group a vault store that is not already assigned to an Index Server group.

■ You can reassign a vault store from one Index Server group to another Index Server group provided that the current Index Server group has not indexed anything in that vault store.

To assign a vault store to a different indexer

1   In the Administration Console expand the Enterprise Vault container.

2   Expand the **Directory** container.

3   Expand the Enterprise Vault site.

4   Expand the **Vault Store Groups** container.

5   Expand the vault store group that contains the vault store that you want to modify.

6   Right-click the vault store that you want to assign to a different indexer and click **Properties**.

7   In the vault store properties click the **Indexers** tab.

The Indexer section shows whether the vault store is currently indexed by a single Index Server, by an Index Server group, or is not indexed.

8   Click **Change**.

The list shows the Index Server groups to which you can assign the vault store.

9   Click the Index Server group to which you want to assign the vault store.

10 You can run a connectivity test to check network performance. The test helps you to determine whether the network provides acceptable performance within the Index Server group. The test determines the response time for ping requests between the vault store and an Index Server that is in the Index Server group.

To run the connectivity test:

- Click **Connectivity Test**. The dialog expands to show the **Connectivity Test** section.

- Click **Run Test**.
  The test may take a few seconds to run. The list shows a summary of the results. To see the complete details, click **Report**.

11 When you have selected the new Index Server group, click **OK**.

12 Click **OK** to close the vault store properties.

You can also unassign a vault store from an Index Server group.

Reviewing the default settings for the site

This chapter includes the following topics:

- Reviewing the default settings for the Enterprise Vault site

Reviewing the default settings for the Enterprise Vault site

Check the default settings that are configured in the Enterprise Vault site properties.

Site properties include the following settings. Note that you can override some of these at a lower level. For example, you can override the site archiving schedule for a particular task by setting the schedule in the task properties.

Table 26-1   Site properties

Tab	Settings
General	■ The Vault site alias and description. ■ The protocol and port to use for the Web Access application. ■ A system message for users of the Web Access application, if required. ■ The following site properties settings apply only to Exchange Server archiving: PST holding area details. ■ A note for administrators, if required.

Table 26-1 Site properties *(continued)*

Tab	Settings
Archive Settings	■ The default retention category. ■ Whether the retention category of moved items is always updated, or updated only when either the record type changes, or the item expiry date is later or unchanged. ■ Whether users can delete items from their archives. ■ Whether the items that users have deleted can be recovered. ■ The length of time for which the deleted items remain available for recovery.
Storage Expiry	■ The schedule to run storage expiry to delete from archives any items that are older than the retention period assigned. ■ Whether expiry is based on an item's modified date or its archived date.
Site Schedule	■ The schedule to run automatic, background archiving.
Archive Usage Limit	■ If required, you can set limits on the size of archives.
Indexing	■ Indexing level: brief or full. ■ Email content that should not be indexed, such as disclaimers. ■ How long indexing subtasks are retained before they are deleted.
Advanced	■ Advanced settings that you can use to tune Enterprise Vault indexing within the Enterprise Vault site. **Note:** Do not change the Indexing settings unless your technical support provider advises you to do so.
Monitoring	■ Performance counters for monitoring Enterprise Vault.

To review the default settings for the Enterprise Vault site

1 In the Administration Console, expand the contents of the left pane until the Enterprise Vault site is visible.

2 Right-click the Enterprise Vault site and then, on the shortcut menu, click **Properties**.

   Alternatively, select the site and click the **Review Site Properties** button on the toolbar.

3 Click **Help** on any of the site properties tabs for further information.

Setting the archiving schedule for the Enterprise Vault site

Each archiving task or service runs according to a schedule that you define. The possible schedules for each task are as follows:

- The default schedule, which is the one that you set in the site properties. This schedule applies to all archiving tasks in your Enterprise Vault site.

- The task's own schedule, which is the one that you set by editing its properties. You edit this schedule if you want to provide specific settings for that task, overriding those in the site properties.

To set the archiving schedule for the Enterprise Vault site

1   In the left pane of the Administration Console, expand the Enterprise Vault site hierarchy until the name of the site is visible.

2   Right-click the site name and then click **Properties**.

3   Click the **Site Schedule** tab.

4   Modify the schedule as required. The online Help gives detailed instructions on using the **Site Schedule** tab.

    The blocks of time are colored blue when the schedule is on and white when it is off.

About the Web Access application settings

In the Administration Console, on the General page of site properties, the protocol and port for accessing the Enterprise Vault Web Access application can be set.

The default URL for the Web Access application is set to /EnterpriseVault, which is the name of the virtual directory in IIS for the Web Access application. When a client contacts the Web Access application to access an archive, Enterprise Vault creates the full URL dynamically.

In a default configuration, the Web Access application is accessed using HTTP over port 80. The full URL for the Web Access application is then:

http://*FQDN*/EnterpriseVault

where *FQDN* is the fully qualified domain name of the Enterprise Vault server that hosts the Storage service for the user's archive.

If your IIS computer requires a different port or secured connections, then you can set the required values using the options **Use TCP Port** or **Use HTTPS on SSL Port**.

Note: If you change the protocol or port that is used to access the Web Access application after items have been archived, existing shortcuts will no longer work.

See "Customizing security for the Enterprise Vault Web Access components" on page 118.

Setting up Enterprise Vault Search

This chapter includes the following topics:

About Enterprise Vault Search

Enterprise Vault Search provides Enterprise Vault client users with browse and search access to their archives.

The Mobile edition of Enterprise Vault Search lets users access their archives through the web browsers on their Android, iOS, or Windows Mobile smartphones.

Table 27-1   Setup steps for Enterprise Vault Search

Step	Action	Description
Step 1	Define one or more search policies to specify the range of Enterprise Vault Search facilities that you want to make available to users.	See "Defining search policies for Enterprise Vault Search" on page 215.
Step 2	Set up one or more search provisioning groups to identify the targets (users and user groups) to whom you want to assign a search policy.	See "Setting up provisioning groups for Enterprise Vault Search" on page 217.
Step 3	Create and configure one or more Client Access Provisioning tasks to apply the required search policies to the targets of the provisioning groups.	See "Creating and configuring Client Access Provisioning tasks for Enterprise Vault Search" on page 219.
Step 4	Configure user browsers for Enterprise Vault Search.	See "Configuring user browsers for Enterprise Vault Search" on page 220.
Step 5	Setting up Enterprise Vault Search Mobile edition.	See "Setting up Enterprise Vault Search Mobile edition" on page 222.

Before you proceed, it is important to check that your Enterprise Vault servers meet the requirements for Enterprise Vault Search.

See "Server requirements for Enterprise Vault Search" on page 101.

Defining search policies for Enterprise Vault Search

A search policy defines the range of Enterprise Vault Search facilities that you want to make available to users. With a search policy, you can choose to let Enterprise Vault Search users do the following:

- Show the reading pane. This pane displays a preview of the currently selected item in Enterprise Vault Search. For performance reasons, you may want to hide the reading pane to stop recalls from slow storage media, such as tape or optical disks.

- Export the items that are listed in Enterprise Vault Search to an `.nsf`, `.pst`, or `.zip` file, depending on the archive type.
  Some export formats are appropriate for use with certain types of items only. For example, it is not possible to export Outlook messages to a `.nsf` file, or

Notes messages to a `.pst` file. A user who chooses to export both Outlook and Notes messages to a single file can export them to a `.zip` file only.

■ Copy and move archived items out of an archive, within an archive, and from one archive to another. Choosing to allow these actions also allows users to create, rename, move, and delete folders in their archives.

■ Delete archived items. Note that, even if you define a search policy to grant delete permissions, users can only delete items if you have configured the Enterprise Vault site appropriately. In the Administration Console, open the **Site Properties** dialog box for the Enterprise Vault site and then, on the **Archive Settings** tab, ensure that **Users can delete items from their archives** is checked.

■ When using the advanced search facilities in Enterprise Vault Search, choose from extra options on the **Select search property** dropdown list. These extra properties make it easier to build search queries for the items that the Enterprise Vault records management and classification features have tagged.

Installing Enterprise Vault creates a default search policy automatically. You can modify the properties of this default policy and define custom search policies. Then you can assign each policy to a different search provisioning group.

To view and modify the properties of the default search policy

1 In the left pane of the Administration Console, expand your Enterprise Vault site.

2 Expand the **Policies** container.

3 Click the **Search** container.

4 In the right pane, right-click **Default Search Policy** and then click **Properties**.

You can change the settings on the **Features** and **Advanced Search** tabs, but you cannot change the settings on the other tabs.

To define a new search policy

1 In the left pane of the Administration Console, expand your Enterprise Vault site.

2 Expand the **Policies** container.

3 Right-click the **Search** container, and then click **New** > **Policy**.

The **New Search Policy** wizard appears.

4 Follow the on-screen instructions. The wizard prompts you to specify the following:

■ The name of the policy and an optional description of it.

- The Enterprise Vault Search facilities that you want to make available to users.

Setting up provisioning groups for Enterprise Vault Search

A search provisioning group identifies the users and user groups to whom you want to assign a search policy for Enterprise Vault Search. After you install Enterprise Vault, a default search provisioning group is available with which you can assign the default search policy to all users. If you want to assign a custom search policy to selected users or groups, you must set up a custom provisioning group. The default provisioning group continues to target those users whom you do not assign to a custom provisioning group.

You can set up any number of custom provisioning groups for different sets of targets. However, each provisioning group can target the users in one Active Directory domain or Domino domain, so you require at least as many groups as you have domains.

To view the properties of the default search provisioning group

1   In the left pane of the Administration Console, expand your Enterprise Vault site.

2   Expand the **Client Access** container and then expand the **Search** container.

3   Click the **Provisioning Groups** container.

4   In the right pane, right-click **Default Search Provisioning Group** and then click **Properties**.

    You cannot amend any of the properties.

To set up a custom search provisioning group

1   In the left pane of the Administration Console, expand your Enterprise Vault site.

2   Expand the **Client Access** container and then expand the **Search** container.

3   Right-click the **Provisioning Groups** container, and then click **New** > **Active Directory Provisioning Group** or **New** > **Domino Provisioning Group**.

    The **New Search Provisioning Group** wizard appears.

4   Complete the fields and then click **Create Provisioning Group**. The wizard prompts you to specify the following:

    - The name of the provisioning group.

- The search policy to assign.

- The domain to which the provisioning group applies. You can enter the details of a new domain, if necessary.
  For an Active Directory domain, you must choose a trusted domain in your environment and optionally specify the required Global Catalog server. For a Domino domain, you must specify the name and password for the ID file that Enterprise Vault will use to access the domain, and the fully-distinguished name of any Domino server in the domain.

- The targets (individual users and user groups) of the provisioning group.

- The Enterprise Vault server that is to host the Client Access Provisioning task for this provisioning group. This task applies the required search policy to the targets of the provisioning group. You can host the task on any Enterprise Vault server in your site. However, if the task is to provision a Domino domain then you must ensure that Notes is installed on the server. Enterprise Vault creates the task automatically if one does not already exist for the nominated domain.

The provisioning group takes effect when the Client Access Provisioning task has run.

Changing the order in which Enterprise Vault processes the search provisioning groups

When you set up a search provisioning group, it automatically has the highest ranking in its domain. In consequence, Enterprise Vault processes the new provisioning group before it processes any other groups in the domain. You can change the order in which Enterprise Vault processes the provisioning groups, if necessary.

To change the order in which Enterprise Vault processes the search provisioning groups

1   In the left pane of the Administration Console, expand your Enterprise Vault site.

2   Expand the **Client Access** container and then expand the **Search** container.

3   Click the **Provisioning Groups** container.

4   Right-click a blank area of the right pane, and then click **Properties**.

The **Provisioning Groups Properties** dialog box appears.

5   In the **Provisioning Groups** list, click a group and then click **Move Up** or **Move Down** to raise or lower its priority.

If users are the targets of multiple provisioning groups, Enterprise Vault processes them as members of the topmost group only. Thereafter, Enterprise Vault ignores these users when it processes the lower priority provisioning groups.

Creating and configuring Client Access Provisioning tasks for Enterprise Vault Search

You require one Client Access Provisioning task for each Active Directory domain or Domino domain in which you want to apply search policies for Enterprise Vault Search. At specified times each day, the task applies the required search policy to users who are the targets of a provisioning group with which you have associated the task. You can host the task on any Enterprise Vault server in your site. However, if the task is to provision a Domino domain then you must ensure that Notes is installed on the server.

Besides processing the search provisioning groups for a domain, a Client Access Provisioning task also processes the domain's IMAP (Exchange Mailbox or Internet Mail) provisioning groups. These two types of provisioning group differ slightly in how the task processes them, in the event that the task is stopped before it has finished assigning the required policies to the target users.

■   For a search provisioning group, the task does not assign the search policy to any users. When the task next runs, it starts from the beginning and assigns the policy to all users.

■   For an IMAP provisioning group, those users to whom the task assigned a policy before it stopped retain that policy; the other users are not provisioned. However, when the task next runs, it starts from the beginning and reassigns the policy to all users.

If a suitable Client Access Provisioning task does not exist when you set up a search provisioning group, Enterprise Vault automatically creates one. However, you can manually create and configure this task at any time.

To create and configure a Client Access Provisioning task for Enterprise Vault Search

1   In the left pane of the Administration Console, find and then expand the **Enterprise Vault Servers** container.

2   Expand the container for the server to which you want to add the Client Access Provisioning task.

3   Right-click the **Tasks** container, and then click **New** > **Client Access Provisioning Task**.

    The **New Client Access Provisioning Task** dialog box appears.

4   Complete the fields and then click **OK**. The dialog box prompts you to specify the following:

    ■   The domain with which to associate the task.

    ■   The name of the task.

    ■   Whether to start the task now. If you want to configure the task before it starts, turn off this option and follow the instructions in step 5.
        The settings that you can configure include the times at which the task runs each day and the level of reporting that it undertakes for each provisioning run.

5   To configure the task, right-click it in the right pane, and then click **Properties**.

    The online Help provides detailed information on each field in the properties dialog box.

Configuring user browsers for Enterprise Vault Search

Client users require an HTML5-compatible web browser to benefit from all the new features in Enterprise Vault Search. Older browsers are supported, but the client experience may be compromised.

For the latest information on supported web browsers, see the Enterprise Vault *Compatibility Charts* at http://www.veritas.com/docs/000097605.

Enterprise Vault Search uses the browser's language for the default time and date format in advanced search, the reading pane, and search results. If the browser is set to a language that is not supported, Enterprise Vault Search defaults to English (US). You may want to use a Group Policy Object (GPO) to set the Internet Explorer language for users. Note that users can change their Enterprise Vault Search language in their Enterprise Vault Search regional preferences.

Most users should not experience any problems when they access Enterprise Vault Search. However, they must set the following in their browsers to use Enterprise Vault Search:

- Allow cookies and local storage.

- Enable JavaScript.

- Disable private browsing or the settings that prevent their browsers from storing data about their browsing.

- Disable script debugging.

- If an option to not save encrypted pages to disk is available, disable it.

You can also minimize potential problems by configuring their web browsers to treat Enterprise Vault Search as a trusted site. How you do this varies from one browser to another, but the procedure for Internet Explorer is as described below.

If you use Active Directory, you can employ a group policy to apply the zone change to all the domain users. To do this, you must edit the Internet Explorer Maintenance settings within the policy.

To configure Internet Explorer to trust Enterprise Vault Search

1   On the client computer, open Internet Explorer.

2   On the **Tools** menu, click **Internet Options**.

3   Click the **Security** tab.

4   Click **Trusted sites**, and then click **Sites**.

5   Enter the fully-qualified domain name of the server on which you installed Enterprise Vault Search, and then click **Add**. For example, you might type **vault.company.com**.

