Symantec Enterprise Vault™

Setting up File System Archiving (FSA)

11.0

Symantec

Symantec Enterprise Vault: Setting up File System Archiving (FSA)

Last updated: 2014-11-18.

Legal Notice

Symantec Corporation
350 Ellis Street, Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to help you resolve specific problems with a Symantec product. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information

- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our Technical Support web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apj@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Chapter 1

About this guide

This chapter includes the following topics:

Introducing this guide

This guide describes how to set up Enterprise Vault so that you can archive files that are held on network file servers.

The guide assumes that you know how to administer the following:

- Microsoft Windows Server
- Your file server hardware and software
- Your archive storage hardware and software

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
Symantec 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: ■ On the Windows **Start** menu, click **Start** > **Programs** > **Enterprise Vault** > **Documentation**. ■ 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 Exchange Server Archiving	Describes how to archive items from Microsoft Exchange user mailboxes, journal mailboxes, and public folders.
Setting up Domino Server Archiving	Describes how to archive items from Domino mail files and journal databases.
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 to Internet mail archives.
Setting up SharePoint Server Archiving	Describes how to archive content from Microsoft SharePoint servers.
Setting up SMTP Archiving	Describes how to archive SMTP messages from other messaging servers.
Administrator's Guide	Describes how to perform day-to-day administration procedures.

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

Document	Comments
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.
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.
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.symantec.com/docs/TECH38537

“How To” articles on the Symantec Support website

Most of the information in the Enterprise Vault administration guides is also available online as articles on the Symantec Support website. You can access these articles by searching the Internet with any popular search engine, such as Google, or by following the procedure below.

To access the "How To" articles on the Symantec Support website

1. Type the following in the address bar of your web browser, and then press **Enter**:

   http://www.symantec.com/business/support/all_products.jsp

2. In the Supported Products A-Z page, choose the required product, such as Enterprise Vault for Microsoft Exchange.
3. Search for a word or phrase by using the Knowledge Base Search feature, or browse the list of most popular subjects.

Enterprise Vault training modules

The Enterprise Vault Tech Center (http://go.symantec.com/education_evtc) provides free, publicly available training modules for Enterprise Vault. Modules are added regularly and currently include the following:

- Installation
- Configuration
- Getting Started Wizard
- Preparing for Exchange 2010 Archiving
- Assigning Exchange 2007 and Exchange 2010 Permissions for Enterprise Vault
- Enterprise Vault File System Archiving

More advanced instructor-led training, virtual training, and on-demand classes are also available. For information about them, see http://go.symantec.com/education_enterprisevault.

Comment on the documentation

Let us know what you like and dislike about the documentation. Were you able to find the information you needed quickly? Was the information clearly presented? Report errors and omissions, or tell us what you would find useful in future versions of our guides and online help.

Please include the following information with your comment:

- The title and product version of the guide on which you want to comment.
- The topic (if relevant) on which you want to comment.
- Your name.

Email your comment to evdocs@symantec.com. Please only use this address to comment on product documentation.

We appreciate your feedback.

Chapter 2

About File System Archiving

This chapter includes the following topics:

About File System Archiving

You can set up Enterprise Vault File System Archiving (FSA) to archive files from network shares. Users can then access the archived files through facilities such as Enterprise Vault Search, or by using shortcuts in the original locations.

The *Enterprise Vault Compatibility Charts* document provides a full list of the target platforms, operating systems and protocols that Enterprise Vault supports for FSA.

The document also lists the supported operating systems for client access of archived items, including opening Internet and Placeholder shortcuts to archived items. The *Enterprise Vault Compatibility Charts* document is available at the following address on the Symantec Support website:

http://www.symantec.com/docs/TECH38537

By archiving from the file system, you can gain the following immediate benefits on the volumes that are being archived:

- It is easy to archive files. You may have files that you want to add to your archive system, perhaps because of legal requirements. You can create an archiving policy to archive them all immediately.
- Files that are archived are indexed, so they are searchable.
- Previous versions of archived files are retained. When a user creates a new version of a file that has been archived, that new version will be archived when it is matched by the rules you define. All the earlier archived versions of the file are retained and are searchable.
- There may be an immediate space usage reduction.

The Retention Folder feature enables you to create a hierarchy of folders automatically on file servers, to be managed by Enterprise Vault and archived according to assigned policies. For example, you could create a hierarchy of retention folders in every user's home folder.

The File Blocking feature enables you to prevent unwanted files from being saved on monitored server volumes.

FSA Reporting provides summary reports on the active data on your file servers, and on the data that has been archived from them.

The following video provides a short demonstration of Enterprise Vault File System Archiving:

Enterprise Vault File System Archiving Demo.

Free training modules for File System Archiving are available from the Enterprise Vault Tech Center at http://go.symantec.com/education_evtc.

A separate guide contains best practices information for implementing File System Archiving with Enterprise Vault. See the following article on the Symantec Support website:

http://www.symantec.com/docs/TECH175137

For more information on migrating and consolidating file servers that have content that has been archived with Enterprise Vault, see the following article on the Symantec Support website:

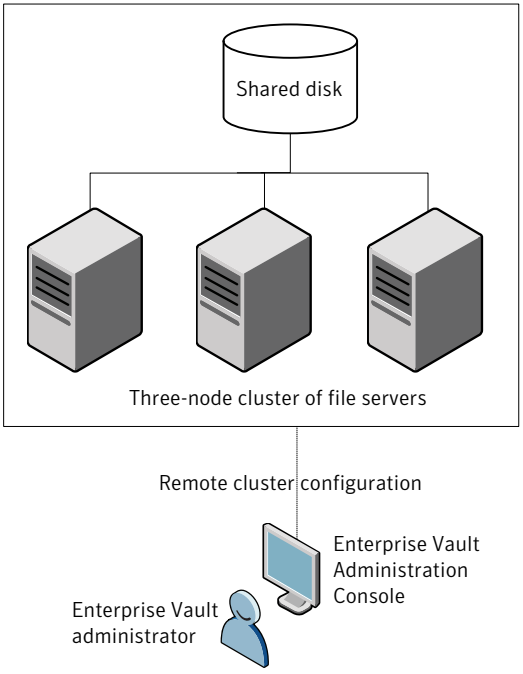
http://www.symantec.com/docs/TECH147519

About using FSA with clustered file servers

If your Windows file servers are grouped in a cluster, you can make the FSA services that run on them highly available. You must add an FSA resource to the cluster resource group or service group, and configure the FSA resource for high availability. The FSA resource monitors the state of the FSA services on the online node. If a problem occurs with the FSA services on the online node, then the cluster resource group or service group that contains the FSA resource fails over to the next available node.

Figure 2-1 shows an example environment in which three file servers are clustered.

Figure 2-1 Example FSA cluster configuration



Note that you can make the FSA services highly available only when there is a shared disk resource.

See "About configuring FSA with clustered file servers" on page 68.

About setting up File System Archiving

Very briefly, setting up File System Archiving involves the following tasks:

- Preparing the file server as necessary, and then adding it as a target file server in the Administration Console. You must install the Enterprise Vault FSA Agent on a Windows file server on which you want to leave placeholder shortcuts, implement File Blocking, or collect data for FSA Reporting.
- Creating volume policies to define how and what to archive from target volumes. Optionally you can also create folder policies, to override the volume policies for specific target folders.
- Adding the target volumes to the Administration Console, and assigning the volume policies.
- Adding target folders, and assigning the parent volume policy or a folder policy. You can define an archive point for each folder that you want to associate with a separate archive. A folder with an archive point forms the top of an archive. Files from the folder and its subfolders are stored in the same archive.
- Configuring other features as required, such as File Blocking, retention folders, and FSA Reporting.
- Configuring the File System Archiving tasks to schedule archiving and associated activities, and to determine the mode in which the archiving is to run.

Table 2-1 shows the properties of the Enterprise Vault Administration Console containers that you can use to control File System Archiving.

Table 2-1 Controlling File System Archiving from the Administration Console

Item	Properties
Target file server (under Targets\File Servers)	■ Whether to archive the file server. ■ Configuration settings for pass-through recall for placeholder shortcuts. ■ Configuration settings for File Blocking. ■ Configuration settings for deletion of archived files on placeholder deletion. ■ Configuration settings for FSA Reporting.

Table 2-1 Controlling File System Archiving from the Administration Console *(continued)*

Item	Properties
Target Volume (under Targets\File Servers\<server>)	■ Whether to archive the volume. ■ The File System Archiving task that is to process the volume. ■ The File System Archiving policy to apply when processing the volume. ■ For NTFS volumes, whether to enable pass-through recall for placeholder shortcuts on this volume. A target volume is processed according to the File System Archiving task schedule, but can be processed manually by using the Run Now option.
Target Folder (under Targets\File Servers\<server>\<volume>)	■ Whether to archive the folder. ■ Whether to archive the subfolders of the folder. ■ The FSA policy to apply when processing the folder. ■ The location of archive points, which mark a folder that forms the top of an archive.

Volume policy
 	
(under Policies\File)
	Each target volume is assigned a volume policy, which defines the following:
	
	■ The File Blocking rules to apply to the volume, if File Blocking is configured.
	■ For NTFS volumes, whether to use quotas.
	■ The type of shortcut to leave, if the archiving rules specify that a shortcut is to be created.
	■ For placeholder shortcuts:
	  ■ Whether to delete archived files on placeholder deletion.
	  ■ Whether to delete placeholders for the items that are deleted from archives.
	■ The retention category to use for archived files.
	■ The archiving rules to apply. These rules determine which files to archive, and when to create shortcuts.
	■ Whether to archive files that have explicit permissions, and files that are under Dynamic Access Control. These files are subject to a change in permissions when archived.

Table 2-1 Controlling File System Archiving from the Administration Console *(continued)*

Item	Properties

Folder policy
 	
(under Policies\File)
	Folder policies are optional. Use them when you want to override the volume policy for specific folders.
	
	A folder policy defines the following:
	
	■ The type of shortcut to leave, if the archiving rules specify that a shortcut is to be created.
	■ For placeholder shortcuts:
	  ■ Whether to delete archived files on placeholder deletion.
	  ■ Whether to delete placeholders for the items that are deleted from archives.
	■ The retention category to use for archived files.
	■ The archiving rules to apply. These rules determine which files to archive, and when to create shortcuts.
	■ Whether to archive files that have explicit permissions, and files that are under Dynamic Access Control. These files are subject to a change in permissions when archived.

File System Archiving Task (under Enterprise Vault Servers\<server>\Tasks)	Processes target volumes and folders. The task properties define the following: ■ Whether to run in report mode or normal mode. ■ Schedule settings, including the option for Run Now. ■ Settings to control generation of normal and pruning reports. ■ Synchronization schedule. ■ Pruning options and schedule.

About FSA policies

In the Enterprise Vault Administration Console you define FSA policies to control which files are archived by FSA.

There are three types of FSA policy:

- Volume policies apply to entire target volumes, unless overridden by folder policies.
- Folder policies are applied to specific target folders. These settings override the volume policy settings.

  To make for easier management, we recommend that you do not apply folder policies to folders that have a short life, such as temporary folders. It is better

to apply folder policies to folders that will have a long life, such as a user's root folder.

- Retention folder polices are a special type of FSA policy that enable you to define a hierarchy of folders to create under a target folder.
  See "About retention folders" on page 33.

Each volume policy and folder policy includes one or more archiving rules. You define these rules to select the files you want Enterprise Vault to archive or delete. You can apply the archiving rules in any order. In combination with the other policy settings such as quota settings, the result is a flexible means to archive precisely what is required.

For example, you can create policies that do the following:

- Start archiving when the volume is 80% full and continue until the volume is 60% full.
- Archive all files older than 30 days except Hidden and System files.
- Archive `*.zip` and `*.avi` files that are older than three days and larger than 20 MB.
- Delete `*.bak` files that have not been accessed in the last week, without archiving them.
- Archive `*.doc` files and do not create a shortcut for each file until one month after it was last modified.

A number of predefined file groups are available to enable you to quickly add the required file types to a policy.

You can edit the settings of the supplied Default FSA Volume Policy and Default FSA Folder Policy, or create new policies as required.

File System Archiving can archive all file types. However, some file types such as executable files and .PST files are not suitable candidates for file archiving. The Default Volume Policy and Default Folder Policy include archiving rules that you can use to exclude unsuitable file types from archiving and shortcut creation.

See "About excluding specific Mac and Windows file types from archiving" on page 92.

About target volumes, folders, and archive points

When you have added a target file server to the Administration Console, you can do the following:

- Add file server shares as target volumes for FSA to process.

- Add target folders to each target volume, to control which folders Enterprise Vault can archive from.
- Create archive points on the target folders and subfolders. Each archive point marks the top of a folder structure that Enterprise Vault archives within a single archive.

Enterprise Vault creates an archive for each archive point that it finds. By default the Enterprise Vault File System Archiving task gives the archive the same name as the folder to which the archive point applies. The site defaults are used to supply the other attributes of the archive, including the indexing level. You can override these defaults if you want.

Where possible, Enterprise Vault uses Alternate Data Streams (ADS) to indicate archive points. These stream archive points are used on NTFS volumes, on NetApp filers, and on EMC Celerra/VNX devices. If the file system does not support ADS, Enterprise Vault uses hidden XML files to mark archive points.

About client access to FSA-archived items

Users can access archived items as follows:

- If FSA creates shortcuts in the item's original location, users can access an archived item by double-clicking its shortcut on the file server.
- If shortcuts are not created, users can access the archived items by using the Enterprise Vault search facilities.

About archived file permissions

In the archive no explicit file permissions apply, and no Dynamic Access Control (DAC) permissions apply. The result is that an archived file has the permissions of its parent folder, less any DAC permissions.

If Enterprise Vault leaves a placeholder shortcut, the placeholder has all the permissions of the original file.

The absence of explicit file permissions and all DAC permissions in the archive has the following consequences:

- A user who has conventional (non-DAC) permission to access a folder can find and access any file in the associated archive folder. However, if the user did not have permission to access the original file, the user cannot access the archived file from its placeholder.
- A user who has conventional (non-DAC) permission to delete items from a folder can delete the archived version of any file from the associated archive folder.

However, if the user did not have permission to delete the original file, the user cannot delete its placeholder.

- A user who has access to a file through DAC alone cannot access the file in the archive.
  Note that to allow access to files in the archive, you can set permissions manually on an archive from the Enterprise Vault Administration Console. If you set permissions on an archive they are applied to every folder in the archive.
- If a file is restored from the archive, the restored file has the original parent folder permissions, less any DAC-related permissions that were applied directly to the file.

You can choose whether to archive files that have explicit permissions, and files that are under Dynamic Access Control.

See "About options for archiving files that have explicit permissions, and files under DAC" on page 94.

The File System Archiving task automatically synchronizes archive folder permissions with file server folder permissions on a scheduled basis. The automatic synchronization can run once or twice each day. It is possible to turn off the automatic synchronization, in which case you must synchronize manually.

Note: On Windows Server 2008 R2 and Windows Server 2012 the method of setting access permissions for a share has changed. The File Sharing dialog that is accessed from the Sharing tab of the folder's properties sets file and folder permissions only. You must also use Advanced Sharing to grant share permissions, which apply when access is made across a network.

About FSA shortcut files

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

- An internet (URL) shortcut. This is a .url text file that contains a hypertext link to the archived file.
  See "About internet shortcuts" on page 28.
- A placeholder. This is a special file that appears exactly as the original file but, when opened, forces Enterprise Vault to fetch the archived file.
  See "About placeholder shortcuts" on page 28.

About internet shortcuts

When FSA archives a file it can optionally leave an internet (URL) shortcut. An internet shortcut is a `.url` text file containing a hypertext link to the archived file. FSA can place internet shortcuts on any network share. When a user double-clicks an internet shortcut, the archived file is retrieved and is shown in the appropriate application. If you open an internet shortcut from within an application, the application opens the contents of the shortcut, not the archived file.

Internet shortcuts have a suffix of `.url`. This suffix is appended to the file's existing suffix. For example, the shortcut for a Word document file named `document1.docx` is named `document1.docx.url`. The inclusion of the original suffix enables you to determine the original file type that the internet shortcut references.

Note: If you choose the Windows Explorer option **Hide known file types**, Windows still displays the original file type of an internet shortcut. For example, the internet shortcut `document1.docx.url` appears as `document1.docx`.

Note: If you attempt to recall a file that is larger than 4 GB from an internet shortcut using Internet Explorer 7.0, the file is inaccessible. Enterprise Vault displays a message stating that files larger than 4 GB cannot be opened. This restriction is due to a limitation in Microsoft Internet Explorer. Note that placeholder shortcuts are not affected.

To work around this restriction, you can restore the file by using the **Copy to File System** or **Move to File System** menu option in facilities such as Enterprise Vault Search or Archive Explorer.

About placeholder shortcuts

When FSA archives a file it can optionally leave a placeholder shortcut. Placeholder shortcuts behave exactly as the original files. A placeholder shortcut has the same file extension as the file to which it is a shortcut. When a user opens a placeholder shortcut, the original file is retrieved automatically.

A placeholder shortcut shows the size of the file that it replaced, although the shortcut itself takes up very little space.

Placeholder shortcuts are supported on NTFS devices, NetApp filers, and EMC Celerra/VNX devices. To use placeholders on a Windows file server the FSA Agent must be installed on the file server.

See "About the FSA Agent" on page 32.

For details of the exact requirements for placeholders, see the Enterprise Vault *Compatibility Charts*.

When you define an FSA policy that specifies leaving placeholder shortcuts, you can choose whether to do the following:

- Delete placeholders for the items that have been deleted from archives.
- Delete archived files when placeholders are deleted.

Table 2-2 describes the behavior of placeholder shortcuts when you open, copy, move, or delete them.

Table 2-2 Characteristics of placeholder shortcuts

Action on placeholder	Effect
Open	The file is recalled from the archive. **Note:** If pass-through recall is in effect, Enterprise Vault recalls the file to disk only if the calling application requires a writeable version. See "About pass-through recall for placeholder shortcuts" on page 31. A file that is recalled to the file server replaces the placeholder shortcut. ■ If the recalled file remains unmodified, then Enterprise Vault converts the file back to a placeholder on the next archiving service run. The only exception is if the archiving policy's shortcut creation rules are based on the last access time. In that case, Enterprise Vault reverts the file only when the shortcut creation rules are met. ■ If the recalled file becomes modified, then Enterprise Vault converts the file back to a placeholder according to the archiving policy's shortcut creation rules.

Table 2-2 Characteristics of placeholder shortcuts *(continued)*

Action on placeholder	Effect
Copy	The source file is restored and then copied. The destination file is a copy of the restored original file. **Note:** The copy operation does not restore the source file to disk if pass-through recall is in effect. See "About pass-through recall for placeholder shortcuts" on page 31. Enterprise Vault converts a restored original file back to a placeholder on the next archiving service run. The only exception is if the archiving policy's shortcut creation rules are based on the last access time. In that case, Enterprise Vault reverts the file only when the shortcut creation rules are met.
Move	If the destination is on the same volume, the placeholder is moved. If the destination is on a different volume, the archived file is restored and then moved to the destination.
Delete	You can configure Enterprise Vault to delete archived files when their placeholders are deleted, if you want. You must configure some settings for the file server, and apply an archiving policy with the appropriate settings. See "About configuring the deletion of archived files on placeholder deletion" on page 96.

Note the following restrictions and limitations that relate to placeholders:

- Unwanted placeholder recalls can occur if you use the Windows Explorer preview pane that is provided in recent versions of Windows. When you select a placeholder, Windows recalls the file to display the preview. This restriction is due to a limitation with the previewing of offline files.
- Enterprise Vault cannot create placeholder shortcuts on NTFS file systems for files with extended attributes, such as the following:
  - Files that were migrated from Novell file systems or from HPFS (OS/2) file systems
  - Files that were previously archived with applications such as EMC DiskXtender

  Enterprise Vault archives files that have extented attributes, but the placeholder creation fails. This limitation is due to a Microsoft restriction: placeholders use reparse points, which cannot contain extended attributes.

EVEARemovalUtility is a command line utility that removes extended attributes from files, so that Enterprise Vault can create placeholders for them successfully. For more information about EVEARemovalUtility, see the *Utilities* guide.

- On NetApp C-Mode filers, recall of large files (larger than 50 MB) may time out. For information about increasing the timeout value on the Vserver, see the NetApp documentation.

About pass-through recall for placeholder shortcuts

You can configure the pass-through recall of placeholder shortcuts on Windows file servers, and for read-only file systems on NetApp filers that run Data ONTAP 7.3 or later. For EMC Celerra/VNX devices, Enterprise Vault supports the Celerra/VNX pass-through facility.

Note: Due to a NetApp restriction, pass-through is not supported for Data ONTAP 8.2 C-Mode.

If pass-through recall is configured, then on receipt of a read request for a placeholder Enterprise Vault passes the data directly through to the calling application. Enterprise Vault recalls the file to the file server, subject to permissions, only if the calling application makes a write request: for example if the application requires a writeable file, or if the user attempts to save changes to a file.

Note: Some applications such as Excel always recall to disk even when pass-through recall is enabled.

Pass-through recall can be useful in the following circumstances:

- With placeholders on read-only file systems, such as snapshots. A normal placeholder recall to a read-only file system fails because Enterprise Vault cannot write the recalled file to the file system.
- With Windows file servers when there is limited space on the file server, or when users have strict quotas for space usage. Recalled files normally occupy space on the target file system, and therefore count towards a user's space quota.

Pass-through recall uses a disk cache to reduce recall times for large files. For Windows file servers the disk cache is located on the file server. For NetApp filers the disk cache is located on the Enterprise Vault server.

For Windows file servers you can enable or disable pass-through recall for each target volume.

About the FSA Agent

To use placeholder shortcuts, File Blocking, or FSA Reporting with a Windows file server, you must install the FSA Agent on the file server.

The FSA Agent consists of the following FSA services:

- Enterprise Vault File Placeholder service
- Enterprise Vault File Blocking service
- Enterprise Vault File Collector service (used by FSA Reporting)

Note: Do not install the FSA Agent on Enterprise Vault servers.

You can install the FSA Agent on a Windows file server either from the Administration Console, or manually.

See "About installing the FSA Agent on a Windows file server" on page 81.

NetApp filers and EMC Celerra/VNX devices do not run the FSA Agent.

Table 2-3 describes how Enterprise Vault provides support for placeholders, File Blocking, and FSA Reporting data collection on different types of file server.

Table 2-3 How Enterprise Vault provides placeholders, File Blocking, and FSA Reporting data collection

File server type	Placeholders	File Blocking	FSA Reporting data collection
Windows file server	FSA Agent (File Placeholder service)	FSA Agent (File Blocking service)	FSA Agent (File Collector service)
NetApp filer	The Enterprise Vault server runs an equivalent process to the File Placeholder service.	A Windows server with the FSA Agent installed acts as a File Blocking agent server.	An FSA Reporting proxy server performs the data collection. For more details, see the *Reporting* guide.
EMC Celerra/VNX device	The Celerra/VNX device uses the Enterprise Vault Web Access application to fetch items from the archive.	Not supported.	

About retention folders

The retention folder feature enables you to create single folders or a hierarchy of folders automatically on file servers, to be managed by Enterprise Vault and archived according to assigned policies. For example, you can create a hierarchy of retention folders in every user's home folder. You can specify that the retention folder hierarchy is added to the root of the FSA target folder, or to each subfolder.

If a user deletes or moves any folders in the retention folder hierarchy, then by default Enterprise Vault recreates the folders during the next run of the File System Archiving task in Normal mode. If you do not want Enterprise Vault to recreate deleted or moved folders you can set a registry value.

Enterprise Vault archives the items that are placed in the retention folders according to the policy that is assigned to each folder. Different folders in a retention folder hierarchy can have different policies assigned.

You define the archives to use for the retention folders by specifying where archive points are to be created.

About File Blocking

The File Blocking feature for Windows file servers and NetApp filers prevents unwanted file types from being saved on monitored server volumes. File Blocking can be performed independently from archiving: a File System Archiving task can also process the volumes, but there is no requirement to do this.

You configure File Blocking at the volume level, by applying a volume policy in which you have defined File Blocking rules. The File Blocking rules determine the following:

- Which files are blocked or allowed.
- Which folders to monitor, or to ignore.
- The actions to take when a policy violation occurs. For example, you can allow a file to be created, but send a warning message to the user and log an event in the event log.

The File Blocking rules enable you to block files according to:

- File type. Inappropriate file types can be blocked immediately.
- Content. Content-checking enables you to trap files that have been renamed to disguise their file types. File Blocking quarantines those files that are blocked as a result of content-checking. Additionally, it is possible to scan the contents of compressed files, such as ZIP files.

Note: Files stored within .RAR and .CAB files cannot be blocked or quarantined. However, you can create rules to block .RAR and .CAB files.

If required, you can edit the properties of the target file server to define a list of users whose files are never blocked.

The File Blocking rule enables you to configure a notification to send when the rule is broken. The following notification types are available:

- Messenger Service messages (NET SEND)
- Event log entries
- Email
- SNMP traps

See "About configuring File Blocking" on page 132.

About FSA Reporting

FSA Reporting provides summary analysis reports on the active data on your file servers, and on the data that has been archived from them.

FSA Reporting's data analysis reports include information on the following:

- The number of archived files for each file server, and the space used and saved as a result of archiving. You can also view the 10 largest files in a volume.
- Active and archived space usage by different file groups, per server and per archive point.
- Numbers of unaccessed or duplicated files, and the space they are occupying.
- Used and free space on the drives of each file server.
- Storage growth trends for the FSA archiving targets on a file server. Trends are shown for both the file server and the vault store.

Many of the reports provide either an overall view for all the file servers that are configured for FSA Reporting, or a detailed view for a named file server.

