Symantec Enterprise Vault™

Setting up File System Archiving (FSA)

9.0

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

Last updated: July 18, 2010.

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 respond to specific queries about product features and functionality. 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 Web site 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 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_apac@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 products:

- Microsoft Windows 2000, Windows Server 2003, or Windows Server 2008
- 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 Help	Includes all the following documentation so that you can search across all files. You can access this file by doing either of the following: ■ On the Windows **Start** menu, click **Start** > **Programs** > **Enterprise Vault** > **Documentation**. ■ In the Administration Console, click **Help** > **Help on Enterprise Vault**.
Introduction and Planning	Provides an overview of Enterprise Vault functionality.
Deployment Scanner	Describes how to check the prerequisite 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 SharePoint Server Archiving	Describes how to archive the documents that are held on 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, backup, and recovery procedures.

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

Document	Comments
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.
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://entsupport.symantec.com/docs/276547

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

Setting up File System Archiving (FSA)

This chapter includes the following topics:

About File System Archiving

You can set up Enterprise Vault File System Archiving to archive files from network shares (volumes). Users can then access the archived files using shortcuts in the original locations, Archive Explorer, or the browser search page.

When you configure archiving for a volume, you place an archive point to control which folders are archived and which archive is used to store files from a particular folder and its subfolders.

Internet and placeholder shortcuts

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 containing a hypertext link to the archived file.
- 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. If you want to use placeholders on a Windows file server, then you must install the FSA Agent on the file server.
  See "The FSA Agent" on page 17.

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

Note: Unwanted placeholder recalls can occur if you use the Windows Explorer preview pane that is provided with Windows Vista and Windows Server 2008. 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.

File Blocking

On Windows file servers and NetApp file servers you can configure the File Blocking feature.

The File Blocking feature enables you to do the following:

- Limit users' disk space by monitoring and enforcing disk usage policies in real time.
- Prevent unwanted files from being saved on monitored server volumes.

You configure File Blocking within a volume policy and then apply that policy to disk volumes. It is also possible for a File System Archiving task to process the volumes, but there is no requirement to do this.

See "File Blocking configuration" on page 69.

The FSA Agent

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)

For Windows file servers, you must install the FSA Agent on the file server if you want to use placeholder shortcuts, File Blocking, or FSA Reporting.

NetApp filers and EMC Celerra devices do not run the FSA Agent:

- To provide placeholder shortcuts, the Enterprise Vault server runs an equivalent process to the File Placeholder service.
- File Blocking on EMC Celerra devices is not supported. To provide File Blocking for a NetApp filer, you must configure a Windows server in the Administration Console as a file server. You must install the FSA Agent on the Windows server to provide a File Blocking agent server for the NetApp filer.

Note: An Enterprise Vault server cannot act as the File Blocking agent server for a NetApp filer. Do not install the FSA Agent on an Enterprise Vault server.

- To configure FSA Reporting for a NetApp or EMC Celerra device you must configure an FSA Reporting proxy server to perform the data collection. For more details, see the *Reporting* guide.

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

See "Installing the FSA Agent on a Windows file server" on page 22.

Note: You can make the FSA services highly available in a clustered file server environment.

See "About FSA clustering" on page 89.

Client access to archived items

Items that have been archived by FSA are available to clients as follows:

- If shortcuts are created in the item's original location, users can access an archived item simply by double-clicking the shortcut on the file server.
- If shortcuts are not created, users can access the archived items in the archives using Enterprise Vault archive search or Archive Explorer from a stand-alone browser session.
  When Archive Explorer is launched from within Outlook, it does not display FSA archives. To browse these archives, users need to start Archive Explorer in a separate browser session, using a URL in the form:

  `http://EV_IIS_server/EnterpriseVault/archiveexplorerui.asp`

Note: You cannot use the Enterprise Vault search applications to restore large files that File System Archiving has archived. This restriction applies only to items that a search has found.

Preparing to configure FSA

Before you perform the tasks described in this chapter, ensure that you have done the following:

- Checked that the prerequisites for your planned system are satisfied.
- Installed and configured your core Enterprise Vault services.
- Prepared the target Windows and NetApp file servers.

See the *Installing and Configuring* manual for instructions. Preparing EMC Celerra file servers is described in this chapter, as it requires information about your Enterprise Vault server configuration.

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://entsupport.symantec.com/docs/276547.

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 with 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.asp

   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.

Steps to configure FSA for a file server

The following steps summarize the tasks that you need to perform to configure File System Archiving.

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

See "File Blocking configuration" on page 69.

- Add a File System Archiving task.
  See "Adding a File System Archiving task" on page 20.
- Add the file server as a File System Archiving target in the Administration Console. For Windows file servers you must install the FSA Agent on the file server.
  See "Adding file servers as archiving targets" on page 21.
- Create your archiving policies.
  See "Creating FSA archiving policies" on page 32.
- Add an archiving target volume, and apply the required volume policy.
  See "Adding a volume" on page 42.
- Add archiving target folders and archive points as required.
  See "Adding folders and archive points" on page 44.
- Configure pass-through recall for placeholder shortcuts, if required.
  See "Configuring pass-through recall for placeholder shortcuts" on page 49.
- Schedule the File System Archiving task so that it archives the new file server at the required times.
  See "Scheduling" on page 55.

Adding a File System Archiving task

Add a File System Archiving task on the Enterprise Vault server using 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 will be displayed in the right-hand pane. Double-click the task object to display the properties of this task.

Adding file servers as archiving targets

You can now add the file servers to Enterprise Vault as archiving targets.

Adding a Windows file server

You can add a Windows file server as an archiving target to 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 need the FSA Agent 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 at a later date 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 "Installing the FSA Agent on a Windows file server" on page 22.

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

See "Adding a file server target with FSA Reporting" in the *Reporting* guide.

To add a Windows file server

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 Server** 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.

   You will need to provide the following information:

   - The fully-qualified DNS name of the file server you are adding. You can browse to select the server.

- Additionally, if you choose to install the FSA Agent, the wizard asks for the password to 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.

Installing the FSA Agent on a Windows file server

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.
- Gather data for FSA Reporting.

Note: Do not install the FSA Agent on NetApp file servers, on EMC Celerra devices, or on Enterprise Vault servers.

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.

You can install the FSA Agent using either the following methods:

- Run the Install FSA Agent wizard from the Administration Console. You require the user name and password of the Vault Service account. The Vault Service account must have administrator permissions on the file server.
- Install the FSA Agent manually, by using one of the Windows Installer kits that are located on the Enterprise Vault server. Enterprise Vault contains both a 32-bit version and a 64-bit version of the MSI kit. The 64-bit version supports AMD64 and Intel EM64T. There is currently no support for Intel Itanium.

Note: To install FSA Agent on Windows Server 2008 using the Install FSA Agent wizard, you must temporarily turn off the Windows Firewall on the target file server. You do not need to turn off the Windows Firewall if you install the FSA Agent manually.

For details of the prerequisite versions and service packs of the Windows operating system on the file server, see the Enterprise Vault *Compatibility Charts* at http://entsupport.symantec.com/docs/276547.

The other prerequisites for the FSA Agent on the file server are as follows:

- Windows Installer 3.1
- Internet Explorer 6.0 or later
- .NET 2.0 SP2 except for Windows Server 2008, which requires .NET 3.5 SP1.