6   Close the **Trusted sites** dialog box, and then close the **Internet Options** dialog box.

Configuring Enterprise Vault Search for use in Forefront TMG and similar environments

By default, Enterprise Vault Search implements security best practices for all supported browsers. In some environments, these restrictions can affect the functionality of Enterprise Vault Search. For example, if you implement forms-based authentication through Forefront Threat Management Gateway (TMG), the reading pane of Enterprise Vault Search may contain the logon screen rather than a preview of the selected item.

This issue arises because Enterprise Vault Search uses an attribute to enforce the Restricted Sites zone settings in the reading pane. In fact, this mechanism is needed for Internet Explorer 9 and earlier only; version 10 and later uses a different security mechanism, which Enterprise Vault Search also implements. However, because version 10 and later still respects the older security mechanism, the reading pane does not work in these later versions either. So, if your users do not run Internet Explorer 9 and earlier, you can configure Enterprise Vault to not use the attribute to enforce the Restricted Sites zone settings. The reading pane then works without reducing security.

To configure Enterprise Vault Search for use in Forefront TMG and similar environments

1   Locate the following file on the Enterprise Vault server:

```
C:\Program Files (x86)\Enterprise
Vault\EVSearch\EVSearchClient\Web.config
```

2   Open the file in a text editor such as Windows Notepad.

3   Find the following line, and change the value from 1 to 0:

```
<add key="UseRestrictedSecurity" value="1"/>
```

A value of 1 enforces the security restrictions, whereas 0 relaxes them.

4   Save and close the file.

Setting up Enterprise Vault Search Mobile edition

Designed for use on Android, iOS, and Windows Mobile devices, Enterprise Vault Search Mobile edition enables users to access their archives through the web browsers on their smartphones. Those users for whom you provision Enterprise Vault Search on the desktop and tablet can also run the Mobile edition on their smartphones.

Enterprise Vault Search Mobile edition is a browser-based application that you deploy for intranet or Internet access using Microsoft Internet Information Services (IIS).

Caution: You can install the required components on the Enterprise Vault server. However, if you want to give your users Internet access to Enterprise Vault Search without exposing your Enterprise Vault server to unnecessary security risks, it is advisable to install the components on a proxy server.

Carrying out preinstallation tasks for Enterprise Vault Search Mobile edition

Before installing Enterprise Vault Search Mobile edition, you must perform the following tasks:

- If you want to install Enterprise Vault Search Mobile edition on a proxy server, ensure that the server meets the minimum requirements.
  See "Requirements for installing Enterprise Vault Search Mobile edition on a proxy server" on page 102.

- Obtain a digital certificate from a certification authority for setting up HTTPS.

- In a configuration providing direct access to the Enterprise Vault Search web server from the Internet, do the following:

  - Verify that the firewall or firewalls are configured to allow HTTPS access to the server on which you plan to install Enterprise Vault Search Mobile edition.

  - Configure any reverse proxy server that is installed in the DMZ.

  - Ensure that the browsers of end-users are configured to allow cookies and local storage, enable JavaScript, and disable private browsing.

Installing Enterprise Vault Search Mobile edition

Whether you want to install the required components for Enterprise Vault Search Mobile edition on the Enterprise Vault server or on a proxy server, follow the steps below.

To install Enterprise Vault Search Mobile edition

1 On the server where you want to install Enterprise Vault Search Mobile edition, log in as the Vault Service account.

2 Load the Enterprise Vault installation media.

3 Do one of the following:

- If an AutoPlay dialog box appears, click **Run Setup.exe**.

- If AutoPlay is not enabled, use Windows Explorer to open the root folder of the installation media and then double-click the file Setup.exe.

4 In the left pane of the Veritas Enterprise Vault Install Launcher, click **Enterprise Vault**.

5 Click **Server Installation**.

6 Choose the required installation option.

To install Enterprise Vault Search Mobile edition on a proxy server, choose **Installation on an additional server**.

7 Follow the instructions in the Enterprise Vault installation wizard.

When the wizard prompts you to select the features that you want to install, do one of the following:

- For installation on a proxy server, uncheck all the options except for **Search Access Components**.
  When you click **Next**, the wizard requests the Vault Site alias. This alias is the DNS alias for the Enterprise Vault site.

- For installation on an Enterprise Vault server, choose all the required components.
  If you choose to install the Enterprise Vault services, or you have previously installed them on this server, then you cannot uncheck the **Search Access Components** option. The components will be automatically installed.

8 Follow the on-screen instructions to complete the remaining steps in the installation wizard.

9 Ensure the security of transmitted data by configuring the Enterprise Vault Search website for HTTPS.

The Enterprise Vault Search website is configured in the Default Web Site in IIS. To use HTTPS, you must first configure the Default Web Site in IIS for HTTPS, and install a valid SSL certificate. See the IIS documentation for instructions.

Configuring the maximum number of permitted login attempts to Enterprise Vault Search Mobile edition

By default, users who make five unsuccessful attempts to log in to Enterprise Vault Search Mobile edition are barred for 24 hours from making further login attempts from the same device. You can configure the maximum number of login attempts that you want to permit and the number of hours for which barred users are locked out.

To configure the maximum number of permitted login attempts

1 Locate the following file on the Enterprise Vault server:

```
C:\Program Files (x86)\Enterprise
Vault\EVSearch\EVSearchClient\Web.config
```

2 Open the file in a text editor such as Windows Notepad.

3 Find the following lines and change the values to the required ones.

```
<add key="EVSMobileMaxFailedAttemptsAllowed" value="5" />
<add key="EVSMobileLoginRestrictedTimeoutInHours" value="24" />
```

4 Save and close the file.

Verifying the installation of Enterprise Vault Search Mobile edition

Before you make Enterprise Vault Search Mobile edition available to users, follow the steps below to verify the installation.

To verify the installation of Enterprise Vault Search Mobile edition

1 Open a web browser on a smartphone that has Internet access.

2 In the **Address** field, enter the Mobile Search URL as follows:

https://*server*/enterprisevault/search

Where *server* is the name or IP address of the server on which you installed the search components.

3 Click **Go** or press **Enter** to display the Sign In page.

4 Enter the details of a user who has access to at least one archive.

5 Click **Sign In**.

If your authentication is valid, you see the home page of Enterprise Vault Search.

6 Perform a search to verify that Enterprise Vault Search can return search results.

7 Click a message in the search results and verify that you can see its contents.

Managing metadata stores

This chapter includes the following topics:

- About metadata stores

- About metadata store PowerShell cmdlets

- About fast browsing and metadata store indexes

About metadata stores

A metadata store contains various index attributes that are extracted from an Enterprise Vault archive. The metadata store provides fast access to index metadata for various Enterprise Vault client applications. Enterprise Vault creates metadata stores automatically as required.

The metadata store for an archive is kept in the associated Vault Store database. The metadata store increases the size of this database. For sizing information, see the Enterprise Vault *SQL Best Practices Guide* at the following location:

http://www.veritas.com/docs/000021697

In the Administration Console, the **Archive Settings** tab of **Site Properties** enables you to control which archive types are automatically enabled for fast browsing. You can also enable fast browsing for existing archives. Enterprise Vault always creates metadata stores for archives that are accessed using IMAP. See the *Setting up IMAP* guide.

Enterprise Vault can create metadata stores for archives to provide faster browsing for Enterprise Vault Search. When you enable users for Enterprise Vault Search, Enterprise Vault only creates the associated metadata stores after those users have used Search.

See "About Enterprise Vault Search" on page 214.

If you want to create the metadata stores for some users before they use Enterprise Vault search, you can use the `New-EVMDSBuildTask` PowerShell cmdlet.

About metadata store PowerShell cmdlets

Enterprise Vault provides the following PowerShell cmdlets that help you to manage archive metadata stores.

- `New-EVMDSBuildTask`. This cmdlet creates an indexing task that builds or rebuilds a metadata store for an archive. The cmdlet is most likely to be useful if you want to create the metadata stores for some users before they use Enterprise Vault Search.

  This cmdlet automatically enables the archive for fast browsing so you do not need to set fast browsing in the Administration Console.

  You can import a CSV file to specify the archives that you want to process. See the Help for the `New-EVMDSBuildTask` cmdlet.

  You can also pipe the output from `Get-EVMDSStatus` to `New-EVMDSBuildTask` to process multiple archives. For an example, see the Help for the `New-EVMDSBuildTask` cmdlet.

- `Get-EVMDSStatus`. This cmdlet gets the current status of the metadata store for an archive. You can also determine the number of items that are missing from an archive's metadata store.

  The status is one of the following: Disabled, Build Pending, Building, Ready, Build Failed.

  You can import a CSV file to specify the archives for which you want the status. For an example, see the Help for `Get-EVMDSStatus` cmdlet.

About fast browsing and metadata store indexes

When an archive is enabled for fast browsing, Enterprise Vault creates a metadata store for that archive. The metadata store is an optimized index in that archive's vault store database. Enterprise Vault Search uses this index to provide a responsive view of the archive contents when a user is browsing the archive.

Enterprise Vault Search works without the metadata store but is more responsive when the store is present.

The metadata store for an archive is created by an **EVMDSBuildTask** task. You use the **Monitor Indexing Tasks** option in the Administration Console to monitor and manage EVMDSBuildTask tasks. You can filter the task view by "Metadata Store" to see just the metadata store tasks.

Section **5**

Clustering Enterprise Vault with VCS

- Chapter 29. Introducing clustering with VCS
- Chapter 30. Installing and configuring Storage Foundation HA for Windows
- Chapter 31. Configuring the VCS service group for Enterprise Vault
- Chapter 32. Running the Enterprise Vault Configuration wizard
- Chapter 33. Implementing an SFW HA-VVR disaster recovery solution with Enterprise Vault
- Chapter 34. Troubleshooting clustering with VCS

Introducing clustering with VCS

This chapter includes the following topics:

- Supported VCS configurations and software

- About Enterprise Vault and the VCS GenericService agent

- Typical Enterprise Vault configuration in a VCS cluster

- Order in which to install and configure the components in a VCS environment

Supported VCS configurations and software

Note: This documentation uses the terms *VCS* and *Storage Foundation HA for Windows (SFW HA)* throughout. However, in version 7.0 of the cluster software, these terms became *Veritas InfoScale Availability* and *Veritas InfoScale Enterprise* respectively.

Both active/passive and N+1 configurations are supported, but active/active configurations are not.

In an active/passive configuration, a dedicated spare server is available for each Enterprise Vault server, ready and waiting for the primary server to go down. In an N+1 configuration, there is a computer for each Enterprise Vault server and then one or more spare servers waiting for any of the active servers to fail over.

The following software must be installed:

- A supported version of VCS

- Enterprise Vault

- A supported version of Windows Server

For supported versions of software, see the Enterprise Vault *Compatibility Charts*, at http://www.veritas.com/docs/000097605.

Neither Compliance Accelerator nor Discovery Accelerator must be installed on any server in the planned cluster. These products are not supported within a cluster. However, an unclustered Compliance Accelerator or Discovery Accelerator can reference a clustered Enterprise Vault virtual server.

About Enterprise Vault and the VCS GenericService agent

The VCS GenericService agent brings online the following Enterprise Vault services, monitors their status, and takes them offline:

- Admin service

- Directory service

- Indexing service

- Shopping service

- Storage service

- Task Controller service

- SMTP service (only if the Enterprise Vault SMTP Archiving components are installed and configured on the Enterprise Vault server)

See the *Cluster Server Bundled Agents Reference Guide* for detailed information on the GenericService agent, including the resource type definitions, attribute definitions, and sample configurations.

The GenericService agent detects an application failure if a configured service is not running. When this happens, the Enterprise Vault service group is failed over to the next available system in the service group's system list, and the services are started on the new system. This ensures continuous availability for the data that Enterprise Vault is managing and archiving.

Typical Enterprise Vault configuration in a VCS cluster

Figure 29-1 illustrates a typical configuration.

Figure 29-1   Active/passive failover configuration
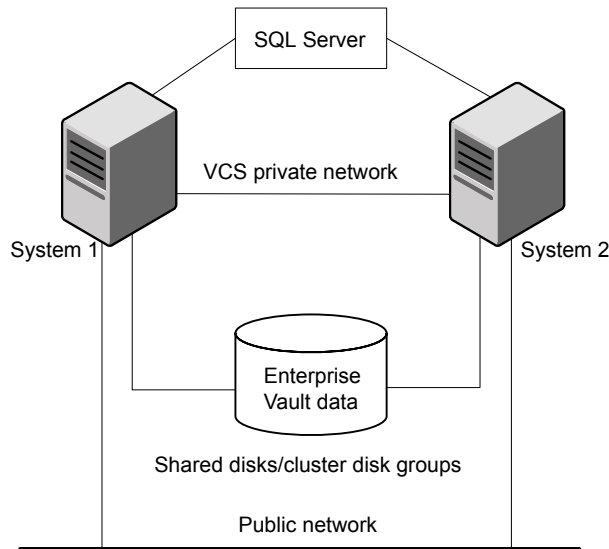
Here, the volumes for the Enterprise Vault services data are configured in a cluster disk group on shared storage. The Enterprise Vault virtual server is configured on the active node (System 1). If System 1 fails, System 2 becomes the active node, and the Enterprise Vault virtual server comes online on System 2.

Order in which to install and configure the components in a VCS environment

The order in which you install and configure the various components in a VCS environment is important.

To install and configure the components in a VCS environment

1 On each of the cluster nodes, install the Enterprise Vault server components and all the required VCS components.

   If you want to include the Enterprise Vault SMTP service as a generic service, then you must install the Enterprise Vault server components and the Enterprise Vault SMTP Archiving components on each of the cluster nodes.

2 Complete the installation and configuration of Storage Foundation HA for Windows.

   As part of the installation process, take care to install the Enterprise Vault Cluster Setup wizard.

3 Configure the disk groups and volumes.

4 Run the Enterprise Vault Cluster Setup wizard to configure the Enterprise Vault service group.

5 Test that the nodes in the cluster fail over correctly.

6 Run the Enterprise Vault Configuration wizard to configure the primary Enterprise Vault cluster node.

7 Optionally, run the Enterprise Vault Getting Started wizard to set up Enterprise Vault.

8 Configure the failover Enterprise Vault cluster nodes.

9 Test that the nodes in the cluster still fail over correctly.

Installing and configuring Storage Foundation HA for Windows

This chapter includes the following topics:

- Installing and configuring Storage Foundation HA for Windows with Enterprise Vault

- Managing disk groups and volumes in a Storage Foundation HA environment

Installing and configuring Storage Foundation HA for Windows with Enterprise Vault

Except where noted, you can get detailed instructions on how to perform the steps outlined in this section from the *Solutions Guide* for Storage Foundation and High Availability Solutions.

To install and configure Storage Foundation HA for Windows with Enterprise Vault

1   On each node that is to be a part of the cluster, install all the required components for Storage Foundation HA for Windows (SFW HA) 6.1 or 7.0.

There are several stages to this process. For each node, you must do the following:

- Review the product installation requirements, disk space requirements, and requirements for SFW HA.

- Configure the network and storage.

- ■ Install SFW HA. As part of this process, take care to install the Enterprise Vault Cluster Setup wizard.

2 Run the VCS Configuration wizard to configure the cluster.

3 Configure the disk group and volumes from the first node. You can use the Veritas Enterprise Administrator or equivalent disk management software to do this.

You must create shared volumes to store the following:

- ■ Indexing service data

- ■ Enterprise Vault Storage queue

- ■ Shopping service data

- ■ Vault store partitions

- ■ PST holding folders

- ■ SMTP holding folder (only required if the Enterprise Vault SMTP Archiving components are installed)

- ■ Enterprise Vault server cache

- ■ EMC Centera staging areas

- ■ Registry replication data

For performance reasons we recommend that you take care to place the shared data in suitable locations. Some data requires separate disks.