In order to access FSA Reporting's reports, the Enterprise Vault Reporting component must be installed and configured on a machine with the required prerequisites, including Microsoft SQL Server Reporting Services. You use the SQL Server Reporting Services Report Manager web application to view the reports.

You must also configure FSA Reporting for each target file server for which you want to obtain reports. The Administration Console provides wizards to help you do the following:

- The first time that you enable a target file server target for FSA Reporting, a wizard helps you to set up an FSA Reporting database to hold the FSA Reporting scan data.

  When you enable another target file server for FSA Reporting, you can assign the file server to an existing FSA Reporting database, or create another database. Multiple FSA Reporting databases can provide scalability if you obtain FSA Reporting data for many file servers.
- For a Windows file server, install the FSA Agent on the file server if the agent is not already present.
- For a non-Windows file server you must select another server to act as the FSA Reporting proxy server. The FSA Reporting proxy server gathers the FSA Reporting data for one or more non-Windows file servers.

  Any of the following can act as an FSA Reporting proxy server, subject to some additional prerequisites:

  - An Enterprise Vault server in the Enterprise Vault site.
  - A Windows server that is configured as a file server archiving target in the Enterprise Vault site.
  - A Windows server on the network.

For information on configuring and managing FSA Reporting, and on viewing and interpreting the FSA reports, see the *Reporting* guide.

About FSAUtility

FSAUtility is a command-line utility with which you can do the following:

- Recreate archive points on the original path.
- Recreate the placeholders for archived files in their original location.
- Move placeholders from one location to another location and move the archived files to the corresponding destination archive, which is represented by the archive point on the path.
- Migrate placeholders from a source path to a destination path without any movement of the archived data.
- Delete orphaned placeholders for which no corresponding item exists in the archive.
- Restore all archived files, or archived files of the specified file types, to their original location or a new location.

- Recall the archived files that correspond to placeholders that are present in a folder.

The utility works with archive points and placeholders on Windows file servers, NetApp filers, and EMC Celerra/VNX devices.

For details of the utility, see the *Utilities* guide.

For more information on migrating and consolidating file servers that have content that has been archived with Enterprise Vault, see the following article on the Symantec Support website:

http://www.symantec.com/docs/TECH147519

Chapter 3

Steps to configure File System Archiving

This chapter includes the following topics:

Steps to configure File System Archiving

Table 3-1 describes the process to set up one or more file servers for File System Archiving.

Note: If you want to configure FSA with clustered file servers, refer to the appropriate instructions. See "About configuring FSA with clustered file servers" on page 68.

Note: If you want to implement File Blocking on the server, read about configuring File Blocking before you proceed.

See "About configuring File Blocking" on page 132.

Table 3-1 Steps to configure File System Archiving

Step	Action	Description
Step 1	Check that your planned system meets the required prerequisites for FSA.	See the Enterprise Vault *Installing and Configuring* guide.
Step 2	Install and configure the Enterprise Vault servers, and perform the initial setup of Enterprise Vault.	See the Enterprise Vault *Installing and Configuring* guide.

Table 3-1 Steps to configure File System Archiving *(continued)*

Step	Action	Description
Step 3	Add the file server to FSA.	Follow the appropriate step for the file server type: ■ See "Adding a Windows file server to File System Archiving" on page 39. ■ See "Adding a NetApp filer to File System Archiving" on page 48. ■ See "Adding a NetApp C-Mode Vserver to File System Archiving " on page 51. ■ See "Adding a Celerra/VNX device to File System Archiving" on page 55.
Step 4	Create the required FSA archiving policies.	See "Creating FSA volume policies and folder policies" on page 88.
Step 5	Configure the deletion of archived files on placeholder deletion, if required.	See "About configuring the deletion of archived files on placeholder deletion" on page 96.
Step 6	Add one or more target volumes for archiving. Then add the required target folders and archive points.	See "About adding target volumes, target folders, and archive points for FSA" on page 102.
Step 7	Configure additional features, if required.	■ Configure pass-through recall for placeholder shortcuts, if required. See "About configuring pass-through recall for placeholder shortcuts" on page 117. ■ Set up retention folders, if required. See "Configuring retention folders" on page 124.
Step 8	Configure the File System Archiving tasks that process the target volumes.	See " About configuring and running FSA tasks" on page 146. Set up file system filtering, if required. See "Configuring file system filters" on page 157.
Step 9	Make sure that the file servers are suitably backed up and virus-checked.	■ See "About backing up the target file servers" on page 162. ■ See "About virus-checking the target file servers" on page 163.

Chapter 4

Adding a Windows file server to File System Archiving

This chapter includes the following topics:

Adding a Windows file server to File System Archiving

Table 4-1 lists the steps that are required to add a Windows file server to FSA.

Table 4-1 Steps to add a Windows file server to FSA

Step	Action	Description
Step 1	If you use the Windows Encrypting File System (EFS), you must perform some configuration steps.	See "Using FSA with the Windows Encrypting File System (EFS)" on page 40.
Step 2	For Windows Server 2012 file servers, be aware of how FSA works with new features in this operating system.	See "About archiving from Windows Server 2012 file servers" on page 41.
Step 3	Note the requirements for the accounts that you use in Enterprise Vault to configure and manage file servers.	See "Account requirements for managing FSA with Windows file servers" on page 43.
Step 4	Ensure that the Vault Service account has the required permissions and privileges on the file server.	See "Permissions and privileges required by the Vault Service account on Windows file servers" on page 44.
Step 5	If the file server's firewall is on, configure the firewall for FSA.	See "Configuring a file server's firewall for FSA" on page 45.
Step 6	Add the file server as an FSA archiving target.	See " Adding a Windows file server as an archiving target" on page 46.

Using FSA with the Windows Encrypting File System (EFS)

FSA is compatible with the Windows Encrypting File System (EFS) on some versions of Windows.

For details, see the Enterprise Vault *Compatibility Charts* at http://www.symantec.com/docs/TECH38537.

To use FSA with EFS you must perform some configuration steps before you can create an archive point for an encrypted folder or volume.

To use FSA the Windows Encrypting File System (EFS)

1. Configure the Vault Service account as an EFS recovery agent for the domain.
2. Enable the file server and the Enterprise Vault server as remote servers for file encryption or decryption. See the following Microsoft Technet article:

http://technet.microsoft.com/en-us/library/cc757963.aspx

Set up the remote server delegation as follows:

- With the file server selected as the remote server, trust it for delegation to the CIFS service and the Protected Storage service on the Enterprise Vault server and the Active Directory (certification authority) server.
- With the Enterprise Vault server selected as the remote server, trust it for delegation to the CIFS service and the Protected Storage service on the file server and the Active Directory (certification authority) server.

About archiving from Windows Server 2012 file servers

Read this section if you have Windows Server 2012 file servers that you want to configure as targets for File System Archiving. Some of the new features in Windows Server 2012 have implications that you need to be aware of when you are setting up FSA.

About the ReFS and CSVFS file systems and FSA

Windows Server 2012 introduces two new file system types:

- Resilient File System, ReFS
- Cluster Shared Volume File System, CSVFS

Due to the lack of the necessary constructs from Microsoft, ReFS and CSVFS are unsupported for File System Archiving. If you attempt to add a volume or a folder in either format as a target for FSA, the Administration Console blocks the action and displays an explanatory dialog.

If an NTFS volume is designated in the CSVFS format, the shares on the volume become inaccessible to Enterprise Vault. Archiving does not succeed and placeholder recalls fail.

About Dynamic Access Control and FSA

Windows Server 2012 introduces Dynamic Access Control (DAC), which extends the ability to set permissions by using additional access control entries on files and folders.

FSA volume policies and folder policies let you choose whether to archive files that are under Dynamic Access Control, as well as files that have explicit permissions. The default policy setting is not to archive these files.

Before you choose to archive these files, note that in the archive no DAC permissions apply, and no explicit permissions apply. An archived file has the permissions of its parent folder, less any DAC permissions.

See "About options for archiving files that have explicit permissions, and files under DAC" on page 94.

About archiving Windows Server 2012 deduplicated files with FSA

Windows Server 2012 includes a new file-level data deduplication mechanism.

By default, FSA archives Windows Server 2012 deduplicated files. Options on the **Archiving Rules** tab and the **Shortcuts** tab of the Enterprise Vault FSA Volume policies and Folder policies enable you to turn off archiving or shortcut creation for Windows Server 2012 deduplicated files, if you want.

If you decide to turn off archiving or shortcut creation for Windows Server 2012 deduplicated files, bear in mind that Windows does not deduplicate files immediately. Enterprise Vault applies the deduplicated file policy settings to a file only if the file is in a deduplicated state when Enterprise Vault assesses it for archiving or for shortcut creation. The order of events can lead to different archiving outcomes. For example, suppose that you set the policy options for Windows Server 2012 deduplicated files as follows:

[*Selected*] **Do not archive Windows Server 2012 deduplicated files**

[*Unselected*] **Do not create shortcuts for Windows Server 2012 deduplicated files**

The following scenario may then occur:

- Enterprise Vault archives a file before Windows has deduplicated it. Since the file is not in a deduplicated state when Enterprise Vault assesses it, the policy setting for archiving Windows Server 2012 deduplicated files is not considered.
- While the file awaits shortcut creation on the file server, Windows deduplicates it.
- Enterprise Vault then creates a shortcut for the file, adhering to the policy setting for creating shortcuts for deduplicated files.

The same policy settings can have different results if the deduplicated file is modified before Enterprise Vault creates a shortcut for it. Once Windows has deduplicated the file, Enterprise Vault does not rearchive it, because of the policy setting for deduplicated files. Enterprise Vault does not create a shortcut for the modified file, because for shortcut creation Enterprise Vault requires the latest version of the file to be in the archive.

Account requirements for managing FSA with Windows file servers

You can configure and manage file servers in Enterprise Vault with the Vault Service account, or an account that belongs to a suitable Enterprise Vault administrator role. The predefined Enterprise Vault 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 must be a member of the local Administrators group on the computer on which you run the Administration Console.

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

- The account must have Full control on any share that is configured as a target volume, and must 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.

The Vault Service account requires some additional permissions and privileges on the file server.

See "Permissions and privileges required by the Vault Service account on Windows file servers" on page 44.

Note that to perform the following actions, you must use an account that has additional permissions:

- To install the FSA Agent you must use an account that is a member of the local Administrators group on the file server. This requirement applies both for installation from the Administration Console and for manual installation of the FSA Agent.
- To configure or reconfigure the FSA resource for a file server cluster, you must run the FSA Cluster Configuration wizard with account that is a member of the local Administrators group on each node of the file server cluster. The account must also have Full Control permission on the `FSA Cluster` folder of the Enterprise Vault server. The `FSA Cluster` folder is a subfolder of the `Utilities` folder under the Enterprise Vault installation folder. For example:

  ```
  C:\Program Files (x86)\Enterprise Vault\Utilities\FSA Cluster
  ```

Permissions and privileges required by the Vault Service account on Windows file servers

The FSA Agent and other FSA processes run on target Windows file servers under the Vault Service account. To perform the required tasks, the Vault Service account requires certain permissions and privileges on the file server:

- The Vault Service account can run as a member of the built-in local Print Operators group on the file server, with an additional set of minimal permissions and privileges.
- Alternatively, the Vault Service account can run as a member of the local Administrators group on the file server. The Administrator rights allow the account to perform the additional tasks of installing the FSA Agent and configuring the resource for a file server cluster. However, granting local Administrator rights to the Vault Service account on a file server may not always be advisable. For example:
  - Your company may forbid the granting of local Administrator rights to computer service accounts.
  - If the file server is a domain controller, you should not make the Vault Service account a local Administrator. An account that is a member of the local Administrators group on a domain controller is promoted to a Domain Administrator. We recommend that you do not make the Vault Service account a Domain Administrator.

If the Vault Service account is not a member of the local Administrators group, you must use a suitable account that is a member of that group when you install the FSA Agent, or if you configure the FSA resource for a Windows Server failover cluster.

See "Account requirements for managing FSA with Windows file servers" on page 43.

Note the following:

- When you install the FSA Agent, either from the Administration Console or manually, Enterprise Vault adds the Vault Service account to the Print Operators group on the file server, and configures the additional set of minimal permissions and privileges.
- If you do not install the FSA Agent on a file server, you must grant the required permissions and privileges to the Vault Service account manually.
  See "Granting permissions to the Vault Service account if you do not install the FSA Agent" on page 45.

- To support the FSA resource on VCS-clustered file servers, you must make the Vault Service account a member of the local Administrators group on the VCS cluster nodes.

An appendix to this guide lists the permissions and privileges that the Vault Service account requires on a Windows file server.

See "About the permissions and privileges required for the Vault Service account on Windows file servers" on page 172.

Granting permissions to the Vault Service account if you do not install the FSA Agent

If you do not intend to install the FSA Agent on a target Windows file server, you must do one of the following manually:

- Add the Vault Service account to the local Administrators group on the file server.
- Add the Vault Service account to the built-in local Print Operators group on the file server, and grant the additional required permissions and privileges.
  See "About the permissions and privileges required for the Vault Service account on Windows file servers" on page 172.

Configuring a file server's firewall for FSA

Read this section if the Windows file server that you want to configure as an FSA target is protected by a firewall.

You must perform some configuration steps to allow Enterprise Vault to communicate successfully with the file server through the firewall. Unless you perform the required configuration steps, the following problems will occur:

- Installation of the FSA Agent from the Administration Console fails.
- The File System Archiving task fails. You may receive the following messages from DTrace or in the File System Archiving task report:
  - The RPC server is unavailable. (Exception from HRESULT: 0x800706BA)
  - Error making file a placeholder file. Catastrophic failure (Exception from HRESULT: 0x8000FFFF)

For information on how to configure a firewall for FSA, see the following technical note on the Symantec Support website:

http://www.symantec.com/docs/TECH76080

Adding a Windows file server as an archiving target

You can add a Windows file server as an archiving target for Enterprise Vault by using the New File Server wizard.

The wizard helps you to install the FSA Agent on the file server, if required. You must install the FSA Agent on a Windows file server if you want to do any of the following on the file server:

- Replace archived files with placeholder shortcuts
- Implement File Blocking
- Use FSA Reporting

If you do not install the FSA Agent from the New File Server wizard, you can install it later using the Install FSA Agent wizard. Alternatively, you can install the FSA Agent manually.

Note: Do not install the FSA Agent on an Enterprise Vault server.

See "About installing the FSA Agent on a Windows file server" on page 81.

Note: If you want to use FSA Reporting with the file server, you can configure FSA Reporting when you add the file server as an archiving target.

See "Adding a file server as an archiving target with FSA Reporting data collection enabled" in the *Reporting* guide.

To add a Windows file server as an archiving target

1. If you want to install the FSA Agent during the procedure, run the Administration Console with an account that is a member of the local Administrators group on the file server.
2. In the Administration Console, expand the Enterprise Vault site until the **Targets** container is visible.
3. Expand the **Targets** container.
4. Right-click the **File Server** container and, on the shortcut menu, click **New** and then **File Server**. The **New File Server** wizard starts.
5. Work through the wizard to finish adding the file server.

   You will need to provide the following information:

   - The fully-qualified DNS name of the file server that you want to add. You can browse to select the server.

- If you choose to install the FSA Agent, the password for the Vault Service account.

When you have added the file server, you can start adding the volumes that you want File System Archiving to process.

Chapter 5

Adding a NetApp filer to File System Archiving

This chapter includes the following topics:

Adding a NetApp filer to File System Archiving

Table 5-1 lists the steps that are required to add a NetApp filer to FSA.

Table 5-1 Steps to add a NetApp filer to FSA

Step	Action	Description
Step 1	Set the required permissions on the file server.	See "Setting the permissions for FSA on a NetApp filer" on page 48.
Step 2	Add the file server as an FSA archiving target.	See "Adding a NetApp filer as an archiving target" on page 49.

Setting the permissions for FSA on a NetApp filer

Before configuring a NetApp filer as an archiving target, you must give the Vault Service account administrative permissions on the NetApp filer.

Note: If you want to use another account to configure the NetApp filer from Enterprise Vault, repeat the procedure for that account also.

To set the permissions for FSA on a NetApp filer

1. Add the Vault Service account as an Administrator on the NetApp filer by following these steps in the order listed:
   - Log on to a Windows server as a user who already has administrative rights on the NetApp filer.
   - On the Windows desktop, right-click **My Computer** and then, on the shortcut menu, click **Manage**.
   - In Computer Management, select **Connect to another computer** from the **Action** menu and then enter the name of the NetApp filer.
2. Expand **Local Users and Groups** and click **Groups**.
3. In the right pane, right-click **Administrators** and then, on the shortcut menu, click **Add to Group**.
4. Click **Add** to add the Vault Service account to the list of group members.

Adding a NetApp filer as an archiving target

Before you add a NetApp filer as an FSA archiving target, make sure that you have set the required file server permissions.

See "Setting the permissions for FSA on a NetApp filer" on page 48.

Note: If you want to use FSA Reporting with the NetApp filer, you can configure FSA Reporting when you add the NetApp filer as an archiving target.

See "Adding a file server as an archiving target with FSA Reporting data collection enabled" in the *Reporting* guide.

To add a NetApp filer as an archiving target

1. In the Administration Console, expand the Enterprise Vault site until the **Targets** container is visible.
2. Expand the **Targets** container.

3 Right-click the **File Servers** container and, on the shortcut menu, click **New** and then **File Server**. The **New File Server** wizard starts.

4 Work through the wizard.

Do not select the option to install the FSA Agent.

The wizard prompts you for the fully-qualified DNS name of the NetApp filer. You can browse to select the NetApp filer.

Chapter 6

Adding a NetApp C-Mode Vserver to File System Archiving

This chapter includes the following topics:

Adding a NetApp C-Mode Vserver to File System Archiving

Enterprise Vault FSA supports NetApp C-Mode version 8.2 or later.

Table 6-1 lists the steps that are required to add a NetApp C-Mode Vserver to FSA.

Table 6-1 Steps to add a NetApp C-Mode Vserver to FSA

Step	Action	Description
Step 1	Grant the required permission on each Vserver.	See "Granting the required permission on each Vserver" on page 52.
Step 2	Configure the FPolicy server details	See "Configuring the FPolicy server details" on page 53.

Table 6-1 Steps to add a NetApp C-Mode Vserver to FSA *(continued)*

Step	Action	Description
Step 3	Add the NetApp C-Mode Vserver as an FSA archiving target.	See "Adding a NetApp C-Mode Vserver as an archiving target" on page 53.

To recall large files, you may need to change the NetApp C-Mode Vserver timeout settings.

See "Points to note about File System Archiving on NetApp C-Mode file servers" on page 54.

Granting the required permission on each Vserver

Before you add a NetApp C-Mode Vserver as an FSA target, you need to grant permission to a domain user to register the FPolicy on the Vserver.

Note: There can be only one user account configured per Enterprise Vault site for all the Vservers. If you change the user account details, you must ensure that this user has ONTAPI permissions on all the Vservers. Additionally, the data LIF associated with the Vserver must have both data and management access. Refer to the NetApp documentation for more information.

To grant the required permission on the Vserver

1. Log on to the cluster console as a cluster administrator.
2. To grant the required permission, type the following at the command prompt:

   ```
   security login create -vserver vservername -username
   DomainName\UserName -application ontapi -authmethod domain
   ```

   where:

   - *vservername* is the name of the Vserver.
   - The value of `-username` must be specified in the format of *DomainName**UserName*, where *DomainName* is the Active directory domain of the user account.

   Note: The value specified in `-username` is case-sensitive.

Configuring the FPolicy server details

To configure the FPolicy server details you need to provide the following information:

- The credentials of the domain user account that is used to register the FPolicy on the Vserver. This user account is granted ONTAPI access permission on the Vserver.
  See "Granting the required permission on each Vserver" on page 52.
- The port number for Enterprise Vault FPolicy servers. The Vserver's FPolicy engine attempts to establish a connection with the Enterprise Vault FPolicy server using the specified port.

To configure the FPolicy user account credentials

1. Expand the Administration Console tree until the **Targets** container is visible.
2. Expand **Targets**.
3. Right-click the **File Servers** container and, on the shortcut menu, click **Properties**.
4. Click the **NetApp C-Mode** tab.
5. In the **Account** text box, enter the user account credentials in the format of *DomainName**UserName*, where *DomainName* is the name of the Active directory domain of the user account.

   Note: The value you enter here is case-sensitive. When you create the login and grant ONTAPI permission for this user on the NetApp C-Mode Vserver, make sure that you use the correct case.
6. Enter the password.
7. In the **Port Number** text box, enter the FPolicy server port number.

   Note: The port number should not be greater than 65535.
8. Click **OK**.

Adding a NetApp C-Mode Vserver as an archiving target

Before you add a NetApp C-Mode Vserver as an FSA archiving target, make sure that you have set the required file server permissions.

See "Granting the required permission on each Vserver" on page 52.

To add a NetApp Vserver as an archiving target

1. In the Administration Console, expand the Enterprise Vault site until the **Targets** container is visible.
2. Expand **Targets**.
3. Right-click the **File Servers** container and, on the shortcut menu, click **New** and then **File Server**. The **New File Server** wizard starts.
4. Work through the wizard.

   Do not select the option to install the FSA Agent.

   You will need to provide the fully-qualified DNS name of the NetApp C-Mode Vserver. You can browse to select the NetApp C-Mode Vserver.

Note: A NetApp restriction prevents archiving from a NetApp C-Mode Vserver if the path to the files exceeds 512 characters.

Points to note about File System Archiving on NetApp C-Mode file servers

On NetApp C-Mode file servers, recall of large files may time out. To avoid this, set the privilege level to advanced and increase the timeout values on the Vserver. The following table lists the parameters that you need to configure on each Vserver:

Parameter	Recommended value
`-reqs-cancel-timeout`	0h
`-reqs-abort-timeout`	200s
`-max-server-reqs`	10000

You may need to adjust these values to suit your configuration. For information on how to configure these settings, see the NetApp documentation.

To use File Blocking or FSA Reporting on NetApp C-Mode Vservers, you must install an Enterprise Vault 11.0.1 or later FSA Agent.

Pass-through is not supported for Data ONTAP 8.2 C-Mode.

A NetApp restriction prevents archiving from a NetApp C-Mode Vserver if the path to the files exceeds 512 characters.

Chapter 7

Adding an EMC Celerra/VNX device to File System Archiving

This chapter includes the following topics:

Adding a Celerra/VNX device to File System Archiving

Table 7-1 lists the steps that are required to add an EMC Celerra or VNX device to File System Archiving.

Table 7-1 Steps to add a Celerra/VNX device to FSA

Step	Action	Description
Step 1	Prepare the Celerra/VNX device for FSA.	See "Preparing a Celerra/VNX device for FSA" on page 56.
Step 2	Add the device as an FSA archiving target.	See "Adding a Celerra/VNX device as an archiving target" on page 65.

Table 7-1 Steps to add a Celerra/VNX device to FSA *(continued)*

Step	Action	Description
Step 3	Specify a cache location for the temporary files that Enterprise Vault retrieves from the Celerra/VNX.	See "Specifying a cache location for retrieved Celerra/VNX files" on page 67.

Preparing a Celerra/VNX device for FSA

This section describes how to prepare an EMC Celerra/VNX device for File System Archiving.

The procedure includes steps to ensure that the Celerra/VNX device is configured to support alternate data streams (ADS). Enterprise Vault uses ADS to indicate archive points. If you intend to use placeholder shortcuts on the Celerra/VNX, you must also enable the FileMover functionality on the Celerra/VNX and configure an HTTP or HTTPS connection for recall requests.

Another section provides example commands for this procedure.

See "Example commands to prepare a Celerra/VNX device for FSA " on page 63.

If you want to configure the pass-through behavior on placeholder recall, read about the read_policy_override parameter before you proceed.

See "Configuring Celerra/VNX pass-through behavior for placeholder shortcuts" on page 60.

Note: See this technical note on the Symantec Support website for troubleshooting information on the following procedure:

http://www.symantec.com/docs/TECH52430

Note: An EMC restriction prevents archiving from a Celerra/VNX device if the path to the files exceeds 1024 characters.

To prepare an EMC Celerra/VNX device for FSA

1. Log on to the Celerra/VNX Control Station.
2. Ensure that the Celerra/VNX device is configured to support alternate data streams (ADS), which Enterprise Vault uses to indicate archive points.

   The Celerra/VNX shadow stream parameter controls support for ADS:

- If the shadow stream parameter is set to 1, ADS support is enabled. 1 is the default value.
- If the shadow stream parameter is set to 0, ADS is disabled.

To determine the current value of the shadow stream parameter, enter the following command on the Celerra/VNX Network Server:

```
server_param server_x -facility shadow -info stream
```

where *server_x* is the name of the Data Mover.

The command returns information about the parameter, including its current value.

If the current value is not 1, enter the following command on the Celerra/VNX Network Server:

```
server_param server_x -facility shadow -modify stream -value 1
```

where *server_x* is the name of the Data Mover.

3 Add a Celerra/VNX account for Enterprise Vault to use for authentication on the Celerra/VNX device, by entering the following command:

```
/nas/sbin/server_user server_x -add -md5 -passwd
DataMover_user_name
```

where:

server_x is the name of the Data Mover.

DataMover_user_name is the name of the account. This user is a Data Mover user, not a domain user.

Note the following:

- Specify the full path for the command, `/nas/sbin/server_user`.
- You require root privileges to execute this command.
- If the system prompts you for a User ID and a Group ID, a suitable number in both cases is **1000**, unless you use this value elsewhere.
- If the system prompts you for a home directory, press Enter to continue, without specifying a directory.
- When the system prompts you for a password, enter a suitable password for the user account.

4 Enable the file system for Celerra/VNX FileMover using this command syntax:

```
fs_dhsm -modify fs_name -state enabled
```

where:

fs_name is the name of the file system on the Celerra/VNX.