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 target virtual file server" on page 96.

To install the FSA Agent using the Install FSA Agent wizard

1. On a Windows Server 2008 file server, turn off the Windows Firewall.
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 install the FSA Agent and, on the shortcut menu, click **Install FSA Agent**. The **Install FSA Agent** wizard starts.
6. Work through the wizard.
7. On a Windows Server 2008 file server, turn the Windows Firewall back on when the installation is finished.

To install the FSA Agent manually

1. Find the FSA Agent files on the Enterprise Vault server. The files are located in the `evpush\Agent` folder under the Enterprise Vault installation folder, typically `C:\Program Files\Enterprise Vault\evpush\Agent`.
2. Run the required executable files on the file server:
   - On a 32-bit Windows system run `vcredist_x86.exe`
   - On a 64-bit Windows system, run `vcredist_x86.exe` and then `vcredist_x64.exe`
3. Run the required MSI file on the file server:
   - On a 32-bit Windows system, run the following:
     `Enterprise Vault File System Archiving.msi`
   - On a 64-bit Windows system, run the following:

```
Enterprise Vault File System Archiving x64.msi
```

4 When the installation of the FSA Agent is complete, start the following services manually on the file server, if they are not already started:

- Enterprise Vault File Blocking Service
- Enterprise Vault File Collector Service
- Enterprise Vault File Placeholder Service

Adding a NetApp file server

Before you add a NetApp Filer, ensure that you have set the permissions correctly. See the "Additional prerequisites for File System Archiving (FSA)" section of the *Installing and Configuring* manual for instructions.

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

See "Adding a file server target with FSA Reporting" in the *Reporting* guide.

To add 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.

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.

Do not select the option to install the FSA Agent.

You will be prompted for the fully-qualified DNS name of the file server you are adding. You can browse to select the server.

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

Adding an EMC Celerra device

This section describes how to prepare the EMC Celerra file server for archiving, and how to add the Celerra device as an archiving target.

Preparing an EMC Celerra device

You must ensure that the Celerra 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, you must also enable the FileMover functionality on the Celerra and create an HTTP connection.

Note: 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 pass-through behavior for placeholder shortcuts" on page 29.

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

http://entsupport.symantec.com/docs/289676

To prepare an EMC Celerra device

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

   The Celerra 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 stream parameter, enter the following command syntax on the Celerra 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.

   To enable ADS support, use the following command syntax on the Celerra 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 account for Enterprise Vault to use for authentication on the Celerra device. The syntax is as follows:

```
/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 that you want Enterprise Vault to use for authentication. This user is a Data Mover user, not a domain user.

Make sure that you specify the full path for the **server_user** command, `/nas/sbin/server_user`. You require root privileges to execute this command.

4 Enable the file system for Celerra 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.

5 Configure the HTTP server on the Data Mover to accept Celerra FileMover API connections using this command syntax:

```
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 device.

The command also tests the connectivity between the Celerra device and the Enterprise Vault server over http.

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

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

6 Configure the HTTP connection to use for recall requests, using this command syntax:

```
fs_dhsm -connection fs_name -create -type http
-secondary ev_url -user user -password user_password -cgi n
```

where:

fs_name is the name of the Celerra file system.

ev_url is the URL of the Enterprise Vault Web Access application. The Celerra is case-sensitive, so this URL must use the correct case. See "Specifying the correct URL for the Web Access application" on page 27.

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.

Note that you cannot include a TCP port number in the URL that you specify with the **-secondary** parameter. For example, if you use a non-default port such as port 85 for the Web Access application, you cannot specify the port as follows:

```
-secondary http://evserver.demo.local:85/EnterpriseVault
```

A workaround is available if you have configured the Web Access application to use a TCP port other than default port (port 80).

See "Specifying a non-default TCP port for the Web Access application" on page 28.

7 Add the Vault Service account as a member of the Administrators group of the Celerra CIFS server:

- From Windows, click **Start** > **All Programs** > **Administrative Tools** > **Computer Management**. The Computer Management console appears.
- Select **Action** > **Connect to another computer**. Enter the name of the CIFS server.
- Add the Vault Service account to the Administrators group.

Specifying the correct URL for the Web Access application

One of the parameters to the `fs_dhsm` command is *ev_url*, the URL of the Enterprise Vault Web Access application. If the Celerra 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".

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

Specifying a non-default TCP port for the Web Access application

Note that you cannot include a TCP port number in the URL that you specify with the `-secondary` parameter of the `fs_dhsm -connection` command. If you attempt to include a TCP 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 will fail:

```
Error: The host name in the secondary url evserver.demo.local:85 is
either missing or formatted incorrectly.
```

If you have configured the Web Access application to use a TCP port other than default port (port 80), you can use the following workaround to use a non-default port with the Celerra.

To specify a non-default TCP port for the Web Access application

1. Create an IIS Web site that uses the default TCP port, port 80.
2. In the new Web site, create a virtual directory that is named **EnterpriseVault**. Set a redirection URL for this virtual directory to the original **EnterpriseVault** virtual directory on the non-default port.

3 Configure the Web Access application to use default TCP port 80 on the **General** tab of the Enterprise Vault Site properties.

4 Use the **-httpPort** parameter with the **fs_dhsm –connection** command to specify the non-default port, as follows:

```
fs_dhsm -connection fs_name -create -type http
-secondary ev_url -user user -password user_password -cgi n
-httpPort port_number
```

For example:

```
fs_dhsm -connection fsa_fs -create -type http
-secondary http://EVServer.demo.local/EnterpriseVault
-user vaultadmin@demo.local -password p4ssw0rd -cgi n
-httpPort 85
```

Configuring Celerra pass-through behavior for placeholder shortcuts

You can use EMC Celerra's read policy override with placeholder recalls, if required. The Celerra's `-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. The Celerra Network Server then recalls the file only if a write request is received.

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

Note: If you configure Celerra 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's pass-through behavior, include the `-read_policy_override` parameter in one of the following commands:

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

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 on read request before the data is returned.
- `passthrough`. Retrieve the data without recalling the data to the Celerra.
- `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 uses a value of `passthrough` by default.
- The Celerra uses a value of `passthrough` if the Celerra file system is read only.
- The Celerra 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.

Example configuration

The following example configures a Celerra to use placeholder shortcuts.

```
$ server_param server_2 -facility shadow -modify stream -value 1
$ /nas/bin/server_user server_2 -add -md5 -passwd
celerraaccessaccount@demo.local
$ fs_dhsm -modify fsa_fs -state enabled
$ server_http server_2 -append dhsm -users
archiveaccessaccount@demo.local -hosts 192.168.1.1
$ 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
```

where:

- FSA will use the account CelerraAccessAccount@demo.local to authenticate on the Celerra.
- The Celerra will use the account ArchiveAccessAccount to authenticate to Enterprise Vault.

- The Celerra file system name is fsa_fs.
- The server name is server_2.
- The IP address of the FSA task computer is 192.168.1.1.
- Pass-though is configured on the HTTP connection.
- The URL of the Enterprise Vault Web Access Application is http://EVServer.demo.local/EnterpriseVault.
- The password for the archive access account is p4ssw0rd.

Adding the Celerra device as an archiving target

Once you have prepared the Celerra device, you can use the Administration Console to add the Celerra device as an archiving target.