See the *Enterprise Vault Performance Guide* at http://www.veritas.com/docs/000005725 for details.

See "Managing disk groups and volumes in a Storage Foundation HA environment" on page 235.

4 Mount the volumes on the system where you will configure the Enterprise Vault service group.

5 Run the Enterprise Vault Cluster Setup wizard to configure the Enterprise Vault service group.

See "About configuring the VCS service group for Enterprise Vault" on page 237.

6 Test that the nodes in the cluster fail over correctly.

7 Install Enterprise Vault on all systems in the cluster.

8 Run the Enterprise Vault Configuration wizard to create the Enterprise Vault services and resources.

9 Verify the cluster configuration and test the failover capability.

Managing disk groups and volumes in a Storage Foundation HA environment

This section describes how to perform the following activities:

- Importing a dynamic disk group.

- Mounting a shared volume.

- Unmounting a volume and deporting a disk group.

While you set up an SFW HA environment, keep the following points in mind:

- You must mount the volumes on the system where you will configure the Enterprise Vault service resource group.

- When a disk group is initially created, it is imported on the node where it is created.

- A disk group can be imported on one node only at a time.

- To move a disk group from one node to another, unmount the volumes in the group, deport the group from its current node, import it to a new node, and mount the volumes.

To import a dynamic disk group

1 Start the Veritas Enterprise Administrator.

2 Right-click a disk name in the dynamic disk group or the dynamic disk group name in the tree view, and then click **Import Dynamic Disk Group** on the context menu.

3 Follow the on-screen instructions.

To mount a volume

1 If you have yet to do so, open the Veritas Enterprise Administrator and import the dynamic disk group.

2 Right-click the volume, and then click **File System** > **Change Drive Letter and Path**.

3 In the Drive Letter and Paths dialog box, click **Add**.

4 Select one of the following options, depending on whether you want to assign a drive letter to the volume or mount it as a folder.

To assign a drive letter.	Click **Assign a Drive Letter**, and then choose the required letter.
To mount the volume as a folder.	Click **Mount as an empty NTFS folder**, and then click **Browse** to locate an empty folder on the shared disk.

5 Click **OK**.

To unmount a volume and deport the dynamic disk group

1 In the Veritas Enterprise Administrator, right-click the volume and then click **File System** > **Change Drive Letter and Path**.

2 In the Drive Letter and Paths dialog box, click **Remove**.

3 Click **OK**.

4 Right-click the disk, and then click **Deport Dynamic Group**.

5 Click **Yes** to confirm that you want to deport the disk group.

Configuring the VCS service group for Enterprise Vault

This chapter includes the following topics:

- About configuring the VCS service group for Enterprise Vault

- Before you configure the VCS service group for Enterprise Vault

- Creating a VCS service group for Enterprise Vault

- Modifying an existing VCS service group

- Deleting a VCS service group

About configuring the VCS service group for Enterprise Vault

In VCS, a service group represents a virtual server. Each service group contains a set of resources, which you can bring online or offline when a group fails over to another node in the cluster. You can arrange a combination of these resources to make a complete Enterprise Vault server.

These resources include the following:

- GenericService resources

- IP address

- Computer name (Lanman resource)

- Microsoft Message Queue (MSMQ resource)

- Disk/storage (MountV and DiskGroup resources)

- NIC

Before you can configure Enterprise Vault in a cluster, you must configure a service group to represent the Enterprise Vault server. VCS provides several ways to configure a service group, including the Enterprise Vault Cluster Setup wizard. You can also use Cluster Manager (Java Console or Web Console) or the command line.

We recommend that Enterprise Vault cluster groups contain resources related to Enterprise Vault only.

Before you configure the VCS service group for Enterprise Vault

Before you configure an Enterprise Vault service group, do the following:

- Verify your DNS server settings. You must ensure that a static DNS entry maps the virtual IP address with the virtual server name (which will be the same as the Enterprise Vault server name).
  Note that the Enterprise Vault Cluster Setup wizard does not support service groups that contain multiple IP address or computer name (Lanman) resources.

- Verify that the Veritas Command Server service is running on all systems in the cluster.

- Verify that the High Availability Daemon (HAD) is running on the system from where you will run the Enterprise Vault Cluster Setup wizard.

- Ensure that you have Cluster Administrator privileges. You must also be a Local Administrator on the node where you run the wizard.

- Verify that Microsoft Message Queue (MSMQ) is installed locally on each node.

- Mount the shared volumes that you have created to store the following:
  - Indexing service data
  - Shopping service data
  - Vault store partitions
  - PST holding folders
  - SMTP holding folder
  - EMC Centera staging areas

Unmount the volumes from other nodes in the cluster.

Creating a VCS service group for Enterprise Vault

As part of the process of installing Storage Foundation HA for Windows, you installed the Enterprise Vault Cluster Setup wizard. This wizard lets you create a VCS service group for Enterprise Vault.

To create a VCS service group for Enterprise Vault

1   Start the Enterprise Vault Cluster Setup Wizard.

2   Review the information in the Welcome page, and then click **Next** to display the Wizard Options page.

3   Click **Create service group**, and then click **Next** to display the Service Group Configuration page.

4   In the **Service Group Name** box, type a name for the group, such as EVGRP1.

5   Move to the **Systems in Priority Order** box those systems on which you want to configure the service group.

   If you want to change the priority of the systems in the **Systems in Priority Order** box, click a system and then click the up-arrow or down-arrow button.

6   Click **Next** to validate the configuration and display the Virtual Server Configuration page.

7   Complete the fields by following these steps in the order listed:

   ■   In the **Virtual Server Name** box, type the server name that you mapped to the virtual IP address when you set up the static DNS entry.

   ■   In the **Virtual IP address** box, type the address that you mapped to the virtual server. This should be in the same subnet as the current computer, but it should not currently be in use on the network.

   ■   Enter the subnet mask for the subnet to which the virtual IP address belongs.

   ■   For each system in the cluster, select the public network adapter name. The wizard lists all the TCP/IP-enabled adapters on the system, including the private network adapters if they are TCP/IP enabled. Be sure to select the adapters to assign to the public network, and not those assigned to the private network.

   ■   Click **Advanced** to specify details for the Lanman resource. You must select the distinguished name of the organizational unit for the virtual server. By default, the Lanman resource adds the virtual server to the default container Computers. The user account for VCS Helper service must have adequate privileges on the specified container to create and update computer accounts.

8 In the Virtual Server Configuration page, click **Next** to display the MSMQ and RegRep Directory Details page.

This page enables you to virtualize the MSMQ resource so that it can be accessed using its virtual name. This resource also ensures that the queue state is maintained after failover.

9 Complete the fields as follows:

- In the **MSMQ Directory** field, enter the path to the required directory.

- In the **Replication Directory** field, enter the path to the registry replication directory. The replication data contains a list of the registry keys to replicate.

We recommend that you configure the MSMQ and replication directories on different volumes. A volume is available for selection only if you have configured it on the shared disk.

10 Click **Next** to display the Storage Location Details page.

This page lets you select the volumes that you want to configure for Enterprise Vault services.

The available volumes do not include those that you selected in the previous page of the wizard, when specifying the storage locations for MSMQ and registry replication.

11 In the Available Volumes box, select each volume on which you have configured the services and then click the right-arrow button to move it to the Selected Volumes box. You must select the volumes that you configured for each of the following:

- Indexing service data

- Shopping service data

- Vault store partitions

- PST holding folders

- SMTP holding folder

- EMC Centera staging areas

12 Click **Next** to display the Service Group Summary page.

13 Review your configuration. If you want to modify an attribute name for any reason, follow these steps in the order listed:

- Click the resource, and then click the attribute that you want to modify.

- Click the **Edit** icon at the end of the table row.

- In the Edit Attribute dialog box, enter the attribute values.

- Click **OK**.

- Repeat the procedure for each resource and attribute.

14 Click **Next** to display the Completion page.

15 Click **Bring the service group online**, and then click **Finish**.

When you have finished adding the service group, check that it can fail over between nodes without error.

Modifying an existing VCS service group

Table 31-1 lists the items that you can modify in a service group.

Table 31-1 Modifiable service group items

Item	Notes
System list	You can add nodes to or remove them from the cluster. If you want to remove a node, make sure that it is not the active one.
Volumes	You can add or remove volumes. If you remove a volume on which an Enterprise Vault service is configured, the service ceases to be highly available and is not monitored.
Virtual IP	You can change the virtual IP address if the service group is offline. You cannot change the virtual server name, which is fixed when you create the service group.

You can modify an Enterprise Vault service group in several ways, including the Enterprise Vault Cluster Setup wizard, Cluster Manager (both Java Console and Web Console), and the command line. The following steps describe how to modify the service group with the Enterprise Vault Cluster Setup wizard.

Before you proceed, note the following:

- You must run the wizard from a node on which the service group is online. You can then use the wizard to add resources to or remove them from the configuration.

- You must take the service group partially offline to change the resource attributes. However, the MountV and VMDg resources for the service group should be online on the node where you run the wizard and offline on all other nodes. Mount all the volumes created to store Storage service data (vault stores), registry replication information, Shopping service data, SMTP holding folder, Indexing data and MSMQ data.

- If you want to modify the system list or volumes, the service group must be online.

- Do not modify an existing VCS service group that contains an operational Enterprise Vault server.

To modify an existing VCS service group

1   Start the Enterprise Vault Cluster Setup wizard.

2   Review the information in the Welcome page, and then click **Next** to display the Wizard Options page.

3   Click **Modify service group**, and then click **Next**.

4   Follow the instructions to modify the service group.

    Note that if you add a system to an online service group, any resources with local attributes may briefly have a status of UNKNOWN. After you add the new node to the group, run the Enterprise Vault Configuration wizard on this node to configure the Enterprise Vault services for it.

Deleting a VCS service group

Follow the steps below to delete a service group with the Enterprise Vault Cluster Setup wizard.

To delete a VCS service group

1   Start the Enterprise Vault Cluster Setup wizard.

2   Review the information in the Welcome page, and then click **Next** to display the Wizard Options page.

3   Click **Delete service group**, and then click **Next**.

4   In the Service Group Summary page, click **Next**.

5   When the wizard prompts you to confirm that you want to delete the service group, click **Yes**.

6   Click **Finish**.

Running the Enterprise Vault Configuration wizard

This chapter includes the following topics:

- Before you run the Enterprise Vault Configuration wizard
- Setting up Enterprise Vault in an active/passive VCS configuration
- About setting up Enterprise Vault in a VCS N+1 configuration

Before you run the Enterprise Vault Configuration wizard

The Enterprise Vault Configuration Wizard provides options for setting up Enterprise Vault in a VCS cluster.

Before you run the Enterprise Vault Configuration wizard, ensure the following:

- The Enterprise Vault service group exists and is online on the first node in the cluster.
  See "About configuring the VCS service group for Enterprise Vault" on page 237.
- You have installed SFW HA 6.1 or 7.0.

Setting up Enterprise Vault in an active/passive VCS configuration

As well as describing how to set up cluster support in a first-time installation of Enterprise Vault, this section describes how to upgrade an existing, standard installation of Enterprise Vault to a clustered environment.

Adding VCS cluster support in a first-time Enterprise Vault installation

You must run the Enterprise Vault Configuration wizard on each node of the cluster. On the first node, choose the option to create a new Enterprise Vault server with cluster support. On each additional node, choose the option to add it as a failover node for an existing clustered server.

If you want to add the Enterprise Vault SMTP service as a generic service resource, then you must install the Enterprise Vault SMTP Archiving components with the Enterprise Vault server on all the nodes in the cluster.

To create a new Enterprise Vault server with cluster support

1   Start the Enterprise Vault Configuration wizard.

2   Click **Create a new Enterprise Vault server with cluster support**, and then click **Next**.

3   Follow the on-screen instructions.

Note the following important points as you proceed through the wizard:

- When the wizard prompts you for the computer DNS alias, enter an unqualified DNS alias that points to the virtual server name.

- Take care to review the storage locations for the Indexing and Shopping services, when the wizard prompts you to do so.

- When the wizard prompts you to select the data locations, specify a server cache location that is on a shared drive in the cluster.

4   In the Finish page, ensure that **Bring all the resources online** is unchecked, and then click **Finish**.

5   Follow the steps below to set the path to the index metadata folder, which must be on a shared drive in the cluster. The index metadata folder is the folder in which Enterprise Vault stores indexing configuration data and reporting data.

- Use the Cluster Manager console to bring the Enterprise Vault Directory service and Admin service online.

- In the left pane of the Enterprise Vault Administration Console, browse to **Enterprise Vault Servers** > **EVServer.*domain*.local** > **Services**.

- In the right pane, right-click **Enterprise Vault Indexing Service**, and then click **Properties**.

- On the **General** tab of the Service Properties dialog box, set the **Index metadata location** path to that of the shared drive in the cluster (for example, `V:\indexmetadata`).

- Click **OK** to save the change that you have made.

- Use the Cluster Manager console to bring the Enterprise Vault Indexing service online

6 After you have configured the server on the first node, run the wizard from each additional node that you want to configure as a failover node.

Note that the path to the Enterprise Vault program folder must be the same on all nodes in the cluster; for example, `C:\Program Files (x86)\Enterprise Vault`. If the path varies from one node to another, problems can occur during failover.

To add a failover node for an existing clustered server

1 Ensure that the Enterprise Vault service group is online on a different node in the cluster. The service group must not be online on the node that you are configuring. The node that you are configuring must be a possible failover node for the resources.

2 If the Enterprise Vault SMTP service is included as a generic service resource in the service group, then ensure that you install the Enterprise Vault SMTP Archiving components with the Enterprise Vault server on the failover node.

3 Start the Enterprise Vault Configuration wizard.

4 Click **Add this node as a failover node for an existing clustered server**, and then click **Next**.

5 Follow the on-screen instructions.

When the wizard prompts you for the name of the service group to which you want to add the node, select the name of the service group that you chose for the first node.

6 In the summary page, review the information, and then click **Next**.

The wizard informs you that it will create the Enterprise Vault service group on the new node.

7 In the Finish page, click **Finish** to exit the wizard.

8 Check that you can bring the resources online on the failover node. You can do this with Cluster Explorer, by clicking **Switch To** on the context menu.

Troubleshooting configuration of the Monitoring database

If during the running of the Enterprise Vault configuration wizard you receive errors indicating that configuring of the Enterprise Vault Monitoring database has failed, complete the configuration wizard and then run the Monitoring Configuration Utility to configure the Monitoring database and the Monitoring agents manually.

For information on how to do this, see the following Enterprise Vault technical note on the Veritas Support website:

http://www.veritas.com/docs/000033005

The technical note also describes how to troubleshoot issues with Monitoring agents.

Upgrading an existing Enterprise Vault installation to a VCS cluster

If you have an existing Enterprise Vault installation on a single, unclustered server, you can convert it to a failover cluster. To be eligible for conversion to a cluster, the existing Enterprise Vault installation must meet the following conditions:

- Enterprise Vault should already be configured in a non-clustered configuration, and it must not already be part of a cluster.

- Enterprise Vault servers must be configured using DNS aliases rather than standard address records.

- The Enterprise Vault server must have a full set of Indexing, Shopping, Task Controller, and Storage services.

- If Enterprise Vault SMTP Archiving is required, you must also install the Enterprise Vault SMTP Archiving components on all the nodes in the service group.

- Neither Compliance Accelerator nor Discovery Accelerator must be installed on any server in the planned cluster. These products are not supported within a cluster. However, an unclustered Compliance Accelerator or Discovery Accelerator can reference a clustered Enterprise Vault virtual server.

To upgrade an existing Enterprise Vault installation to a VCS cluster

1   Check that your setup meets the requirements for the Enterprise Vault service group.

See "Before you configure the VCS service group for Enterprise Vault"
on page 238.