Note: If you do not want to use placeholder shortcuts with the Celerra/VNX, you can omit steps 5 to 8.

---

5 Configure the HTTP server on the Data Mover to accept Celerra/VNX FileMover API connections, by using the following command:

```
server_http server_x -append dhsm -users DataMover_user_name
-hosts ip_address_policy_engine
```

where:

server_x is the name of the Data Mover.

DataMover_user_name is the name of the Data Mover account that you want Enterprise Vault to use for authentication.

ip_address_policy_engine is the IP address of the computer that runs the Enterprise Vault FSA task that will process the Celerra/VNX device.

The command also tests the connectivity between the Celerra/VNX device and the Enterprise Vault server over HTTP.

If you intend to configure FSA Reporting for the Celerra/VNX device, the Data Mover must also accept connections from the computer that acts as the FSA Reporting proxy server.

See "Preparing an EMC Celerra/VNX device to work with an FSA Reporting proxy server" in the *Reporting* guide.

6 Run the following command to make sure that the connection is active:

```
server_http server_x -service DHSM -start
```

where *server_x* is the name of the Data Mover.

7 Configure an HTTP or HTTPS connection to use for recall requests, using this command syntax:

```
fs_dhsm -connection fs_name -create -type http|https
[-read_policy_override setting] -secondary ev_url -user user
-password user_password -cgi n [-httpport|httpsport port_number]
```

where:

fs_name is the name of the Celerra/VNX file system.

`-type` specifies the connection type (`http` or `https`).

`-read_policy_override` is an optional parameter to set the pass-through behavior for placeholder shortcuts.

See "Configuring Celerra/VNX pass-through behavior for placeholder shortcuts" on page 60.

ev_url is the URL of the Enterprise Vault Web Access application. The Celerra/VNX is case-sensitive, so this URL must use the correct case. You cannot include a port number in the URL.

See "The format of the Web Access application URL in the Celerra/VNX fs_dhsm command" on page 61.

user is the Vault Service account that will have access to all the archives from which files are restored.

user_password is the password to the Vault Service account.

`-httpport` or `-httpsport` specifies the HTTP or HTTPS port number. This parameter is required if the Web Access application uses a port other than the default port (port 80 for HTTP, or port 443 for HTTPS).

8 If you require the Celerra/VNX Data Mover HTTP server to use the Secure Sockets Layer (SSL), configure SSL.

See "Configuring the Data Mover HTTP server to use SSL" on page 62.

Note: You must use SSL if you enable the following Windows security setting, either in the Windows Local Security Policy or as part of Group Policy:

System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing

---

9 Add the Vault Service account as a member of the Administrators group of the Celerra/VNX CIFS server:

- In Windows, start Computer Management.

- In the Computer Management console, select **Action** > **Connect to another computer**. Enter the name of the CIFS server.
- Add the Vault Service account to the Administrators group.

Configuring Celerra/VNX pass-through behavior for placeholder shortcuts

You can use the EMC Celerra/VNX read policy override with placeholder recalls, if required. The Celerra/VNX `-read_policy_override` parameter determines how a read request is handled for a file in secondary storage. For example, you can opt to pass a file directly through to the client without recalling it to the Celerra/VNX. The Celerra/VNX Network Server then recalls the file only if a write request is received.

For pass-through, the Celerra/VNX uses the same cache on the Enterprise Vault server that you set up for Enterprise Vault to use when retrieving files for the Celerra/VNX.

Note: If you configure Celerra/VNX pass-through, do not configure the Enterprise Vault option to delete archived files on placeholder deletion, as this combination can lead to data loss.

To configure the Celerra/VNX pass-through behavior, include the `-read_policy_override` parameter in one of the following commands:

- The `fs_dhsm -connection` command to define the HTTP or HTTPS connection that the Celerra/VNX uses for recall requests. This method sets the pass-through behavior for all the placeholders that are created through the connection.
- The `fs_dhsm -modify` command to configure a Celerra/VNX file system. This method sets the pass-through behavior for all the placeholders on the file system.

The syntax of the `-read_policy_override` parameter is as follows:

```
-read_policy_override [none | full | passthrough | partial]
```

The effect of the values is as follows:

- `none` (the default value). The setting has no effect.
- `full`. Recall the whole file to the Celerra/VNX on read request before the data is returned.
- `passthrough`. Retrieve the data without recalling the data to the Celerra/VNX.
- `partial`. Retrieve only the blocks that are required to satisfy the client read request.

Note the following:

- If you do not set a read policy override for either the file system or the connection, the Celerra/VNX uses a value of `passthrough` by default.
- The Celerra/VNX uses a value of `passthrough` if the Celerra/VNX file system is read only.
- The Celerra/VNX uses a value of `passthrough` if attempts to recall data produce an error that is due to insufficient space or quotas.

For example, the following command syntax configures pass-through for a file system:

```
fs_dhsm -modify fs_name -read_policy_override passthrough
```

where *`fs_name`* is the name of the file system on the Celerra/VNX.

The format of the Web Access application URL in the Celerra/VNX fs_dhsm command

When you configure the Celerra/VNX connection to use for FSA recall requests, one of the required parameters to the `fs_dhsm` command is:

```
-secondary ev_url
```

where *`ev_url`* is the URL of the Enterprise Vault Web Access application.

The format of *`ev_url`* is as follows:

```
http://server_name/EnterpriseVault
```

where *`server_name`* is the name of the Enterprise Vault server that hosts the Storage service for the Celerra/VNX archiving target, as specified in the ComputerEntryTable of the Directory database. This name is the same as the display name of the Enterprise Vault server in the Administration Console.

You can determine the *`server_name`* from the Administration Console as follows:

- In the Administration Console, expand **Enterprise Vault Servers** under the site container in the left pane.
- Identify the Enterprise Vault server that hosts the Storage service for the Celerra/VNX archiving target.
- *`server_name`* is the display name of the Enterprise Vault server as shown under the **Enterprise Vault Servers** node. For example, if the file server name is shown as **server1alias.mydomain.com (server1)**, then *server_name* is **server1alias.mydomain.com**.

The Celerra/VNX is case-sensitive, so make sure that you supply the URL in the correct case.

Note: If the Celerra/VNX fails to find a connection with the server name that you specify in the URL, the files are archived but no placeholders are created. The File System Archiving task report's "Shortcut status" column then shows the error "NO_MATCHING_CONNECTION".

You cannot include a port number in the URL. For example, if you use a non-default port such as port 8080 for the Web Access application, do not attempt to specify the port as follows:

```
-secondary http://evserver.demo.local:8080/EnterpriseVault
```

If you attempt to include a port number, the `fs_dhsm -connection` command fails with a message similar to the following, and the archiving and recall of files on the Celerra/VNX will fail:

```
Error: The host name in the secondary url evserver.demo.local:8080
is either missing or formatted incorrectly.
```

If the Web Access application uses a port other than the default port (port 80 for HTTP, or port 443 for HTTPS), use the `-httpport` or `-httpsport` parameter of the `fs_dhsm` command to specify the port number.

Configuring the Data Mover HTTP server to use SSL

If you use placeholder shortcuts on a Celerra/VNX device you can configure the Celerra/VNX Data Mover HTTP server to use the Secure Sockets Layer (SSL), if required.

Note: You must use SSL if you enable the following Windows security setting, either in the Windows Local Security Policy or as part of Group Policy:

System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing

---

To configure the Data Mover HTTP server to use SSL

1. Install an SSL certificate on the Celerra/VNX device. Refer to your Celerra/VNX documentation for more information.
2. Run the following command on the Celerra/VNX device:

   ```
   server_http server_x -modify dhsm -ssl required
   ```

   where *server_x* is the name of the Data Mover.

3 Run the appropriate command on the Celerra/VNX device as follows:

- If Windows on the Enterprise Vault server computer is configured to use FIPS-compliant algorithms, you must use basic (plain text) authentication:
  `server_http server_x -modify dhsm -authentication basic`
- Otherwise, you must use digest authentication:
  `server_http server_x -modify dhsm -authentication digest`

Note: You can work around any errors that relate to SSL certificates by using the IgnoreSSLCertificateError registry value, if required.

See IgnoreSSLCertificateError in the *Registry Values* guide.

---

4 When you run the New File Server wizard in the Enterprise Vault Administration Console to add the Celerra/VNX device as an archiving target, select the configuration option **Celerra device is connected on HTTPS**.

If the Celerra/VNX device is already configured as a target for FSA, do as follows:

- In the Enterprise Vault Administration Console, expand the **File Servers** container under **Targets** to show the target file servers.
  Right-click the target Celerra/VNX file server, and click **Properties**.
- On the **EMC Celerra** tab, and select **Celerra device is connected on HTTPS**.
- Click **OK** to save your changes and close the Properties dialog box.

Example commands to prepare a Celerra/VNX device for FSA

The following example shows some commands to prepare a Celerra/VNX to use placeholder shortcuts. In this example, neither the Web Access application nor the Data Mover HTTP server uses SSL.

```
$ server_param server_2 -facility shadow -modify stream -value 1

$ /nas/bin/server_user server_2 -add -md5 -passwd
celerraaccessaccount

$ fs_dhsm -modify fsa_fs -state enabled

$ server_http server_2 -append dhsm -users celerraaccessaccount
-hosts 192.168.1.1
```

```
$ server_http server_2 -service DHSM -start

$ fs_dhsm -connection fsa_fs -create -type http
-read_policy_override passthrough
-secondary http://EVServer.demo.local/EnterpriseVault
-user vaultadmin@demo.local -password p4ssw0rd -cgi n -httpport 8080
```

where:

- The Data Mover server name is `server_2`.
- FSA will use the Data Mover account `celerraaccessaccount` to authenticate on the Celerra/VNX.
- The Celerra/VNX file system name is `fsa_fs`.
- The IP address of the File System Archiving task computer is 192.168.1.1.
- Pass-though is enabled for the Celerra/VNX device.
- The URL of the Enterprise Vault Web Access Application is `http://EVServer.demo.local/EnterpriseVault`.
- The Vault Service account that will have access to all the archives from which files are restored is `vaultadmin@demo.local`.
- The password for the Vault Service account is `p4ssw0rd`.
- The Web Access application uses an HTTP connection on the non-default port 8080.

In the following example, both the Web Access application and the Data Mover HTTP server use SSL.

```
$ server_param server_3 -facility shadow -modify stream -value 1

$ /nas/bin/server_user server_3 -add -md5 -passwd
celerraaccessaccount

$ fs_dhsm -modify fsa_fs -state enabled

$ server_http server_3 -append dhsm -users celerraaccessaccount
-hosts 192.168.1.1

$ server_http server_3 -service DHSM -start

$ fs_dhsm -connection fsa_fs -create -type https
-read_policy_override passthrough
-secondary https://EVServer.demo.local/EnterpriseVault
```

```
-user vaultadmin@demo.local -password p4ssw0rd -cgi n -httpsport 4334

$ server_http server_3 -modify dhsm -ssl required

$ server_http server_3 -modify dhsm -authentication digest
```

where:

- The Data Mover server name is `server_3`.
- FSA will use the Data Mover account `celerraaccessaccount` to authenticate on the Celerra/VNX.
- The Celerra/VNX file system name is `fsa_fs`.
- The IP address of the File System Archiving task computer is 192.168.1.1.
- Pass-though is enabled for the Celerra/VNX device.
- The URL of the Enterprise Vault Web Access application is `https://EVServer.demo.local/EnterpriseVault`.
- The Vault Service account that will have access to all the archives from which files are restored is `vaultadmin@demo.local`.
- The password for the Vault Service account is `p4ssw0rd`.
- The Web Access application uses an HTTPS connection on non-default port 4334.
- You do not use the Windows security setting “System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing”.
- You must also select the configuration option **Celerra device is connected on HTTPS** for the target file server in the Vault Administration Console.

Adding a Celerra/VNX device as an archiving target

After you have prepared a Celerra/VNX device for FSA, you can use the Administration Console to add the Celerra/VNX device as an archiving target.

Note: If you want to use FSA Reporting with the Celerra/VNX device, you can configure FSA Reporting when you add the device as an archiving target.

See “Adding a file server as an archiving target with FSA Reporting data collection enabled” in the *Reporting* guide.

To add a Celerra/VNX device as an archiving target

1. In the Administration Console, expand the Enterprise Vault site until the **Targets** container is visible.
2. Expand the **Targets** container.
3. Right-click the **File Servers** container and, on the shortcut menu, click **New** and then **File Server**. The **New File Server** wizard starts.
4. Work through the wizard to finish adding the file server:
   - On the first page of the wizard, click **Next**.
   - On the second page, enter the DNS name of the Celerra/VNX device. Do not select the option to install the FSA Agent. Then click **Next**.
   - On the third page, choose whether to use placeholder shortcuts.
     If you are using placeholder shortcuts, enter the details of the account you configured on the Celerra/VNX that has permission to use DHSM, and the Celerra/VNX port number on which the Data Mover services are configured. You must also specify whether the Celerra/VNX device is connected on HTTPS. Select this box if the Celerra/VNX Data Mover HTTP server uses the Secure Sockets Layer (SSL).

     Note: The Data Mover HTTP server must use SSL if you enable the following Windows security setting, either in the Windows Local Security Policy or as part of Group Policy:

     System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing

     ---

     You can change these details later if required, by editing the target file server properties.
     Click **Next** to continue.
   - On the summary page, click **Next** to add the Celerra/VNX device.
   - On the final page, click **Close** to exit from the wizard.

   Before you add target volumes for the Celerra/VNX device, ensure that the Enterprise Vault server that archives from the Celerra/VNX has its cache location configured.

   See "Specifying a cache location for retrieved Celerra/VNX files" on page 67.

Specifying a cache location for retrieved Celerra/VNX files

To improve performance, an Enterprise Vault server that retrieves files from an EMC Celerra/VNX device uses a cache location for temporary files.

Before you add target volumes for a Celerra/VNX device, ensure that the Enterprise Vault server that archives from the Celerra/VNX has its cache location configured.

Note: If you configure pass-through recall for NetApp filers, the Enterprise Vault server also uses this cache location for the files that it retrieves from NetApp filers.

To specify a cache location for retrieved Celerra/VNX files

1. In the Administration Console, expand the Enterprise Vault site until the **Enterprise Vault Servers** container is visible.
2. Expand the **Enterprise Vault Servers** container.
3. Right-click the server that will archive from the Celerra/VNX and, on the shortcut menu, click **Properties**.
4. Click the **Cache** tab.
5. Under **Cache Location**, enter an existing path on the Enterprise Vault server. The Vault Service account must have read and write access to the location.

   For more information on configuring the cache, click **Help** on the **Cache** tab.

Chapter 8

Configuring FSA with clustered file servers

This chapter includes the following topics:

About configuring FSA with clustered file servers

In an environment where Windows file servers are grouped in a cluster, you can make the FSA services that run on them highly available.

See "About using FSA with clustered file servers" on page 21.

FSA supports the following server cluster software:

- Windows Server Failover Clustering (formerly known as *Microsoft Cluster Server*, or *MSCS*)
- Veritas Cluster Server (VCS)

Refer to the Enterprise Vault *Compatibility Charts* for details of the supported versions of this software, and the supported versions of Windows. The *Compatibility Charts* document is available on the Symantec Enterprise Support site at this address:

http://www.symantec.com/docs/TECH38537

The following cluster types are supported:

- Active/passive cluster. To support high availability, the shared cluster resources are made available on one node of the cluster at a time. If a failure on the active cluster node occurs, the shared resources fail over to the passive node and users may continue to connect to the cluster without interruption.
- Active/active cluster. To support load balancing and high availability, the cluster resources are split among two or more nodes. Each node in the cluster is the preferred owner of different resources. In the event of a failure of either cluster node, the shared resources on that node fail over to the remaining cluster nodes.

Enterprise Vault supports multiple nodes in any combination of active/passive and active/active. We have validated configurations with up to four nodes.

You can configure a single-node cluster, if you first set a registry value on the computer that runs the Administration Console and on the clustered file server node.

Steps to configure FSA with clustered file servers

Table 8-1 describes the process to configure File System Archiving with clustered file servers.

Table 8-1 Steps to configure File System Archiving with clustered file servers

Step	Action	Description
Step 1	Prepare the cluster for configuring the FSA services.	See "Preparing to set up FSA services in a cluster" on page 70.
Step 2	For a VCS cluster, set up the required authentication on the Enterprise Vault server computer on which you run the Enterprise Vault Administration Console.	See "About authenticating the Administration Console with VCS for an FSA cluster" on page 72.

Table 8-1 Steps to configure File System Archiving with clustered file servers *(continued)*

Step	Action	Description
Step 3	Add the virtual file server as an archiving target and install the FSA Agent services on each node.	See "Adding the virtual file server as an FSA target" on page 75.
Step 4	Add an FSA resource to the cluster resource groups or service groups and make the resource highly available.	See "Configuring or reconfiguring the FSA resource" on page 77.

Note: If you have problems when following the process, refer to the troubleshooting information.

See "Troubleshooting the configuration of FSA with clustered file servers" on page 78.

Preparing to set up FSA services in a cluster

Before you set up FSA services for a file server cluster, perform the following steps:

- We recommend that you place the Enterprise Vault Administration Console and the target file servers in the same domain. If you place the Administration Console and the target file servers in separate domains, you must set up a domain trust relationship.
- Check that DNS entries are correct. There should be a reverse lookup entry for each of the following:
  - Each cluster node that is to support the FSA services resource.
  - The virtual file server that is to be added as a target file server for FSA.
- If you intend to set up a single-node cluster, you must first create the registry value SingleNodeFSA on the computer that runs the Administration Console and on the clustered file server node. Create SingleNodeFSA under the following registry key, and give it a DWORD value of 1:

On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \KVS
   \Enterprise Vault
    \FSA
```

On a 64-bit installation of Windows:

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

If you want to set up a single-node cluster, create this registry value before you do either of the following:

- Install the FSA Agent on the file server, if you perform this task from the Administration Console.
- Run the FSA Cluster Configuration wizard.

For more information on SingleNodeFSA, see its entry in the *Registry Values* guide.

- Ensure that the cluster group to which you want to add the FSA resource also has a shared disk resource (sometimes referred to as a physical disk resource or Mount/MountV resource). Only VCS or Windows Server failover cluster groups for which you have configured a shared disk resource are available for selection when you run the FSA Cluster Configuration wizard.
- The Vault Service account requires some specific permissions if you add the FSA resource to a file server cluster.
  See "Permissions required by the Vault Service account to support the FSA resource on clustered file servers" on page 176.
- For VCS configurations, make sure that the Public network connection is set as the top connection in the Connections list. Perform this procedure on each node in the cluster that is to include FSA services.

To ensure that the Public network is the top entry in the Connections list of each node

1. On a node that is to include FSA services, right-click **My Network Places**, and then click **Properties**.
2. On the **Advanced** menu, click **Advanced Settings**.
3. On the **Adapters and Bindings** tab, ensure that the Public network is the top entry in the Connections list.
4. Repeat steps 1 to 3 for each node that is to include FSA services.

About authenticating the Administration Console with VCS for an FSA cluster

Before you set up the FSA clustering feature on a VCS cluster you must set up the required authentication on the Enterprise Vault server computer that runs the Enterprise Vault Administration Console. Follow the appropriate instructions, depending on whether the cluster uses the Symantec Product Authentication Service (SPAS, formerly known as the Veritas Authentication Service):

- See "Authenticating the Administration Console when SPAS is used" on page 72.
- See "Authenticating the Administration Console when SPAS is not used" on page 73.

Authenticating the Administration Console when SPAS is used

If your VCS cluster uses SPAS, set up authentication for the Administration Console by performing the following procedures in the order shown:

- Install the SPAS client on the Enterprise Vault server computer on which you run the Enterprise Vault Administration Console.
- Set up a trust between the Administration Console computer and the Veritas Security Service Root Broker for VCS (VCS SS Broker). Set up the trust only once, not for each node.

To install the SPAS client on the Administration Console server

1. Obtain the SPAS binaries. These binaries are included in the **Symantec_Product_Authentication_Service** folder of the VCS media kit. If you cannot locate the SPAS binaries, contact Symantec support.

   Note: The version of the SPAS binaries that you install on the Enterprise Vault server must be the same as the version that is installed on the VCS cluster nodes.

2. Run the SPAS installer on the Enterprise Vault server computer on which you run the Enterprise Vault Administration Console.

   Select the **Typical** installation option, which installs the client feature only.

   For detailed information on how to set up SPAS, consult *Symantec Product Authentication Services QuickStart*.

To set up a trust between the Administration Console computer and the VCS SS Broker

1. Open a Command Prompt window on the Enterprise Vault Administration Console computer.
2. Navigate to the `bin` folder of the SPAS client installation, for example:

   ```
   C:\Program Files (x86)\Veritas\Security\Authentication\bin
   ```

3. Enter the following command:

   ```
   vssat setuptrust --broker VCS_Broker_Name:2821 --securitylevel
   high
   ```

   where *VCS_Broker_Name* is the VCS SS Broker node name.

   For example:

   ```
   vssat setuptrust --broker VCSNODEONE:2821 --securitylevel high
   ```

   Note that you must precede the `broker` parameter and the `securitylevel` parameter with double dashes, as shown. The port number must be 2821.

   If the trust is successfully created, the following message appears:

   ```
   setuptrust
   --------------------------
   --------------------------
   Setup Trust with Broker:   VCS_Broker_Name
   --------------------------
   ```

Authenticating the Administration Console when SPAS is not used

If you configured the VCS cluster to use VCS User Privileges instead of SPAS, set up authentication for the Administration Console by performing the following procedures in the order shown.

- Add the Vault Service account to the VCS cluster
- Install the SPAS client on the Enterprise Vault server computer on which you run the Enterprise Vault Administration Console.

To add the Vault Service account to the VCS cluster

1 Open a Command Prompt window on any of the VCS cluster nodes, and navigate to the following location:

```
VCS_installation_folder\cluster server\bin
```

2 Enter the following command to place the cluster in read-write mode:

```
haconf -makerw
```

3 Enter the following command to add the Vault Service account.