The New File Server wizard asks you the following:

- The fully-qualified DNS name of the file server you are adding. You can browse to select the server.
- Whether to use placeholder shortcuts. If you choose placeholder shortcuts you must provide the details of an account on the Celerra Data Mover that has the Celerra dhsm permission.

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

See "Adding a file server target with FSA Reporting" in the *Reporting* guide.

To add the Celerra 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 screen, click **Next**.
   - On the second screen, enter the DNS name of the Celerra device. Do not select the option to install the FSA Agent. Click **Next**.
   - On the third screen, choose whether to use placeholder shortcuts. If you choose to use placeholder shortcuts, enter the details of the account you configured on the Celerra that has permission to use the dhsm feature.

You can change the account details later, if required, by editing the properties of the Celerra.
Click **Next** to continue.

- On the summary screen, click **Next** to add the Celerra device.
- On the final screen, click **Close** to exit from the wizard.

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

Creating FSA archiving policies

You must create the FSA archiving policies that you require:

- Edit the settings of the Default FSA Volume policy, or create new volume policies, as required.
  See "Creating a volume policy" on page 32.
- To override a volume policy for individual folders, modify the settings in the Default FSA Folder Policy, or create new folder policies, as required.
  See "Creating a folder policy" on page 34.

Note: Retention Folder policies are special policies that allow you to add a predefined folder hierarchy to folders in a target volume. There is separate documentation for adding folder targets that use retention folder policies. See "Configuring retention folders" on page 62.

Creating a volume policy

A volume policy's settings are applied to a complete volume, unless overridden by a folder policy.

The volume policy determines the following:

- What File Blocking rules to apply to the volume.
  See "File Blocking configuration" on page 69.
- Whether to enable quotas for the volume, and what quotas to use.
- Which retention category to apply to the files that are archived with this policy.
- The archiving rules to apply for the volume. Each archiving rule specifies:
  - 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 on archiving policy rules" on page 34.

- The action to take on the files that match the criteria you specify.
- Whether and when to create shortcuts for the matching files. You can create shortcuts immediately or some time later, according to criteria that you specify.
  See "Shortcut creation options" on page 35.

- The type of shortcut to leave to an archived file, if the archiving rules specify that a shortcut is created. You can choose to leave a placeholder shortcut or an Internet link.

  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 "Deleting archived files on placeholder deletion" on page 37.

  If you decide to leave placeholder shortcuts, you must install the FSA Agent on any Windows file servers to which this policy is applied.

- Whether to archive the files that have explicit permissions set on them. When Enterprise Vault archives files, it gives the archived version the same permissions as the folder that contained the original file.
  See "Files with explicit permissions" on page 42.

To create a new 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. Work through the New Policy wizard.

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

1. In the Administration Console, right-click the policy that you want to copy and then, on the shortcut menu, click **Copy Policy**.
2. Enter a new name and description for the policy.
3. Click **OK** to save the copy.
4. Double-click the new copy to display its properties.
5. Edit the properties of the copy as required.

Creating a folder policy

A folder policy contains settings that are to be applied to specific folders. These settings override volume policy settings.

To make for easier management, you are recommended not to apply folder policies to folders that have a short life, such as temporary folders. It is better to create folder policies for folders that will have a long life, such as a user's root folder.

To create a new folder 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 **Folder** and then, on the shortcut menu, click **New** and then **Policy**.
5. Work through the **New Policy** wizard.

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

1. In the Administration Console, right-click the policy that you want to copy and then, on the shortcut menu, click **Copy Policy**.
2. Enter a new name and description for the policy.
3. Click **OK** to save the copy.
4. Double-click the new copy to display its properties.
5. Edit the properties of the copy as required.

Tips on archiving policy rules

The archiving policy rules control exactly which files are archived.

When you create policy rules, remember the following:

- A 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 "Web Pages" 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 "Web Pages".
File Groups are in the "File Groups" Administration Console container, under the "File" policies container.

- The **Remove safety copies** setting for the vault store may temporarily prevent Enterprise Vault from creating shortcuts.
See "Shortcut creation options" on page 35.
- 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.

Shortcut creation options

The Enterprise Vault archiving task creates shortcuts during normal archiving runs. The task creates the shortcuts according to rules that you define in the archiving policy. If you want to create shortcuts at any other time you must use **Run Now** to run the archiving task.

The shortcut creation options are as follows:

- **Shortcut creation**. You can select any of the following:
  - **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 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.
- **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-modified 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 archived. This option enables you to ensure that shortcuts are not created for frequently-modfied files.
- **Created time is**. Specifies that Enterprise Vault must create shortcuts when the specified time has elapsed since the file was created.

Note the following:

- If you specify more than one of the time conditions, Enterprise Vault does not create shortcuts until all the conditions are satisfied.
- 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 2-1 shows how the **Remove safety copies** settings can affect shortcut creation.

Table 2-1 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
After backup	Delete original file after backup	Create shortcut after backup	Create shortcut later, after backup

See "Tips on shortcut creation" on page 36.

See "NetApp placeholder shortcut file sizes" on page 37.

Tips on shortcut creation

- The 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 rule at time the shortcut is created. If you change the rule after a file is archived and before the shortcut is created, Enterprise Vault uses the new criteria.
- Be careful that you do not specify a setting 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 this tab, it is possible that Enterprise Vault never creates the shortcuts.
The conflict can occur because the archiving task processes the files that match the settings on **'Time and Size'** tab. If the archiving 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

NetApp placeholder shortcut file sizes

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 file server. 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.

Deleting 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.

See "How the 'Delete archived file when placeholder is deleted' feature works" on page 37.

See "Configuring the deletion of archived files on placeholder deletion" on page 39.

How the 'Delete archived file when placeholder is deleted' feature works

FSA's archiving policies provide the optional setting "Delete archived file when placeholder is deleted" if you choose to leave placeholder shortcuts.

For Windows and NetApp file servers, Enterprise Vault maintains a local 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.

When a placeholder is deleted on an Windows or NetApp file server, 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 DOD cache value 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.

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.

Enterprise Vault uses a different mechanism with EMC Celerra file server placeholders, as follows:

- To configure archived file deletion with Celerra 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 placeholders, Enterprise Vault does not use a DOD cache. When a Celerra 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 target root volume.
- You must enable FileMover logging on the Celerra device. Enterprise Vault uses the Celerra FileMover log's records of deleted placeholders to determine which archived files to delete.

- The deletion of the archived Celerra files does not occur immediately upon placeholder deletion. Deletion from the Celerra takes place daily according to the schedule that is specified in the properties of the File System Archiving task.

Configuring the deletion of archived files on placeholder deletion

To configure the deletion of archived files on placeholder deletion, follow the procedure that is appropriate for the type of file server.

Note that Enterprise Vault does not delete 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 "Prevent deletion of archived items in this category" set. The retention category setting takes precedence.

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

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

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 "How the 'Delete archived file when placeholder is deleted' feature works" on page 37.

To configure deletion of archived files on placeholder deletion for EMC Celerra file servers

1. Configure a target volume under the target Celerra file server 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 file system:

   - If you configure any additional target volumes that point to specific folders in the same Celerra 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 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 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
  \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 file when its placeholder is deleted".
  Alternatively you can turn off Celerra 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 Configure the daily deletion schedule for the archived files whose placeholders were deleted.