2   Run the Enterprise Vault Cluster Setup wizard to create an Enterprise Vault service group and add to the group the server that you are going to configure.

3   Ensure that the following items are all on highly-available shared storage devices.

- Indexing service data

- Shopping service data

- Vault store partitions

- PST holding folders

- SMTP holding folder

- EMC Centera staging areas

If they are not, correct the locations in the Enterprise Vault Directory database and then move the associated data to the new locations.

See "Moving Enterprise Vault data to highly-available locations" on page 247.

4   Start the Enterprise Vault Convert to Cluster wizard.

5   Read the introductory information, and then click **Next**.

6   When the following page appears, check **All locations are highly available storage devices**, and then click **Next**.

7   If the wizard detects that there are messages in the Enterprise Vault MSMQ queues, choose whether to proceed with the conversion without migrating them to the clustered MSMQ queues.

Wait until the queues have cleared and then rerun the Convert to Cluster wizard. Any messages that are still in the queues are ignored in the new cluster. To accelerate the process of clearing the queues, stop the Task Controller service and ensure that File System Archiving is not performing an archiving run.

8   When the wizard prompts you to choose a service group in which to create the cluster resources for each Enterprise Vault service, select the group that you created earlier.

9   Click **Next** to create the cluster resources, and then review the list of actions that the wizard has carried out.

10 Click **Finish** to close the wizard.

11 Using the DNS snap-in to the Microsoft Management Console (MMC), change the computer name alias to point to the virtual server name rather than the local name.

12 Use Veritas Cluster Manager to bring the resources in the cluster online.

Moving Enterprise Vault data to highly-available locations

In outline, the procedure for moving the data to highly-available locations is as follows:

- Stop the Indexing, Shopping, Storage, and Task Controller services.

- Make a backup copy of the Enterprise Vault Directory database and data files.

- Use the Vault Administration Console or run a SQL query against the Enterprise Vault directory to move the data, as described below.

IndexRootPathEntry [IndexRootPath]	■ Move the contents of this location to a highly available location. ■ Update the database using SQL to point at the new location.

The SQL to view the current location is as follows:

```
SELECT *
FROM IndexRootPathEntry
WHERE (IndexRootPathEntryId = '<ID FROM
LOG FILE>')
```

The SQL to update the location is as follows:

```
UPDATE IndexRootPathEntry
SET IndexRootPath = '<THE NEW LOCATION>'
WHERE (IndexRootPathEntryId = '<ID FROM
LOG FILE>')
```

PartitionEntry [AccountName]	■ Move the pool entry authorization (`.pea`) file to a highly available location. ■ Use the Vault Administration Console to view the properties of the EMC Centera partition and then, on the **Connection** tab, edit the **Pool Entry Authorization File Location** box to point at the new location.
PartitionEntry [PartitionRoot Path]	■ Move the contents of this location to a highly available location. ■ Update the database using SQL to point at the new location.

The SQL to view the current location is as follows:

```
SELECT *
FROM PartitionEntry
WHERE (PartitionEntryId = '<ID FROM LOG
FILE>')
```

The SQL to update the location is as follows:

```
UPDATE PartitionEntry
SET PartitionRootPath = '<THE NEW
LOCATION>'
WHERE (PartitionEntryId = '<ID FROM LOG
FILE>')
```

PartitionEntry/Locations [SecondaryLocation]	■ Move the secondary storage files to a highly available location.
	■ Update the database using SQL to point at the new location.

The SQL to view the current location is as follows:

```
SELECT *
FROM PartitionEntry
INNER JOIN Locations ON
PartitionEntry.SecondaryLocation =
Locations.LocationIdentity
WHERE (PartitionEntry.PartitionEntryId =
'<ID FROM LOG FILE>')
```

The SQL to update the location is as follows:

```
UPDATE Locations
SET Location = '<NEW LOCATION>'
WHERE LocationIdentity =
(SELECT SecondaryLocation FROM PartitionEntry
WHERE PartitionEntryId = '<ID FROM LOG
FILE>')
```

PartitionEntry [StagingRoot Path]	■ Move the contents of this location to a highly available location.
	■ Update the database using SQL to point at the new location.

The SQL to view the current location is as follows:

```
SELECT *
FROM PartitionEntry
WHERE (PartitionEntryId = '<ID FROM LOG
FILE>')
```

The SQL to update the location is as follows:

```
UPDATE PartitionEntry
SET StagingRootPath = '<THE NEW LOCATION>'
WHERE (PartitionEntryId = '<ID FROM LOG
FILE>')
```

PSTMigratorTask [Migration Directory]	**1**	Move the contents of this location to a highly available location.
	2	Use the Vault Administration Console to view the properties of the PST Migrator Task and update the Temporary files folder.
ShoppingServiceEntry [ShoppingRootPath]	■	Move the contents of this location to a highly available location.
	■	Use the Vault Administration Console to edit the Shopping service location to the new highly available location.
SiteEntry [PSTHolding Directory]	■	Move the contents of this location to a highly available location.
	■	Use the Vault Administration Console to view the site properties and update the PST Holding Folder property to point at the new location.
SmtpArchivingTask [HoldingFolder]	■	Move the contents of this location to a highly available location.
	■	Use the Vault Administration Console to view the properties of the SMTP Archiving task, and update the SMTP Holding Folder property to point at the new location.

Adding SMTP Archiving to an existing clustered Enterprise Vault server

You may want to add the Enterprise Vault SMTP Archiving feature to an existing Enterprise Vault cluster.

To add SMTP Archiving to an existing clustered Enterprise Vault server

1 Install the Enterprise Vault server and the SMTP Archiving components on all the nodes in the Enterprise Vault cluster.

2 Create a new SMTP Archiving task on the clustered Enterprise Vault server. Before Enterprise Vault creates the SMTP Archiving task, it detects the presence of the Enterprise Vault SMTP service on the active node and other nodes, and configures the SMTP service as generic service resource.

3 If Enterprise Vault does not detect the SMTP Archiving components on some of the cluster nodes, it displays a list of the nodes affected, and a warning to install the SMTP Archiving components. You can continue to create the SMTP Archiving task, and install the SMTP Archiving components on the listed nodes at a later time. If you do not install the components on all the nodes in the cluster, Enterprise Vault cannot fail over to the nodes where the components are not installed.

About setting up Enterprise Vault in a VCS N+1 configuration

As a cheaper alternative to setting up an active/passive cluster, you can set up Enterprise Vault in a VCS N+1 configuration. Here, the cluster contains any number of Enterprise Vault servers and a single spare node.

There are two basic types of N+1 configuration. For example, in a cluster that contains two Enterprise Vault servers, you can choose between these configuration types:

- The clustered Enterprise Vault servers run on two nodes, and there is a shared spare node.
- The two Enterprise Vault servers are configured to run on any of the three nodes in the cluster.

Configuring two Enterprise Vault server nodes and a spare node in a VCS N+1 cluster

Figure 32-1 illustrates a configuration in which there is a spare node in addition to the two nodes on which the Enterprise Vault servers are running. Remember that a cluster can contain many Enterprise Vault servers, depending on the number of available nodes.

Figure 32-1   Three-node VCS cluster with two Enterprise Vault server nodes and a spare node
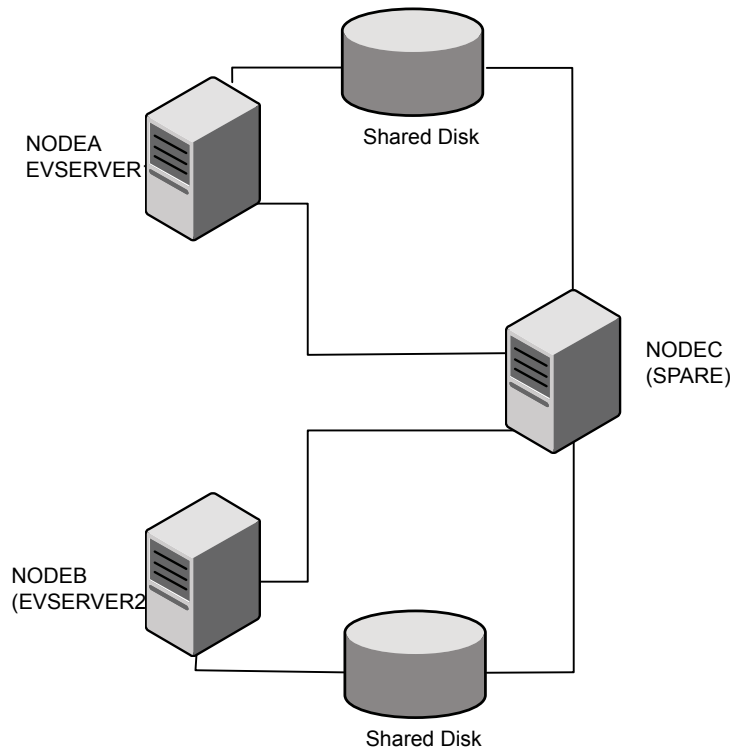
You configure the service group for EVSERVER1 to run on both NODEA and NODEC, and the service group for EVSERVER2 to run on both NODEB and NODEC. EVSERVER1 and EVSERVER2 are both virtual computer names from the service group.

To configure two Enterprise Vault server nodes and a spare node in a VCS N+1 cluster

1 Mount the volumes on the system where you will configure the Enterprise Vault service group.

See "Managing disk groups and volumes in a Storage Foundation HA environment" on page 235.

2 On either NODEA or NODEC, run the Enterprise Vault Cluster Setup wizard and create a service group called EVSERVER1 for these two nodes.

3 On either NODEB or NODEC, run the Enterprise Vault Cluster Setup wizard and create a service group called EVSERVER2 for these two nodes.

4 Take the actions described below on NODEA and NODEB, depending on whether you are performing a first-time installation of Enterprise Vault or upgrading an existing installation.

Node	New installation	Upgrade installation
NODEA	Run the Enterprise Vault Configuration wizard. Choose to configure a new Enterprise Vault server with cluster group for EVSERVER1.	Run the Convert to Cluster wizard. Choose to create the service resources in the EVSERVER1 service group.
NODEB	Run the Enterprise Vault Configuration wizard. Choose to configure a new Enterprise Vault server with cluster group for EVSERVER2.	Run the Convert to Cluster wizard. Choose to create the service resources in the EVSERVER2 service group.

5 On NODEC, run the Enterprise Vault Configuration wizard and choose to add this node as a failover node for an existing clustered server. Select either service group.

When you bring the service groups online on NODEA and NODEB, Cluster Explorer may falsely indicate a problem with the GenericService resources (their icons in the left pane may have question marks). This is because VCS assumes that each resource is simultaneously online on two nodes. You can ignore this situation.

Configuring two Enterprise Vault servers to run on any of the three nodes in a VCS cluster

Figure 32-2 illustrates a configuration in which the two Enterprise Vault servers are configured to run on any of three nodes in a VCS cluster. This has the advantage that if NODEB fails, the server moves to NODEC. NODEB can then be brought back online and act as a failover server for EVSERVER1 and EVSERVER2.

Figure 32-2　　　Three-node VCS cluster with two Enterprise Vault servers
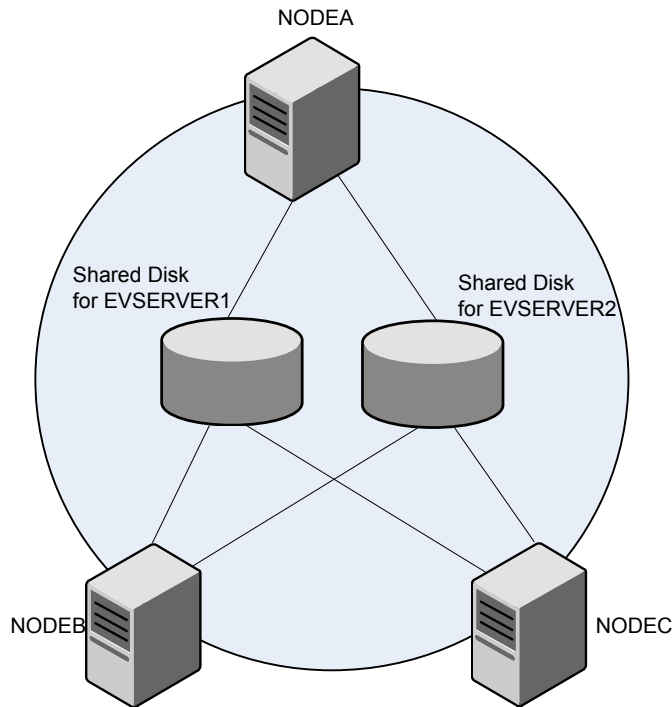
To configure two Enterprise Vault servers to run on any of the three nodes in a VCS cluster

1　Mount the volumes on the system where you will configure the Enterprise Vault service group.

　　See "Managing disk groups and volumes in a Storage Foundation HA environment" on page 235.

2　With the Enterprise Vault Cluster Setup wizard, create a service group for EVSERVER1 that contains nodes NODEA, NODEB, and NODEC.

3　With the Enterprise Vault Cluster Setup wizard, create a service group for EVSERVER2 that contains nodes NODEA, NODEB, and NODEC.

4 Take the actions described below on NODEA and NODEB, depending on whether you are performing a first-time installation of Enterprise Vault or upgrading an existing installation.

Node	New installation	Upgrade installation
NODEA	Run the Enterprise Vault Configuration wizard. Choose to configure a new Enterprise Vault server with cluster group for EVSERVER1.	Run the Convert to Cluster wizard. Choose to create the service resources in the EVSERVER1 service group.
NODEB	Run the Enterprise Vault Configuration wizard. Choose to configure a new Enterprise Vault server with cluster group for EVSERVER2.	Run the Convert to Cluster wizard. Choose to create the service resources in the EVSERVER2 service group.

5 On NODEC, run the Enterprise Vault Configuration wizard and choose to add this node as a failover node for an existing clustered server. Select either service group.

Notice that the only difference in configuration between this option and option 1 is that, when you create the service groups, you must select all the nodes rather than a subset of the nodes.

You can take a similar approach if you require your system to have more than one spare server (N+2, N+3, N+4, and so on). In each case, you must configure a node for each Enterprise Vault server and then add the spare nodes as failover nodes.

Disallowing two Enterprise Vault servers on the same node in a VCS cluster

You cannot run multiple Enterprise Vault service groups on the same node in an active/active cluster configuration. When configuring the cluster in an N+x configuration, you can stop this from happening by setting the Limits and Prerequisites attributes for every node.

For more information on these steps, see the *Cluster Server Administrator's Guide*.

To disallow two Enterprise Vault servers on the same node in a VCS cluster

1 Use Veritas Cluster Manager to log on to the cluster.

2 Click anywhere in the Cluster Monitor panel to open Cluster Explorer.

3 For each node in the cluster, perform the following steps in the order listed:

- In the configuration tree at the left, click the node whose attributes you want to edit.

- In the View panel, click the **Properties** tab.

- Click **Show all attributes** to open the Attributes View dialog box.

- Find the Limits attribute.

- Click the **Edit** icon at the right of the row.

- In the Edit Attribute dialog box, add a key called EnterpriseVault and give it a value of 1.

- Click **OK** to close the dialog box and return to the Attributes View dialog box.

- Repeat for the Prerequisites attribute on each Enterprise Vault service group.

When both the Limits and Prerequisites attributes have a key called EnterpriseVault with a value of 1, two Enterprise Vault servers cannot run on the same node.

Implementing an SFW HA-VVR disaster recovery solution with Enterprise Vault

This chapter includes the following topics:

- About installing and configuring SFW HA-VVR with Enterprise Vault

- Overview of the steps for installing and configuring SFW HA-VVR

- Setting up the VCS cluster on the primary site

- Setting up the VCS cluster on the secondary site

- Adding the VVR components for replication

- Adding the GCO components for wide-area recovery

About installing and configuring SFW HA-VVR with Enterprise Vault

The procedure for installing and configuring SFW HA-VVR with Enterprise Vault is similar to the procedure that the *Solutions Guide* for Storage Foundation and High Availability Solutions describes.