```
hauser -add Vault_Service_account -priv Administrator
```

where *Vault_Service_account* is the Vault Service account. Enter the account in the format *accountname*, for example `vaultadmin`. When `hauser` prompts you for the account password, enter the Vault Service account password.

If the authentication fails, try repeating the command with the account in the format *accountname*`@`*domain.ext*, for example `vaultadmin@demo.local`.

4 Enter the following command to verify that the Vault Service account has been added to the VCS user list as an administrator:

```
hauser -display Vault_Service_account
```

The output should be as follows:

```
Vault_Service_account : ClusterAdministrator
```

5 Save the cluster configuration:

```
haconf -dump -makero
```

To install the SPAS client on the Administration Console server

1 Obtain the SPAS binaries. These binaries are included in the **Symantec_Product_Authentication_Service** folder of the VCS media kit. If you cannot locate the SPAS binaries, contact Symantec support.

Note: The version of the SPAS binaries that you install on the Enterprise Vault server must be the same as the version that is installed on the VCS cluster nodes.

---

2 Run the SPAS installer on the Enterprise Vault server computer on which you run the Enterprise Vault Administration Console.

Select the **Typical** installation option, which installs the client feature only.

For detailed information on how to set up SPAS, consult *Symantec Product Authentication Services QuickStart*.

Adding the virtual file server as an FSA target

We recommend that you add the virtual file server as a target file server for FSA, rather than adding the individual cluster nodes as targets.

To add a virtual file server as an FSA target

1. If you intend to install the FSA Agent in step 6, then if the cluster nodes' firewalls are on, ensure that the firewalls are suitably configured.

   See "Configuring a file server's firewall for FSA" on page 45.

   Alternatively, install the FSA Agent manually on each node in the cluster. You can perform the manual installation of the FSA Agent before or after you add the target file server.

   See "Installing the FSA Agent manually" on page 84.

2. Start the Enterprise Vault Administration Console. If you want to install the FSA Agent or to add an FSA Resource to the cluster group during this procedure, you must run the Administration Console with an account that is a member of the local Administrators group on each file server node. If you want to add an FSA Resource you must also use an account that has Full Control permission on the `FSA Cluster` folder of the Enterprise Vault server. The `FSA Cluster` folder is a subfolder of the `Utilities` folder under the Enterprise Vault installation folder. For example:

   ```
   C:\Program Files (x86)\Enterprise Vault\Utilities\FSA Cluster
   ```

3. In the left pane of the Enterprise Vault Administration Console, expand the Enterprise Vault site until the **Targets** container is visible.

4. Expand the **Targets** container.

5. Right-click the **File Server** container and on the shortcut menu, click **New** and then **File Server**. The New File Server wizard starts.

6. Enter the name of the virtual file server.

   Select the option to install the FSA Agent on the file server, unless you plan to install the FSA Agent manually. If you choose to install the FSA Agent, the wizard prompts you for the Vault Service account password. The wizard then installs the FSA Agent services on each node. After the services are installed, the wizard sets the services' logon credentials to use the Vault Service account, and then starts the services on each node.

7 To add an FSA resource to the cluster group now, click **Configure FSA Cluster** to launch the FSA Cluster Configuration wizard. Alternatively you can run the FSA Cluster Configuration wizard later, if you prefer.

The FSA Cluster Configuration wizard takes you through the steps to add the FSA resource to the set of resources that comprise a cluster resource group or service group. It also enables you to configure the FSA resource for high availability, if required. If you configure the FSA resource for high availability you can then monitor the FSA services and, if there is a problem with the node on which they are running, automatically move them to a working node in the cluster.

See "Configuring or reconfiguring the FSA resource" on page 77.

On the final screen of the FSA Cluster Configuration wizard, click **View log** to view details of the configuration changes in `FSACluster.log`. When the FSA Cluster Configuration wizard finishes, it returns you to the New File Server wizard.

8 The final screens of the New File Server wizard vary, depending on whether you have already configured the FSA Reporting database:

- If you have not configured FSA Reporting, the wizard displays a message that begins "FSA Reporting is not configured". It then skips to the final wizard page. You can configure FSA Reporting when the wizard has finished, if required.
  See "About FSA Reporting" on page 34.
- If you have configured FSA Reporting, the New File Server wizard asks you if you want to enable data collection for FSA Reporting. If you choose to enable data collection the wizard then gives you the option to configure a non-default data collection schedule for the file server. You can perform these tasks later, if you want. For more details, see the help on the wizard pages.

9 When the FSA Agent installation is complete, you can configure the file server's properties and add target volumes as required.

Note the following if you configure File Blocking in a clustered environment where multiple cluster groups can come online on the same cluster node. You must ensure that the following settings have the same values for all the virtual servers that can be online concurrently on the same node:

- The quarantined files location.
- The list of file blocking exemption files.

These settings are on the **File Blocking** tab of the File Server Properties.

Note that if you configure pass-through recall for a file server cluster, all the cluster nodes must use identical pass-through recall settings.

See "About configuring pass-through recall for a file server cluster" on page 119.

Configuring or reconfiguring the FSA resource

You can add the FSA resource to the cluster groups or reconfigure the FSA resource settings by running the FSA Cluster Configuration wizard.

Note: You must run the FSA Cluster Configuration wizard with an account that is a member of the local Administrators group on each node of the file server cluster. The account must also have Full Control permission on the `FSA Cluster` folder of the Enterprise Vault server. The `FSA Cluster` folder is a subfolder of the `Utilities` folder under the Enterprise Vault installation folder. For example:

```
C:\Program Files (x86)\Enterprise Vault\Utilities\FSA Cluster
```

To configure or reconfigure the FSA resource

1. Start the FSA Cluster Configuration wizard in one of the following ways:
   - When you add the virtual file server as a target, click **Configure FSA Cluster** in the New File Server wizard
   - If you have already added the clustered file server as a target, then in the left pane of the Enterprise Vault Administration Console, right-click the clustered file server target and then click **FSA Cluster Configuration**.
2. When the welcome page of the FSA Cluster Configuration wizard appears, click **Next**.
3. Select **Add**, **remove**, **or reconfigure the FSA resource for groups that have shared disks**, and then click **Next**.
4. Select the cluster groups that are to include the FSA resource.

   If you check **Services HA** for a selected group, and there is a problem with the node on which the FSA services are running, then the FSA services and all the other resources in the group automatically failover to a working node in the cluster. In effect, by checking **Services HA**, you make the failure of the FSA services on one node a sufficient reason to move all the resources to another node.

5 Click **Next**, and then wait for the FSA Cluster Configuration wizard to apply your requested settings to the cluster group.

6 The wizard displays a summary of the changes that it has made to the cluster group. You can click **View log** to view details of the configuration changes in `FSACluster.log`. Click **Finish** to close the wizard.

Removing the FSA resource from all cluster groups

When you have no further need to make the FSA services highly available, you can remove them from the cluster groups to which you previously added them.

Note: You must run the FSA Cluster Configuration wizard with an account that is a member of the local Administrators group on each node of the file server cluster. The account must also have Full Control permission on the `FSA Cluster` folder of the Enterprise Vault server. The `FSA Cluster` folder is a subfolder of the `Utilities` folder under the Enterprise Vault installation folder. For example:

```
C:\Program Files (x86)\Enterprise Vault\Utilities\FSA Cluster
```

To remove the FSA resource from all cluster groups

1 In the left pane of the Vault Administration Console, right-click a clustered file server and then click **FSA Cluster Configuration**.

2 When the welcome page of the FSA Cluster Configuration wizard appears, click **Next**.

3 Select **Remove the FSA resource from all groups**, and then click **Next**.

4 Click **Yes** to confirm that you want to remove the FSA resource from the cluster groups.

5 Click **Finish**.

Troubleshooting the configuration of FSA with clustered file servers

If you experience problems when you configure FSA clusters, try the following troubleshooting steps.

To troubleshoot the configuration of FSA with clustered file servers

1. Verify that you have installed and configured the FSA services on each node to which the cluster group can fail over.
2. Ensure that the ClusSvc service (for Windows Server Failover Clustering) or Had service (for Veritas Cluster Server) is configured and running on the file server.
3. Check the log files. The FSA Cluster Configuration wizard stores details of the changes that it has made in the file `FSACluster.log`, which is located in the `\Utilities\FSA Cluster` subfolder of the Enterprise Vault program folder (for example, `C:\Program Files (x86)\Enterprise Vault`).

   The wizard creates additional log files on the individual cluster nodes when you configure a group for FSA services high availability. These log files are named `FSA-MSCSType.log` or `FSA-VCSType.log`, depending on whether you are using Windows Server Failover Clustering or Veritas Cluster Server, and they are stored in the FSA Agent installation folder.

   The LogLevel registry value determines the level of logging. This registry value is located under the following registry key:

   On a 32-bit installation of Windows:

   ```
   HKEY_LOCAL_MACHINE
    \SOFTWARE
     \KVS
      \Enterprise Vault
       \FSA
   ```

   On a 64-bit installation of Windows:

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

   LogLevel can have a value in the range 0 through 5, where 0 or 1 records critical messages only, whereas 5 records debug and diagnostic messages.
4. You can run DTrace on the FSA Cluster Configuration wizard — on the Enterprise Vault server that hosts the Enterprise Vault Administration Console, run DTrace on FSAClusterWizard.

   You can also run DTrace on the FSA cluster node — on the FSA cluster node where the FSA resource is online, run DTrace on FSAClusterAssist and the Placeholder service.

   If the DTrace **view** command does not include FSAClusterWizard or FSAClusterAssist in the list of processes that are available to monitor, register the file with DTrace as follows:

   - Enter the following command from DTrace:

```
set FSAClusterWizard.exe
```

or

```
set FSAClusterAssist.exe
```

- Then register the name when DTrace prompts you.

For more information on DTrace, see the *Utilities* manual.

'Failed to collect clustering data' error on starting FSA Cluster Configuration wizard

The following error message can appear when you start the FSA Cluster Configuration wizard in the Enterprise Vault Administration Console:

```
"Failed to collect clustering data
from file server 'servername'.

See the "Installing and Configuring
Enterprise Vault" manual for guidance."
```

This message may appear because the Symantec Product Authentication Service is not available in the VCS cluster and the Vault Service account cannot authenticate and log in to the VCS cluster.

Note that this error message is not specific to this situation. It may also be displayed for other cluster-related issues.

If the Symantec Product Authentication Service is not available, then you need to add the Vault Service account to the VCS user list.

See "Authenticating the Administration Console when SPAS is not used" on page 73.

Chapter 9

Installing the FSA Agent

This chapter includes the following topics:

About installing the FSA Agent on a Windows file server

If you want to use placeholder shortcuts, File Blocking, or FSA Reporting with a Windows file server, you must install the FSA Agent on the file server.

Note the following:

- Do not install the FSA Agent on Enterprise Vault servers, NetApp filers, or EMC Celerra/VNX devices.
- You cannot install the FSA Agent on a Windows file server that is running Windows Server 2003 x86 or x64 or Windows Server 2008 x86.

For details of the supported versions and required service packs of the Windows operating system, see the Enterprise Vault *Compatibility Charts* at http://www.symantec.com/docs/TECH38537.

For a Windows server other than a Server Core installation, the FSA Agent requires the following prerequisites on the file server:

- Windows Installer 3.1
- .NET Framework 3.5 SP1 or SP2

For a Windows Server 2008 Server Core installation, the prerequisites are that the following optional Windows features are enabled:

- ServerCore-WOW64 (installed by default)
- NetFx2-ServerCore
- NetFx2-ServerCore-WOW64

For a Windows Server 2012 Server Core installation, the prerequisites are that the following optional Windows features are enabled:

- ServerCore-WOW64
- NetFx3
- NetFx3ServerFeatures

Note: FSA Agent installation requires an up-to-date VeriSign root certificate on the target computer. Certificate updates usually happen automatically over the Internet. If the certificate is out-of-date, for example because the computer has no Internet connection, the FSA Agent installation fails with a 'Signature verification failed' error in the FSA Agent installation log. For more details and for instructions on how to update the root certificate, see the following technical note on the Symantec Support website:

http://www.symantec.com/docs/TECH179712

You can install the FSA Agent on the file server from the Administration Console, or manually.

Table 9-1 lists the options for installing the FSA Agent.

Table 9-1 Options for installing the FSA Agent

Method	Notes	Description
Installation from the Administration Console. ("Push install")	If the file server's firewall is on, the firewall must be suitably configured to allow access. You must run the Administration Console with an account that is a member of the local Administrators group on the file server. Requires the password of the Vault Service account.	See "Installing the FSA Agent using the Install FSA Agent wizard" on page 83.

Table 9-1 Options for installing the FSA Agent *(continued)*

Method	Notes	Description
Manual installation on the file server.	Does not require access through the file server's firewall. The MSI installation kits and other required files are provided on the Enterprise Vault server. You must use an account that is a member of the local Administrators group on the file server. Requires the user name and password of the Vault Service account.	See "Installing the FSA Agent manually" on page 84.

Note: Before you install any antivirus product on a file server on which you have installed the FSA Agent, we recommend that you stop the File Placeholder Service on the file server. After completing the installation of the antivirus product, you must restart the File Placeholder Service.

See "About the FSA Agent" on page 32.

Installing the FSA Agent using the Install FSA Agent wizard

The following procedure describes how to install the FSA Agent on a target Windows file server by using the Enterprise Vault Administration Console's Install FSA Agent wizard.

Note: If you have not yet added the file server as an archiving target in the Administration Console, you can install the FSA Agent as part of that procedure

See " Adding a Windows file server as an archiving target" on page 46.

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

See "Adding the virtual file server as an FSA target" on page 75.

To install the FSA Agent using the Install FSA Agent wizard

1. If the file server's firewall is on, ensure that the firewall is suitably configured, otherwise the installation will fail.

   See "Configuring a file server's firewall for FSA" on page 45.

   Alternatively, perform a manual installation of the FSA Agent.

   See "Installing the FSA Agent manually" on page 84.
2. Run the Administration Console with an account that is a member of the local Administrators group on the file server.
3. In the Administration Console, expand the Enterprise Vault site until the **Targets** container is visible.
4. Expand the **Targets** container.
5. Expand the **File Servers** container.
6. Right-click the server on which you want to install the FSA Agent and, on the shortcut menu, click **Install FSA Agent**.
7. Work through the wizard.

Installing the FSA Agent manually

Follow the procedure below to perform a manual installation of the FSA Agent and its prerequisites on a Windows server.

The FSA Agent supports AMD64 and Intel EM64T, but it does not currently support Intel Itanium.

To install the FSA Agent manually

1. Find the FSA Agent files on the Enterprise Vault server. The files are in the `evpush\Agent` folder under the Enterprise Vault installation folder; for example, `C:\Program Files (x86)\Enterprise Vault\evpush\Agent`.
2. Install the required Microsoft Visual C++ redistributable packages on the file server:
   - `vcredist_x86.exe`
   - `vc2005redist_x86.exe`
   - `vcredist_x64.exe`
3. Copy the `Enterprise Vault File System Archiving x64.msi` file to the file server.
4. Log on to the file server with an account that is a member of the local Administrators group on the file server.

5 Perform an interactive installation or silent installation of the FSA Agent. With a silent installation, no notification messages appear on the console.

- To perform an interactive installation, double-click the MSI file, or open a Command Prompt window and enter a command similar to the following:

  ```
  msiexec.exe /i path_to_.msi_file /L*v logfilename
  ```

  The installer prompts you to specify the installation folder and the credentials of the user account that will log on to use this application. You must specify the name and password of the Vault Service account. The installer uses these credentials to configure the FSA services.

  If you used an msiexec.exe command, any installation messages appear in the specified log file.

- To perform a silent installation, open a Command Prompt window and enter a command similar to the following:

  ```
  msiexec.exe /i path_to_.msi_file /L*v logfilename
  [INSTALLDIR=installpath]
  IS_NET_API_LOGON_USERNAME=Domain\Username
  IS_NET_API_LOGON_PASSWORD=password /q
  ```

  Any installation messages appear in the log file specified. Note that the logon user name must be the Vault Service account in the format *Domain\Username*.

  You can use INSTALLDIR to specify an installation location other than the default path on the system drive, if required.

For example, the following command performs a silent installation of the FSA Agent:

```
msiexec.exe /i "C:\TEMP\FSA\Agent\Enterprise Vault File System
Archiving x64.msi" /L*v fsainstall.log
IS_NET_API_LOGON_USERNAME=DOMAIN1\VSA
IS_NET_API_LOGON_PASSWORD=Ev@ult-723 /q
```

6 When the installation of the FSA Agent is complete, start the following services from the Windows Services MMC snap-in, if they are not already started:

- Enterprise Vault File Blocking service
- Enterprise Vault File Collector service
- Enterprise Vault File Placeholder service

About FSA Agent uninstallation

You can uninstall the FSA Agent from a Windows file server by using the Add or Remove Programs facility in the Windows Control Panel.

You should not install the FSA Agent on a computer on which Enterprise Vault is also installed. If you do have a computer on which both Enterprise Vault and the FSA Agent are installed, you must uninstall Enterprise Vault before you can uninstall the FSA Agent. In this case you may prefer to disable the FSA Agent instead of uninstalling it.

Updating the logon credentials of the FSA Agent services

The FSA Agent services use the Vault Service account credentials to log on. If you change the Vault Service account password then for each computer that has the FSA Agent installed you must update the properties of the FSA Agent services to use the new password.

- For target Windows file servers, use the Update Service Credentials wizard in the Administration Console. Run the wizard on each target Windows file server that has the FSA Agent installed.
  See "To update the logon credentials of the FSA Agent services on target Windows file servers" on page 86.
- For FSA Reporting proxy servers that are not target Windows file servers or Enterprise Vault servers, you must update the logon credentials of the FSA Agent services manually.
  See "To update the logon credentials of the FSA Agent services manually" on page 87.

Note: Enterprise Vault servers do not run the FSA Agent services.

To update the logon credentials of the FSA Agent services on target Windows file servers

1. If the file server's firewall is on, ensure that the firewall is suitably configured, otherwise the update will fail.

   See "Configuring a file server's firewall for FSA" on page 45.

   Alternatively, you can perform a manual update of the services.

   See "To update the logon credentials of the FSA Agent services manually" on page 87.
2. In the Administration Console, expand the Enterprise Vault site until the **Targets** container is visible.
3. Expand the **Targets** container.

4 Expand the **File Servers** container.

5 Right-click the server on which you want to update the logon credentials and click **Update Service Credentials**.

6 Work through the wizard.

The wizard prompts you for the Vault Service account password. It then updates the logon credentials of the FSA Agent services, and starts or restarts the services to implement the change.

To update the logon credentials of the FSA Agent services manually

1 Open the Windows Services MMC snap-in on the computer.

Perform the remaining steps for each installed FSA Agent service:

- Enterprise Vault File Blocking service
- Enterprise Vault File Collector service
- Enterprise Vault File Placeholder service

2 Right-click the service and choose **Properties**.

3 On the **Log On** tab, edit **Password** to specify the new Vault Service account password.

4 Edit **Confirm password** to confirm the new password.

5 Click **OK** to exit from the properties.

6 Restart the service for the change to take effect.

Chapter 10

Defining volume and folder policies

This chapter includes the following topics:

About defining FSA volume and folder policies

This section describes how to set up volume policies and folder policies for File System Archiving.

There is separate documentation on how to create and assign retention folder policies.

See "Configuring retention folders" on page 124.

Creating FSA volume policies and folder policies

You can create a new policy by using the New Policy wizard, or make a copy of an existing policy to modify as required.

To create an FSA volume policy or folder policy with the New Policy wizard

1. In the Administration Console, expand the Enterprise Vault site until the **Policies** container is visible.
2. Expand the **Policies** container.
3. Expand the **File** container.
4. Right-click **Volume** or **Folder** as required and on the shortcut menu, click **New** and then **Policy**.
5. Work through the New Policy wizard.

   See "About FSA volume policy and folder policy properties" on page 89.

To copy an FSA policy to use as a template for a new policy

1. In the Administration Console, expand the Enterprise Vault site until the **Policies** container is visible.
2. Expand the **Policies** container.
3. Expand the **File** container.
4. Select **Volume** or **Folder**, as required.
5. Right-click the policy that you want to copy and then, on the shortcut menu, click **Copy Policy**.
6. Enter a new name and description for the policy.
7. Click **OK** to save the copy.
8. Double-click the new copy to display its properties.
9. Edit the properties of the copy as required.

   See "About FSA volume policy and folder policy properties" on page 89.

About FSA volume policy and folder policy properties

FSA volume and folder policies define the following:

- For volume policies only: File Blocking rules to apply to the volume, if required. See "About configuring File Blocking" on page 132.
- For volume policies only: whether to enable quotas for the volume, and what quotas to use.
- The retention category to apply to the files that are archived with the policy.
- The type of shortcut to leave to an archived file, if the archiving rules specify that a shortcut is created.

See "About selecting the shortcut type for an FSA policy" on page 90.

- The archiving rules to apply in the policy. You define these rules to select the files to match the rule, Enterprise Vault to archive or delete. The rules are applied in the order in which you list them.
  See "About FSA policy archiving rules" on page 91.
- Whether to archive files that have explicit permissions, and files that are under Dynamic Access Control.
  See "About options for archiving files that have explicit permissions, and files under DAC" on page 94.

About selecting the shortcut type for an FSA policy

The **Shortcuts** tab of the properties of an FSA volume policy or folder policy specifies the type of shortcut to leave to an archived file, when the archiving rules specify that a shortcut is to be created. You can choose to leave a placeholder shortcut or an internet link.

See "About FSA shortcut files" on page 27.

If you choose to leave a placeholder shortcut, you must make sure that the FSA Agent is installed on any Windows file servers to which the policy is applied.

If you leave a placeholder shortcut you can choose whether to do the following:

- Delete placeholders for the items that have been deleted from archives.
- Delete archived files when placeholders are deleted.
  See "About configuring the deletion of archived files on placeholder deletion" on page 96.

If you leave placeholder shortcuts, make sure that your system does not recall the archived files inadvertently.

See "About preventing unwanted file recalls from placeholder shortcuts" on page 167.

About choosing not to display the file size in NetApp placeholder shortcuts

By default, a placeholder shortcut shows the size of the file that it replaced, although the shortcut itself takes up very little space.

Enterprise Vault incurs a performance overhead when it determines the original file size for a placeholder on a NetApp filer. This overhead can become significant under some circumstances. To avoid the performance overhead, you can use the registry value SetNetappPHOriginalSize to turn off the file size determination process for NetApp placeholders. NetApp placeholders then show a file size of 0 KB.

For more details, see the description of SetNetappPHOriginalSize in the *Registry Values* manual.

About FSA policy archiving rules

When you create an FSA volume policy or folder policy you must define the archiving rules to apply, and the order in which to apply them. Each archiving rule specifies the following:

- The file criteria to match, such as the file type, the time that the file was last modified or last accessed, the file size, and file attributes.
  See "Tips for creating FSA policy archiving rules" on page 91.
- The action to take on the files that match the file criteria. You can choose **Archive**, **Do not archive**, **Delete**, or **Archive copy and reset**. For more information, see the help in the Administration Console for the rule's **General** tab.
- Whether and when to create shortcuts for the matching files. If you choose to create shortcuts you can create them immediately or some time later, according to criteria that you specify.
  See "FSA shortcut creation options" on page 92.

Tips for creating FSA policy archiving rules

Note the following when you create archiving rules in FSA's volume policies and folder policies:

- An archiving rule is applied to a file when all the criteria match. You may find that some files that you expect to be matched by a rule are not matched because, for example, the attributes are not matched exactly.
- Do not apply too many rules in a policy. This makes it easier to apply the same policy to multiple volumes or folders. Also, by keeping it simple, you are less likely to get results you do not expect.
- You can use File Groups to simplify rule creation. A file group enables you to specify several different file types to that are to be treated together for the purposes of file archiving.
  For example, you could create a file group called "webpages" and within it have the file types *.htm, *.html, and *.gif. Within a File System Archiving policy you could then define a rule that applied to "webpages".
  File Groups are in the "File Groups" Administration Console container, under the "File" policies container.
- If appropriate, you can add rules to prevent the archiving of specific files.

See "About excluding specific Mac and Windows file types from archiving" on page 92.

- The **Remove safety copies** setting for the vault store may temporarily prevent Enterprise Vault from creating shortcuts.
  See "FSA shortcut creation options" on page 92.
- When you have set up File System Archiving for a volume or folder, perform an archive run in Report Mode and then check the report to make sure that the rules are matching the files you expect.

About excluding specific Mac and Windows file types from archiving

While FSA can archive any file that it encounters on a file system, some file types may not be good candidates for archiving, such as operating system files, and PST or NSF files.

Enterprise Vault includes two predefined file groups called Mac Files and Windows Files, which define a set of Mac file types and Windows file types respectively. If you archive from a file server that includes Mac files or Windows files, you can use these file groups to create rules to prevent these file types from being archived.

The Default Volume Policy and Default Folder Policy include two rules called Exclude Mac Files and the Exclude Windows Files. These rules are also available in the New Policy wizard. We recommend that you use these rules to exclude system file types that may not be good candidates for archiving or for being turned into shortcuts.

Note that these rules are not enabled by default.

Before you use these rules, examine the list of file types in the related file group. The file types have been added as result of feedback from the existing installed base. Edit the list of file types to match your exclusion requirements, if necessary.

Note: File Blocking cannot perform content checking for the supplied file types in the Mac Files file group and the Windows Files file group.

FSA shortcut creation options

The **Shortcut Creation** tab of an FSA policy archiving rule provides the following shortcut creation options:

- **None. Archive and delete file**. Do not create any shortcuts to archived files. Enterprise Vault archives the files that meet the archiving criteria and then deletes the files.

- **Create shortcut immediately**. Archive the files that meet the archiving criteria and then create shortcuts to the archived files.
- **Create shortcut later**. Archive the files that meet the archiving criteria but do not delete the files. Enterprise Vault leaves the files on the file server until they meet the date criteria you define on this tab. This option enables you to archive the files but to leave the original files in place until they are no longer needed. This means that a user can read or edit the files without them being recalled from the archive.

  You can select one or more of the following time conditions. If you specify more than one time condition, Enterprise Vault does not create shortcuts until all the conditions are satisfied.

  - **Last archive time is**. Enterprise Vault creates shortcuts when the specified time has elapsed since the last time the file was archived. This option enables you to ensure that shortcuts are not created for frequently-archived files.
  - **Last access time is**. Enterprise Vault creates shortcuts when the specified time has elapsed since the last time the file was accessed. This option enables you to ensure that shortcuts are not created for frequently-accessed files.
  - **Last modified time is**. Enterprise Vault creates shortcuts after the specified time has elapsed since the last time the file was modified. This option enables you to ensure that shortcuts are not created for frequently-modified files.
  - **Created time is**. Specifies that Enterprise Vault must create shortcuts when the specified time has elapsed since the file was created.

Note that Enterprise Vault checks the vault store setting for **Remove safety copies** before creating shortcuts. If safety copies cannot be removed because of this setting, Enterprise Vault does not create shortcuts.

Table 10-1 shows how the vault store's **Remove safety copies** setting can affect shortcut creation.

Table 10-1 Effect of Remove Safety Copies setting on shortcut creation

Remove Safety Copies Setting	Shortcut Creation Setting		
	None. Archive and delete file	Create shortcut immediately	Create shortcut later
Immediately after archive	Delete original file	Create shortcut immediately	Create shortcut later
Never	Leave the original file	Leave the original file	Leave the original file

Table 10-1 Effect of Remove Safety Copies setting on shortcut creation *(continued)*

Remove Safety Copies Setting	Shortcut Creation Setting		
	None. Archive and delete file	Create shortcut immediately	Create shortcut later
After backup	Delete original file after backup	Create shortcut after backup	Create shortcut later, after backup

Notes on FSA shortcut creation

- A File System Archiving task does not create a shortcut for a file that is moved to a different folder after being archived.
- Enterprise Vault creates shortcuts according to the archiving rules at the time the shortcut is created. If you change the rules after a file is archived and before the shortcut is created, Enterprise Vault uses the new criteria.
- Be careful not to specify unintentionally a policy archiving rule that means shortcuts are never created. If you use a time selection of **'within the last'** on the **Time and Size** tab and choose **'Create shortcut later'** on the **Shortcut Creation** tab, it is possible that Enterprise Vault never creates the shortcuts. The conflict can occur because the File System Archiving task processes the files that match the settings on **'Time and Size'** tab. If the task does not process the file, the shortcut is not created.
  When you select **'Create shortcut later'** the file must match both the following at the time you want the shortcut to be created:
  - The settings on the **'Time and Size'** tab
  - The settings on the **'Shortcut Creation'** tab

About options for archiving files that have explicit permissions, and files under DAC

FSA volume policies and folder policies let you specify whether to archive the following:

- Files that have explicit permissions. That is, files with permissions applied directly to them. Note that when evaluating a file for explicit permissions, Enterprise Vault ignores Dynamic Access Control (DAC) permissions.

- Files that are under DAC. That is, files whose access is controlled completely or partially through a DAC central access policy, user claim, or device claim.

The default policy setting is not to archive these files.

Before you choose to archive files that have explicit permissions or files that are under Dynamic Access Control, note the following:

- In the archive no explicit file permissions apply, and no DAC permissions apply. The result is that an archived file has the permissions of its parent folder, less any DAC permissions.
- If Enterprise Vault leaves a placeholder shortcut, the placeholder has all the permissions of the original file.

The absence of explicit file permissions and all DAC permissions in the archive has the following consequences:

- A user who has conventional (non-DAC) permission to access a folder can find and access any file in the associated archive folder. However, if the user did not have permission to access the original file, the user cannot access the archived file from its placeholder.
- A user who has conventional (non-DAC) permission to delete items from a folder can delete the archived version of any file from the associated archive folder. However, if the user did not have permission to delete the original file, the user cannot delete its placeholder.
- A user who has access to a file through DAC alone cannot access the file in the archive.
  Note that to allow access to files in the archive, you can set permissions manually on an archive from the Enterprise Vault Administration Console. If you set permissions on an archive they are applied to every folder in the archive.
- If a file is restored from the archive, the restored file has the original parent folder permissions, less any DAC-related permissions that were applied directly to the file.

If a file is recalled from a placeholder, the placeholder's permissions are retained in the recalled file. The recalled file has all the permissions of the original file, unless the permissions of placeholder or the inherited permissions of any of its parent folders were changed.

Chapter 11

Configuring the deletion of archived files on placeholder deletion

This chapter includes the following topics:

About configuring the deletion of archived files on placeholder deletion

If you choose to leave placeholder shortcuts, you can configure Enterprise Vault to delete archived files when their placeholders are deleted. You must configure some settings for the file server, and apply an archiving policy with the appropriate settings.

Note that if you move placeholders to a different location, the archiving policy that applies to the destination location determines whether the archived files are deleted on placeholder deletion.

For Windows file servers and NetApp filers, Enterprise Vault maintains a cache of the "Delete archived file when placeholder is deleted" policy settings. This DOD cache holds the policy setting for each local target volume and target folder, including retention folders. For Windows file servers the DOD cache is located on the file

server. For NetApp filers the DOD cache is located on the Enterprise Vault server. The location is not configurable.

When a placeholder is deleted on a Windows file server or a NetApp filer, Enterprise Vault does as follows:

- It identifies the parent target folder that is closest to the folder from which the placeholder was deleted.
- It obtains from the DOD cache the value of the "Delete archived file when placeholder is deleted" setting that applies to the target folder.
- It uses the value from the DOD cache to determine whether to delete the archived file. If the DOD cache value specifies deletion, Enterprise Vault immediately deletes the archived file.

If Enterprise Vault is unable to identify the parent target folder for a deleted placeholder, it logs an error in the event log. It does not delete the archived file.

Note: Enterprise Vault updates the DOD cache every hour by default. A delay of up to an hour may therefore occur before Enterprise Vault's deletion behavior reflects a change to this policy setting.

See "Configuring the deletion of archived files on placeholder deletion for Windows file servers and NetApp filers" on page 98.

For EMC Celerra/VNX devices Enterprise Vault uses a different mechanism:

- To configure archived file deletion with Celerra/VNX you must configure a target volume whose share points to the root of the file system. The "Delete archived file when placeholder is deleted" policy setting that applies to this root volume determines this policy setting for all of the file system's archived files. The root volume's policy setting overrides any "Delete archived file when placeholder is deleted" policy setting that you apply to any other target volumes or target folders in the same file system.
- For Celerra/VNX placeholders, Enterprise Vault does not use a DOD cache. When a Celerra/VNX placeholder is deleted, Enterprise Vault examines the value of the "Delete archived file when placeholder is deleted" setting for the policy that applies to the Celerra/VNX target root volume.
- You must enable FileMover logging on the Celerra/VNX device. Enterprise Vault uses the Celerra/VNX FileMover log's records of deleted placeholders to determine which archived files to delete.
- The deletion of the archived Celerra/VNX files does not occur immediately upon placeholder deletion. Deletion from the Celerra/VNX takes place daily according

to the schedule that is specified in the properties of the File System Archiving task.

See "Configuring the deletion of files on placeholder deletion for EMC Celerra/VNX devices" on page 99.

Configuring the deletion of archived files on placeholder deletion for Windows file servers and NetApp filers

Use the following procedure to configure the deletion of archived files when placeholders are deleted, for Windows file servers and NetApp filers.

Note that Enterprise Vault does not delete the archived files in the following circumstances:

- For NTFS volumes on which pass-through recall is enabled. This combination of settings can result in data loss.
- If the archiving policy applies a retention category with the setting **Prevent user deletion of items with this category** selected.
- For NetApp filers that run Data ONTAP 7.3, if the path to the folder that contains the placeholder exceeds 256 characters. This path length limit is due to a NetApp Data ONTAP 7.3 FPolicy restriction.
- For NetApp filers that run Data ONTAP 8.2 (C-Mode), if the path to the folder that contains the placeholder exceeds 512 characters. This path length limit is due to a NetApp Data ONTAP 8.2 FPolicy restriction.

To configure deletion of archived files on placeholder deletion for Windows file servers and NetApp filers

1. Select the **Delete archived file** option on the **Delete Placeholder** tab of the file server's properties.
2. We recommend that you specify a safety folder when you use the **Delete archived file** option. An archived item is not deleted if its placeholder is deleted from a safety folder. On the **Delete Placeholder** tab, specify the folders to use as safety folders.

   A safety folder is useful when a user deletes a file accidentally. You can restore files temporarily from backups to the safety folder so that the user can find the file. The user can delete placeholders from the safety folder without deleting the corresponding archived items.
3. Where required in your file archiving policies, check **Delete archived file when placeholder is deleted** on the **Shortcuts** tab.

Note: Enterprise Vault does not act on the changes to this setting until it updates the DOD cache.

See "About configuring the deletion of archived files on placeholder deletion" on page 96.

Configuring the deletion of files on placeholder deletion for EMC Celerra/VNX devices

Use the following procedure to configure the deletion of archived files when placeholders are deleted, for EMC Celerra and VNX devices.

Note: Do not configure this option for Celerra/VNX devices if you configure the pass-through setting on the Celerra/VNX device. The combination of these options can result in data loss.

Enterprise Vault does not delete the archived files if the archiving policy applies a retention category with the setting **Prevent user deletion of items with this category** selected.

To configure deletion of archived files on placeholder deletion for EMC Celerra/VNX devices

1. Configure a target volume under the target Celerra/VNX device whose share points to the root of the file system.
2. Apply an archiving policy to the root volume in which the setting **Delete archived file when placeholder is deleted** is selected on the **Shortcuts** tab.

   Note that this root volume policy setting controls the deletion of archived files on placeholder deletion for all of the Celerra/VNX file system:

   - If you configure any additional target volumes that point to specific folders in the same Celerra/VNX file system, Enterprise Vault ignores the policy setting that applies to the folder volume.
   - Enterprise Vault ignores the "Delete archived file when placeholder is deleted" policy setting in any folder policies that apply to target folders.
3. Enable FileMover logging on the Celerra/VNX device. Logging must be enabled for file deletion to work. You can test whether logging is enabled from the **EMC Celerra** tab in the properties of the Celerra/VNX target volume.

   Note: Enterprise Vault performs archived file deletion for all of the placeholder deletions that are listed in the log. The file deletion occurs even if the placeholder deletion took place before you applied the "Delete archived file when placeholder is deleted" policy setting. If possible, do not enable FileMover logging before you apply the policy setting.

   ---
4. Set the `DeleteOnDelete` registry value on the Enterprise Vault server whose File System Archiving task processes the root volume.

   Set the value as follows:

   - Start the Windows registry editor `regedit` on the Enterprise Vault server.
   - Find the following registry key:

     ```
     HKEY_LOCAL_MACHINE
      \SOFTWARE
       \Wow6432Node
        \KVS
         \Enterprise Vault
          \FSA
           \ArchivedFilesFlags
     ```

   You must create the **ArchivedFilesFlags** key if it does not exist.

- Create a DWORD registry value named **DeleteOnDelete** under the **ArchivedFilesFlags** key, if this registry value does not already exist.
- Give **DeleteOnDelete** a value of **1**. This value means “Delete an archived Celerra/VNX file when its placeholder is deleted”.
  Alternatively you can turn off Celerra/VNX archived file deletion on placeholder deletion by setting this value to **0**.
- Save the changes and quit the registry editor.

5 Restart the Enterprise Vault Admin service on the Enterprise Vault server, to activate the registry change.

6 On the properties of the File System Archiving task, configure the daily deletion schedule for the archived files whose placeholders were deleted.

See “Scheduling the deletion of archived files on placeholder deletion for EMC Celerra/VNX” on page 149.

Chapter 12

Configuring target volumes, target folders, and archive points

This chapter includes the following topics:

About adding target volumes, target folders, and archive points for FSA

You must add shares on a target file server as target volumes for FSA to process.

When you add a target volume, the New Volume wizard lets you specify the following:

- The vault store to use for the files that are archived from the volume.
- The File System Archiving task to use to process the volume.
- The volume policy to apply when files are archived from the volume.

If FSA Reporting is configured, the wizard also lets you choose whether to enable FSA Reporting for this volume. For information on FSA Reporting, see the *Reporting* guide.

After you add a target volume you must add one or more target folders to control which folders FSA can archive from.

When you add a target folder the New Folder wizard lets you do the following:

- Specify the archiving policy to use for the target folder and its subfolders.
- Create an archive point for the folder, and for each of its immediate subfolders, if required. Each archive point defines the top of a folder structure that Enterprise Vault archives within a single archive.

To create an archive point at the root of a target volume you can specify a backslash (\ ) as the path to the target folder when you add the target folder.

If you want, you can choose to auto-enable the creation of archive points on the immediate subfolders of a target folder. The target folder is then referred to as an **auto-enabling folder**. When the File System Archiving task runs in normal mode it creates archive points for any new subfolders that are immediately below the auto-enabling folder. Auto-enabling can be useful for example when a target folder contains a subfolder for each user, and you want a separate archive for each user. When you add a subfolder for a new user, the File System Arching task creates an archive point on the subfolder during the next normal archiving run.

To ensure that an archive does not fill up too quickly you need to consider the size of the folder structure below each archive point.

When an archive point is created, it has no archive ID immediately assigned to it. An archive ID is normally assigned on the first occasion that a File System Archiving task processes the folder. When a File System Archiving task finds an archive point with no archive ID or an invalid archive ID it checks the Directory database to determine whether any archive IDs are already associated with the folder path. If the folder path has no associated archive IDs, Enterprise Vault creates an archive and assigns the archive ID to the archive point. If one or more archives already exist for the folder path, Enterprise Vault assigns the oldest existing archive to the archive point. In the case where multiple archives exist for a folder path, Enterprise Vault reports this fact.

See “About the checks for existing archives for an FSA folder path” on page 104.

By default the File System Archiving task gives an archive the same name as the folder to which the archive point applies. The site defaults are used to supply the other attributes of the archive. You can override these defaults if you want.

About the checks for existing archives for an FSA folder path

Under some circumstances an FSA folder path can become associated with more than one archive.

When a File System Archiving task processes a folder that has an archive point with no archive ID or an invalid archive ID, it checks the Directory database records to determine whether any archive IDs are already associated with the folder path. It then proceeds as follows:

- If no archive ID is associated with the folder path, Enterprise Vault creates an archive and assigns the archive ID to the archive point.
- If one archive ID is associated with the folder path, Enterprise Vault assigns that archive ID to the archive point.
- If more than one archive ID is associated with the folder path, Enterprise Vault does the following:
  - Assigns the archive ID of the oldest existing archive to the archive point.
  - Indicates the existence of multiple archives for the folder path in the File System Archiving task report. The report lists the archive IDs of the multiple archives, and indicates that the oldest archive will be used for archiving.
  - Generates a warning event with event ID 41484 in the Enterprise Vault event log. The event lists the archive IDs of the multiple archives for the folder path, and indicates that the oldest archive will be used for archiving.

  After Enterprise Vault has assigned an archive ID to the archive point, no further warnings are issued about the existence of multiple archives for the folder path.

Note: When Enterprise Vault checks for existing archives for a folder path, the check is restricted to the records from vault stores that belong to the Enterprise Vault storage server that hosts the vault store for the target volume.

Adding a target volume for FSA

When you have added a target file server you must add one or more target volumes for FSA to process.

If you add an EMC Celerra/VNX volume, note the following:

- Before you add a target volume for a Celerra/VNX device, ensure that the Enterprise Vault server that archives from the Celerra/VNX has its cache location configured.
  See "Specifying a cache location for retrieved Celerra/VNX files" on page 67.

- If you use the archiving policy setting "Delete archived file when placeholder is deleted", some restrictions and requirements apply.
  See "About configuring the deletion of archived files on placeholder deletion" on page 96.
- An EMC restriction prevents archiving from a Celerra/VNX device if the path to the files exceeds 1024 characters.

To add a target volume for FSA

1. If you have not already done so, create at least one File System Archiving task. The New Volume wizard requires a File System Archiving task to assign to the target volume. You can configure or change the assigned File System Archiving task later if required.

   See "Adding a File System Archiving task" on page 147.
2. In the Administration Console, expand the Enterprise Vault site until the **Targets** container is visible.
3. Expand the **Targets** container.
4. Expand the **File Servers** container to show the file servers that have been added as targets.
5. Right-click the file server to which you want to add a target volume and then, on the shortcut menu, click **New** and then **Volume**.
6. Work through the New Volume wizard to add the target volume.

Adding a target folder and archive points for FSA

The Administration Console's New Folder wizard lets you set up file archiving from a folder and its subfolders within a target volume. The New Folder wizard lets you do the following:

- Specify the archiving policy to use for the target folder and its subfolders.
- Create archive points for the folder and its subfolders as required.

Note: You can also use the ArchivePoints command-line tool to create and manage archive points. For information, see ArchivePoints in the *Utilities* manual.

Note: An EMC restriction prevents archiving from a Celerra/VNX device if the path to the files exceeds 1024 characters.

To add a target folder and archive points for FSA

1. In the Administration Console, expand the Enterprise Vault site until the **File Servers** container is visible.
2. Expand the **File Servers** container to show the file servers that have been added as targets.
3. Expand the node for the appropriate file server.
4. Right-click the volume that contains the folder you want to add as a target, and on the shortcut menu click **New** and then **Folder**.

   The New Folder wizard starts.
5. Specify the relative path of the folder that you want to add, or click **Browse** to select the folder.

   Note: If the path to the folder contains more than 244 characters, you cannot select the folder by browsing to it. You must type in the path manually. This restriction is due to a limitation in the Windows browse dialog.

   ---
6. Specify the archiving policy to use for the folder. You can select from:
   - The volume policy.
   - A folder policy.
   - A retention folder policy. Retention folder policies let you add a predefined folder hierarchy to the target folder.
     See "Configuring retention folders" on page 124.

   Note that if you apply a folder policy and a file is not matched by the rules in the folder policy then, by default, Enterprise Vault tries to find a match in the volume policy rules. If you want to force Enterprise Vault not to apply the volume policy rules, edit the folder properties later in the Administration Console and select **Ignore volume rules for this folder**.

   Note: Zero-length files are never archived by File System Archiving.

   ---
7. Specify whether to archive from the target folder, and whether to archive from its subfolders. You can defer archiving, if required. You can start or suspend archiving later from the target folder properties.
8. Create archive points as required. You can create any of the following:
   - An archive point for the target folder.

- An archive point for each immediate subfolder of the target folder. A new archive will be created for each existing immediate subfolder. If you have many folders to enable, this option may be easier than running the New Folder wizard many times.
- An archive point for each immediate subfolder of the target folder, and for new immediate subfolders when they are created. The target folder is referred to as an **auto-enabling folder**.
  If you choose this option, make sure that there is no archive point on any of the parent folders, or on the volume.
- No archive point. This option enables you to use the same archive as for higher-level folders, but to choose a different archiving policy for the target folder.

If you choose either of the first two options, you can set the initial properties of the archive points if required. Otherwise, Enterprise Vault uses the default values when it creates the archives. To set the archive point properties click **Properties**.

See "Archive point properties" on page 109.

Note: If you create an auto-enabling folder, you cannot set the initial properties of the archive points. Enterprise Vault uses the default values.

About managing archive points

You can manage FSA archive points from the Administration Console.

See "Viewing, editing, or deleting archive points in the Administration Console" on page 108.

You can also manage archive points by using the ArchivePoints command-line utility. For information on how to use the ArchivePoints utility to create, delete, list, and update archive points, see ArchivePoints in the *Utilities* guide.

You can get a list of archive points by processing a file server or a target volume with a File System Archiving task in Report Mode. The report lists all the archive points on the server or the volume.

See "About File System Archiving task reports" on page 153.

Note: If you delete a volume from a target file server in the Administration Console, Enterprise Vault does not delete any associated archive points automatically.

See "Deleting a target volume from FSA" on page 114.

Viewing, editing, or deleting archive points in the Administration Console

You can use the Administration Console to view, edit, or delete archive points on FSA target volumes.

To view, edit, or delete archive points in the Administration Console

1. In the Administration Console, expand **Targets**.
2. Expand **File Servers**.
3. Expand the file server that hosts the volume you want to manage.
4. Right-click the volume you want to manage and, on the shortcut menu, click **Archive Points**.
5. Expand the **Archive Points** listing. Archive points and auto-enabling folders are indicated as follows:

    Folder with an archive point

    Auto-enabling folder

6. To edit the properties of an archive point, click the folder that has the archive point and then click **Edit**.

   If you change any properties for an archive point, the changed properties are applied to the archive when a File System Archiving task processes the folder that contains the archive point.

   Note: Be careful if you edit the properties of an archive point. Before you save any changes to the archive point properties, check that all the displayed values on both tabs are the values that you want to apply to the archive.

   See "Archive point properties" on page 109.

7 To delete an archive point, click the folder that has the archive point and then click **Remove**.

8 To remove archive points that have been added by an auto-enabling folder, perform the following steps in the order listed:

- Click the auto-enabling folder to select it and then click **Edit**.
- Select **Do not create archive points for immediate subfolders**.
- Select **Delete existing archive points from immediate subfolders**.
- Click **OK**.

Archive point properties

The properties of an FSA archive point determine the properties of the associated File System archive.

The properties of an archive point are listed on two tabs:

- The General tab.
  See "Archive point properties: General tab" on page 109.
- The Indexing tab.
  See "Archive point properties: Indexing tab" on page 110.

Archive point properties: General tab

Table 12-1 describes the settings on the **General** tab of the archive point properties.

Table 12-1 Archive point properties: General tab

Setting	Description	Default value for a new archive point
Name	The name to use for the archive that is associated with the archive point, with any **Prefix** if specified. **Note:** In the New Folder wizard, if you select the option to create an archive point on each immediate subfolder, Enterprise Vault enforces the use of the subfolder name for **Name**.	The name of the folder on which the archive point resides.

Table 12-1 Archive point properties: General tab *(continued)*

Setting	Description	Default value for a new archive point
Use folder name	Whether to use the folder name for **Name**. This option is not available in the New Folder wizard if you choose the option to create an archive point on each immediate subfolder.	Use the folder name (for an archive point on the target folder). Use the subfolder name (for archive points on immediate subfolders of a target folder).
Prefix	A prefix that Enterprise Vault prepends to **Name** to make the full archive name. A prefix may be useful when you create a target folder and choose the option to create an archive point for each immediate subfolder.	None.
Description	A description for the archive, if required. The description appears in the list of file system archives under **Archives** > **File System** in the Administration Console.	None.
Owner	The archive billing owner.	None.
Delete expired items from this archive automatically	Controls whether Enterprise Vault deletes expired items from the archive automatically.	Do not delete expired items automatically.

Note: You can also set the name, description, and billing owner for an archive on the **General** tab of the archive's properties. You can also set the deletion of expired items for an archive on the **Advanced** tab of the archive's properties.

Archive point properties: Indexing tab

Table 12-2 describes the settings on the **Indexing** tab of the archive point properties.

If you do not specify values for the archive point when you create a target folder, Enterprise Vault uses the default values on the **Indexing** tab of the Enterprise Vault site properties.

Table 12-2 Archive point properties: Indexing tab

Setting	Description
Indexing level	Determines whether the content of archived items is indexed and therefore searchable. **Brief** indexes the metadata of archived items such as the file name and the item date, but not any content. A brief index is smaller than a full index, but users cannot search for any content in the archived items. Brief indexes may occupy approximately 4% of the space of the original data. It is not possible to give an exact size for the index because the size depends on the data that is indexed. **Full** indexes the metadata and the content of archived items. Users can search for the content of items. Full indexes with a 128 character preview length may occupy approximately 12% of the space of the original data. It is not possible to give an exact size for the index because the size depends on the data that is indexed.
Preview length (characters)	If you choose **Full** as the indexing level you can control the amount of preview text that Enterprise Vault shows in a search results list. You can set the preview length to **128** or **1000** characters. The size of the index increases when you increase the preview length.
Create previews of attachments	If you choose **Full** as the indexing level you can optionally choose to create previews of attachment content. These previews cannot be viewed in this release of Enterprise Vault. The size of an index increases if you select this option.
Defer indexing	Select this option if you do not want Enterprise Vault to index files as they are archived. Deferral of indexing can be useful if you want to archive files as quickly as possible. However, because the archived files are not indexed you cannot use an Enterprise Vault search application to search them. Additionally, the HTML preview of items in Enterprise Vault search applications is not available. If indexing is currently deferred for an archive point and you want to start indexing, clear **Defer indexing**. Enterprise Vault then performs an automatic rebuild of the index when the next item is added to the archive or deleted from the archive. The rebuild indexes all the items in the archive, but it does not create HTML previews of previously archived items.

Note: You can also set the Indexing properties except for **Defer Indexing** on the **Indexing** tab of the File System archive's properties. To defer indexing or to cancel deferred indexing, you must edit the archive point properties.

Effects of modifying, moving, or deleting folders

You need to be aware of the effects of deleting, renaming, moving, or copying folders to which you have assigned folder policies or archive points.

- See "Effects of modifying folders with folder policies" on page 112.
- See "Effects of modifying folders with archive points" on page 113.

Effects of modifying folders with folder policies

Table 12-3 describes the effects of deleting, renaming, moving, or copying a folder to which you have assigned a folder policy.

Table 12-3 Effects of modifying folders with folder policies

When you do this to a folder with a folder policy	This is the result
Delete	Enterprise Vault logs the fact that the folder is missing and then continues to process the volume. The folder still appears in the Administration Console and you need to delete it there. There will be warnings in the File System Archiving report files until you do so. Items previously archived from the folder can be searched for.
Rename	The name is updated in the Administration Console.
Move	The folder policy works as before. The archive point that controls the new location dictates the archive that is used. There may a warning in the File System Archiving report file for the first archiving run after the deletion. This warning is not logged on subsequent runs. Whether you get a warning depends on the order in which File System Archiving processes the folders. If File System Archiving processes first the folder from which the folder was moved, a warning is logged because the folder appears to be missing. When File System Archiving processes the destination folder, it finds the moved folder and so does not log the warning again. If File System Archiving processes first the folder into which the folder was moved, no warning is logged.
Copy	The folder is treated as a new folder, with no folder policy.

Effects of modifying folders with archive points

Table 12-4 describes the effects of deleting, renaming, moving, or copying a folder that has an archive point.

Table 12-4 Effects of modifying folders with archive points

When you do this to an archive point folder	This is the result
Delete	If you restore the folder, the archive point is restored. If you create a new folder with the same name at the same location and you add an archive point, the new folder is archived to the deleted folder's archive. If the folder path has more than one archive associated with it, the folder is archived to the oldest existing archive and the File System Archiving task report indicates which archive has been assigned for archiving from the folder path. See "About the checks for existing archives for an FSA folder path" on page 104.
Rename	The name is updated in the Administration Console, Enterprise Vault Search, and Archive Explorer. Archiving is not affected.
Move	If the move is within the same physical volume, the archive point still works as before. If the move is to a different physical volume, the moved folder does not have an archive point. (The File System Archiving task removes the archive point on the next run.)
Copy	The new folder does not have an archive point. (The File System Archiving task removes the copied archive point on the next run.)

About deleting target folders, volumes, and file servers

If you no longer wish to archive from target folders, target volumes, or target file servers you can delete them from the Administration Console.

See "Deleting a target folder from FSA" on page 114.

See "Deleting a target volume from FSA" on page 114.

See "Deleting a target file server from FSA" on page 116.

Deleting a target folder from FSA

You can delete a target folder from the Administration Console if required. You cannot delete a folder that Enterprise Vault is currently processing.

Note: If you only want to suspend archiving from a folder temporarily, you can edit the folder's properties, and uncheck the option to archive the folder.

To delete a target folder from FSA

1. In the Administration Console, expand the Enterprise Vault site, and then expand the **Enterprise Vault Servers** container.
2. Expand the container for the Enterprise Vault server whose File System Archiving task processes the associated target volume, and select **Tasks**.
3. Right-click the File System Archiving task that processes the volume whose target folder you want to delete, and on the shortcut menu click **Stop**.
4. Expand the **Targets** container and then the **File Servers** container.
5. Expand the container for the target file server, and select the target volume that contains the folder.
6. Right-click the folder that you want to delete and on the shortcut menu select **Delete**.
7. Click **Yes** to confirm that you want to delete the folder.
8. Restart the File System Archiving task, if required.

Deleting a target volume from FSA

You can delete a target volume and all of its target folders from Enterprise Vault when you no longer want to archive from the volume.

You cannot delete a volume that Enterprise Vault is currently processing.

Note: If you only want to suspend archiving from a volume temporarily, you can edit the volume's properties and uncheck the option to archive the volume.

Note that if you delete a target volume in the Administration Console, Enterprise Vault does not delete any associated archive points automatically.

If you do not delete the archive points and then you re-add the volume for archiving, Enterprise Vault uses the existing archive points, which remain associated with the original vault store.

This can result in the following scenario:

- You configure a volume for archiving, and specify that the volume is to use vault store 1.
- When Enterprise Vault archives from the volume, it associates the archive points with vault store 1.
- You then remove the volume from Enterprise Vault, without deleting the archive points.
- You add the volume for archiving again, but you specify that the volume is to use vault store 2.
- Enterprise Vault continues to archive any files under the original archive points to vault store 1.
- If you add a folder under one of the original archive points, the folder is archived to vault store 1, not vault store 2.

If required, delete the target volume's archive points before you delete the target volume.

See "About managing archive points" on page 107.

To delete a target volume from FSA

1. In the Administration Console, expand the Enterprise Vault site, and then expand the **Enterprise Vault Servers** container.
2. Expand the container for the Enterprise Vault server whose File System Archiving task processes the target volume, and select **Tasks**.
3. Right-click the File System Archiving task that processes the volume, and on the shortcut menu click **Stop**.
4. Expand the **Targets** container and then the **File Servers** container.
5. Expand the container for the target file server, and select the target volume that you want to delete.
6. On the shortcut menu select **Delete**.
7. Enterprise Vault displays a warning that deleting the volume deletes all its target folders.

   Click **Yes** to confirm that you want to delete the volume.
8. After Enterprise Vault has deleted the target volume you may need to refresh the container for the file server before Enterprise Vault no longer displays the target volume.

   If necessary, right-click the container for the file server and select **Refresh**.
9. Restart the File System Archiving task, if required.

Deleting a target file server from FSA

You can delete a target file server from Enterprise Vault if you no longer want FSA to process it. Note that deleting a target file server does not delete files or archived files; it merely removes the target file server from the Administration Console.

Note that if you want only to suspend archiving from a file server temporarily, you can do either of the following:

- Edit the target file server's properties, and uncheck the option to archive the file server.
- Stop the File System Archiving tasks that process the file server. If the tasks process other file servers this action also stops archiving from those file servers.

You cannot delete a file server that Enterprise Vault is currently processing.

To delete a target file server from FSA

1. In the Administration Console, delete all the target volumes from the target file server.

   See "Deleting a target volume from FSA" on page 114.

2. In the **File Servers** container, right-click the target file server that you want to delete and then, on the shortcut menu, click **Delete**.
3. Click **Yes** to confirm that you want to delete the file server.

Chapter 13

Configuring pass-through recall for placeholder shortcuts

This chapter includes the following topics:

About configuring pass-through recall for placeholder shortcuts

This section describes the configuration of pass-through recall of placeholder shortcuts on Windows file servers, and for read-only file systems on NetApp filers that run Data ONTAP 7.3 or later.

Note: Due to a NetApp restriction, pass-through is not supported on Data ONTAP 8.2 C-Mode.

For EMC Celerra/VNX devices, Enterprise Vault supports the Celerra/VNX pass-through facility.

See "Configuring Celerra/VNX pass-through behavior for placeholder shortcuts" on page 60.

Note the following:

- Pass-through recall is ignored for read-write file systems on NetApp filers.
- FSA ignores the volume policy and folder policy setting **Delete archived file when placeholder is deleted** for NTFS target volumes on which pass-through recall is enabled.

Pass-through recall uses a disk cache to help reduce recall times for large files. When you configure pass-through recall you must specify a location for the disk cache:

- For Windows file servers you must specify a location on the file server.
- For NetApp filers you must specify a location on the Enterprise Vault server.

A set of pass-through recall registry values enables you to specify the following for Windows file servers:

- The maximum recall rate for pass-through recall. By default, no maximum rate is applied. If you set a maximum rate you can bypass the limit for administrators, if you want.
- A list of programs that are prohibited from receiving files by pass-through recall. By default, no programs are prohibited.

Configuring pass-through recall for a Windows file server

Configure pass-through recall for a Windows file server as follows.

Note: Some additional instructions apply for clustered file servers.

See "About configuring pass-through recall for a file server cluster" on page 119.

To configure pass-through recall for a Windows file server

1. Ensure that the FSA Agent is installed on the file server.

   See "About installing the FSA Agent on a Windows file server" on page 81.

2. In the Administration Console, expand the Enterprise Vault site until the **Targets** container is visible.
3. Expand the **Targets** container, and then expand the **File Servers** container
4. Right-click the Windows file server for which you want to configure pass-through recall and then, on the shortcut menu, click **Properties**.

   The settings for pass-through recall are on the file server properties **General** tab.

5 Select **Configure pass-through recall**.

6 Enter a location on the file server for the disk cache that Enterprise Vault uses when it recalls files. We recommend that you specify a location on a high-performance disk. The Vault Service account must have write permission on the folder.

7 Select a disk cache size. Typically there is little benefit in increasing the cache size from its default setting.

8 Click **OK** to save the changes to the file server's properties.

9 Enable pass-through recall for each existing volume on the file server on which you want to use this feature. Select **Enable pass-through recall** on the **General** tab of the volume's properties.

Note: If you add new volumes for archiving on the file server, Enterprise Vault does not enable them for pass-through recall. You must enable new volumes for pass-through recall manually, if required.

Note: Enterprise Vault trims the pass-through recall disk cache automatically when the disk cache becomes full. If you want to trim the cache manually, you must first stop the Enterprise Vault Placeholder service on the Windows file server. Remember to restart the Placeholder service when you have finished deleting files from the cache.

You can use registry values to set a pass-through recall rate, or to prohibit programs from receiving files by pass-through recall.

See "Registry values for pass-through recall on Windows file servers" on page 120.

About configuring pass-through recall for a file server cluster

Note that if you configure pass-through recall for a file server cluster, all the cluster nodes must use identical pass-through recall settings.

In the file server properties for the target virtual file server, make sure that the pass-through recall settings are configured as follows:

- The "Configure pass-through recall" setting is checked.
- The disk cache location is a local path such as `C:\FSACacheFolder`. This path must be valid for a local disk on each cluster node.

Note: If the cluster configuration supports only one active node, you may alternatively specify a location on the cluster's shared disk. For example, you can use a shared disk location for an A/P, A/P/P, or A/P/P/P configuration, but not for an A/A/P configuration, where A represents an active node and P represents a passive node.

- The disk cache size is specified. We recommend that you make the cache size as large as possible.

Registry values for pass-through recall on Windows file servers

A set of pass-through recall registry values enables you to specify the following for Windows file servers:

- The maximum pass-through recall rate.
- Whether the pass-through recall rate is applied on the file server. By default, the maximum rate is not applied.
- Whether the maximum pass-through recall rate is waived for members of the local Administrators group on the file server. By default, if a limit is applied it is not waived for local administrators.
- A list of programs that are prohibited from receiving files by pass-through recall. By default, no programs are prohibited.

The registry values are located under the following registry key on the file server:

On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \KVS
   \Enterprise Vault
    \FSA
     \PlaceholderService
      \PassThrough
```