See "Scheduling the deletion of archived files for EMC Celerra" on page 56.

Files with explicit permissions

When you create or edit an archiving policy you can choose what to do with the files that have explicit permissions set on them:

- **Ignore them**. Select this option if you want Enterprise Vault not to archive the files that have explicit permissions.
- **Archive them**. Select this option if you want Enterprise Vault to archive the files that have explicit permissions.

Note the following when deciding whether to archive these files:

- When Enterprise Vault archives a file, it gives the archived file the same permissions as the folder that contained the original file. Enterprise Vault gives the shortcut the same permissions as the original file.
- Someone with access to the original folder can find and access the archived version of the file, even if the original file's permissions denied access. The same person cannot use a shortcut to access the file.

From Enterprise Vault 8.0 SP1 onwards, a new installation of Enterprise Vault provides the following defaults for this setting:

- The supplied setting in the Default FSA Volume Policy and the Default FSA Folder Policy is **Ignore them**.
- The New Policy wizard's default setting is always **Ignore them**.

Note that before Enterprise Vault 8.0 SP1 the defaults were as follows:

- The supplied setting in the Default FSA Volume Policy and the Default FSA Folder Policy was **Archive them**.
- The New Policy wizard's supplied default setting was **Ignore them**, but if you changed the setting then the default reflected the previous choice.

On upgrade, Enterprise Vault retains the current setting in the existing archiving policies.

Adding a volume

This section describes how to add a volume so that it can be processed by File System Archiving.

Adding a volume

Use the New Volume wizard to add a file server volume for Enterprise Vault to process.

The New Volume wizard asks you the following:

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

If FSA Reporting is configured, the wizard also lets you choose whether to enable FSA Reporting for this volume.

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

- Before you add the first volume for a Celerra device you must specify a cache location for Enterprise Vault to use for temporary files.
  See "Specifying a cache location for EMC Celerra" on page 43.
- If you use the archiving policy setting "Delete archived file when placeholder is deleted", certain restrictions and requirements apply.
  See "Deleting archived files on placeholder deletion" on page 37.

To add a volume

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 Server** container to show the file servers that have been added.
4. Right-click the file server from which you want to add a volume and then, on the shortcut menu, click **New** and then **Volume**.
5. Work through the wizard to finish adding the volume.

Specifying a cache location for EMC Celerra

In order to improve performance, an Enterprise Vault server that retrieves files from an EMC Celerra device requires a location to use for temporary files.

Before you add the first volume on a Celerra device you must specify a folder that is local to the Enterprise Vault server that can be used for caching temporary files.

To specify a cache location

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 and, on the shortcut menu, click **Properties**.

4 Click the **Cache** tab.

5 Under **Cache Location**, enter an existing path on the server that can be used to cache files retrieved from the Celerra.

Adding folders and archive points

You can use the New Folder wizard to configure how Enterprise Vault archives a folder and its subfolders under a target volume.

The New Folder wizard enables you to do the following:

- Add archive points, to control which folders are archived and which archive is used to store the files from a folder and its subfolders.
- Apply a specific archiving policy to a folder and its subfolders.

About archive points

To archive files from a target volume, you must add archive points to control which folders can be archived. An 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 creates an archive with 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, but you can override these defaults.

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.

The easiest way to manage archive points is to use the Administration Console. Additionally, there is a command-line tool, ArchivePoints. For information on how to use ArchivePoints to create, delete, list, show contents, and update archive points, see ArchivePoints in the *Utilities* manual.

Note: You cannot use the Administration Console to create an archive point at the root of a target volume. If you want to create an archive point at the volume root you must use the ArchivePoints command-line tool.

Where possible, Enterprise Vault uses Alternate Data Streams (ADS) to indicate archive points. These stream archive points are used on NTFS volumes, on NetApp

devices, and on EMC Celerra devices. If the file system does not support ADS, Enterprise Vault uses hidden XML files to mark archive points.

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 volume" on page 85.

Adding a folder and archive points

The New Folder wizard lets you set up file archiving from a folder within a target volume. The New Folder wizard lets you do the following:

- Specify the archiving policy to use for the folder.
- Add archive points for the folder, and also for its subfolders if required.
  You can choose to place archive points on all the subfolders of a folder if required, and auto-enable the creation of archive points on new subfolders when they are created .

To add a folder and archive points

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.
3. Expand the node for the appropriate file server.
4. Right-click the volume that contains the folder you want to add and then, 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.
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 62.

   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 folder, and whether to archive from its subfolders. You can suspend archiving if required. You can start or suspend archiving later from the folder properties.

8 Add archive points for the folder, and also for its subfolders if required.

You can choose to place archive points on all the subfolders of a folder. If you have many folders to enable this option may be easier than running the New Folder wizard many times.

You can create any of the following:

- An archive point for the selected folder.
- An archive point for each subfolder of the selected folder. A new archive will be created for each existing subfolder.
- Archive points for subfolders of the existing folder and for new subfolders when they are created. The existing folder is referred to as an **auto-enabling folder**. The archive points for subfolders are created when the archiving task runs in normal mode.
  This can be useful when you have a folder containing users' subfolders and want to create an archive point for each user's subfolder. When you add subfolders for new users, archive points are automatically created.
  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 selected folder.

Listing, editing, and deleting archive points

The easiest way to manage archive points is to use the Administration Console. Alternatively you can use the ArchivePoints command-line tool. For information on how to use ArchivePoints to create, delete, list, show contents, and update archive points, see ArchivePoints in the *Utilities* manual.

Note that you can also get a list of archive points by processing a server or volume in Report Mode. The report that is generated lists all the archive points.

To list, edit, or delete archive points

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 are shown as follows:

    Folder with archive point

    Auto-enabling folder

6. To edit an archive point, click the archive point to select it and then click **Edit**.
7. To delete an archive point, click the archive point to select it 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**.

Results of modifying folders

This section describes the effects of deleting, renaming, moving, or copying folders that have archive points or folder policies.

Table 2-2 describes the results of performing these actions on folders that have archive points.

Table 2-2 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 and then add an archive point, the new folder is archived to a new archive.
Rename	The name is updated in both the Administration Console 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 new folder's does not have an archive point. (File System Archiving removes the archive point on the next run.)
Copy	The new folder does not have an archive point. (File System Archiving removes the copied archive point on the next run.)

Table 2-3 describes the results of performing these actions on folders that have folder policies.

Table 2-3 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 are visible in Archive Explorer and can be searched for.
Rename	The name is updated in both the Administration Console and Archive Explorer.

Table 2-3 Folders with folder policies *(continued)*

When you do this to a folder with a folder policy	This is the result
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.

Configuring pass-through recall for placeholder shortcuts

For Windows and NetApp file servers you can configure Enterprise Vault to perform pass-through recall for placeholder shortcuts. Enterprise Vault then passes the data directly through to the calling application on receipt of a read request for a placeholder. 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.

Note: For EMC Celerra file servers, Enterprise Vault supports the Celerra pass-through facility.

See "Configuring Celerra pass-through behavior for placeholder shortcuts" on page 29.

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.

Note: For NetApp file servers the pass-through recall feature works only with read-only file systems. Pass-through recall is ignored for read-write file systems.

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

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 file servers, the disk cache is located on the Enterprise Vault server.