In this scenario, there is a source host on the primary site and a destination host on the secondary site. The application data is stored on the primary site and replicated to the secondary site by using the Veritas Volume Replicator (VVR). The

primary site provides data and services during normal operation. If a disaster occurs on the primary site and its data is destroyed, a secondary host can take over the role of the primary host to make the data accessible. The application can be restarted on that host.

Figure 33-1 shows an SFW HA-VVR configuration.

Figure 33-1 SFW HA-VVR configuration
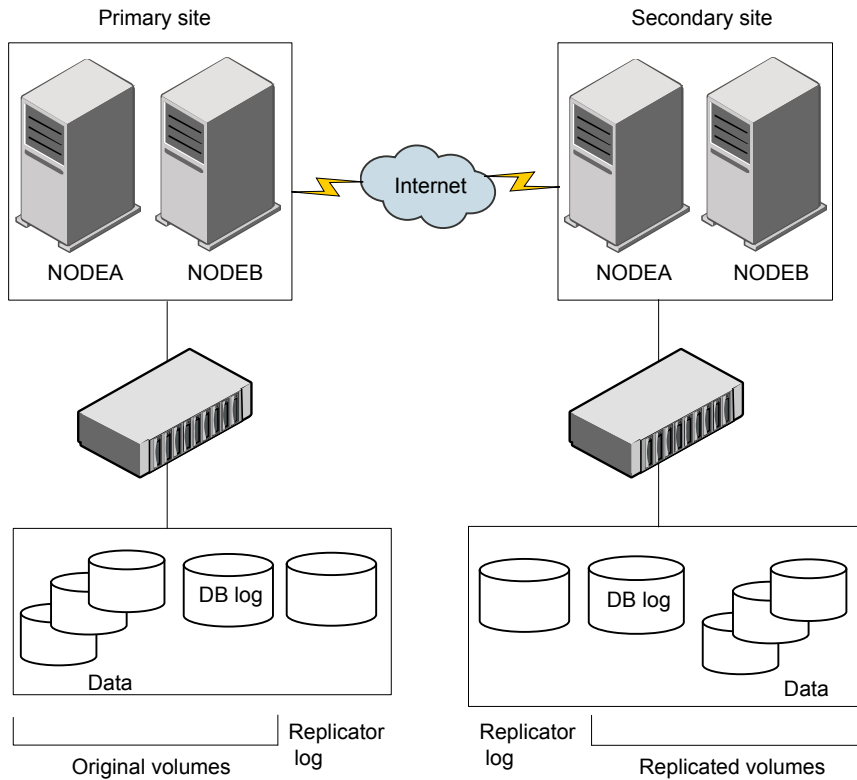
This example has one disk group on each site for the application. Note that a VVR replicator log is needed on each site. If there are multiple disk groups, an additional replicator log is required for each one.

Overview of the steps for installing and configuring SFW HA-VVR

Table 33-1 lists the tasks that you must perform to install and configure SFW HA-VVR.

Table 33-1   Installing and configuring SFW HA-VVR

Step	Task	See this section for more details
Step 1	Set up the VCS cluster on the primary site.	See "Setting up the VCS cluster on the primary site" on page 259.
Step 2	Set up the VCS cluster on the secondary site.	See "Setting up the VCS cluster on the secondary site" on page 260.
Step 3	Add the VVR components for replication.	See "Adding the VVR components for replication" on page 261.
Step 4	Add the Global Cluster Option (GCO) components for wide-area recovery.	See "Adding the GCO components for wide-area recovery" on page 261.

Setting up the VCS cluster on the primary site

Complete the following steps to set up the cluster on the primary site. Except where noted, you can obtain more information on how to perform these steps from the *Solutions Guide* for Storage Foundation and High Availability Solutions.

To set up the VCS cluster on the primary site

1 Install SFW HA 6.1 or 7.0 on each node that is to be a part of the cluster on the primary site.

There are several stages to this process:

- Review the product installation requirements, disk space requirements, and requirements for SFW HA.

- Install Windows and configure the network settings.

- Install SFW HA on the primary site. Be sure to select the VVR and GCO options during the installation.

- Using the VVR Security Service Configuration wizard, configure the Veritas Volume Replicator Security Service (VxSAS).

2 Configure the cluster by running the VCS Configuration wizard.

3 Install Enterprise Vault.

4   Configure the disk group and volumes. You must create shared volumes to store the following:

- Indexing service data

- Shopping service data

- Vault store partitions

- PST holding folders

- SMTP holding folder

- EMC Centera staging areas

We also recommend that you create separate volumes to store the MSMQ and registry replication data.

5   Configure the VCS service group at the primary site.

See "About configuring the VCS service group for Enterprise Vault" on page 237.

6   Verify the cluster configuration, and test the failover capability.

Setting up the VCS cluster on the secondary site

The process of setting up a cluster on the secondary site is similar to that on the primary site. Except where noted, you can obtain more information on how to perform these steps from the *Solutions Guide* for Storage Foundation and High Availability Solutions.

To set up the VCS cluster on the secondary site

1   Create a parallel environment on the secondary site.

2   Configure the cluster by running the VCS Configuration wizard.

3   Install Enterprise Vault.

4   Configure the disk groups and volumes on the secondary site.

The disk group and volume setup on the secondary site must be identical to that on the primary site. The disks, disk groups, and volumes must be the same sizes, have the same names, and must be of the same type.

5   Configure the VCS service group at the secondary site, taking care to specify the same service group name that you specified on the primary site.

6   Verify the cluster configuration, and test the failover capability.

Adding the VVR components for replication

This section provides information on configuring the VVR components for replication. You can obtain more information on how to perform these steps from the *Solutions Guide* for Storage Foundation and High Availability Solutions.

To add the VVR components for replication

1   Create a replicator log volume at each site.

2   Set up the replicated data sets for VVR on the hosts for the primary and secondary sites. Note that the Setup Replicated Data Set wizard lets you configure replicated data sets for both sites.

3   Create the VVR RVG service group.

    You must run the Volume Replicator Agent Configuration wizard from the system that contains the application service group.

Adding the GCO components for wide-area recovery

You require the Global Cluster Option (GCO) components to manage global clustering for wide-area disaster recovery. For information on how to perform the steps below, see the *Solutions Guide* for Storage Foundation and High Availability Solutions.

To add the GCO components for wide-area recovery

1   Ensure that your environment meets the requirements for global cluster operations.

2   Link clusters by adding a remote cluster.

3   Convert the local service group to a global group.

4   Perform additional global cluster administration tasks.

Troubleshooting clustering with VCS

This chapter includes the following topics:

- VCS logging

- Enterprise Vault Cluster Setup wizard error messages

- Viewing the clustered message queues for an Enterprise Vault virtual server

VCS logging

VCS generates two error message logs: the engine logs and the agent logs. Log file names are appended by letters, where A indicates the first log file, B the second, C the third, and so on; for example, `agent_A.txt`.

The agent log is located at `%VCS_HOME%\log` (typically `c:\Program Files\Veritas\cluster server\log`). The format of agent log messages is as follows:

Timestamp Mnemonic Severity Message_ID Message_Text

where:

Timestamp	Shows the date and time when the message was logged.
Mnemonic	Identifies the product (for example, VCS).
Severity	Indicates the severity of the error, which can be CRITICAL, ERROR, WARNING, NOTICE, or INFO. CRITICAL messages are the most severe, whereas INFO messages are the least severe.

Message_ID   Is the unique numeric ID of the error message. The prefix V-16 denotes VCS.

Message_Text   Is the message generated by VCS.

For example, a typical agent log message looks like this:

```
2006/01/24 11:04:17 VCS ERROR V-16-10051-6026 GenericService:
CLSEV1-EnterpriseVaultAdminService:monitor:
The LanmanResName attribute has not been configured.
```

Enterprise Vault Cluster Setup wizard error messages

Table 34-1 describes some messages that you may see when you run the Enterprise Vault Cluster Setup wizard.

Table 34-1   Enterprise Vault Cluster Setup wizard error messages

Message	Explanation
Access Denied. You must have Administrator privileges to run the wizard.	Only users who are members of the local administrator's group can run this wizard.
VCS not running on the local machine. Either the service has not been started or it is in a stale state.	Verify that the VCS service has started and is running on the local machine.
MSMQ is not configured properly.	The wizard verifies that MSMQ is installed and configured on all the nodes. The error message is shown if MSMQ is not installed on one node or the configuration is different. To resolve the problem, verify that MSMQ has been installed and configured before proceeding with the Enterprise Vault Cluster Setup wizard.
The required resource type MSMQ is not installed on this system.	The wizard verifies that the MSMQ resource type is installed on the system. This resource type is installed with VCS.

Viewing the clustered message queues for an Enterprise Vault virtual server

By default, in a clustered Enterprise Vault installation, the Computer Management snap-in does not show the Enterprise Vault message queues. Instead, the snap-in shows the queues for the local computer only.

To view the clustered message queues for an Enterprise Vault virtual server

1   Ensure that the Enterprise Vault virtual server is online on the node from which you want to view the queues.

2   Open a Command Prompt window with administrator privileges.

3   In the Command Prompt window, change to the Enterprise Vault installation folder (for example, `C:\Program Files (x86)\Enterprise Vault`).

4   Enter the following command:

    `ClusterCompMgmt`

5   In the Computer Management snap-in, expand **Services and Applications** and then expand **Message Queuing**. The Enterprise Vault message queues are listed under **Private Queues**.

Section 6

Clustering Enterprise Vault with Windows Server Failover Clustering

Introducing clustering with Windows Server Failover Clustering

This chapter includes the following topics:

About clustering Enterprise Vault with Windows Server Failover Clustering

You can cluster Enterprise Vault in a Windows Server failover cluster to provide a high availability solution for Enterprise Vault. If you are setting up Enterprise Vault in an environment where Microsoft Exchange and SQL server are clustered, you may want to cluster Enterprise Vault to ensure that you can meet your service level agreements, recovery times, and recovery point objectives.

High availability is provided by creating an Enterprise Vault cluster server that can fail over between physical nodes in the cluster. When Enterprise Vault services are running on a cluster server they operate with virtual IP addresses, a virtual computer name, virtual Microsoft Message Queues, and highly available shared disks. When

a failure occurs, the cluster software can move the cluster server's resources to a different physical node in the cluster.

To cluster Enterprise Vault in a failover cluster, you need a working knowledge of Windows Server Failover Clustering. See your Microsoft documentation for detailed information.

Supported Windows Server Failover Clustering configurations

An Enterprise Vault cluster consists of:

- One or more primary nodes, each normally hosting an Enterprise Vault cluster server.

- One or more failover nodes: standbys that can take over the job of hosting an Enterprise Vault cluster server if a primary node fails.

Enterprise Vault does not permit "active/active" cluster configurations. That is, only one Enterprise Vault cluster server can run on a clustered node at any one time. You can configure Enterprise Vault in any operation mode that adheres to this restriction, such as:

- An active/passive failover pair: a primary node with a dedicated failover node.

- N+1 (hot standby server): two or more primary nodes share a single failover node. Only one node failure can be accommodated at any one time.

- N+M: an extension of the hot standby concept with N primary nodes and M failover nodes. Only M node failures can be accommodated at one time.

- N+M *any-to-any*: identical to N+M, except that there is no need to fail back to the original node after a failover. When the original node becomes available again, it can operate as a failover node.

Required software and restrictions on clustering Enterprise Vault with Windows Server Failover Clustering

You must install a supported version of Windows Server on each primary and failover node.

Each node must run the same version of Windows.

If the cluster is to support Enterprise Vault SMTP Archiving, then you must install the Enterprise Vault SMTP Archiving components on each node in the cluster.

For details of supported versions for clustering, see the Enterprise Vault *Compatibility Charts* at http://www.veritas.com/docs/000097605.

Note the following restrictions:

- Neither Compliance Accelerator nor Discovery Accelerator must be installed on any server in the planned cluster. These products are not supported within a cluster. However, an unclustered Compliance Accelerator or Discovery Accelerator can reference an Enterprise Vault cluster server.

- The Enterprise Vault Configuration wizard does not support cluster services that contain multiple client access point resources or IP address resources.

- We recommend that Enterprise Vault clusters contain only resources related to Enterprise Vault.

Typical Enterprise Vault configuration in a Windows Server failover cluster

Figure 35-1 illustrates a typical configuration.

Figure 35-1   Enterprise Vault in an active/passive failover pair configuration
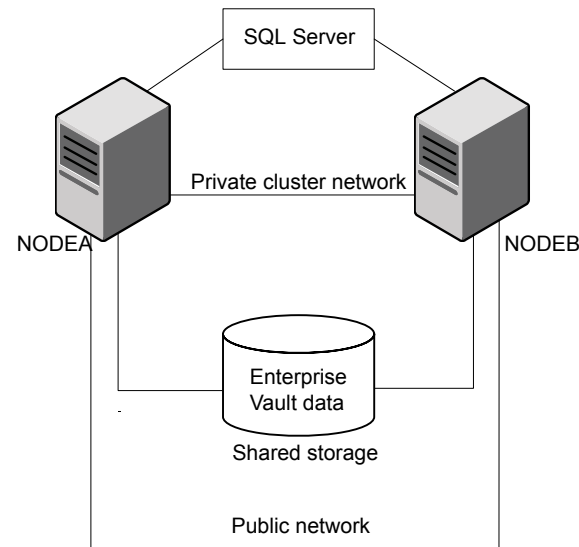
In this example:

- NODEA and NODEB are the two Enterprise Vault nodes in the failover cluster. NODEA is the primary node. NODEB is the failover node.

- The SQL server and Microsoft Exchange may also be configured in the cluster: this does not affect Enterprise Vault.

- The volumes for the Enterprise Vault services data are configured on shared storage.

- The Enterprise Vault cluster server is configured on the primary node, NODEA. If NODEA fails, the cluster server's resources fail over to NODEB, and the cluster server comes online on NODEB.

Control of Enterprise Vault services in a Windows Server failover cluster

Whether you configure Enterprise Vault as a server with cluster support, or as a failover node for an existing clustered server, the Configuration wizard installs the following set of Enterprise Vault services on the node:

- Directory service

- Indexing service

- Shopping service

- Storage service

- Task Controller service

An Admin service is already present from when Enterprise Vault was installed. If you installed the Enterprise Vault SMTP Archiving components, the Enterprise Vault SMTP service also exists.

The presence of this set of services is mandatory on each node, to ensure a common configuration on all nodes in the cluster. You cannot remove Enterprise Vault services in a clustered configuration.

The Configuration wizard sets the Enterprise Vault services to manual startup, to enable the cluster software to start and stop them as required.

Note: In a clustered configuration, you cannot start or stop services using the Administration Console or the EVService utility. If you stop a service using Windows Service Control manager, the cluster software assumes this is due to a system failure, and will restart the service or initiate a failover. To start or stop Enterprise Vault services safely, use only Failover Cluster Manager.

About cluster services and Enterprise Vault service resources in a Windows Server failover cluster

Before configuring an Enterprise Vault server as a server with cluster support, you must create a cluster service, which will become the Enterprise Vault cluster server. The Enterprise Vault Configuration wizard adds the following Enterprise Vault service resources to the cluster service to control and monitor the equivalent Enterprise Vault services on the active node:

- Admin service resource

- Directory service resource

- Indexing service resource

- Shopping service resource

- Storage service resource

- Task Controller service resource

- SMTP service resource (only if the SMTP Archiving components are installed on the node)

The Configuration wizard also adds one more resource to the cluster service: an Enterprise Vault Server Instance resource. All the other Enterprise Vault resources in the cluster service are configured to be dependent on this resource, directly or indirectly. Its purpose is to prevent failovers to nodes already running Enterprise Vault, avoiding an active/active operation mode.