On a 64-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \FSA
      \PlaceholderService
       \PassThrough
```

Table 13-1 describes the registry values.

Table 13-1 Registry values for pass-through recall on Windows file servers

Registry value	Content	Description
EnableRecallLimitForPassThrough	DWORD	Determines whether users are subject to the maximum pass-through recall rate that PassThruRecallLimitMaxRecalls and PassThruRecallLimitTimeInterval define. The default is value 0, which means that the maximum pass-through recall rate does not apply to users. Change the value to 1 to impose the rate for users.
PassThruRecallLimitMaxRecalls	DWORD	Defines the maximum number of pass-through recalls that are allowed in the period that PassThruRecallLimitTimeInterval defines. The default is 20. For example, if PassThruRecallLimitMaxRecalls is set to 20 and PasssThruRecallLimitTimeInterval is set to 10, the maximum recall rate is set to 20 recalls in 10 seconds.
PassThruRecallLimitTimeInterval	DWORD	Specifies the period in seconds for the maximum pass-through recall rate. The default is 10. If the maximum recall rate is reached, Enterprise Vault imposes an additional interval equal to the PassThruRecallLimitTimeInterval before it resets the count. For example, if the maximum recall rate is set at 20 recalls in 10 seconds and a user achieves 20 recalls in 8 seconds, Enterprise Vault imposes a 10-second block on further recalls before it resets the count for the user.

Table 13-1 Registry values for pass-through recall on Windows file servers *(continued)*

Registry value	Content	Description
BypassPassThruRecallLimitsForAdmins	DWORD	Determines whether members of the local Administrators group on the file server are subject to the maximum pass-through recall rate. This setting applies only if EnableRecallLimitForPassThrough is set to 1. The default is value 0, which means that the rate limit applies to local administrators. Change the value to 1 to waive the rate limit for local administrators.
ExcludedExes	String	Specifies a list of programs that are prohibited from receiving archived items by pass-through recall. Separate each program in the list with a semicolon.

For more information on the registry values for pass-through recall on Windows file servers, see the *Registry Values* manual.

Configuring pass-through recall for a NetApp filer

Configure pass-through recall for a NetApp filer as follows.

Note: For NetApp filers the pass-through recall feature works only with read-only file systems. Pass-through recall is ignored for read-write file systems. Additionally, due to a NetApp restriction pass-through is not supported for Data ONTAP 8.2 C-Mode.

To configure pass-through recall for a NetApp filer

1. In the Administration Console, expand the Enterprise Vault site until the **Targets** container is visible.
2. Expand the **Targets** container, and then expand the **File Servers** container.

3 Right-click the NetApp filer for which you want to configure pass-through recall and then, on the shortcut menu, click **Properties**.

The settings for pass-through recall are on the **General** tab of the file server properties.

4 Select **Configure pass-through recall**.

5 Click **OK** to save the changes to the file server's properties.

6 Ensure that a disk cache location is configured on the Enterprise Vault server whose File System Archiving task manages the archiving from the NetApp filer.

The cache is used when the files are retrieved from the NetApp filer.

See "To configure the cache location on the Enterprise Vault server" on page 123.

To configure the cache location on the Enterprise Vault server

1 In the Administration Console, expand the Enterprise Vault site until the **Enterprise Vault Servers** container is visible.

2 Expand the **Enterprise Vault Servers** container.

3 Right-click the Enterprise Vault server whose File System Archiving task manages the archiving from the NetApp filer. Then on the shortcut menu, click **Properties**.

4 Click the **Cache** tab.

5 Under **Cache Location**, enter an existing path on the Enterprise Vault server for the cache. The Vault Service account must have read and write access to the location.

For more information on configuring the cache, click **Help** on the **Cache** tab.

Note: If the Enterprise Vault server archives from an EMC Celerra/VNX device, this cache location is also used for retrieved Celerra/VNX files.

Chapter 14

Configuring and managing retention folders

This chapter includes the following topics:

Configuring retention folders

The retention folder feature enables you to create single folders or a hierarchy of folders automatically on file servers, to be managed by Enterprise Vault and archived according to assigned policies.

See "About retention folders" on page 33.

You can configure retention folders using the Administration Console. The configuration steps are as follows:

- Make sure that you have a suitable folder policy to use as the default folder policy for the retention folders. Create a suitable folder policy if required.
  See "Creating FSA volume policies and folder policies" on page 88.
- Create a retention folder policy to define the hierarchy of folders to be created on the FSA target, and the folder policy to use on each retention folder.
  See "Creating a retention folder policy" on page 125.
- Add the FSA target folder under which you want the retention folders created, assign the retention folder policy, and specify where archive points are to be created.

See "Adding a target folder with a retention folder policy from the Administration Console" on page 125.

- By default Enterprise Vault recreates folders in the hierarchy that are deleted or moved. You can turn off this default retention behavior, if you want.
  See "About controlling whether FSA recreates deleted or moved retention folders" on page 127.
- The folder hierarchies are created on the file server on the next Normal mode archiving run.
  To test the effect of an assigned retention folder policy you can perform an archiving run in Report mode.
  See "About testing the effects of a retention folder configuration" on page 127.

You can also assign retention folder policies using the command line interface.

See "About assigning a retention folder policy using the Command Line Interface (CLI)" on page 127.

Creating a retention folder policy

A retention folder policy defines a hierarchy of retention folders to be created on an FSA target, and the folder policy to use for each retention folder.

To create a retention folder policy

1. In the Administration Console, expand the site and click **Policies > File**.
2. Right-click the Retention Folders container and select **New** and then **Policy**. The New Policy wizard starts.
3. In the New Policy wizard, create the required folder hierarchy:
   - You can import a folder hierarchy by using the **Import** option.
   - You can create a folder hierarchy or customize an imported hierarchy using the **Add Folder**, **Rename Folder**, and **Delete Folder** options.
4. Assign a default folder policy to use for the retention folders in the hierarchy.
5. If required, use the **Policy** option to assign a different policy to specific folders in the hierarchy.

Adding a target folder with a retention folder policy from the Administration Console

When you have created a suitable FSA retention folder policy you can add the target folder on which to create the retention folders. When you assign the retention folder policy to the target folder you must specify where to create archive points.

Note: You cannot assign a retention folder policy to an existing target folder, unless the target folder already has a retention folder policy assigned.

To add a target folder with a retention folder policy from the Administration Console

1. In the Administration Console, expand the site and click **Targets > File Servers**.
2. Expand the node for the relevant file server.
3. Right-click the volume that contains the folder you want to use as the target for the retention folders, and select **New > Folder** to start the New Folder wizard.
4. Specify the location of the target folder.
5. On the next page of the wizard select **Use Retention Folder policy** and choose the Retention Folder policy to apply.
6. On the next page of the wizard select where the Retention Folder policy is to be applied, as follows:
   - To the top-level target folder.
   - To subfolders of the target folder. If you choose this option you can select whether to apply the policy automatically to any new folders that get added to the target folder.
7. On the next page of the wizard select whether and where to create archive points. You can select from the following options:
   - If you chose to apply the retention folder policy on the subfolders of the target folder, you can choose to create a separate archive point on every immediate subfolder of the target folder.
   - Create an archive point on the target folder. The target folder and its subfolders use the same archive.
   - Do not create an archive point. The target folder and it subfolders use the same archive as the parent folder. If the target folder is a root folder then there is no parent folder, so the target folder and its subfolders are not archived.

   If you choose to create any archive points, you can define the properties of the resultant archive by clicking **Properties**.

   See "Archive point properties" on page 109.
8. Click **Finish** to complete the wizard.

   Enterprise Vault creates the retention folders on the file server when the File System Archiving task next runs.

About controlling whether FSA recreates deleted or moved retention folders

By default, Enterprise Vault recreates deleted or moved folders in the folder hierarchy that the retention folder policy defines. You can change this default behavior if you want, so that Enterprise Vault does not recreate these folders.

To change the default behavior, you must create the registry entry `ApplyRtnPolicyOnlyOnExistingFolders` on the Enterprise Vault server that runs the File System Archiving task. For details, see the description of `ApplyRtnPolicyOnlyOnExistingFolders` in the *Registry Values* manual.

About testing the effects of a retention folder configuration

After you have completed the configuration process for retention folders, Enterprise Vault creates the folder hierarchy on the file server when the File System Archiving task next runs in Normal mode.

To see what folders will be created by a retention folder policy, you can run the File System Archiving task in Report mode.

See "About File System Archiving task reports" on page 153.

The following retention folder information is included in the File System Archiving task report:

- Folders that were created on the file server as a result of a retention folder policy, and the policy that is assigned to each folder.
- Any errors that occur when processing a retention folder target.
- Any missing retention folder targets.

About assigning a retention folder policy using the Command Line Interface (CLI)

You can assign retention folder policies to FSA target folders using a command-line interface.

The CLI executable is `Enterprise Vault\RtnFolder.exe`.

The command takes the following parameters (include the colon in the parameter name):

- `/Policy:`*`policy_name`*
- `/Target:`*`UNC_path_of_target`*
- `/Settings:`*`XML_settings_file_name`*

The XML settings file defines the following:

- How the policy is to be applied on top-level folders on the target and on subfolders.
- Archive point options.

See "The format of the RtnFolder.exe settings file" on page 128.

You can include wild cards when defining target volumes and final target folders only.

The following examples using wild cards are correct:

```
/Target:\\ServerA\C$*\MyFolder\AB*

/Target:\\ServerA\C$*\MyFolder\A*B*

/Target:\\ServerA\C$*\MyFolder\A*B
```

The following example is not correct, because wild cards can only be included in the volume name and final folder name:

```
/Target:\\ServerA\C$*\MyFol*der\AB*
```

See "Example RtnFolder.exe commands" on page 130.

The format of the RtnFolder.exe settings file

An example settings file for `RtnFolder.exe` is included in the Enterprise Vault installation folder. The example settings file is named `RtnFolderSettings.xml`.

The following example shows the XML format of the settings file.

```
<?xml version="1.0" encoding="utf-8" ?>
  <Policy>
    <Apply>
      <ApplyToSubFolders>1</ApplyToSubFolders>
      <ArchiveThisFolder>1</ArchiveThisFolder>
      <ArchiveSubFolders>0</ArchiveSubFolders>
      <AutoUpdate>0</AutoUpdate>
    </Apply>
    <ArchivePoint>
      <OnSubFolders>1</OnSubFolders>
      <DoNotCreate>0</DoNotCreate>
    </ArchivePoint>
  </Policy>
```

The `<Apply>` element tags define how to apply the policy, as specified in Table 14-1.

Table 14-1 <Apply> element tags for the XML settings file

Tag	Value
ApplyToSubFolders	0—Apply the Retention Folder policy to top-level folders only on the FSA target. 1—Apply the Retention Folder policy to subfolders under top-level folders on the FSA target, but not to the top-level folders on the FSA target.
ArchiveThisFolder	0—Do not archive the folders that this Retention Folder policy manages. 1—Archive the folders that this Retention Folder Policy manages.
ArchiveSubFolders	0—Do not archive any folders in the Retention Folder hierarchy that the Retention Folder policy does not manage. 1—Archive all folders in the Retention Folder hierarchy, even if the Retention Folder policy does not manage them.
AutoUpdate	0—Do not apply the Retention Folder policy on new subfolders that are created under top-level folders in the Retention Folder hierarchy. This option is valid only if the tag ApplyToSubFolders is 1. 1—Apply the retention folder policy on any new subfolder that are created under top-level folders in the Retention Folder hierarchy. This option is valid only if the tag ApplyToSubFolders is 1.

The `<ArchivePoint>` element tags define where to create archive points, as specified in Table 14-2.

Table 14-2 <ArchivePoint> element tags for the XML settings file

Tag	Description
OnSubFolders	0—Create an archive point on top-level folders in the Retention Folder hierarchy. This option is valid irrespective of the value of the tag ApplyToSubFolders. 1—Create archive points on the subfolders under top-level folders in the Retention Folder hierarchy. This option is valid only if the tag ApplyToSubFolders is 1.

Table 14-2 <ArchivePoint> element tags for the XML settings file *(continued)*

Tag	Description
DoNotCreate	0—Use OnSubFolders tag value. 1—Do not create an archive point. The administrator takes responsibility for manually creating archive points. Alternatively, if an archive point exists above the top-level folders in the Retention Folder hierarchy, the archive is used for all folders in the Retention Folder hierarchy.

Example RtnFolder.exe commands

The following example command applies the Retention Folder policy "Finance Retention" to folders on the FSA target `\\Server\C$\MyFolder`, using settings in the file `RtnFolderSettings.xml`. This file is in the Enterprise Vault folder.

```
RtnFolder.exe /Policy:"Finance Retention"
/Target:"\\ServerA\C$\MyFolder"

/Settings: RtnFolderSettings.xml
```

The following example command uses wildcards in defining the target volume and folder. The Retention Folder policy, "Finance Retention", is applied to all folders that match the path, `*C*\MyFolder\MyFolder\AB*`, on the target server, ServerA. The policy is applied according to the settings in the file, `RtnFolderSettings.xml`, which is in the Enterprise Vault folder.

```
RtnFolder.exe /Policy:"Finance Retention"
/Target:"\\ServerA\*C*\MyFolder\AB*"