Note the following:

- NetApp file servers must be running Data ONTAP 7.3 or later for pass-through recall.
- There is a setting **Delete archived file when placeholder is deleted** on the **Shortcuts** tab of volume policy properties and folder policy properties. That setting is ignored on NTFS volumes if pass-through recall is enabled on the volume.

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 if you configure pass-through recall for a file server cluster.

See "Configuring pass-through recall for a file server cluster" on page 52.

To configure pass-through recall for a Windows file server

1. Ensure that the FSA Agent is installed on the file server. The FSA Agent must be the version that is provided with Enterprise Vault 8.0 SP1 or later.

   See "Installing the FSA Agent on a Windows file server" on page 22.

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. We recommend that you make the cache size as large as possible.
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 52.

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 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.

The registry values are located under the following registry key:

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

Table 2-4 describes the registry values.

Table 2-4 Registry values for pass-through recall on Windows file servers

Registry value	Content	Description
ExcludedExes	String	Enables you to specify a semi-colon-separated list of programs that are prohibited from receiving archived items by pass-through recall.
EnableRecallLimitForPassThrough	DWORD	Determines whether users are subject to the pass-through recall limit that is set by PassThruRecallLimitMaxRecalls and PassThruRecallLimitTimeInterval. The default is 0 (recall limits do not apply to users).
BypassPassThruRecallLimitsForAdmins	DWORD	Determines whether administrators are subject to the pass-through recall limit. Only applies if EnableRecallLimitForPassThrough is set to 1. The default is 0 (recall limits apply to administrators).
PassThruRecallLimitMaxRecalls	DWORD	For Windows file servers you can specify a maximum rate of pass-through recall on each computer that runs a Placeholder Service. The registry values PassThruRecallLimitMaxRecalls and PassThruRecallLimitTimeInterval set the maximum rate. PassThruRecallLimitMaxRecalls defines the maximum number of pass-through recalls that can occur within the period that is set by PassThruRecallLimitTimeInterval. The default is 20 recalls.
PassThruRecallLimitTimeInterval	DWORD	Specifies the time in which you can retrieve the maximum number of items for pass-through recall, as defined by PassThruRecallLimitMaxRecalls. The default is 10 seconds.

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 file server

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

To configure pass-through recall for a NetApp file server

1. Ensure that the file server is running Data ONTAP 7.3 or later, which is required to support pass-through recall.
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 NetApp 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 **General** tab of the file server properties.
5. Select **Configure pass-through recall**.
6. Click **OK** to save the changes to the file server's properties.
7. Ensure that a disk cache location is configured on the Enterprise Vault server whose File System Archiving task manages the archiving from the NetApp file server.

   See "To configure the cache location on the Enterprise Vault server" on page 54.

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 file server. 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 that can be used to cache the files that are retrieved from the NetApp filer.

Scheduling

This section comprises the following topics:

Scheduling File System Archiving

A File System Archiving task processes its target servers according to the schedule that you define for that task. You can define an individual schedule for each File System Archiving task, or you can use the site schedule.

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 File System Archiving

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. Define the schedule that you require and then click **OK**.

Scheduling expiry

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.

Scheduling the deletion of archived files for EMC Celerra

You can configure the deletion of archived files when their placeholders are deleted.

See "Deleting archived files on placeholder deletion" on page 37.

The deletion of the archived EMC Celerra files 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 for EMC Celerra

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 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**.

Scheduling permissions synchronization

File System Archiving automatically synchronizes archive permissions with folder permissions. The automatic synchronization run takes place once or twice each day.

It is possible to turn off automatic synchronization. If you chose to do this you would then need to synchronize manually.

To view or modify the 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**.

Using Run Now

This section comprises the following topics:

Processing a volume immediately

Normally, File System Archiving processes each volume as part of a scheduled run. Sometimes, though, you may want to process a particular volume outside this schedule. On such occasions, you can use "Run Now" to process the volume immediately. "Run Now" is often useful when you are piloting or demonstrating Enterprise Vault.

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 a volume immediately

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, typically `C:\Program Files\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 "File System Archiving task reports" on page 60.

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**.

Processing a file server immediately

Normally, File System Archiving processes file servers according to the schedule that you specify for the File System Archiving task. Sometimes, though, you may want to process file servers outside this schedule. On such occasions, you can use Run Now to start the tasks immediately. Run Now is often useful when you are piloting or demonstrating Enterprise Vault.

Note the following:

- If the 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 a volume immediately" on page 57.
- 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 task immediately

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, typically `C:\Program Files\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 "File System Archiving task reports" on page 60.
     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.

File System Archiving task reports

The File System Archiving task creates reports in the `Reports\FSA` subfolder of the Enterprise Vault installation folder.

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 folder 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\Enterprise
Vault\Reports\FSA\ArchiveTask1\ArchiveScheduled\InProgress
```

If task 'ArchiveTask1' completes its processing on 20-Feb-2009 at 12:29.07, the report files are moved to the following folder:

```
C:\Program Files\Enterprise
Vault\Reports\FSA\ArchiveTask1\ArchiveScheduled\Completed\2009-02-20
12-29-07
```

Table 2-5 lists the folder names that are used for the different run modes.

Table 2-5 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

In the report folder, the names of the report files are as follows:

TaskName`_`*RunMode*`_`*RunNumber*`.txt`

where:

- *TaskName* is the name of the 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 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
```

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 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**.

Configuring and managing 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 may want to create a hierarchy of retention folders in every user's home folder.

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.

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 FSA archiving task in Normal mode. Hence the folders are retained.

If you do not want Enterprise Vault to recreate deleted or moved folders you can set a registry value.

See "Controlling whether Enterprise Vault recreates deleted or moved retention folders" on page 68.

Configuring retention folders

You configure retention folders using the Administration Console. The required steps are as follows:

- Create a suitable folder policy to use as the default folder policy for the retention folders.
- 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 folder.
- Add the FSA target on which you want the retention folders created, assign the Retention Folder policy, and specify where archive points are to be created.

You can specify that the retention folder hierarchy is added to the root of the FSA target, or to each subfolder.

The folders 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 "Creating and managing retention folders" on page 68.

You can also assign policies to folders using a command line interface.

See "Assigning a Retention Folder policy using the Command Line Interface (CLI)" on page 65.

Creating a Retention Folder policy

The Retention Folder policy defines the retention folder hierarchy to be created on the FSA target, and the folder policy to use on 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 Retention Folder Policy wizard starts.
3. In the wizard, create the required folder hierarchy. You can import a folder hierarchy using the **Import** button, if you want. You can create a hierarchy or customize an imported hierarchy using the **Add Folder**, **Rename Folder**, and **Delete Folder** buttons.
4. Assign a default folder policy to use for the retention folders in the hierarchy.
5. If required, use the **Policy** button to assign a different policy to specific folders.

Adding the FSA target and assigning a Retention Folder policy and archive points

You can now add the FSA target on which to create the retention folders, assign the Retention Folder policy, and specify where to create archive points.

To create an FSA target for a Retention Folder policy

1. In the Administration Console, expand the site and click **Targets > File server**.
2. 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.
3. Specify the location of the target folder.
4. Select the Retention Folder policy to apply.

5 Select where the Retention Folder policy is to be applied, as follows:

- To the top-level target folder.
- To sub-folders of the target folder. If you choose this option you can select whether to apply the policy to any new folders that get added to the target folder.