What happens at failover in a Windows Server failover cluster

If an active node fails, the Enterprise Vault cluster server attempts to fail over to the next available node in the cluster service's preferred node list, assuming all the resources have that node as a possible owner. The Server Instance resource fails over first, provided the failover node is not already running an Enterprise Vault cluster server. The remaining resources then fail over in order of dependency. The resources start the Enterprise Vault services on the failover node, ensuring continuing availability for the data that Enterprise Vault is managing and archiving.

Preparing to cluster with Windows Server Failover Clustering

This chapter includes the following topics:

- Preparing to cluster Enterprise Vault with Windows Server Failover Clustering

- Setting up the shared disks and volumes for a Windows Server failover cluster

- Setting up the Enterprise Vault cluster services for a Windows Server failover cluster

Preparing to cluster Enterprise Vault with Windows Server Failover Clustering

The following procedure outlines the preparations that you must take before you can cluster a new or existing Enterprise Vault installation in a failover cluster. See your Microsoft documentation for detailed information.

To prepare to cluster Enterprise Vault with Windows Server Failover Clustering

1   Decide on the operation mode for your cluster, including:

- The number of primary nodes (each normally hosting an Enterprise Vault cluster server).

- The number of failover nodes.

- Which nodes are to be the preferred owners of each cluster server.

2   Ensure that your setup meets the requirements.

See "Required software and restrictions on clustering Enterprise Vault with Windows Server Failover Clustering" on page 267.

3   Set up the shared disks and volumes for the cluster.

See "Setting up the shared disks and volumes for a Windows Server failover cluster" on page 272.

4   Use Failover Cluster Manager to create the cluster and to add the primary and failover nodes.

5   Set up a cluster service, including the required resources, for each Enterprise Vault cluster server.

See "Setting up the Enterprise Vault cluster services for a Windows Server failover cluster" on page 273.

Setting up the shared disks and volumes for a Windows Server failover cluster

You must set up shared storage and volumes for the cluster, ready to accept the shared data. Each Enterprise Vault cluster server requires one or more volumes in which to store the following:

- MSMQ data

- Enterprise Vault Storage queue

- Indexing service data

- Storage service data (vault store partitions)

- Shopping service data

- PST holding folders

- SMTP holding folder

- EMC Centera staging areas

It is good practice for MSMQ data, the Enterprise Vault Storage queue, Indexing service data, Storage service data, and the SMTP holding folder to each have a separate storage device resource. Placing them on the same drives may result in degraded performance. You can however place MSMQ data and the Enterprise Vault Storage queue on the same storage device resource because MSMQ and the Storage queue have similar performance.

For performance reasons we recommend that you take care to place the shared data in suitable locations. Some data requires separate disks.

See the *Enterprise Vault Performance Guide* at http://www.veritas.com/docs/000005725 for details.

For example, if you are setting up two Enterprise Vault cluster servers, EVSERVER1 and EVSERVER2, you might allocate the shared storage for the cluster as follows:

Cluster	■ Volume H: Quorum data
EVServer1	■ Volume I: MSMQ data
	■ Volume J: Indexing service data
	■ Volume K: Vault store data
	■ Volume L: PST holding folders, Shopping service data, EMC Centera staging areas
	■ Volume M: Enterprise Vault Storage queue
	■ Volume N: SMTP holding folder
EVServer2	■ Volume I: MSMQ data
	■ Volume J: Indexing service data
	■ Volume K: Vault store data
	■ Volume L: PST holding folders, Shopping service data, EMC Centera staging areas
	■ Volume M: Enterprise Vault Storage queue
	■ Volume N: SMTP holding folder

Note the following when setting up the shared disks and volumes:

■ You must configure the storage for different cluster services on different storage devices, as only one server can connect to a storage device at a time.

■ Configure shared disks and volumes such that the required nodes will be able to access the clustered disk resources on failover. For example, in a 2+1 configuration, the failover node must have access to the quorum data volume, plus all the volumes that the cluster servers use.

Setting up the Enterprise Vault cluster services for a Windows Server failover cluster

You must create and configure a cluster service for each cluster server that the cluster is to support. For example, for an N+M cluster, you require N cluster services. We recommend that Enterprise Vault clusters contain only resources related to Enterprise Vault.

Note: The Enterprise Vault Configuration wizard does not support cluster services that contain multiple client access point resources or IP address resources.

Table 36-1   Required resources for Enterprise Vault cluster services

Resource type	Dependencies	Parameters	Comment
Storage Device or Volume Manager Disk Group	None	Specify the required disk volume.	Configure one disk resource for each volume you have set up for use by this cluster server.
Client Access Point	IP Address resource	■ Use the cluster service name as the client access point. ■ We recommend that you check **DNS Registration Must Succeed**. ■ Check **Enable Kerberos Authentication**. This is required by the Message Queuing resource.	Configure one client access point resource.
Message Queuing	■ The Storage Device resource for this cluster server's MSMQ data ■ The Client Access Point resource	None	Configure one message queuing resource.

To set up the Enterprise Vault cluster services for a Windows Server failover cluster

1   Start Windows **Failover Cluster Manager**.

2   In the left pane of Failover Cluster Manager, right-click **Roles** and click **Configure roles**.

3   On the **Select Role** page of the **High Availability Wizard**, select **Other Server** and click **Next**.

4 On the **Client Access Point** page of the **High Availability Wizard**, enter the cluster network name and IP address and click **Next**.

5 On the **Select Storage** page of the **High Availability Wizard**, select the cluster disks that you set up previously.

See "Setting up the shared disks and volumes for a Windows Server failover cluster" on page 272.

6 Add the required resources to the cluster service. Add one resource of each resource type listed in the table, except where noted. We recommend you use the following naming format for the resources:

7 On the **Confirmation** page click **Next**. The wizard completes the configuration automatically.

8 On the **Summary** page click **Finish**.

9 In Failover Cluster Manager right-click the cluster that you created and click **Add Resource > More Resources > Message Queuing**.

10 Right-click the new resource and click **Properties**.

11 In the **New Message Queuing Properties** window, click the **Dependencies** tab.

12 Add the MSMQ disk and client access point to the resource list and then click **OK**.

13 The service is now configured. Check that the cluster can fail over between nodes without error.

Configuring Enterprise Vault in a Windows Server failover cluster

This chapter includes the following topics:

- About configuring Enterprise Vault in a Windows Server failover cluster

- Setting up a new Enterprise Vault installation with Windows Server Failover Clustering support

- Converting an existing Enterprise Vault installation to a Windows Server failover cluster

- Modifying an existing Enterprise Vault cluster

About configuring Enterprise Vault in a Windows Server failover cluster

This chapter describes:

- Setting up a new Enterprise Vault installation with cluster support.

- Converting an existing Enterprise Vault installation to a cluster.

- Modifying an existing Enterprise Vault cluster to add another Enterprise Vault clustered server or failover node, or to add more shared storage.

Before proceeding, you must have performed the preparatory steps for clustering.

See "Preparing to cluster Enterprise Vault with Windows Server Failover Clustering" on page 271.

Setting up a new Enterprise Vault installation with Windows Server Failover Clustering support

This section describes how to set up a first-time Enterprise Vault installation as a cluster.

Note: If during the running of the Enterprise Vault Configuration wizard you receive an error that is related to the configuring of the Enterprise Vault Monitoring database, complete the wizard and refer to Troubleshooting configuration of the Enterprise Vault Monitoring database.

To set up a new Enterprise Vault installation with Windows Server Failover Clustering support

1 Install Enterprise Vault on all the nodes that are to run Enterprise Vault, both primary and failover, but do not run the Enterprise Vault Configuration wizard on any node at this stage.

   If Enterprise Vault SMTP Archiving is required in the cluster, you must also install the SMTP Archiving components on each node.

Caution: The Enterprise Vault installation folder on all nodes should be the same. For example, if you install Enterprise Vault in the `C:\Program Files (x86)\Enterprise Vault` folder on the primary node, you must install it in the `C:\Program Files (x86)\Enterprise Vault` folder on the failover node. If you do not do this, you may experience problems when you configure Enterprise Vault on the failover node.

---

2 Configure the Enterprise Vault servers that are to act as clustered servers.

   See "Configuring a new Enterprise Vault server with Windows Server Failover Clustering support" on page 278.

3 Configure Enterprise Vault on the nodes that are to act as failover nodes.

   See "Configuring a failover node in a Windows Server failover cluster" on page 282.

4 Test the cluster to ensure the failovers work as planned.

Configuring a new Enterprise Vault server with Windows Server Failover Clustering support

Perform one of the following procedures on a newly installed Enterprise Vault server to configure it as an Enterprise Vault server with cluster support. Choose the appropriate procedure depending on which of the following you want to do:

- Create an Enterprise Vault Directory on the Enterprise Vault server. This is mandatory for the first Enterprise Vault server you configure. The Directory is a container for Enterprise Vault Sites, which define common settings for Enterprise Vault servers. Every Enterprise Vault server must belong to just one Site. The configuration process creates a new Site in the new Directory and adds the Enterprise Vault server to that Site. It also creates a Directory database on the SQL server you specify.

- Join an Enterprise Vault Directory on another Enterprise Vault server. You can add the Enterprise Vault server to an existing Enterprise Vault Site in the Directory, or create a new Site in the Directory and add the Enterprise Vault server to that.

Follow this procedure if you want to create a new Enterprise Vault Directory. You must use this procedure if there is no existing Directory.

To configure a server with a new Directory

1 Use Failover Cluster Manager to ensure that a suitable cluster service that you prepared earlier is online on the Enterprise Vault server node.

2 Start the Enterprise Vault Configuration wizard on the server node.

3 Click **Create a new Enterprise Vault server with Cluster support**, and then click **Next**.

4 The wizard lists the cluster services that are currently online on this node. Select the prepared cluster service, and then click **Next**.

5 On the next Wizard page you can choose whether to create a new Vault Directory or to use an existing Vault Directory. Select **Yes** to create a new Vault Directory on this computer. This creates a new Enterprise Vault site. Click **Next**.

6 Select the language you want Enterprise Vault to use when populating the default settings in the Administration Console. Then click **Next**.

7 The wizard asks for details of the Vault Service account. This is the account you created earlier as part of the preinstallation tasks for Enterprise Vault. Use the format *domain_name\username*. Alternatively, click the **...** button and browse for the account.

Enter the password details and then click **Next**.

The wizard then displays a couple of messages relating to the Vault Service account having been granted user rights on the computer, and the creation of the Directory Service.

8 When prompted, enter the location of the SQL Server to use for the Enterprise Vault Directory database and click **Next**.

9 The wizard prompts you to enter the locations for the Enterprise Vault Directory database and transaction log. For performance reasons it is good practice to place these on separate disks. If default locations are shown, change them if they are incorrect. If you specified a SQL server on a remote computer, the paths must be valid paths on that computer, such as `\\DC\C$\Program Files\Microsoft SQL Server\MSSQL\Data.`

Then click **Next**.

10 When prompted, enter the location of the SQL Server to use for the Enterprise Vault Monitoring database. Leave **Start Monitoring immediately** selected to begin monitoring as soon as the configuration is complete on this Enterprise Vault server. Then click **Next**.

11 The wizard prompts you to enter the locations for the Enterprise Vault Monitoring database and transaction log. For performance reasons it is good practice to place these on separate disks. If default locations are shown, change them if they are incorrect. If you specified a SQL server on a remote computer, the paths must be valid paths on that computer.

Then click **Next**.

12 The wizard then prompts you for a name and description for the new Vault Site.

A **Vault Site alias** is created automatically. This is the client access point for the cluster service that you selected in step 4.

13 Click **Next** to continue.

14 The wizard confirms the Enterprise Vault Site and Enterprise Vault Directory computer you have selected. It prompts you to specify the **Computer Alias** for the computer you are currently configuring.

Enter the client access point for the Enterprise Vault cluster service that you selected in step 4, and click **Next** to update the Enterprise Vault Directory.

15 There is a prompt that asks whether you are sure that you do not want to use a DNS alias. Click **Yes** and then click **Next** again on the wizard page.

16 The wizard lists the Enterprise Vault services that are to be added to this computer. Click **Next** to add the services.

17 The wizard lists the Enterprise Vault services that it has now added. Note that in a cluster configuration you are not allowed to add or remove services. Click **Next** to continue.

18 The wizard shows a summary of the services it has added. Click **Next** to continue.

19 The Configuration wizard indicates that it needs to create cluster resources for each of the Enterprise Vault services.

20 The final wizard page displays a list of the actions the wizard has performed, and the results. Select **Run the Enterprise Vault Administration Console** and then click **Finish** to exit the wizard.

Note: Do not select the option to run the Getting Started wizard.

---

21 Follow the steps below to set the path to the index metadata folder, which must be on a shared drive in the cluster. The index metadata folder is the folder in which Enterprise Vault stores indexing configuration data and reporting data.

- Bring the Enterprise Vault Directory service and Admin service online.

- In the left pane of the Enterprise Vault Administration Console, browse to **Enterprise Vault Servers** > **EVServer.*domain*.local** > **Services**.

- In the right pane, right-click **Enterprise Vault Indexing Service**, and then click **Properties**.

- On the **General** tab of the Service Properties dialog box, set the **Index metadata location** path to that of the shared drive in the cluster.

- Click **OK** to save the change that you have made, and then restart the Indexing service.

Follow this procedure if you want to join an existing Directory. The existing Directory does not need to be in the cluster.

To configure a server and join an existing Directory

1 Use Failover Cluster Manager to ensure that a suitable cluster service that you prepared earlier is online on the Enterprise Vault server node.

2 Start the Enterprise Vault Configuration wizard on the Enterprise Vault server node.

3 Click **Create a new Enterprise Vault server with Cluster support**, and then click **Next**.

4 The wizard lists the cluster services that are currently online on this node. Select the prepared cluster service, and then click **Next**.

5 On the next wizard page, select **No** to join an Enterprise Vault Directory on another Enterprise Vault server, and specify the DNS alias for the remote Enterprise Vault server.

Click **Next** and continue.

6 On the next wizard page, do one of the following:

- Select the option to create a new Vault Site in the remote Enterprise Vault Directory.

- Click **Next** and continue from step 7.

- Or select the option to join an existing Vault Site in the remote Enterprise Vault Directory, and select a Vault Site from the list displayed.

- Then click **Next** and continue from step 10.

7 The wizard prompts you for a name and description for the new Vault Site.

8 The vault site alias, which is created automatically when the first Enterprise Vault server is added to the site, will be the DNS alias for the remote Enterprise Vault server you specified in step 6.

9 Click **Next** to continue.

10 The wizard confirms the Enterprise Vault Site and Enterprise Vault Directory computer you have selected. It prompts you to specify the **DNS Alias** for the computer you are currently configuring.

11 Enter the client access point of the Enterprise Vault cluster service.

12 Click **Next** to update the Enterprise Vault Directory.

13 The wizard lists the Enterprise Vault services that are to be added to this computer. Click **Next** to add the services.

14 The wizard lists the Enterprise Vault services that it has now added, giving you the option to check their properties. Note that in a cluster configuration you are not allowed to add or remove services. Click **Next** to continue.

15 The wizard displays the storage locations for the Indexing and Shopping services. These locations default to the first disk resource in the selected cluster service. If the locations are suitable, click **Next**. If you want to specify different storage locations, click **Back** and edit the properties of the service. The wizard displays a warning if you try to modify these to a local location such as `E:\Shopping`.

16 The Configuration wizard indicates that it needs to create cluster resources for each of the Enterprise Vault services.

17 The final wizard page displays a list of the actions the wizard has performed, and the results. Click **Finish** to exit the wizard.

18 Follow the steps below to set the path to the index metadata folder, which must be on a shared drive in the cluster. The index metadata folder is the folder in which Enterprise Vault stores indexing configuration data and reporting data.