/Settings: RtnFolderSettings.xml
```

Managing retention folders

This section covers the following topics:

- How to disable the archiving of retention folders.
  See "Disabling the archiving of retention folders for an FSA target" on page 131.
- Change the retention folder policy that is assigned to a target folder.
  See "Assigning a different retention folder policy to a target folder" on page 131.

Disabling the archiving of retention folders for an FSA target

You can disable the archiving of top-level folders or subfolders (or both) in the retention folder hierarchy for an FSA target by unchecking the appropriate Archiving boxes in the FSA target properties.

To disable archiving of some or all retention folders on an FSA target

1. In the Administration Console, expand the site and click **Targets > File server**.
2. Expand the relevant file server and select the volume that contains the target folder.
3. Right-click the target folder whose properties you want to change, and select **Properties**.
4. On the File Server Properties dialog, select or clear the following settings:
   - **Archive top-level folders in Retention Folder hierarchy**. Check this to archive top-level folders.
   - **Archive subfolders in Retention Folder hierarchy**. Check this to archive subfolders.

   For example, if you select only **Archive subfolders in Retention Folder hierarchy**, the top-level folders are not archived but all subfolders are archived.
5. Click **OK** to apply the changes and close the dialog.

Assigning a different retention folder policy to a target folder

You can assign a different retention folder policy to an FSA target folder that has a retention folder policy already assigned.

Note: You can only assign a retention folder policy to an exsiting FSA target folder if the target folder has a retention folder policy already assigned.

To assign a different retention folder policy to a target folder

1. In the Administration Console, expand the site and click **Targets > File server**.
2. Expand the node for the target file server, and select the volume that contains the target folder.
3. Right-click the target folder whose retention folder policy you want to change, and select **Properties**.
4. On the **Retention Folder Properties** dialog, click **Select Policy**.
5. On the **Select Policy** dialog, select the required retention folder policy.

Chapter 15

Configuring File Blocking

This chapter includes the following topics:

About configuring File Blocking

You can configure File Blocking for the following devices:

- Windows computers. File Blocking is carried out by a File Blocking service that is installed on the Windows computer as part of the FSA Agent.
- NetApp filers with Data ONTAP 7.3 or later and Data ONTAP 8.2 (C-Mode). The File Blocking is carried out by a File Blocking service that runs on a Windows file server. When you configure File Blocking for a NetApp filer you must select a target Windows file server to perform the File Blocking. It is possible for a Windows file server to run File Blocking for more than one NetApp filer, but for best performance you are recommended to use a different Windows file server for each NetApp filer.

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

File Blocking quarantines those files that are blocked because of content-checking. As part of configuring File Blocking you must create quarantine locations as follows:

- You must create a local quarantine location for each file server. For NetApp filers, the local quarantine location must be on the Windows file server that runs the File Blocking service for the NetApp filer.
- Optionally you can define a central quarantine location. Enterprise Vault then uses the central quarantine unless the central quarantine location is not available. If the central quarantine location is not defined or is not available, Enterprise Vault uses the file server's local quarantine location.
  Note that if the central quarantine location later becomes available, the files that are in local quarantine locations are not automatically moved to the central quarantine location.
- If neither a central quarantine location nor the local quarantine location is available, Enterprise Vault logs an error in the event log, and the file is not quarantined.

Steps to configure File Blocking

Table 15-1 outlines the steps that are required to configure File Blocking for a Windows file server or a NetApp filer.

Note: To use File Blocking in a Windows clustered file server environment, you must configure an FSA resource in the cluster group that holds the virtual server resource. See "About using FSA with clustered file servers" on page 21.

Table 15-1 Steps to configure File Blocking

Step	Action	Description
Step 1	This step applies for NetApp filers only. Ensure that you have a target Windows file server that can run the File Blocking service on behalf of the NetApp filer. The Windows file server must have the FSA Agent installed. A Windows file server can perform File Blocking for more than one NetApp filer, but for best performance you are recommended to use one Windows file server per NetApp filer. **Note:** An Enterprise Vault server cannot act as a File Blocking agent server for a NetApp filer.	If necessary, add the Windows file server as a target in the Vault Administration Console. The Windows file server must have the FSA Agent installed. See "Adding a Windows file server to File System Archiving" on page 39.
Step 2	Add the file server on which you want to perform File Blocking as a target file server in the Administration Console.	■ For a Windows server, the FSA Agent must be installed. ■ For a NetApp filer, when you are prompted for the File Blocking agent server, specify the Windows target file server that you identified in Step 1.
Step 3	Define a local quarantine location for the file server.	See "Defining a local quarantine location for File Blocking" on page 135.
Step 4	Optionally, define a central quarantine location. If a central quarantine location is not configured or not available, the local quarantine locations are used.	See "Defining a central quarantine location for File Blocking" on page 136.
Step 5	Specify how Enterprise Vault is to send mail when a File Blocking rule requires a mail notification.	See "Specifying the mail notification delivery mechanism for File Blocking" on page 136.
Step 6	Include File Blocking rules in a volume policy, and apply the policy as required.	See "Including File Blocking rules in a policy" on page 137.
Step 7	Optionally, specify for each file server, a list of users whose files are exempt from File Blocking.	See "Exempting File Blocking for specific users" on page 145.

Defining a local quarantine location for File Blocking

You must define a local quarantine location on a file server where File Blocking can quarantine files that are blocked because of content-checking.

Note: For NetApp filers, the quarantine location must be on the Windows file server that is running the File Blocking service for the NetApp filer.

Note the following if you configure File Blocking in a clustered environment where multiple cluster groups can come online on the same cluster node. The quarantine location must have the same value for all the virtual servers that can be online concurrently on the same node.

To define a local quarantine location on a file server

1 Decide on a suitable quarantine location on the file server.

Note: The Vault Service account must have write access to the location.

Note: Do not select a location to which a File Blocking rule will be applied.

Note: To avoid the risk of quarantined files filling the system drive, do not place a quarantine location on the system drive. Specify a location that has sufficient free space to hold the quarantined files, and monitor regularly the space that the quarantined files occupy.

2 Expand the Administration Console tree until the **Targets** container is visible.

3 Expand the **Targets** container.

4 Expand the **File Servers** container.

5 Right-click the server on which you want to set the quarantine location and, on the shortcut menu, click **Properties**.

6 On the **File Blocking** tab, enter the path to the folder you want to use for quarantine. Click the browse button if you want to select the location from a list.

7 Click **OK**.

Defining a central quarantine location for File Blocking

Optionally, you can define a central quarantine location where File Blocking stores the quarantined files for all file servers.

To define a central quarantine location for File Blocking

1. Decide which server will host the central quarantine location and choose a suitable location on that server.

   Note: The Vault Service account must have write access to the location.

   Note: Do not select a location to which a File Blocking rule will be applied.

   Note: To avoid the risk of quarantined files filling a system drive, do not place a quarantine location on a system drive. Specify a location that has sufficient free space to hold the quarantined files, and monitor regularly the space that the quarantined files occupy.

2. Expand the Administration Console tree until the **Targets** container is visible.
3. Expand **Targets**.
4. Right-click the **File Servers** container and, on the shortcut menu, click **Properties**.
5. On the **File Blocking** tab, select **Enable centralized quarantine** and then enter the path to the folder you want to use for the central quarantine. Click the browse button if you want to select the location from a list.
6. Click **OK**.

Specifying the mail notification delivery mechanism for File Blocking

You must specify how Enterprise Vault is to send mail when a File Blocking rule requires a mail notification.

You can choose to send either SMTP mail or Exchange Server mail. If you choose to send Exchange Server mail then Outlook must be installed on each file server.

Note: If a File Blocking rule triggers a mail notification but Enterprise Vault is unable to send the notification, Enterprise Vault generates an error message in the Enterprise Vault event log. The message indicates the reason for the failure. If repeated failures occur due to insufficient information on the **Mail** tab of the **File Servers** container, Enterprise Vault generates an error message once every 24 hours.

To specify the mail notification delivery mechanism for File Blocking

1. Expand the Administration Console tree until the **Targets** container is visible.
2. Expand **Targets**.
3. Right-click the **File Servers** container and, on the shortcut menu, click **Properties**.
4. Click the **Mail** tab.
5. Select your preferred delivery mechanism: either SMTP mail or Exchange Server mail:
   - SMTP mail. Enter the name of the SMTP mail server and the name you want to be used for the sender of the notifications.
   - Exchange Server mail. Enter the name of the Exchange Server and the name of the mailbox that you want to use to send mail.
6. Click **OK**.

Including File Blocking rules in a policy

You can include File Blocking rules when you create a new volume policy, or add File Blocking rules to an existing volume policy.

To include File Blocking rules when creating a volume policy

1. In the Administration Console, expand the Enterprise Vault site until the **Policies** container is visible.
2. Expand the **Policies** container.
3. Expand the **File** container.
4. Right-click **Volume** and then, on the shortcut menu, click **New** and then **Policy**.
5. On the first screen of the **New Policy** wizard, click **Next**.
6. On the second screen of the wizard enter a name for the new policy and, optionally, a description. Click **Next**.

7 On the third screen of the wizard you create the File Blocking rules that you want to apply in the new policy. Click **New**. The **File Blocking Rule** properties appear.

8 Complete the details on each tab to define the File Blocking rule, then click **OK**.

The **New Policy** wizard shows the new rule that you have created. The rule is selected, so it will be enabled when this policy is applied. If you want to disable the rule, clear the checkbox next to the rule.

9 If you want to create more rules to be applied by this policy, click **New**.

10 When you have created the required rules, click **Next** to continue.

11 Work through the remainder of the wizard.

You can create and modify the rules later, if required, by editing the properties of the volume policy.

To add File Blocking rules to an existing volume policy

1 In the Administration Console, expand the Enterprise Vault site until the **Policies** container is visible.

2 Expand the **Policies** container.

3 Expand the **File** container.

4 Click the **Volume** container.

5 In the list of policies, right-click the policy you want to modify and, on the shortcut menu, click **Properties**.

6 Click the **File Blocking Rules** tab. This tab enables you to create the File Blocking rules that you want to apply in this policy.

7 Click **New**. The **File Blocking Rule** properties appear.

8 Complete the details on each tab to define the File Blocking rule, then click **OK**.

9 The **File Blocking Rules** tab shows the new rule that you have created. The rule is selected, so it will be enabled when this policy is applied. If you want to disable the rule, clear the checkbox next to the rule.

10 If you want to create more rules to be applied by this policy, click **New**.

About File Blocking rules

You can define File Blocking rules when adding a new volume policy, or by editing the properties of an existing volume policy. You can have many rules within a single

policy. This section describes the settings that you can configure in a File Blocking rule.

In summary, a File Blocking rule defines the following:

- The folders to monitor.
- The file types to monitor.
- Whether to scan inside compressed files.
- What action to take when a file is found that breaks a rule.

File Blocking rule: General tab

Table 15-2 lists the options on the General tab of File Blocking rule properties.

Table 15-2 File Blocking rule: General tab

Setting	Description	Default Value
Name	The name of the rule. This must be specified.	None.
Description	An optional description of the rule.	None.

File Blocking rule: File Groups tab

Table 15-3 lists the options on the General tab of File Blocking rule properties.

Table 15-3 File Blocking rule: File Groups tab

Setting	Description	Default Value
File groups	A list of the defined file groups. You select the file groups that you want to monitor. You can then block or allow individual file types within those groups. If necessary, you can define more file groups: in the Administration Console, under **Policies**, right-click the **File Groups** container and, on the shortcut menu, click **New** and then **File Group**.	List of groups already defined. No group is selected.
Blocked files	A list of file types to block. Note that *.TMP files are never blocked because this file type is used temporarily when a file is restored.	None.

Table 15-3 File Blocking rule: File Groups tab *(continued)*

Setting	Description	Default Value
Allowed files	A list of file types to allow.	None.

Note: File Blocking cannot perform content checking for the supplied file types in the Mac Files file group and the Windows Files file group.

Note: Files stored within .RAR and .CAB files cannot be blocked or quarantined. However, you can create rules to block .RAR and .CAB files.

File Blocking rule: File Blocking Options tab

Table 15-4 lists the options on the File Blocking Options tab of File Blocking rule properties.

Table 15-4 File Blocking rule: File Blocking Options tab

Setting	Description	Default Value
File action	Whether to block or allow a file that breaks the rule. You could, for example, allow the file to be created but send an appropriate notification to an administrator.	File is blocked.
Check file content	Whether to scan inside files to determine their types. This would catch, for example, a .MP3 file that had been renamed to .TXT	Content is not checked.
Scan inside archive	Whether to scan the contents of files within compressed files such as ZIP files. Selecting this option may have some impact on performance. Note that files stored within .RAR and .CAB files cannot be blocked or quarantined. However, you can create rules to block .RAR and .CAB files.	Compressed files are not scanned.

File Blocking rule: Notifications tab

Table 15-5 lists the options on the Notifications tab of File Blocking rule properties.

Table 15-5 File Blocking rule: Notifications tab

Setting	Description	Default Value
Notify using Messenger Service	Enables automatic notifications using the Windows Messenger Service. **Note:** Microsoft does not support the Windows Messenger service from Windows Server 2008 onwards. File Blocking notifications that use the Messenger service have no effect with file servers that run Windows Server 2008 or later.	No notification.
Send email	Enables automatic notifications by email.	No notification.
Run custom command	Enables you to run a command when a rule is broken. For example you could specify a NET SEND command or a batch file to run. The command runs under the local System account.	No notification.
Log the event	Enables logging to the Enterprise Vault event log.	No notification.
"Configure notifications" button	Enables you to configure the notification. See "File Blocking rule: Configure notifications option" on page 141.	

File Blocking rule: Configure notifications option

Click **Configure notifications** on the Notifications tab of the File Blocking rule properties to define the delivery and content of the message to send when the rule is broken. The tabs that are available depend on the notification methods you selected.

Table 15-6 Notification tabs options

Tab name	Description
Message	The text of the message that you want to be sent when the rule is broken. You can enter plain text on this tab. Click **Advanced** to do any of the following: ■ Include variable text such as the path to the file that was blocked, or the name of the user that broke the File Blocking rule. See "File Blocking rule: Notification message variables" on page 143. ■ Save the message as a template message for future use. ■ Load a previously saved template message.
Messenger	Enables you to choose to send a Windows Messenger Service notification message to any combination of the following: ■ A specific member of the Administrators group. ■ The user who broke the File Blocking rule. ■ An SNMP trap. This sends the computer name, the file name, the user name, and the message that is defined on the Message tab. **Note:** Microsoft does not support the Windows Messenger service from Windows Server 2008 onwards. File Blocking notifications that use the Messenger service have no effect with file servers that run Windows Server 2008 or later.
Logging	Enables you to choose to log File Blocking violations to the following: ■ Enterprise Vault audit database. ■ Enterprise Vault event log.
Email	Enables you to specify the mail header information to be used when a mail notification is sent.

Table 15-6 Notification tabs options *(continued)*

Tab name	Description
Custom Command	This enables you to define commands to be run automatically when a File Blocking rule is broken. Do not specify a command that requires interaction with the desktop. For example, you could specify a batch file to run or a NET SEND command. You can enter multiple commands, one per line. Note that if the computer is running Windows 2008, file blocking custom commands can fail because the Windows task scheduler does not correctly parse quotation marks in a command line. To fix this problem, you must install the following hotfix from Microsoft: http://support.microsoft.com/kb/951246 **Note:** Custom commands require the Windows "Task Scheduler" service to be running.

File Blocking rule: Notification message variables

You can insert variable information into a File Blocking notification message, such as the path to the file that was blocked. The variables are replaced with the details that are current at the time the message is sent.

Table 15-7 describes the variables that you can use.

Table 15-7 Notification variables

Variable name	Description
[USER]	Current user who caused the action. Includes domain information.
[USER NO DOMAIN]	Current user who caused the action without the domain information.
[USER MAIL ID]	Email ID of the user who caused the action. This ID is taken from Active Directory. Use this variable if the user's logon and email names might be different.
[DOMAIN]	Domain name.
[FILE SPEC]	File path and name that caused the action.
[FILE NAME]	Name of the file that caused the action.
[POLICY NAME]	Name of the policy that is applied to the managed resource.

Table 15-7 Notification variables *(continued)*

Variable name	Description
[OBJECT NAME]	Name of the resource that caused the action.
[OWNER NO DOMAIN]	Name of the owner of the file that caused the action without domain information.
[OWNER]	Name of the owner of the file that caused the action. Includes domain information.
[SERVER NAME]	Name of the server where an alarm has been activated.
[OBJECT NAME SHARE]	Shared name of the resource. For example, you can enter "H" as in "H:\MyDrive" and the share name is inserted.

File Blocking rule: Folder Filters tab

The Folder Filters tab enables you to specify which folders you want File Blocking to monitor. The folder selection is used on every volume to which you apply this policy, so you must specify path names in relation to the root of the volume.

Note: Do not apply a File Blocking rule to a folder that is used for quarantined files.

Table 15-8 lists the options on the Folder filters tab of File Blocking rule properties.

Table 15-8 File Blocking rule: Folder filters tab

Setting	Description	Default Value
Monitored folders	The folders that are to be monitored by File Blocking. You can choose to monitor the whole volume or to monitor specific folders and their subfolders.	No monitored folders.
Ignored folders	A list of folders that are not to be monitored by File Blocking. If you have chosen to monitor specific folders, this list enables to you to specify exceptions to that list.	No ignored folders.

Exempting File Blocking for specific users

It is possible for you to define, for each file server, a list of users whose files are never blocked. Note that the Vault Service account is never blocked. The account is excluded from all file blocking.

Note the following if you configure File Blocking in a clustered environment where multiple cluster groups can come online on the same cluster node. The File Blocking exemptions list must be identical for all the virtual servers that can be online concurrently on the same node.

To exempt File Blocking for specific users

1. Expand the Administration Console tree until the **Targets** container is visible.
2. Expand **Targets**.
3. Expand **File Server**.
4. Right-click the server on which you want the user to be exempt from File Blocking and, on the shortcut menu, click **Properties**.
5. On the **File Blocking** tab, next to **Exemptions**, click **Add**. The **Add Windows Users and Groups** dialog appears.
6. Select the user you want to add to the exemptions list and click **Add**.
7. Click OK to close **Add Windows Users and Groups**.
8. Click **OK** to close **File Server Properties**.

Troubleshooting File Blocking in a clustered environment

If File Blocking does not work on a shared disk, ensure that a volume share is not configured in the Administration Console as a volume target under multiple virtual server targets. It is possible to set this invalid configuration in the Administration Console if multiple cluster groups are online on a common node.

Chapter 16

Configuring and running FSA tasks

This chapter includes the following topics:

About configuring and running FSA tasks

To process target file servers, an Enterprise Vault server must have at least one File System Archiving task.

Each File System Archiving task processes the target volumes to which it is assigned. If any file servers are unreachable, for example due to a network failure, the task processes the target volumes on the reachable file servers and logs the details of the unreachable file servers in the Enterprise Vault event log and in the File System Archiving task report.

You can configure the properties of the File System Archiving task to determine when and how the archiving proceeds.

The properties of a File System Archiving task include the following:

- The schedule for running the task. A Run Now option enables you to start the task manually.
- The schedule for the archive permissions synchronization.
- For EMC Celerra/VNX, the schedule for the deletion of archived files whose placeholders have been deleted, if you have configured this feature.
- The file version pruning options and schedule.
- The settings that control the generation of archiving reports and pruning reports.

To implement custom filters for File System Archiving tasks, you need to configure registry settings.

See "Configuring file system filters" on page 157.

Adding a File System Archiving task

You can add a File System Archiving task to an Enterprise Vault server from the Administration Console.

To add a File System Archiving task

1. In the Administration Console, expand the Enterprise Vault site until the **Enterprise Vault Servers** container is visible.
2. Expand the required server container.
3. Right-click the **Tasks** container, and select **New > File System Archiving Task**.
4. The new task wizard starts.

   Change the default name for the task, if required.
5. The new task is displayed in the right-hand pane. Double-click the task object to display the properties of the task.

Scheduling a File System Archiving task

A File System Archiving task processes its target file server volumes according to the schedule that you define for the task. You can define an individual schedule for each File System Archiving task, or you can use the default site schedule for all tasks. The default site schedule is defined on the **Site Schedule** tab of the site properties.

The File System Archiving task checkpoints its progress. If the task is stopped before it has completely processed a volume, then when the task next starts it continues from the point of interruption.

To schedule a File System Archiving task

1. In the Administration Console, expand the Enterprise Vault site until the **Enterprise Vault Servers** container is visible.
2. Expand **Enterprise Vault Servers**.
3. Expand the Enterprise Vault server that runs the task you want to modify.
4. Click **Tasks**.
5. Right-click the name of the File System Archiving task you want to modify and, on the shortcut menu, click **Properties**.
6. Click the **Schedule** tab.
7. To use a schedule for this task other than the default site schedule, clear **Use site setting**.
8. Define the schedule that you require and then click **OK**.
9. Stop and restart the task for the changes to take effect.

Setting the FSA folder permissions synchronization schedule

A File System Archiving task can synchronize archive folder permissions with file server folder permissions automatically on a scheduled basis. The automatic synchronization can run once or twice each day. If you choose to turn off the automatic synchronization you can synchronize manually.

The permissions of folders within an archive are always synchronized with the NTFS permissions of the corresponding file system folder.

The permissions of the archive itself are synchronized by default with the corresponding file server share, as follows:

- If the archive point folder is a share, the archive point folder permissions are mapped to the archive.
- Otherwise, the target volume share's permissions are mapped to the archive.

If required, you can change this default behavior and synchronize the permissions of an archive with the permissions of the archive point folder, regardless of whether the archive point folder is a share. You can do this by setting the SynchroniseFSASharePermissions registry value.

See “SynchroniseFSASharePermissions” in the *Registry Values* guide.

To set the FSA folder permissions synchronization schedule

1. In the Administration Console, expand the Enterprise Vault site until the **Enterprise Vault Servers** container is visible.
2. Expand **Enterprise Vault Servers**.
3. Expand the Enterprise Vault server that runs the task you want to view or modify.
4. Click **Tasks**.
5. Right-click the name of the File System Archiving task you want to view or modify and, on the shortcut menu, click **Properties**.
6. Click the **Synchronization** tab.
7. Set the schedule you require and then click **OK**.

Scheduling the deletion of archived files on placeholder deletion for EMC Celerra/VNX

The deletion of archived EMC Celerra/VNX files whose placeholders have been deleted does not occur immediately. The deletion takes place once or twice each day, according to the schedule that you define on the properties of the File System Archiving task.

To schedule the deletion of archived files on placeholder deletion for EMC Celerra/VNX

1. In the Administration Console, expand the Enterprise Vault site until the **Enterprise Vault Servers** container is visible.
2. Expand **Enterprise Vault Servers**.
3. Expand the Enterprise Vault server that runs the File System Archiving task to archive from the Celerra/VNX device.
4. Click **Tasks**.
5. Right-click the File System Archiving task and, on the shortcut menu, click **Properties**.
6. Click the **Celerra** tab.
7. Set the AM and PM deletion times that you require.
8. Click **OK**.

Configuring FSA version pruning

By using FSA version pruning, you can control the number of versions of files that are stored in Enterprise Vault archives.

Each time a file is recalled and modified, subsequent archiving means that another version of the file is stored in the archive.

Pruning is the process of deleting the earlier versions of archived files until the required number of versions remains.

To configure FSA version pruning

1. In the Administration Console, expand the Enterprise Vault site until the **Enterprise Vault Servers** container is visible.
2. Expand **Enterprise Vault Servers**.
3. Expand the Enterprise Vault server that runs the task you want to modify.
4. Click **Tasks**.
5. Right-click the name of the File System Archiving task you want to modify and, on the shortcut menu, click **Properties**.
6. Click the **Pruning** tab.
7. Select **Enable pruning**.
8. Next to **Prune to**, select the maximum number of versions of each file you want to retain in the archive.
9. If you also want to prune according to the amount of time that items have been archived, select **Enable age-based pruning** and specify the maximum age allowed for archived items.

   Age-based pruning never deletes the final copy of an archived file, regardless of its age.
10. Under **Scheduled Pruning**, define the schedule that you require and then click **OK**.

Using Run Now to process FSA targets manually

This section comprises the following topics:

Processing an FSA target volume manually

Normally, a File System Archiving task processes its target volumes according to the schedule that you define for the task. If you want to process a particular volume outside of this schedule you can use the **Run Now** option to process a volume on demand.

Note the following:

- **Run Now** reports only on files that are beneath archive points.
- When archiving by quota, the number of files actually archived may not match the number shown in the report. This is because the order in which the files are processed during a report mode run is unlikely to be the same as the order during the normal run.
  File System Archiving archives only sufficient eligible files to meet the quota settings, so there may be more, or fewer, files actually archived than shown in the report.

To process an FSA target volume manually

1. In the Administration Console, expand the Enterprise Vault site until the **Targets** container is visible.
2. Expand the **Targets** container.
3. Expand the **File Servers** container.
4. Expand the target file server whose volume you want to process.
5. Right-click the volume that you want to process and then, on the shortcut menu, click **Run Now**.
6. In the Run Now dialog box, select the options to specify how you want the task to run:
   - **In normal mode**: The volume is processed normally; the files that match the archiving criteria are archived.
   - **In report mode**: Nothing is archived, but Enterprise Vault generates a report that shows you what would be archived if you processed the volume in normal mode.

   The File System Archiving task creates the reports in the `Reports\FSA` subfolder of the Enterprise Vault installation folder, for example `C:\Program Files (x86)\Enterprise Vault`.

   Within `Reports\FSA` there is a subfolder for the task, with further subfolders to indicate the mode in which the task was run.

   See "About File System Archiving task reports" on page 153.

The fields within the file are tab-separated, so the contents can easily be read into a spreadsheet program for analysis.

7 **Run the task for the creation of shortcuts only**: Select this option to restrict the task so that it does not archive, but does create shortcuts. The task creates shortcuts according to the shortcut creation settings in the policy archiving rules. When you select this option the task does not perform archiving. You can choose In report mode to generate a report of shortcuts that would be created if the task ran in normal mode.

8 Click **OK**.

Running a File System Archiving task manually

Typically a File System Archiving task processes file server volumes according to the schedule you set up for the task. If you want to run the task outside of this schedule, you can use the **Run Now** option to run a File System Archiving task on demand.

Note the following:

- If a file server's volumes are archived by different tasks, you need to run each of those tasks in order to archive all the volumes. As an alternative, you can process individual volumes.
  See "Processing an FSA target volume manually" on page 151.
- Run Now reports only on files that are beneath archive points.
- When archiving by quota, the number of files actually archived may not match the number shown in the report. This is because the order in which the files are processed during a report mode run is unlikely to be the same as the order during the normal run.
  File System Archiving archives only sufficient eligible files to meet the quota settings, so there may be more, or fewer, files actually archived than shown in the report.

To run a File System Archiving task manually

1 In the Administration Console, expand the Enterprise Vault site until the **Enterprise Vault Servers** container is visible.

2 Expand the **Enterprise Vault Servers** container.

3 Expand the **Enterprise Vault server** that hosts the task you want to run.

4 Click the **Tasks** container.

5 In the list, right-click the File System Archiving task you want to run and, on the shortcut menu, click **Run Now**.

6 In the Run Now dialog box, select the mode to use. The options are as follows:

- **In normal mode**: The file server is processed normally; the files that match the archiving criteria are archived.
- **In report mode**: Nothing is archived, but Enterprise Vault generates a report that shows you what would be archived if you processed the server in normal mode. The report also includes volumes and folders for which archiving has been disabled.
  The File System Archiving task creates the reports in the `Reports\FSA` subfolder of the Enterprise Vault installation folder, for example `C:\Program Files (x86)\Enterprise Vault`.
  Within `Reports\FSA` there is a subfolder for the task, with further subfolders to indicate the mode in which the task was run.
  See "About File System Archiving task reports" on page 153.
  The fields within the file are tab-separated, so the contents can easily be read into a spreadsheet program for analysis.

7 **Run the task for the creation of shortcuts only**: Select this option to restrict the task so that it does not archive, but does create shortcuts. The task creates shortcuts according to the shortcut creation settings in the policy archiving rules. When you select this option the task does not perform archiving. You can choose **In report mode** to generate a report of shortcuts that would be created if the task ran in normal mode.

8 Click **OK** to start the run.

About File System Archiving task reports

A File System Archiving task can create reports for the following:

- Archiving runs
- File version pruning runs
- Runs to delete archived Celerra/VNX files whose placeholders have been deleted

For archiving runs and file version pruning runs you can use the settings on the **Reports** tab of the File System Archiving task's properties to control the logging level and the number of reports to keep.

The reports are generated in the following places under the Enterprise Vault installation folder:

- Reports for pruning runs and Celerra/VNX file deletion runs are generated in the `Reports` subfolder.
- Reports for archiving runs are generated in the `Reports\FSA` subfolder.

Within `Reports\FSA` there is a subfolder for the task, with further subfolders to indicate the mode in which the task was run.

Until the task has finished processing all its targets, the task keeps the reports in a folder that is called `InProgress`. When the task has finished processing, it moves the reports to a subfolder that is underneath the `Completed` folder. The subfolder name is the date and time that task completed its processing.

For example, if task 'ArchiveTask1' is running in normal, scheduled mode, but has not finished processing, the report files could be in the following folder:

```
C:\Program Files (x86)\Enterprise
Vault\Reports\FSA\ArchiveTask1\ArchiveScheduled\InProgress
```

If task 'ArchiveTask1' completes its processing on 20-Feb-2011 at 12:29.07, the report files are moved to the following folder:

```
C:\Program Files (x86)\Enterprise
Vault\Reports\FSA\ArchiveTask1\ArchiveScheduled\Completed\2011-02-20
12-29-07
```

Table 16-1 lists the folder names that are used for the different archiving run modes.

Table 16-1 File System Archiving task archiving run modes and their associated folder names

Run mode	Folder name
Normal, Scheduled	ArchiveScheduled
Normal, Run Now	ArchiveRunNow
Normal, Run Now, Create shortcuts only	ArchiveRunNowCreateShortcuts
Report, Scheduled	ReportScheduled
Report, Run Now	ReportRunNow
Report, Run Now, Create shortcuts only	ReportRunNowCreateShortcuts

The report files are named as follows:

TaskName`_`*RunMode*`_`*RunNumber*`.txt`

where:

- *TaskName* is the name of the File System Archiving task.
- *RunMode* is the mode in which the task was run.
- *RunNumber* is the sequence number of the run.

It may take many runs before the File System Archiving task has completely processed its target volumes. The task creates a report file for each run. The report for the final run has '_FINAL' added to the name to indicate that processing is complete.

For example, if 'ArchiveTask1' processes according to its schedule, in normal mode, the file names of successive reports could be as follows:

```
ArchiveTask1_ArchiveScheduled_001.txt
ArchiveTask1_ArchiveScheduled_002.txt
ArchiveTask1_ArchiveScheduled_003_FINAL.txt
```

When custom filters are configured for File System Archiving, report files include information about the filters and the files that the filters have processed.

See "About file system filter reports" on page 161.

When a File System Archiving task processes a folder that has an archive point with no archive ID or an invalid archive ID, Enterprise Vault performs a check for existing archives for the folder path. If the check identifies that multiple archive IDs are associated with the folder path, the task report lists the archive ID of each archive that is associated with the folder path, and indicates which archive will be used for archiving.

See "About the checks for existing archives for an FSA folder path" on page 104.

About scheduling storage expiry for FSA

When an item's retention period expires, File System Archiving can automatically delete it. File System Archiving does this according to the schedule that you define with the Administration Console, on the Storage Expiry tab of the site Properties dialog box.

File System Archiving does not delete archived items when either of the following conditions applies:

- On the "Storage Expiry" tab of the site Properties dialog box, the schedule is set to "Never" or you have checked "Run in report mode".
- On the "Advanced" tab of the Archive Properties dialog box, "Delete expired items from this archive automatically" is unchecked.

Chapter 17

Configuring file system filtering

This chapter includes the following topics:

About custom filters for File System Archiving

File system filtering can be used for a variety of reasons, for example:

- To select certain files and process them differently from the rest of the files on the archiving target. Files not selected by a filter are processed according to the Enterprise Vault policy that is assigned to the archiving target .
- To provide additional statistics on files.
- To add proprietary information to files as they are archived by Enterprise Vault.

A filter defines how the File System Archiving task selects and processes files. Files can be selected by matching one or more attributes, such as file name or file type. Additional properties can be added to the Enterprise Vault index for the file.

The action defined for the selected files can be one of the following:

- Apply the policy that is associated with the volume or folder in which the file is located.
- Archive the file with or without creating a shortcut.
- Archive the file and delete the original, without creating a shortcut.
- Delete the file without archiving it.

- Do not archive the file.

A filter can also request the archiving task to shut down.

If required, filters can pass the selected file to a third-party application for additional processing. For example, files can be passed to file classification or file decryption applications. The filter can pass additional information to Enterprise Vault for indexing, or alter the way the file is processed based on its classification. Classification information that is added to files is then available to Enterprise Vault search applications, such as Discovery Accelerator.

If a file that has already been archived is processed by a filter, the following actions are not applied:

- Modifying file properties, index properties or retention category.
- File stream operations.

Only the following subset of filter actions can be applied when processing archived files:

- Create a shortcut.
- Delete the original file on the file server.
- Stop the archiving task.

You can develop proprietary filters for File System Archiving tasks using the File System Filtering API. Generic custom filters for Exchange Server Archiving and Domino Server Archiving are shipped with Enterprise Vault. These allow you to apply filtering without the need to develop filters using the associated filtering API. Currently, no generic custom filter is provided for File System Archiving.

To develop software using Enterprise Vault APIs, your company must be a member of Symantec Technology Enabled Program (STEP). Information about STEP is available at the following address: http://go.symantec.com/step

Configuring file system filters

You use registry settings to implement custom filters, and enable filtering for Enterprise Vault File System Archiving tasks.

See "To configure file system filter registry settings" on page 159.

To control the behavior of the archiving task in the event of filter errors, you can configure the following entries in the XML configuration file, `Enterprise Vault\EVFSAArchivingTask.exe.config`:

- **MoveOnFilterFailure**. This setting controls the action taken by the archiving task if it cannot load a filter.

If the setting is not present in the configuration file, then the default value is "0"; the archiving task stops if it cannot load the filter.

- **MaxFilterError**. During archiving, the archiving task keeps a count of the number of filtering errors reported. The MaxFilterError setting lets you configure the maximum number of errors permitted before the archiving task stops.
  If the setting is not present in the configuration file, the default value is 100.

See "To configure entries in EVFSAArchivingTask.exe.config" on page 160.

After you upgrade Enterprise Vault, you must update the .NET binding redirections in the configuration file to use the newer version of the Enterprise Vault API Runtime. The ReadMeFirst file for the API Runtime describes how to do this.

To configure file system filter registry settings

1 On the Enterprise Vault server, start Regedit and navigate to the following location in the registry:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \External Filtering
      \File System
```

If either **External Filtering** or **File System** keys do not exist, then create them.