6 Select whether to create archive points and, if so, where. You can select from the following options:

- Create no 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.
- Create an archive point on the target folder. The target folder and its subfolders use the same archive.
- 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 subfolder of the target folder.

If you choose to create any archive points, you can define the properties of the resultant archive by clicking **Properties**.

7 Click **Finish** to complete the wizard.

After you have assigned a Retention Folder policy to an FSA target, the folder hierarchy is not created on the file server immediately. It is created when the FSA archiving task next runs.

To change the Retention Folder policy for an existing target folder

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 retention folder policy you want to change, and select **Properties**.

4 On the File Server Properties dialog, click **Change**.

5 On the Choose Policy dialog, select the required Retention Folder policy.

You cannot specify a standard folder policy on an FSA target folder for which you have previously specified a Retention Folder policy.

Assigning a Retention Folder policy using the Command Line Interface (CLI)

You can also assign Retention Folder policies to FSA targets 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 sub-folders.
  - Archive point options.

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*
```

Example command lines

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
```

Example XML settings file

An example XML settings file, `RtnFolderSettings.xml`, is installed in the Enterprise Vault folder.

The following example shows the format of the XML 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 2-6.

Table 2-6 <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 sub-folders under top-level folders on the FSA target, but not to the top-level folders on the FSA target.

Table 2-6 <Apply> element tags for the XML settings file *(continued)*

Tag	Value
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 re 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 2-7.

Table 2-7 <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 sub-folders under top-level folders in the Retention Folder hierarchy. This option is valid only if the tag ApplyToSubFolders is 1.
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.

Creating and managing retention folders

After you have completed the configuration tasks, Enterprise Vault creates the folder hierarchy on the file server when the FSA archiving task runs in Normal mode. To see what folders will be created by a Retention Folder policy, you can run the task in Report mode.

The following Retention Folder information is added to the FSA report in the `Enterprise Vault\Reports` folder:

- 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.

After a Normal mode archiving task run, the retention folder hierarchy that is defined in a Retention Folder policy should exist under the target. If a user deletes one or more retention folders, they will be recreated the next time the archiving task runs.

Controlling whether Enterprise Vault 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.

Disabling 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.

File Blocking configuration

File Blocking enables you to do the following:

- Monitor and enforce disk usage policies in real time.
- Prevent unwanted files from being saved on monitored server volumes.

File Blocking is provided as a component of the FSA Agent. When you add a new file server the wizard gives you the option to include File Blocking. If you have an existing file server, you can add the FSA Agent by right-clicking the file server and selecting "Install FSA Agent".

See "Adding file servers as archiving targets" on page 21.

Note: To use File Blocking in a clustered file server environment, you must configure an FSA resource in the cluster group that holds the virtual server resource. See "About FSA clustering" on page 89.

You configure File Blocking within a volume policy and then apply that policy to disk volumes. It is possible for the volumes also to be processed by a File System Archiving task, but there is no requirement to do this.

You configure File Blocking for a volume by applying a volume policy in which you have defined File Blocking rules. The rules control the file types that are allowed on the volume, which folders to monitor, and the actions to take when a policy violation occurs.

For example, the action could be to allow the file to be created but for a warning message to be sent to the user and the event to be logged.

File Blocking quarantines those files that are blocked because of content-checking. Files that are blocked because of their file types are not moved to quarantine.

In summary, you must do the following to configure File Blocking:

- On Windows file servers, install the FSA Agent.
  See "Adding file servers as archiving targets" on page 21.
- If you are adding File Blocking for a NetApp filer, you must already have installed File Blocking on a Windows file server target that is able to run the File Blocking service on behalf of the NetApp filer.

  Note: Do not install the FSA Agent on an Enterprise Vault server. An Enterprise Vault server cannot act as the File Blocking agent server for a NetApp filer.

  It is possible for a Windows file server to perform File Blocking for more than one NetApp device, but for best performance you are recommended to have one Windows file server per NetApp device.
  See "Adding file servers as archiving targets" on page 21.
- Define local quarantine locations. Each file server requires a quarantine location that is used when Enterprise Vault moves blocked files to quarantine. In the case of NetApp devices, the quarantine location must be on the Windows file server that is running the File Blocking service for the NetApp device.
  See "Creating a local quarantine location" on page 70.
- (Optional) Configure a central quarantine location. When this is defined, it is used in preference to the local quarantine locations on each file server. If the central location is not available, the local quarantine locations are used.
  See "Creating a central quarantine location" on page 71.
- Specify how Enterprise Vault is to send mail when a File Blocking rule requires a mail notification.
  See "Specifying the mail delivery mechanism" on page 72.
- Create a suitable volume policy and apply it as required.
- Optionally, specify for each file server, a list of users whose files are exempt from File Blocking.
  See "Ensuring specific users are never blocked" on page 79.

Creating a local quarantine location

File Blocking quarantines those files that are blocked because of content-checking. You must create a local quarantine location on each file server. If you have also defined a central quarantine location, that central location is used when a File Blocking rule requires that a file is moved to quarantine. However, if the central location is not defined, or is temporarily not available, the local quarantine location is used.

If neither a central nor a local quarantine location is available, Enterprise Vault uses the `Quarantine` subfolder of the Enterprise Vault installation folder locally where the File Blocking agent resides.

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 configure 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.

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**.

Creating a central quarantine location

File Blocking quarantines those files that are blocked because of content-checking. You can, optionally, define a central quarantine location to be used by all file servers to store quarantined files.

If the central quarantine location is not defined or is not available, each file server uses its local quarantine location. Note that, if a central quarantine location later becomes available, files that are in local quarantine locations are not automatically moved to the central quarantine location.

If neither a central nor a local quarantine location is available, Enterprise Vault uses the `Quarantine` subfolder of the Enterprise Vault installation folder locally where the File Blocking agent resides.

To create a central quarantine location

1. Decide which server will host the quarantine location and on a suitable quarantine 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.

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 quarantine. Click the browse button if you want to select the location from a list.
6. Click **OK**.

Specifying the mail delivery mechanism

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 delivery mechanism:

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**.

Adding File Blocking to a policy

To add File Blocking when creating 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 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 to an existing 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**.

File Blocking rules

This section gives an overview of the various settings that you can configure in a File Blocking rule, which is part of a File Blocking policy. You can have many rules within a single policy. You can define File Blocking rules when adding a new volume policy or by editing the properties of an existing policy.

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 2-8 lists the options on the General tab of File Blocking rule properties.

Table 2-8 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 2-9 lists the options on the General tab of File Blocking rule properties.

Table 2-9 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.
Allowed files	A list of file types to allow.	None.

File Blocking rule: File Blocking Options tab

Table 2-10 lists the options on the File Blocking Options tab of File Blocking rule properties.

Table 2-10 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.	Compressed files are not scanned.

File Blocking rule: Notifications tab

Table 2-11 lists the options on the Notifications tab of File Blocking rule properties.

Table 2-11 File Blocking rule: Notifications tab

Setting	Description	Default Value
Notify using Messenger Service	Enables automatic notifications using the Windows Messenger Service.	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 "Notification tabs" on page 77.	

Notification tabs

Click **Configure notifications** on the Notifications tab 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 2-12 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 "Notification variables" on page 78. ■ 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.
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.
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:** Custom commands require the Windows "Task Scheduler" service to be running.