- Bring the Enterprise Vault Directory service and Admin service online.

- In the left pane of the Enterprise Vault Administration Console, browse to **Enterprise Vault Servers** > **EVServer.*domain*.local** > **Services**.

- In the right pane, right-click **Enterprise Vault Indexing Service**, and then click **Properties**.

- On the **General** tab of the Service Properties dialog box, set the **Index metadata location** path to that of the shared drive in the cluster.

- Click **OK** to save the change that you have made, and then restart the Indexing service.

Configuring a failover node in a Windows Server failover cluster

Perform this procedure on the nodes that are to act as failover nodes.

To configure a failover node in a Windows Server failover cluster

1 Ensure that the Enterprise Vault cluster service is online on a different node in the cluster. The cluster service must not be online on the node that you are configuring. The node that you are configuring must be a possible failover node for the resources.

2 If the SMTP service is configured in the cluster resource group, then the failover node must have Enterprise Vault SMTP Archiving components installed.

3 Start the Enterprise Vault Configuration wizard on the node.

4 Click **Configure the node as a failover node for an existing clustered server**, and then click **Next**.

5 The wizard prompts you for the name of the Enterprise Vault cluster service for which you want to add the node as a failover node.

Select the Enterprise Vault cluster service that is configured to fail over to this node and then click **Next**.

6 On the next wizard page, enter the password for the Vault Service account, and then click **Next**.

7 The next wizard page lists the actions the wizard will take if you proceed. To continue click **Next**, then click and then click **OK** to confirm the actions taken.

8 The final wizard page displays a list of the actions the wizard has performed, and the results. Click **Finish** to exit the wizard.

Troubleshooting configuration of the Enterprise Vault Monitoring database

If during the running of the Enterprise Vault Configuration wizard you receive errors indicating that configuring the Enterprise Vault Monitoring database has failed, complete the configuration wizard and then run the Monitoring Configuration Utility to configure the Monitoring database and the Monitoring agents manually.

For information on how to do this, see the following Enterprise Vault technical note on the Veritas Support website:

http://www.veritas.com/docs/000033005

The technical note also describes how to troubleshoot issues with Monitoring agents.

Examples of Enterprise Vault installations in various Windows Server Failover Clustering modes

These examples describe how to set up first-time installations of Enterprise Vault in various cluster operation modes.

Clustering Enterprise Vault in an active/passive failover configuration

This example describes setting up a new Enterprise Vault installation of an "active/passive" failover pair.

Figure 37-1 illustrates a single failover pair, consisting of a primary node, NODEA, running the Enterprise Vault cluster server EVSERVER1, plus a dedicated failover node, NODEB.

Figure 37-1   Failover pair configuration
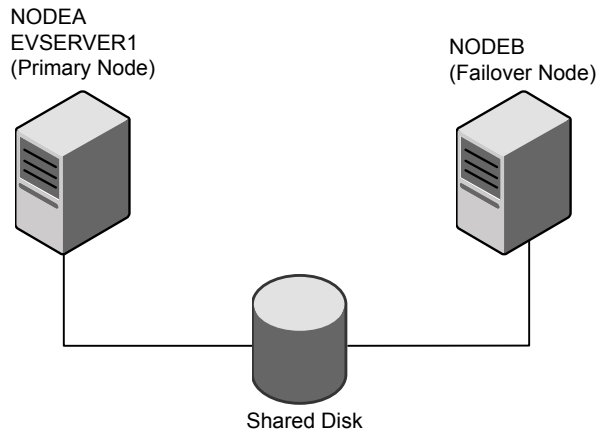
To cluster Enterprise Vault in an active/passive failover configuration

1   Prepare for clustering Enterprise Vault as follows:

   ■   Create a node for the primary server (NODEA).

   ■   Create a node for the failover server (NODEB).

   ■   Create a cluster service EVSERVER1 for the cluster server, with the preferred owners set to NODEA followed by NODEB.

   ■   Add the required resources to cluster service, ensuring that they have NODEA and NODEB as their possible owners.

   ■   Create a DNS entry for the cluster server.

2   Install Enterprise Vault on NODEA and NODEB, without running the Enterprise Vault Configuration wizard.

3   On NODEA, run the Enterprise Vault Configuration wizard and choose to configure a new Enterprise Vault server with cluster support. Select EVSERVER1 as the cluster service in which to create the Enterprise Vault service resources. A Vault Site alias will be created automatically.

4   On NODEB, run the Enterprise Vault Configuration wizard and choose to configure a failover node for an existing clustered server. Select EVSERVER1 as the cluster service for which you want to add this node as a failover node.

5   Test the failover from NODEA to NODEB.

Clustering Enterprise Vault in a 2+1 configuration without "any-to-any" support

Figure 37-2 illustrates a configuration in which there is a single spare node in addition to the two nodes on which the Enterprise Vault servers are running.

Figure 37-2   2+1 configuration without "any-to-any" support
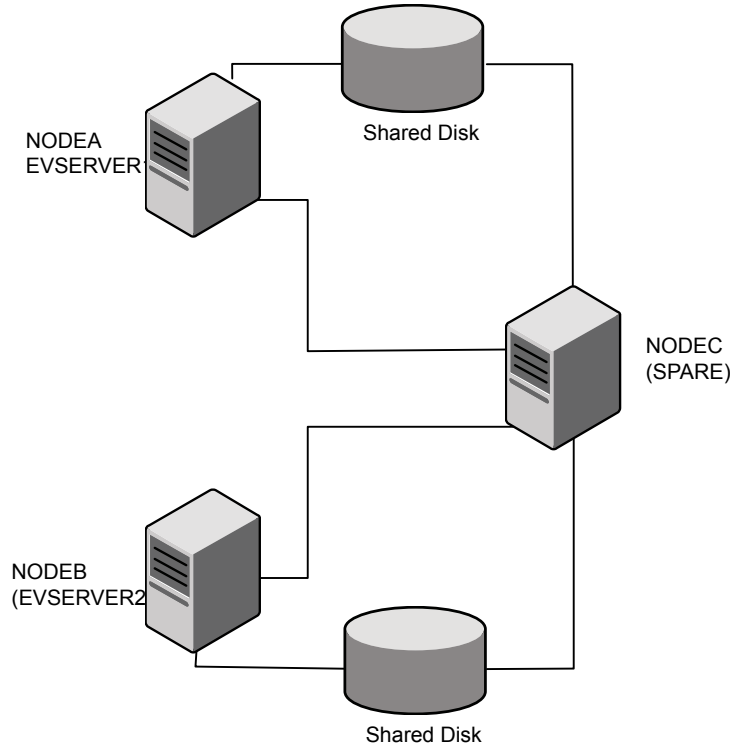
If either NODEA or NODEB fails, the virtual Enterprise Vault server running on that node can fail over to NODEC. This is not an "any-to-any" configuration so if a node fails the resources must be moved back after the node is recovered, in order to return to high availability.

To cluster Enterprise Vault in a 2+1 configuration without "any-to-any" support

1   Prepare for clustering as follows:

  ■   Add three nodes to the cluster (NODEA, NODEB, NODEC).

  ■   Create two cluster services (EVSERVER1, EVSERVER2), and add the required resources to each service.

■ Configure the services and resources so that the following nodes are the preferred owners, in the order shown:

EVSERVER1   NODEA, NODEC

EVSERVER2   NODEB, NODEC

■ Create DNS entries for the cluster servers EVSERVER1 and EVSERVER2.

2 Install Enterprise Vault on NODEA, NODEB, and NODEC, but do not run the Enterprise Vault Configuration wizard.

3 On NODEA, run the Enterprise Vault Configuration wizard and choose to configure a new Enterprise Vault server with cluster support. Select EVSERVER1 as the cluster service in which to create the Enterprise Vault service resources. A Vault Site alias will be created automatically using the cluster server alias.

4 On NODEB, run the Enterprise Vault Configuration wizard and choose to configure a new Enterprise Vault server with cluster support. Select EVSERVER2 as the cluster service in which to create the Enterprise Vault service resources. A Vault Site alias will be created automatically using the cluster server alias.

5 On NODEC, run the Enterprise Vault Configuration wizard, and choose to configure a failover node for the existing clustered server. Select either EVSERVER1 or EVSERVER2 as the cluster service. This node will be configured as a failover node for both EVSERVER1 and EVSERVER2.

6 Test the cluster to confirm that if NODEA fails, the EVSERVER1 resources fail over successfully to NODEC. Then return the EVSERVER1 resources to NODEA and confirm that if NODEB fails, the EVSERVER2 resources fail over successfully to NODEC.

Clustering Enterprise Vault in a 2+1 "any-to-any" configuration

This second option for a 2+1 operation mode involves configuring the Enterprise Vault cluster servers EVSERVER1 and EVSERVER2 to run on any of the three nodes. This has the advantage that, for example, if NODEA fails and EVSERVER1 fails over to NODEC, you can bring NODEA back online to act as the failover node for EVSERVER1 and EVSERVER2.

Figure 37-3   2+1 "any-to-any" configuration
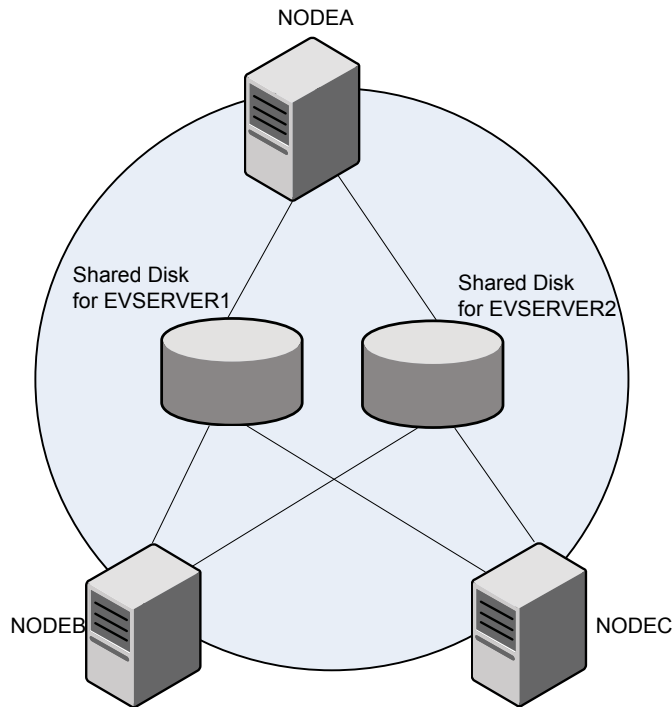
You can extend the setup process for an N+M configuration with any number of primary and failover nodes, up to the total of eight clustered nodes supported by Windows Server Failover Clustering.

To cluster Enterprise Vault in a 2+1 "any-to-any" configuration

1   Prepare for clustering as follows:

- Add three nodes to the cluster (NODEA, NODEB, NODEC).

- Create two cluster services (EVSERVER1, EVSERVER2), and add the required resources to each service.

- Configure the services and resources so that the following nodes are the preferred owners, in the order shown:

   EVSERVER1   NODEA, NODEC, NODEB

EVSERVER2   NODEB, NODEC, NODEA

2   Follow steps 2 to 5 of the 2+1 configuration without "any-to-any" support.

See "Clustering Enterprise Vault in a 2+1 configuration without "any-to-any" support" on page 285.

3   Test the cluster to confirm that if an active node fails, the cluster server fails over to the appropriate node.

4   For example, if you have configured the preferred owners of the cluster services as suggested in step 1:

- Confirm that if NODEA fails, EVSERVER1 fails over successfully to NODEC.

- Then bring NODEA back online as the spare node and confirm that if NODEB fails, EVSERVER2 fails over to NODEA.

Converting an existing Enterprise Vault installation to a Windows Server failover cluster

If you have an existing Enterprise Vault installation on a single, unclustered server, you can convert it to a failover cluster. To be eligible for conversion to a cluster, the existing Enterprise Vault installation must meet the following conditions:

- Enterprise Vault should already be configured in a non-clustered configuration, and it must not already be part of a cluster.

- Enterprise Vault must be configured using DNS aliases rather than fully qualified node names.

- The Enterprise Vault server must have a full set of Indexing, Shopping, Task Controller, and Storage services.

- If Enterprise Vault SMTP Archiving is required, the Enterprise Vault server must have the SMTP Archiving components installed.

- Neither Compliance Accelerator nor Discovery Accelerator must be installed on any server in the planned cluster. These products are not supported within a cluster. However, an unclustered Compliance Accelerator or Discovery Accelerator can reference an Enterprise Vault cluster server.

You can cluster an existing Enterprise Vault installation in any of the operation modes previously described. Note that:

- You can configure a combination of new and existing Enterprise Vault servers as cluster servers, if required.

■ You must perform a new installation of Enterprise Vault on the nodes that are to act as failover nodes.

To convert an existing Enterprise Vault installation to a Windows Server failover cluster

1 Prepare for clustering.

See "Preparing to cluster Enterprise Vault with Windows Server Failover Clustering" on page 271.

2 Install Enterprise Vault on the failover nodes and, if required, on any additional primary nodes you are adding to the existing installation. Do not run the Enterprise Vault Configuration wizard on any node at this stage. For instructions on installing Enterprise Vault, see Sections I and II of this manual.

3 Convert your existing Enterprise Vault servers to servers with cluster support.

See "Converting an existing Enterprise Vault server to a server with Windows Server Failover Clustering support" on page 289.

4 If you are adding any new Enterprise Vault servers, configure the new Enterprise Vault servers as servers with cluster support.

See "Configuring a new Enterprise Vault server with Windows Server Failover Clustering support" on page 278.

5 Configure Enterprise Vault on the failover nodes.

See "Configuring a failover node in a Windows Server failover cluster" on page 282.

6 Test the cluster to ensure the failovers work as planned.

Converting an existing Enterprise Vault server to a server with Windows Server Failover Clustering support

This section describes how to convert an existing Enterprise Vault server to a server with cluster support, including moving data to highly available locations.

To convert an existing Enterprise Vault server to a server with Windows Server Failover Clustering support

1 Ensure that the following items are all on highly available shared storage devices:

■ Indexing service data

■ Shopping service data

■ Vault store partitions

- ■ PST holding folders

- ■ SMTP holding folder *

- ■ EMC Centera staging areas

* The SMTP holding folder is only required if the Enterprise Vault SMTP service is configured as a cluster service in the Enterprise Vault cluster.

If the items are not on highly available shared storage devices, correct the locations in the Enterprise Vault Directory database and then move the associated data to the new locations.

See "Moving Enterprise Vault data to highly available locations" on page 291.

2   Use Failover Cluster Manager to ensure that a suitable cluster service you prepared earlier is online on the Enterprise Vault server node.

3   In Windows, start the Enterprise Vault Convert to Cluster wizard.

4   When the first page of the wizard appears, click **Next** to continue.

5   The wizard makes a number of checks to determine the suitability of the installation for conversion to a cluster. It then displays a warning reminder that, when the wizard has successfully completed, you must update the DNS alias or Hosts file entry that is currently pointing at the physical node, so that it points at the cluster server name.

6   The wizard then displays a list of the current file locations for the Enterprise Vault services and partitions. You must confirm that these locations are all on highly available shared storage devices before continuing. Either select the check box to confirm high-availability, and click **Next** to continue, or click **Cancel** to exit from the wizard and move the required data to highly available locations before running the wizard again.

7   If the wizard detects that there are messages in the Enterprise Vault MSMQ queues, it displays a page indicating the name of each queue and the number of messages on it. The wizard cannot move these messages to the clustered message queues due to permissions constraints. We recommend you cancel from the wizard and leave the services running in a non-clustered environment until Enterprise Vault has cleared the message queues. You can then re-run the Convert to Cluster wizard. If you continue without doing this, the messages remain on the node-specific queues and are not processed. If you want to continue without clearing the queues, select the **Continue converting configuration to a cluster** check box and click **Next**.