2 Create a new string entry for each custom filter under the **File System** key. Filter names must be an unbroken numbered sequence starting at 1.

For the value of a custom filter setting enter a string value that contains the name of the .NET assembly, and the fully-qualified filter class name of the new external filter:

PathToFilterAssembly!FilterClassName

A fully-qualified class name includes the namespace. For example, if the class name is **CustomFilter**, the namespace is **Symantec.EnterpriseVault.FileSystem**, and the filter is implemented in **Symantec.EnterpriseVault.FileSystemCustomFilter.dll** assembly, then the value of the registry setting should be as follows:

Symantec.EnterpriseVault.FileSystemCustomFilter.dll!
Symantec.EnterpriseVault.FileSystem.CustomFilter

Note that the class name is case-sensitive.

3 If you change the registry settings during an archiving run, you need to restart the associated File System Archiving task to implement the changes.

To configure entries in EVFSAArchivingTask.exe.config

1. Take a back-up copy of the file, `Enterprise Vault\EVFSAArchivingTask.exe.config`, and then open the file for editing.
2. Add a section called **<FSAFilter>** to hold the settings. This section must also be declared in the **<configSections>** element. For example,

```
<configSections>
   <section name="FSAFilter"
      type="System.Configuration.DictionarySectionHandler"/>
</configSections>
<FSAFilter>
</FSAFilter>
```

3. Add one or both of the entries, **MoveOnFilterFailure** and **MaxFilterError**, as required. The entries must be in the form:

   <add key="*name*" value = "*value*"/>

   Entries can take the following values:

   - **MoveOnFilterFailure**. "0" (default), or "1". If the setting value is "0", then the archiving task stops if it cannot load a filter. If the setting value is "1", then the archiving task loads the next filter, or continues to archive.
   - **MaxFilterError**. Integer (default 100). The maximum number of filter errors permitted before the archiving task stops.

   The following example shows the file with the settings added:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
   <configSections>
      <section name="FSAFilter"
      type="System.Configuration.DictionarySectionHandler"/>
   </configSections>
   <FSAFilter>
      <add key="MaxFilterError" value = "150"/>
      <add key="MoveOnfilterFailure" value = "1"/>
   </FSAFilter>
   <runtime>
      <generatePublisherEvidence enabled="false"/>
   </runtime>
</configuration>
```

   The settings in this example file have the following effect:

- key="MaxFilterError" value = "150" — The archiving task will stop if more than 150 filtering errors are reported.
- key="MoveOnfilterFailure" value = "1" — If the archiving task cannot load a filter, it will try to load the next filter, or continue to archive.

About file system filter reports

When external filters are configured for File System Archiving, information is added to the File System Archiving task report file. The report files are located in the `Reports\FSA` subfolder of the Enterprise Vault installation folder.

In the detailed information for each file processed, the **Filter Modifications** column shows the filter actions that have been performed on the file. This information is shown in the form:

[*filter_name* - *action*, *action*, ...] [*filter_name* - *action*, *action*, ...] ...

where *filter_name* is the name of the external filter, and *action* identifies the type of action that the filter has performed. *action* can be one of the following:

- **Applied filtering action** The filter has changed the action applied to the file.
- **Modified file properties** File attributes have been modified.
- **Modified index properties** Index properties have been added or removed.
- **Performed file stream operation** A file or alternate data stream has been opened to read or write.
- **Applied retention category** The retention category has been changed.

Summary information for each external filter is displayed in the report section, **External Filter Summary**. The information shows the number of files or alternate data streams on which the filter has performed each action. Failure to load a filter is also reported in this section.

If files that have already been archived are processed by a filter, only the filtering action can be applied. Therefore only **Applied filtering action** is reported for these files.

Chapter 18

Managing the file servers

This chapter includes the following topics:

About managing the target file servers

This section provides guidance on the operational administration of the file servers that are targets for FSA. It includes information on backing up, virus checking, placeholder recall rates, and preventing unwanted file recalls.

About backing up the target file servers

You must back up the file server disks that File System Archiving processes.

For Windows file servers the backup software must be capable of backing up the following:

- Alternate data streams
- Sparse reparse points, if you use placeholder shortcuts

Symantec NetBackup™ and Symantec Backup Exec™ are examples of suitable data protection products.

Enterprise Vault placeholder shortcuts appear to the operating system as markers for offline files. Most backup programs can be configured to ignore offline files. If

you cannot configure your backup program to ignore offline files, every placeholder that the backup program checks may result in the recall of the offline file.

To determine whether your backup software is recalling files, you can do one of the following:

- Use Windows Explorer to list the files that have been backed up. Placeholder shortcuts have their own icon.
- Check the File System Archiving report file. If files were recalled on the previous backup run, successive reports show that an increasing number of files have been turned into placeholder shortcuts.

If you cannot configure your backup program to ignore offline files, you can use an alternative method to prevent file recalls.

See "About preventing unwanted file recalls from placeholder shortcuts" on page 167.

A restore operation on a file server may result in the recall of placeholders if the restore program attempts to perform File Blocking checks. To prevent this problem you can prohibit the restore program's user account from performing File Blocking checks.

See "Preventing file recalls on restore due to File Blocking checks" on page 170.

About virus-checking the target file servers

See the Enterprise Vault *Compatibility Charts* at http://www.symantec.com/docs/TECH38537 for a list of antivirus programs that Symantec has tested for use with Enterprise Vault. Other antivirus programs that have not been tested, but which can be configured to ignore offline files, will probably work with File System Archiving.

Note: Before you install any antivirus product on a file server on which you have installed the FSA Agent, we recommend that you stop the File Placeholder Service. After completing the installation of the antivirus product, you must restart the File Placeholder Service.

If possible, configure your antivirus program to ignore offline files before you run virus scans on disks with Enterprise Vault placeholder shortcuts. Placeholder shortcuts appear to the operating system as markers for offline files. If you cannot configure your antivirus program to ignore offline files, every placeholder that the antivirus program checks results in the recall of the offline file.

If you cannot configure your antivirus program to ignore offline files, you can use an alternative method to prevent file recalls.

See "About preventing unwanted file recalls from placeholder shortcuts" on page 167.

About changing the placeholder recall rate settings

For Windows and NetApp file servers you can change the maximum rate at which a user or program can perform placeholder recalls. The default maximum is 20 recalls in 10 seconds. This limit helps to prevent applications that do not honor the file system offline attribute from recalling all the files that have been archived from a volume. An application receives an Access Denied status if it attempts to exceed the maximum recall rate. How the status is displayed to the user depends on the application. A separate setting lets you waive the maximum recall rate for members of the file server's local Administrators group, if required.

For NetApp file servers, you can also change the number of threads that Enterprise Vault uses for placeholder recalls to each file server. This setting determines the maximum number of simultaneous recalls to the file server. By default Enterprise Vault uses up to 25 threads for placeholder recalls to each NetApp file server.

You may want to adjust these settings if users who perform operations with placeholders frequently receive error messages indicating that the files cannot be recalled.

Note: Do not increase the maximum recall rate excessively, otherwise applications that fail to honor the file system offline attribute may overload the file server with recalls.

See "Changing the placeholder recall rate settings for a Windows file server" on page 164.

See "Changing the placeholder recall rate settings for a NetApp file server" on page 166.

Changing the placeholder recall rate settings for a Windows file server

Registry values control the placeholder recall rate for Windows file servers. The registry values are located under the following registry key on the file server:

On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \KVS
   \Enterprise Vault
    \FSA
     \PlaceholderService
```

On a 64-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \FSA
      \PlaceholderService
```

Table 18-1 describes the registry values for limiting placeholder recall on Windows file servers.

Table 18-1 Registry values for limiting placeholder recall rate on Windows file servers

Registry value	Content	Description
RecallLimitMaxRecalls	DWORD	Defines the maximum number of placeholder recalls that are allowed in the period that RecallLimitTimeInterval defines. The default value is 20. For example, if RecallLimitMaxRecalls is set to 20 and RecallLimitTimeInterval is set to 10, the maximum placeholder recall rate is 20 recalls in 10 seconds.
RecallLimitTimeInterval	DWORD	Specifies the period in seconds for the maximum placeholder recall rate. The default is 10. If the maximum recall rate is reached, Enterprise Vault imposes an additional interval equal to the RecallLimitTimeInterval before it resets the count. For example, if the maximum recall rate is set at 20 recalls in 10 seconds and a user achieves 20 recalls in 8 seconds, Enterprise Vault imposes a 10-second block on further recalls before it resets the count for the user.

Table 18-1 Registry values for limiting placeholder recall rate on Windows file servers *(continued)*

Registry value	Content	Description
BypassRecallLimitsForAdmins	DWORD	Determines whether members of the file server's local Administrators group are subject to the maximum placeholder recall rate. The default is value 0, which means that the recall limit applies to local administrators. Change the value to 1 to waive the recall limit for administrators.

For more information on the registry values for placeholder recall on Windows file servers, see the *Registry Values* manual.

Note: A similar set of registry values controls the maximum rate of pass-through recall on Windows file servers.

See "Registry values for pass-through recall on Windows file servers" on page 120.

To change the placeholder recall rate settings for a Windows file server

1. Start the Windows registry editor on the file server.
2. Modify the placeholder recall registry values as required.
3. To apply the changes, restart the Enterprise Vault Placeholder service on the file server.

Changing the placeholder recall rate settings for a NetApp file server

For a NetApp file sever the placeholder recall rate settings are configured on the properties of the target file server in the Vault Administration Console.

To change the placeholder recall rate settings for a NetApp file server

1. In the Administration Console, expand the Enterprise Vault site until the **Targets** container is visible.
2. Expand the **Targets** container and then the **File Servers** container.
3. Right-click the NetApp file server whose parameters you want to configure, and on the shortcut menu select **Properties**.
4. On the file server properties dialog, select the **NetApp** tab.
5. Configure the placeholder recall settings as follows:

- To process placeholder recalls on the NetApp file server, ensure that **Process placeholder recalls** is selected.
- To change the number of available threads for placeholder recalls, change the value for **Number of recall threads**.
- To change the maximum placeholder recall rate for each user, change the **Limit recalls to a maximum of...** values. You can set the number of recalls and the time period in seconds. If the maximum recall rate is reached, Enterprise Vault imposes an additional interval equal to the time period before it resets the count. For example, if the recall limit is 20 recalls in 10 seconds and a user achieves 20 recalls in 8 seconds, Enterprise Vault imposes a 10-second block on further recalls before it resets the count for the user
- To waive the maximum recall rate for members of the NetApp file server's local Administrators group, select **Ignore recall limits for local administrators**.

6 Click **Apply** to apply the configuration changes.

About preventing unwanted file recalls from placeholder shortcuts

Enterprise Vault placeholder shortcuts appear to the operating system as markers for offline files. You may experience unwanted recalls of files from FSA placeholder shortcuts in some circumstances. For example, if a backup program or an antivirus program does not honor the file system offline attribute it may trigger placeholder recalls.

You can prevent unwanted recalls in the following ways:

- For Windows file servers or NetApp filers, use the supplied `EvFsaBackupMode.exe` program to exclude the appropriate Active Directory account from triggering placeholder recalls.
  See "Using FSA backup mode to prevent file recalls" on page 168.
- For Windows file servers, include the offending program in the list of programs that are prohibited from recalling archived items.
  See "Prohibiting a program from recalling files that FSA has archived" on page 169.
- For EMC Celerra/VNX devices, use the device's backup options to exclude the appropriate Active Directory account from triggering placeholder recalls.
  See "Preventing file recalls on EMC Celerra/VNX" on page 170.

- If a restore operation on a file server performs File Blocking checks which trigger file recalls, you can prohibit the restore program's user account from performing the File Blocking checks.
  See "Preventing file recalls on restore due to File Blocking checks" on page 170.

Using FSA backup mode to prevent file recalls

For Windows file servers and NetApp filers you can use the supplied program `EvFsaBackupMode.exe` to place the file server into FSA backup mode. When the file server is in FSA backup mode, members of the following security groups are prevented from recalling files from placeholders:

- The computer local group Enterprise Vault Backup Operators.
- The domain universal, global, or local group Enterprise Vault Backup Operators.

Other users can continue to recall files as normal.

For example, you can use this mechanism to exclude the accounts that run backup or antivirus programs from recalling files.

Create an Enterprise Vault Backup Operators group in Active Directory and place in this group the required user accounts. You can then use `EvFsaBackupMode.exe` to place the file server into FSA backup mode.

`EvFsaBackupMode.exe` is in the Enterprise Vault installation folder (for example `C:\Program Files (x86)\Enterprise Vault`). You can run `EvFsaBackupMode.exe` from the Enterprise Vault installation folder. Alternatively you can copy it to another folder, or copy it to another computer, which does not need to be an Enterprise Vault server.

The syntax for `EvFsaBackupMode.exe` is as follows:

```
EvFsaBackupMode.exe -backup | -normal Server
[DirectoryComputer]
```

where

- *Server* is the name of the file server that is running a Placeholder service.
- *DirectoryComputer* is the name of the Enterprise Vault Directory service computer. This is required only when you are backing up a NetApp Filer. In this case, *Server* is the name of the NetApp Filer.

For example:

- To place a file server that is named MyServer into FSA backup mode, type the following:

  ```
  EvFsaBackupMode.exe -backup MyServer
  ```

- To return the same file server to normal mode, type the following:

```
EvFsaBackupMode.exe -normal MyServer
```

- To place a NetApp Filer that is named `MyFiler` into FSA backup mode when the Directory service computer is named `MyDirServ`, type the following:

```
EvFsaBackupMode.exe -backup MyFiler MyDirServ
```

- To return the same NetApp Filer to normal mode, type the following:

```
EvFsaBackupMode.exe -normal MyFiler MyDirServ
```

Prohibiting a program from recalling files that FSA has archived

For Windows file servers it is possible to specify a list of programs that are prohibited from recalling items that FSA has archived. This is most likely to be useful if you use an antivirus program or backup program that does not honor the file system offline attribute. The program must be a program that runs on the file server.

You specify the list of programs by editing a registry value named ExcludedExes on each computer that is running an Enterprise Vault Placeholder service. This registry value is a string value under the following registry key:

On a 32-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \KVS
   \Enterprise Vault
    \FSA
     \PlaceholderService
```

On a 64-bit installation of Windows:

```
HKEY_LOCAL_MACHINE
 \SOFTWARE
  \Wow6432Node
   \KVS
    \Enterprise Vault
     \FSA
      \PlaceholderService
```

To specify a list of prohibited programs, edit ExcludedExes to specify the names of the program executable files, separated by semicolons (;).

For example, to exclude Windows Explorer, "MyBackupProgram", and a program called "MyAntivirus", you can specify the following:

```
Explorer.exe;MyBackupProgram.exe;MyAntivirus.exe
```

If you change the list of prohibited programs, you must restart the Enterprise Vault Placeholder service on the file server to make the change take effect.

Note: A second ExcludeExes registry value under the `PlaceholderService\PassThrough` registry key can be used to prevent programs from receiving pass-through recalls.

See "Registry values for pass-through recall on Windows file servers" on page 120.

Preventing file recalls on EMC Celerra/VNX

For an EMC Celerra/VNX device, you can use the device's backup options to prohibit Active Directory groups or Active Directory accounts such as a service account from triggering placeholder recalls from the Celerra/VNX file systems. For example, you can exclude the service account for a backup program or antivirus program.

To prevent members of a group or an individual account from triggering placeholder recalls through the CIFS interface, add the appropriate group or account to the Celerra/VNX Backup Operators group. Then execute the following command to prevent those accounts from recalling placeholders:

```
fs_dhsm -m fs_name -backup offline
```

where *fs_name* is the name of the file system on the Celerra/VNX.

For more details, consult your EMC Celerra/VNX documentation.

Preventing file recalls on restore due to File Blocking checks

A restore operation on a file server may result in the recall of archived files from placeholders if the restore program attempts to perform File Blocking checks. To prevent this problem you can prohibit the restore program's user account from performing File Blocking checks.

To prevent FSA file recalls on restore due to File Blocking checks

1. Create an **Enterprise Vault Backup Operators** security group in Active Directory.
2. Add to the **Enterprise Vault Backup Operators** group the user account under which the restore program runs.
3. Add the **Enterprise Vault Backup Operators** group to the list of users and groups that are excluded from File Blocking on the file server.

Appendix A

Permissions and privileges required for the Vault Service account on Windows file servers

This appendix includes the following topics:

About the permissions and privileges required for the Vault Service account on Windows file servers

If the Vault Service account is not a member of the local Administrators group on an FSA target Windows file server, the account requires a set of minimum permissions and privileges on the file server.

The Vault Service account also requires these permissions and privileges on File Blocking agent servers, and on proxy servers for FSA Reporting.

See "Permissions and privileges required by the Vault Service account on Windows file servers" on page 44.

This appendix describes the required permissions and privileges.

If you install the FSA Agent, the installer configures these permissions and privileges except for the following, which you must set manually:

- Permissions required for Windows Server Failover Clustering, if you configure the FSA resource.
  See "Permissions required by the Vault Service account to support the FSA resource on clustered file servers" on page 176.
- FSA target share and folder permissions:
  See "FSA target share and folder permissions required by the Vault Service account" on page 176.

Note: Ensure that your group policy permissions do not override the required local permissions for the Vault Service account.

If you change the Vault Service account you must ensure that the new account is granted these permissions and privileges. You can use the EVFSASetRightsAndPermissions utility to help you do this.

See "EVFSASetRightsAndPermissions" in the *Utilities* guide.

Group membership requirements for the Vault Service account

If the Vault Service account is not a member of the local **Administrators** group on a target Windows file server, it must be a member of the built-in local **Print Operators** group.

If you install the FSA Agent either from the Administration Console or manually, the installation process adds the Vault Service account to the **Print Operators** group.

DCOM permissions required by the Vault Service account

For target Windows file servers, the Vault Service account requires DCOM Security remote access permission, plus remote launch and remote activation permissions.

You can view and set the required permissions from **Administrative Tools** > **Component Services** > **Computers** > **My Computer**.

On the **COM Security** tab:

- Under **Access Permissions**: The Vault Service account must have **Remote Access** permission in addition to **Local Access** permission.
- Under **Launch and Activation Permissions**: The Vault Service account must have **Remote Launch** and **Remote Activation** permissions in addition to **Local Launch** and **Local Activation** permissions.

WMI control permissions required by the Vault Service account

The Vault Service account requires **Remote Enable** permissions on the Root\CIMV2 namespace on target Windows file servers.

You can view and set the properties of the namespace from **Administrative Tools** > **Computer Management** > **Services and Applications** > **WMI Control**.

On the **Security** tab, expand the **Root** node and select **CIMV2**. For the Vault Service account, **Remote Enable** permission must be allowed.

Local security user rights required by the Vault Service account

If the Vault Service account does not have local administrator rights on a target Windows file server, it requires a set of local user rights.

Table A-1 lists the required user rights.

Table A-1 User rights required by the Vault Service account

Privilege Constant/Value	User right string	Notes
SE_DEBUG_NAME / SeDebugPrivilege	Debug programs	The Enterprise Vault Placeholder service requires this right to read the process name, for excluding certain processes from recalling files.
SE_TAKE_OWNERSHIP_NAME/ SeTakeOwnershipPrivilege	Take ownership of files or other objects	The Vault Service account requires this privilege to modify file properties when performing file archiving or File Blocking operations, for example to change file attributes or to delete files, when it does not have direct access to a file or folder
SE_BACKUP_NAME/ SeBackupPrivilege	Backup files and directories	Required for the archiving of files that the Vault Service account does not have direct access to. The Enterprise Vault Placeholder service requires this right to read the XML and alternate datastream metadata of files on shares.
SE_RESTORE_NAME/ SeRestorePrivilege	Restore files and directories	Required for the restoring of files that the Vault Service account does not have direct access to.
Log on as a service /SeServiceLogonRight	Log on as a service	The Vault Service account requires this right for the FSA Agent services.

To view or set the user right strings, open the **Local Security Settings** Microsoft Management Console (MMC) snap-in and navigate to **Security Settings** > **Local Policies** > **User Rights Assignment**. Windows displays the user right strings in the **Policy** column.

Note: You must make sure that there are no Group policy overrides for these local user rights.

Permissions required by the Vault Service account for the FSA Agent

This section describes the permissions that the Vault Service account requires on a target Windows file server for the FSA Agent.

Note: These permissions are required only if the FSA Agent is installed.

FSA Agent service permissions required by the Vault Service account

The Vault Service account requires the access permission SERVICE_ALL_ACCESS on the service object security descriptor for each of the FSA Agent services:

- Enterprise Vault File Placeholder Service
- Enterprise Vault File Blocking Service
- Enterprise Vault File Collector Service

You can set a service's security descriptor by using a command similar to the following:

```
sc sdset ServiceName ServiceSecurityDescriptor
```

See your Microsoft documentation for details.

Enterprise Vault installation folder permissions required by the Vault Service account

The Vault Service account requires READ/WRITE access on a target file server's Enterprise Vault installation folder, (for example `C:\Program Files (x86)\Enterprise Vault`). This access is required to enable the FSA Agent services to read, write, and create files under the installation folder.

File server registry hive permissions required by the Vault Service account

The Vault Service account requires FULL control access on a target file server's Enterprise Vault registry hive, `HKLM\Software\KVS`. This access is required to enable the FSA Agent services to create, read, and update the information under the hive.

Permissions required by the Vault Service account to support the FSA resource on clustered file servers

The Vault Service account requires the following permissions if you add the FSA resource to a file server cluster:

- For VCS, the Vault Service account must be a member of the local Administrators group on each cluster node.
- For a Windows Server failover cluster, the Vault Service account requires specific cluster permissions if it is not a member of the local Administrators group on each cluster node.
  You must set the cluster permissions to grant the Vault Service account Full Control permissions for managing the cluster.
  The FSA Agent installer does not set these permissions. You must set the permissions manually.

FSA target share and folder permissions required by the Vault Service account

The Vault Service account requires the following permissions on a Windows file server that is a target for FSA:

- Full control on any share that is configured as a target volume.
- NTFS read permission on the folder that the share maps to.

Optionally the Vault Service account also requires browse permissions on the target folders, and on any folders in the paths to the target folders. If these optional permissions are not set, you cannot browse in the Administration Console for the target folder, and so you must specify the path by typing it in.

You must set these target share and folder permissions manually as required.

Index

I

M

N

P

R

S

U

V

W