Notification variables

You can insert variable information into a 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. To insert the variables, click **Advanced** on the Message tab.

Table 2-13 describes the variables that you can use.

Table 2-13 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.
[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.
[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 2-14 lists the options on the Folder filters tab of File Blocking rule properties.

Table 2-14 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.

Ensuring specific users are never blocked

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 a user from File Blocking:

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 to close **Add Windows Users and Groups**.
8. Click **OK** to close **File Server Properties**.

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.

The FSA 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 hundred 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.

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

Managing the file servers

This section contains information on backing up and virus-checking the file servers that File System Archiving processes. It also describes how you can prohibit specific user accounts or programs from recalling archived items back to the file server.

Backing up a file server

You can use your normal backup software to back up the file server disks that File System Archiving processes.

Enterprise Vault placeholder shortcuts appear to the operating system as markers for offline files. Some backup programs can be configured to ignore offline files, but others cannot.

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, 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 find that your backup software causes the Enterprise Vault Placeholder service to recall files, you can do one of the following:

- For Windows file servers or NetApp file servers, use the supplied `EvFsaBackupMode.exe` program to exclude the appropriate Active Directory account from triggering placeholder recalls.
  See "Using EvFsaBackupMode to prevent file recalls " on page 82.
- For Windows file servers, include the backup program in the list of programs that are prohibited from recalling archived items.
  See "Prohibiting a program from recalling files" on page 83.
- For EMC Celerra devices, use the Celerra's backup options to exclude the appropriate Active Directory account from triggering placeholder recalls.
  See "Preventing file recalls on EMC Celerra" on page 84.

Avoiding file recalls on restore due to File Blocking checks

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.

To prevent 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.

Virus-checking a file server

Enterprise Vault placeholder shortcuts appear to the operating system as markers for offline files. Some antivirus programs can be configured to ignore offline files, but others cannot. If you cannot configure your antivirus program to ignore offline files, every placeholder that the program checks results in an offline file being recalled.

If you can configure your antivirus program to ignore offline files, do so before running virus scans on disks with Enterprise Vault placeholder shortcuts.

If you cannot configure your antivirus program to ignore offline files, you can do one of the following:

- For Windows file servers or NetApp file servers, use the supplied `EvFsaBackupMode.exe` program to exclude the appropriate Active Directory account from triggering placeholder recalls.
  See "Using EvFsaBackupMode to prevent file recalls " on page 82.
- For Windows file servers, include the antivirus program in the list of programs that are prohibited from recalling archived items.
  See "Prohibiting a program from recalling files" on page 83.
- For EMC Celerra devices, use the Celerra's backup options to exclude the appropriate Active Directory account from triggering placeholder recalls.
  See "Preventing file recalls on EMC Celerra" on page 84.

See the Enterprise Vault *Compatibility Charts* at http://entsupport.symantec.com/docs/276547 for a list of antivirus programs that Symantec has tested. Other antivirus programs that have not been tested, but which can be configured to ignore offline files, will probably work with File System Archiving.

Using EvFsaBackupMode to prevent file recalls

For Windows file servers and NetApp file servers 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 program folder (normally `C:\Program Files\Enterprise Vault`). You can run `EvFsaBackupMode.exe` from the Enterprise Vault program folder, or copy it to another folder, or copy it to

another computer, which does not need to be an Enterprise Vault server, as required.

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

For Windows file servers it is possible to specify a list of programs that are prohibited from recalling archived items. 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 on each computer that is running an Enterprise Vault Placeholder service. This is a string value, ExcludedExes, under the following registry key:

```
HKEY_LOCAL_MACHINE
 \Software
  \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.

Preventing file recalls on EMC Celerra

For an EMC Celerra device, you can use the Celerra's backup options to prohibit Active Directory groups or Active Directory accounts such as a service account from triggering placeholder recalls from the Celerra 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 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.

For more details, consult your EMC Celerra documentation.

Deleting target folders and volumes

You can delete target folders and volumes if necessary.

Deleting a folder

You can delete a target folder if necessary. If you merely intend to suspend archiving of this folder for a while, edit the folder's properties in the Administration Console and select the option to not archive this folder.

You cannot delete a folder that is currently being processed.

To delete a folder

1. Right-click the folder that you want to delete and then, on the shortcut menu, click **Delete**.
2. Click **Yes** to confirm that you want to delete the folder.

Deleting a volume

You can delete a target volume if necessary. When you delete a volume, you remove the volume and all its folders from the list of volumes that are processed. If you merely intend to suspend archiving of this volume for a while, edit the volume's properties and select the option to not archive this volume.

You cannot delete a volume that is currently being processed.

Note that if you delete a volume from a target file server 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.

To delete a volume

1. In the Administration Console, right-click the volume that you want to delete and then, on the shortcut menu, click **Delete**.

   If there are folders on this volume that have been set up for archiving, there is a warning that deleting the volume deletes all its folders.

2. Click **Yes**.

Deleting a target file server

You can delete a target file server if necessary. When you delete the file server, you remove the server and all its volumes and folders from the list of servers that are processed.

If you merely intend to suspend archiving of this server for a while, you could do either of the following:

- Edit the server's properties, and clear the option to archive this file server.
- Stop the tasks that process this file server. If the tasks process other file servers this would also stop archiving from those servers.

You cannot delete a file server that is currently being processed.

Note that deleting a file server does not delete files or archived files; it merely removes the file server from the Administration Console.

To delete a target file server

1. In the Administration Console, expand the Enterprise Vault site until the **Enterprise Vault Servers** container is visible.
2. For each server with a task that processes the file server you want to delete, do the following in the order listed:
   - Expand the server.
   - Click **Tasks**.
   - Right-click the task that processes the file server you want to delete and, on the shortcut menu, click **Stop**.
3. Expand the **Targets** container.
4. Expand the **File Servers** container.
5. Expand the file server you want to delete.
6. Under the file server your want to delete, do the following for each volume:
   - Right-click the volume and, on the shortcut menu, click **Delete**.

There is a warning that deleting the volume deletes all the folders beneath.

- Click **Yes** to delete the volume.

7 Right-click the file server that you want to delete and then, on the shortcut menu, click **Delete**.

The Administration Console displays a warning that deleting the file server deletes all its archiving volumes and folders.

8 Click **Yes**.

FSA Agent uninstallation

If the FSA Agent is installed on a computer on which Enterprise Vault is also installed, you must uninstall Enterprise Vault before uninstalling the FSA Agent. In this case you may prefer to disable the FSA Agent instead of uninstalling it.

What next?

File System Archiving configuration is complete. You can use the Administration Console to add file servers to the list of servers that are processed by File System Archiving, create new volume policies, add new volumes on the new file server, and create archive points as needed to control which folders are archived.

Chapter 3

Using FSA with clustered file servers

This chapter includes the following topics:

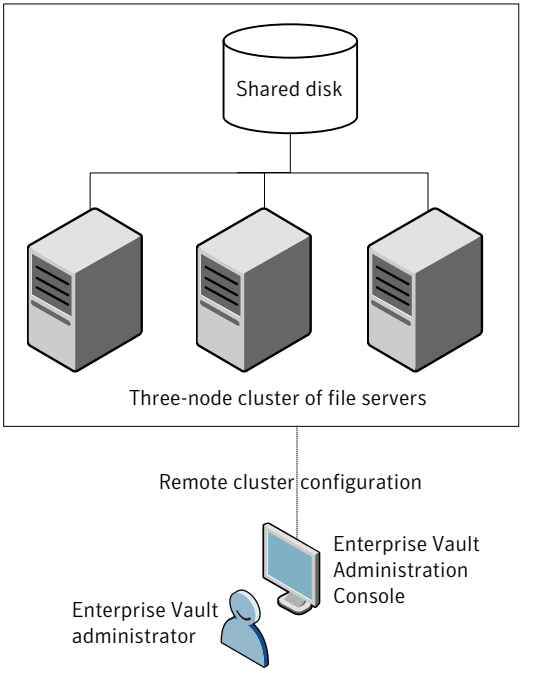
About FSA clustering

In an environment where Windows file servers are grouped in a cluster, you can make the FSA services that are running on them highly available. Then, if the cluster software detects the failure of the FSA services on one node, it can quickly restart the services on another node in the cluster—a process that is commonly known as "failover".

For example, Figure 3-1 shows an environment in which three file servers are clustered together.

All the servers have a shared disk configured; you can make the FSA services highly available only when there is a shared disk resource. If the FSA services on one node in the cluster fail, they fail over automatically to another node in the cluster. This failover results in only a momentary pause in service.

Figure 3-1 Sample FSA cluster configuration



Supported cluster software and cluster types

This FSA clustering feature works with the following cluster software:

- Microsoft server clusters (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://entsupport.symantec.com/docs/276547

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.

Note: You can configure a single-node cluster, but only if you first set a registry value on the computer that runs the Administration Console.

See "Preparation for setting up FSA services in a cluster" on page 91.

Overview of the configuration steps

To configure FSA on a clustered file server, perform the following steps in the order shown:

- Prepare the cluster for configuring the FSA services.
  See "Preparation for setting up FSA services in a cluster" on page 91.
- 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 "Authenticating the Administration Console with VCS" on page 93.
- Add the virtual file server as an archiving target and install the FSA Agent services on each node.
  See "Adding the target virtual file server" on page 96.
- Add an FSA resource to the cluster resource groups or service groups. If required, make the resource highly available.
  See "Configuring or reconfiguring the FSA resource" on page 98.

If you have problems, refer to the troubleshooting information.

See "Troubleshooting" on page 99.

Preparation for setting up FSA services in a cluster

Before you set up the FSA clustering feature, do the following:

- We recommend that you place the Enterprise Vault Administration Console and the target file servers in the same domain. If you place the Vault Administration Console and the target file servers in separate domains, you must set up a domain trust relationship.
- 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. Create SingleNodeFSA under the following registry key, and give it a DWORD value of 1:

  ```
  HKEY_LOCAL_MACHINE
   \SOFTWARE
    \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 services resource also has a shared disk resource (sometimes referred to as a physical disk resource or Mount/MountV resource). Only Veritas or Microsoft Cluster Server groups for which you have configured a shared disk resource are available for selection when you run the FSA Cluster Configuration wizard.
- For VCS configurations, make sure that the Public network connection is set as the top connection in the Connections list. Do 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.

Authenticating the Administration Console with VCS

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 93.
- See "Authenticating the Administration Console when SPAS is not used" on page 94.

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. The path is typically as follows:

   ```
   C:\Program Files\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 target virtual file server

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

To add the target virtual file server

1. If the cluster nodes run Windows Server 2008, note the following:
   - If the nodes are in a Microsoft server cluster you must run the Enterprise Vault Administration Console on a Windows Server 2008 computer.
   - If you select the option to install the FSA Agent in step 5, you must first turn off the Windows Firewall on the Windows Server 2008 nodes. If you prefer not to do this, install the FSA Agent manually on all the nodes in the cluster. You can perform the installation before or after you add the target file server.
     See "Installing the FSA Agent manually" on page 97.
2. In the left pane of the Enterprise Vault 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. Enter the name of the virtual file server. Unless you plan to install the FSA Agent manually, select the option to install the FSA Agent on the new file server. The wizard then installs the FSA Agent services on each node.
6. 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 98.

   When the FSA Cluster Configuration wizard finishes, it returns you to the New File Server wizard.
7. 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 80.
- 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.

8 You can now 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 "Configuring pass-through recall for a file server cluster" on page 52.

Installing the FSA Agent manually

The FSA Agent must be installed on each cluster node. You can install the FSA Agent manually if required, instead of doing so from the **New File Server** wizard.

You install the FSA Agent manually by using one of the Windows Installer kits that are located on the Enterprise Vault server

To install the FSA Agent manually

1 Find the FSA Agent files on the Enterprise Vault server. The files are located in the `evpush\Agent` folder under the Enterprise Vault installation folder, typically `C:\Program Files\Enterprise Vault\evpush\Agent`.

2 Run the required executable files on the file server:

- On a 32-bit Windows system run `vcredist_x86.exe`

- On a 64-bit Windows system, run `vcredist_x86.exe` and then `vcredist_x64.exe`

3 Run the required MSI file on the file server:

- On a 32-bit Windows system, run the following:
  `Enterprise Vault File System Archiving.msi`
- On a 64-bit Windows system, run the following:
  `Enterprise Vault File System Archiving x64.msi`

4 When the installation of the FSA Agent is complete, start the following services manually on the file server, if they are not already started:

- Enterprise Vault File Blocking Service
- Enterprise Vault File Collector Service
- Enterprise Vault File Placeholder Service

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: To configure the resources on a target file server that uses both Windows Server 2008 and Microsoft server clustering, you must run the Enterprise Vault Administration Console on a Windows Server 2008 computer.

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 When the wizard displays a summary of the changes that it has made to the cluster group, click **Finish**.

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: To configure the resources on a target file server that uses both Windows Server 2008 and Microsoft server clustering, you must run the Enterprise Vault Administration Console on a Windows Server 2008 computer.

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

This section gives advice on action you can take if you encounter problems when configuring FSA clustering.

Vault Service account cannot access VCS cluster

If the following message is displayed when you start the FSA Cluster Configuration wizard in the Enterprise Vault Administration Console, it may be because the Symantec Product Authentication Service is not available in the VCS cluster and the Vault Service account cannot authenticate and login to the VCS cluster.

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

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

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 94.

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.

General troubleshooting guidance

If you experience problems when you configure FSA clustering, try the following:

- Verify that you have installed and configured the FSA services on each node to which the cluster group can fail over.
- Ensure that the ClusSvc service (for Microsoft server clusters) or Had service (for Veritas Cluster Server) is configured and running on the file server.
- 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 (typically `C:\Program Files\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 called `FSA-MSCSType.log` or `FSA-VCSType.log`, depending on whether you are

using Microsoft server clusters or Veritas Cluster Server, and they are stored in the FSA Agent installation folder.
The following registry value determines the level of logging:

```
HKEY_LOCAL_MACHINE\Software\KVS\Enterprise Vault\FSA\LogLevel
```

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.

- Run DTrace on the FSA Cluster Configuration wizard.
  If the DTrace **view** command does not include FSAClusterWizard in the list of processes that are available to monitor, register the wizard with DTrace as follows:
  - Enter the following command from DTrace:
    ```
    set FSAClusterWizard.exe
    ```
  - Then register the name when DTrace prompts you.

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

Index

R

S

V

W