8   The wizard lists the cluster services that are currently online on this node. Select the required cluster service, and then click **Next**.

9 The wizard creates the necessary resources, updates the Enterprise Vault services to manual startup, and updates the Directory database tables to remove the local computer name from the computer entry table and the message queue names. The final wizard page displays a list of the actions the wizard has performed, and the results. Click **Finish** to exit the wizard.

10 If you have not already done so, manually update the DNS alias to point at the cluster server name rather than the local node name.

11 Bring the cluster server resources online using Failover Cluster Manager.

Moving Enterprise Vault data to highly available locations

In outline, the procedure for moving the Enterprise Vault data to highly available locations is as follows:

■ Stop the Indexing, Shopping, Storage, and Task Controller services.

■ Make a backup copy of the Enterprise Vault Directory database and data files.

■ Use the Enterprise Vault Administration Console or run a SQL query against the Enterprise Vault Directory to move the data, as described below.

IndexRootPathEntry [IndexRootPath]	■ Move the contents of this location to a highly available location.
	■ Update the database using SQL to point at the new location.
	
	The SQL to view the current location is as follows:
	
	`SELECT *`
	`FROM IndexRootPathEntry`
	`WHERE (IndexRootPathEntryId = '<ID FROM`
	`LOG FILE>')`
	
	The SQL to update the location is as follows:
	
	`UPDATE IndexRootPathEntry`
	`SET IndexRootPath = '<THE NEW LOCATION>'`
	`WHERE (IndexRootPathEntryId = '<ID FROM`
	`LOG FILE>')`

PartitionEntry [AccountName]	■ Move the pool entry authorization (`.pea`) file to a highly available location. ■ Use the Enterprise Vault Administration Console to view the properties of the EMC Centera partition and then, on the **Connection** tab, edit the **Pool Entry Authorization File Location** box to point at the new location.

PartitionEntry [PartitionRootPath]	■ Move the contents of this location to a highly available location.
	■ Update the database using SQL to point at the new location.

The SQL to view the current location is as follows:

```
SELECT *
FROM PartitionEntry
WHERE (PartitionEntryId = '<ID FROM LOG
FILE>')
```

The SQL to update the location is as follows:

```
UPDATE PartitionEntry
SET PartitionRootPath = '<THE NEW
LOCATION>'
WHERE (PartitionEntryId = '<ID FROM LOG
FILE>')
```

PartitionEntry/Locations [SecondaryLocation]	■ Move the secondary storage files to a highly available location.
	■ Update the database using SQL to point at the new location.

The SQL to view the current location is as follows:

```
SELECT *
FROM PartitionEntry
INNER JOIN Locations ON
PartitionEntry.SecondaryLocation =
Locations.LocationIdentity
WHERE (PartitionEntry.PartitionEntryId =
'<ID FROM LOG FILE>')
```

The SQL to update the location is as follows:

```
UPDATE Locations
SET Location = '<NEW LOCATION>'
WHERE LocationIdentity =
(SELECT SecondaryLocation FROM
PartitionEntry
WHERE PartitionEntryId = '<ID FROM LOG
FILE>')
```

PartitionEntry
[StagingRootPath]

- Move the contents of this location to a highly available location.
- Update the database using SQL to point at the new location.

The SQL to view the current location is as follows:

```
SELECT *
FROM PartitionEntry
WHERE (PartitionEntryId = '<ID FROM LOG
FILE>')
```

The SQL to update the location is as follows:

```
UPDATE PartitionEntry
SET StagingRootPath = '<THE NEW LOCATION>'
WHERE (PartitionEntryId = '<ID FROM LOG
FILE>')
```

PSTMigratorTask
[MigrationDirectory]

- Move the contents of this location to a highly available location.
- Use the Enterprise Vault Administration Console to view the properties of the PST Migrator Task and update the Temporary files folder.

ShoppingServiceEntry
[ShoppingRootPath]

- Move the contents of this location to a highly available location.
- Use the Enterprise Vault Administration Console to edit the Shopping service location to the new highly available location.

SiteEntry
[PSTHoldingDirectory]

- Move the contents of this location to a highly available location.
- Use the Enterprise Vault Administration Console to view the site properties and update the PST Holding Folder property to point at the new location.

SmtpArchivingTask
[HoldingFolder]

- Move the contents of this location to a highly available location.
- Use the Vault Administration Console to view the properties of the SMTP Archiving task, and update the SMTP Holding Folder property to point at the new location.

Modifying an existing Enterprise Vault cluster

This section describes how to modify an existing Enterprise Vault cluster to do the following:

- Add a node to host a new Enterprise Vault cluster server or to act as a failover node.

- Add shared storage for a cluster server.

- Add the SMTP service to an existing cluster.

Adding a node to an existing Windows Server failover cluster

You may want to add a node to an existing Enterprise Vault cluster to host a new Enterprise Vault cluster server or to act as a failover node.

To add a node to an existing Windows Server failover cluster

1   Share the required disk volumes on the new node.

2   Use Failover Cluster Manager to add the node to the cluster.

3   If you are adding a new Enterprise Vault cluster server, prepare a new cluster service and add the required resources.

   See "Setting up the Enterprise Vault cluster services for a Windows Server failover cluster" on page 273.

4   Specify the new node as a possible owner of all resources in all the cluster services that are required to run on it.

5   Add the new node at a suitable position in the preferred owners list of any cluster service that is required to run on it.

6   Install Enterprise Vault on the node.

7   Run the Enterprise Vault Configuration wizard and choose either **Create a new Enterprise Vault server with Cluster support** or **Configure the node as a failover node for an existing clustered server**, as required.

8   Test the modified cluster to confirm that failovers to or from the new node work as planned.

Adding shared storage to an existing Windows Server failover cluster for an Enterprise Vault cluster server

You may want to add shared storage to an existing Enterprise Vault cluster to provide more storage for an Enterprise Vault cluster server.

To add shared storage to an existing Windows Server failover cluster for an Enterprise Vault cluster server

1   Set up the additional shared disks and volumes, sharing the volumes on the nodes that require access to them.

2   For the cluster server that is to use the new storage:

    ■   Add a Storage Device resource to the cluster service for each new volume.

        Note: It is important to make the Storage Device resource dependent on the Enterprise Vault Server Instance resource. This prevents two Enterprise Vault cluster servers from running on the same clustered node in an unsupported "active/active" configuration.

        The Enterprise Vault Server Instance resource is not reliant on any disk storage; it does not store data on any disk that is configured within the cluster group.

    ■   Change the Properties of the **Admin Service resource** to add a dependency on each new Storage Device resource.

3   Specify the required nodes as possible owners for the new Storage Device resources, according to your cluster operation mode.

4   Test the modified cluster to confirm that the Enterprise Vault cluster server can access the new shared storage successfully before and after failover.

Adding Enterprise Vault SMTP Archiving to an existing clustered Enterprise Vault server

You may want to add the Enterprise Vault SMTP Archiving feature to an existing Enterprise Vault cluster.

To add SMTP Archiving to an existing clustered Enterprise Vault server

1 Install the Enterprise Vault server and the SMTP Archiving components on all the nodes in the Enterprise Vault cluster.

2 Create a new SMTP Archiving task on the clustered Enterprise Vault server. Before Enterprise Vault creates the SMTP Archiving task, it detects the presence of the Enterprise Vault SMTP service on the active node and other nodes, and configures the SMTP service as generic service resource.

3 If Enterprise Vault does not detect the SMTP Archiving components on some of the cluster nodes, it displays a list of the nodes affected, and a warning to install the SMTP Archiving components. You can continue to create the SMTP Archiving task, and install the SMTP Archiving components on the listed nodes at a later time. If you do not install the components on all the nodes in the cluster, Enterprise Vault cannot fail over to the nodes where the components are not installed.

Troubleshooting clustering with Windows Server Failover Clustering

This chapter includes the following topics:

- About this chapter

- Enterprise Vault event messages and the failover cluster log

- Resource ownership and dependencies when configuring Enterprise Vault in a failover clustered environment

- Registry replication on failover clustered nodes

- Viewing the clustered message queues for an Enterprise Vault cluster server

- Starting and stopping Enterprise Vault services in a Windows Server Failover Clustering environment

- Potential failover issue in a Windows 2012 or later cluster

About this chapter

This chapter describes how to troubleshoot problems with Enterprise Vault in a Windows Server failover cluster.

Enterprise Vault event messages and the failover cluster log

There are no specific Enterprise Vault event messages for clustering, but Enterprise Vault continues to write messages to the standard Application and Enterprise Vault event logs, so check these for errors.

If any failover cluster resources fail to come online, check the event logs and also the cluster log text file, typically `C:\WINDOWS\Cluster\cluster.log`.

To see the operations related to Enterprise Vault, search for "Enterprise Vault".

Resource ownership and dependencies when configuring Enterprise Vault in a failover clustered environment

Resource ownership must be set up correctly to avoid problems when configuring Enterprise Vault in a cluster. The Configuration wizard only lists a cluster service for selection if every resource in it has the node on which you are running the wizard listed as a possible owner.

Resource ownership and resource dependencies must also be set up correctly to ensure failovers work as planned.

See Table 36-1 on page 274.

The Enterprise Vault Configuration wizard sets up the dependencies for the Enterprise Vault service resources and the Server Instance resource when it adds them to the cluster service.

If you add a shared disk to an existing cluster you must ensure you set up the disk resource and dependencies correctly.

See "Adding shared storage to an existing Windows Server failover cluster for an Enterprise Vault cluster server" on page 294.

Registry replication on failover clustered nodes

As part of configuring the cluster server, the Configuration wizard sets up a registry checkpoint on the Admin service resource, to provide the required registry replication on the clustered nodes.

If you suspect problems with registry entries related to an Enterprise Vault cluster server, view the checkpoint to confirm it is set up correctly. Enter the following command using the Windows command line utility `cluster`:

```
cluster resource EnterpriseVaultAdminService /check
```

where `EnterpriseVaultAdminService` is the name of the Admin service resource, for example EVSERVER1-EnterpriseVaultAdminService.

Viewing the clustered message queues for an Enterprise Vault cluster server

By default, in a clustered Enterprise Vault installation, the Computer Management snap-in does not show the Enterprise Vault message queues. Instead, the snap-in shows the queues for the local computer only.

To view the clustered message queues for an Enterprise Vault cluster server

1   Ensure that the Enterprise Vault cluster server is online on the node from which you want to view the queues.

2   Open a Command Prompt window with administrator privileges.

3   In the Command Prompt window, change to the Enterprise Vault installation folder (for example, `C:\Program Files (x86)\Enterprise Vault`).

4   Enter the following command:

```
ClusterCompMgmt
```

5   In the Computer Management snap-in, expand **Services and Applications** and then expand **Message Queuing**. The Enterprise Vault message queues are listed under **Private Queues**.

Starting and stopping Enterprise Vault services in a Windows Server Failover Clustering environment

In a clustered environment, the clustering software must have control of the Enterprise Vault services. To allow this, the Enterprise Vault Configuration wizard sets the startup of these services to manual. Do not attempt to change the startup to automatic.

If a service starts or stops outside of the control of the cluster software, the cluster software assumes that this is due to a change in system condition. For example, if

a service stops, the cluster software assumes a failure and tries to restart the service or initiate a failover.

You should not attempt to start or stop Enterprise Vault services, except through the cluster software in one of the following ways:

- Use Failover Cluster Manager to bring the associated service resource online or offline.

- Use the Windows command-line utility `cluster`. For the syntax of this command, open a Command Prompt window and enter:

  `cluster /?`

  For more details, see the following article on the Microsoft website:

  http://technet2.microsoft.com/WindowsServer/en/library/
  8da99e1e-619f-4deb-acf0-cd8d61ac2ed01033.mspx

To help prevent the starting and stopping of services by other means, Enterprise Vault behaves as follows in a clustered configuration:

- The Enterprise Vault Administration Console buttons for starting and stopping services are unavailable.

- You cannot start or stop services using the EVService utility. However, you can continue to use EVService to control tasks.

- Enterprise Vault blocks attempts to start Enterprise Vault services using the Windows Service Control Manager, and logs an event message. However, Enterprise Vault cannot block the stopping of services using Windows Service Control Manager, so be careful to avoid this.

Potential failover issue in a Windows 2012 or later cluster

During an unplanned shutdown of the active node in a Windows Server 2012 or later cluster, the Enterprise Vault Server Instance resource may not fail over properly to the passive node at the first attempt. However, this should eventually occur according to the timeout and restart policy settings that you have configured for the cluster. For the period that the Enterprise Vault Server Instance resource is offline, so too is the entire Enterprise Vault resource group.

To resolve the issue, open the properties dialog box for the Enterprise Vault Server Instance resource and, on the **Advanced Policies** tab, check **Run this resource in a separate Resource Monitor**.

Automatically preparing an Enterprise Vault server

This appendix includes the following topics:

■ About automatically preparing an Enterprise Vault server

■ Windows features enabled automatically by the 'Prepare my system' option

■ Running the 'Prepare my system' option

About automatically preparing an Enterprise Vault server

The Enterprise Vault Install Launcher **Prepare my system** option automatically checks which Windows features are enabled and adds other features as required.

Windows features enabled automatically by the 'Prepare my system' option

The Enterprise Vault Install Launcher **Prepare my system** option automatically installs all the Windows features and roles that are required by an Enterprise Vault server.

Table A-1 lists the Windows 2012 features that are enabled by **Prepare my system** in the Install Launcher.

Table A-1   Windows 2012 features enabled by **Prepare my system** in the Install Launcher

Path	Feature
\	.NET Framework 4.5 Features
\	Windows TIFF IFilter
\.NET Framework 3.5 Features	.NET Framework 3.5
	HTTP Activation
	Non-HTTP Activation
\.NET Framework 4.5 Features\WCF Services	Named Pipes Activation
	TCP Activation
\Application Server\Windows Process Activation Service Support\	Named Pipes Activation
	TCP Activation
\File Services	File Server Resource Manager
\Message Queuing\Message Queuing Services	Message Queuing Server
\Web Server (IIS)	Web Server
\Web Server (IIS)\Web Server	.NET Extensibility 3.5
\Web Server (IIS)\Web Server\Application Development	ISAPI Extensions
	ISAPI Filters
	ASP
	ASP.NET 3.5
	ASP.NET 4.5
\Web Server (IIS)\Web Server\Common HTTP Features	Default Document
	Directory Browsing
	HTTP Errors
	HTTP Redirection
	Static Content

Table A-1	Windows 2012 features enabled by **Prepare my system** in the Install Launcher *(continued)*

Path	Feature
\Web Server (IIS)\Web Server\Health and Diagnostics	HTTP Logging
	Logging Tools
	Request Monitor
	Tracing
\Web Server (IIS)\Web Server\Management Tools	IIS Management Console
	IIS Management Scripts and Tools
	Management Service
\Web Server (IIS)\Web Server\Performance	Static Content Compression
\Web Server (IIS)\Web Server\Security	Basic Authentication
	IP and Domain Restrictions
	Request Filtering
	URL Authorization
	Windows Authentication

Running the 'Prepare my system' option

To run the Prepare my system option

1   Load the Enterprise Vault media on to the server.

2   If Windows AutoPlay is enabled on the server, Windows shows an AutoPlay dialog box. Click **Run Setup.exe**.

   If AutoPlay is not enabled, use Windows Explorer to open the root folder of the installation media and then double-click the file `Setup.exe`.

   The **Install Launcher** opens.

3   In the list in the left pane of the Install Launcher, click **Enterprise Vault**.

4   Click **Server Preparation**.

5   Click **Prepare my system**. The Windows features are added immediately, with no further prompts. The server may restart automatically after the features have been added.

Index