

Symantec NetBackup™ for Enterprise Vault™ Agent Administrator's Guide

for Windows

Release 7.5



Symantec NetBackup™ for Enterprise Vault™ Agent Administrator's Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version: 7.5

Legal Notice

Copyright © 2012 Symantec Corporation. All rights reserved.

Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

<http://www.symantec.com>

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

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, DVDs, or manuals

Support agreement resources

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

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

Contents

Technical Support	4
Chapter 1	
Introduction to NetBackup Enterprise Vault	11
About Enterprise Vault	11
What's new in Enterprise Vault Agent 7.5	12
About the NetBackup Enterprise Vault Agent	12
About the Enterprise Vault Agent and the backup components	13
Enterprise Vault agent features	16
Enterprise Vault agent requirements	18
Chapter 2	
About NetBackup Enterprise Vault agent installation requirements	21
Installation requirements for NetBackup Enterprise Vault agent	
2	1
Verifying Enterprise Vault agent operating system compatibility	22
NetBackup server and client software requirements	22
Enterprise Vault support for Enterprise Vault Agent	23
About Enterprise Vault agent installation requirements in a cluster	23
Configuring Enterprise Vault Agent to protect Enterprise Vault databases	24
Adding the Enterprise Vault agent license key	26
Configuration requirements for upgrading the Enterprise Vault agent	27
Configuration changes required after Enterprise Vault upgrade	28
Configuring the policy directives after upgrading NetBackup and Enterprise Vault	29
Upgrading to Enterprise Vault 9.0	31
Upgrading to Enterprise Vault 10.0	31

Chapter 3	Configuration	33
	About the Windows and Java user interfaces	33
	Specifying a logon account for the Enterprise Vault server	34
	About VSS-based snapshot configuration	35
	Configuring the local media server for Enterprise Vault backup	36
	Configuration requirements for an Enterprise Vault backup policy	37
	Adding a new Enterprise Vault policy	38
	Enterprise Vault backup policy attributes	40
	Adding schedules to an Enterprise Vault policy	41
	About the types of Enterprise Vault backups	41
	Creating a backup selections list	43
	Adding a client to a policy	46
Chapter 4	About features provided by Enterprise Vault for a backup provider	49
	About Enterprise Vault quiescence before a backup	49
	About quiescing and unquiescing Enterprise Vault services	50
	About granular quiescence	51
	About managing safety copies and backups	52
	About the partition secure notification file	53
	About the archive bit	53
Chapter 5	Performing backups of Enterprise Vault	55
	About Enterprise Vault directives and what data they back up	55
	Manually backing up Enterprise Vault resources	62
	Canceling an Enterprise Vault backup job from the Activity Monitor	63
Chapter 6	Performing restores of Enterprise Vault	65
	Important notes about Enterprise Vault data restore	65
	Stopping the administrative services on Enterprise Vault servers	67
	About the Backup, Archive, and Restore interface	67
	Viewing backup data using the Microsoft SQL Server Management Studio	68
	Restoring Enterprise Vault data	69
	About the Enterprise Vault restore options on the General tab	70
	About the Enterprise Vault Database Settings tab	71
	Specifying the server, clients, and policy type for restores	74

About restoring Enterprise Vault file system data	76
Restoring an Enterprise Vault file system component	77
About restoring Enterprise Vault SQL databases	79
About backup image restore sets	80
Restoring Enterprise Vault SQL database components	82
 Chapter 7	
Disaster recovery	85
Disaster recovery requirements for Enterprise Vault server	85
About disaster recovery of an Enterprise Vault site	86
Recovering a directory database	87
Recovering an auditing database	87
Recovering an FSA Reporting database	88
Recovering a Monitoring database	89
Recovering index locations	89
Recovering a Enterprise Vault vault store group	90
Recovering a fingerprint database	91
Recovering a vault store database	92
Recovering vault store partition	93
Recovering Enterprise Vault partitions	94
Recovering an Enterprise Vault server	94
Recovering an Enterprise Vault server on a different system	96
 Chapter 8	
Enterprise Vault Agent support for EV 7.5, 8.0 and later	99
Policy configuration for Enterprise Vault 8.0 and later versions	100
Open partition, vault store database, and fingerprint database consistencies	100
Closed and ready partition consistencies	100
Index location consistencies	101
Directory database consistencies	101
Notes about Enterprise Vault 10.0 backups	101
Exclude file list for index locations	102
Exclude file list for vault partitions	102
Excluding files from the exclude list	102
Directives for Enterprise Vault 7.5 policy creation	103
About planning backup schedules	104
About hosts for Enterprise Vault policies	105
About Enterprise Vault tools	106
About Enterprise Vault agent backups	106
Privileges for Enterprise Vault backup	107
About Enterprise Vault agent restores	108
Changing the socket buffer size for large restores	108

	Useful tips about Enterprise Vault agent	109
	Enterprise Vault agent functionality and support for EV 7.5 and later	109
	Differential incremental backup taken after a restore fails for EV 7.5 and later versions	110
Chapter 9	Troubleshooting	111
	About troubleshooting	111
	About debug logging	111
	How to enable debug logging	112
	Setting the debug level	113
	About status reports	114
	About operational reports	114
	About progress reports	114
	About NetBackup status-related troubleshooting information	115
	NetBackup status code 2	115
	NetBackup status code 13	116
	NetBackup status code 39	116
	NetBackup status code 59	117
	NetBackup status code 69	117
	NetBackup status code 156	118
	NetBackup status code 1800	120
Appendix A	NetBackup Enterprise Vault Migrator	123
	About the Enterprise Vault Migrator	123
	About configuring a backup policy for migration	124
	About configuring Enterprise Vault for collection and migration	129
	About NetBackup Enterprise Vault migrator registration	130
	Register NetBackup Enterprise Vault migrator	131
	Testing the Enterprise Vault migrator configuration	131
	Setting the recommended DCOM settings	134
	Restoring Enterprise Vault migrated data from NetBackup	136
	Restoring migrated data using the command line interface	137
	Restoring migrated data using a Backup, Archive, and Restore user interface	137
	Troubleshooting the Enterprise Vault migrator	138
	Enterprise Vault migrator version information	138
	About troubleshooting issues with the migrator	139
	About Log Collection	141
	Index	147

Introduction to NetBackup Enterprise Vault

This chapter includes the following topics:

- [About Enterprise Vault](#)
- [What's new in Enterprise Vault Agent 7.5](#)
- [About the NetBackup Enterprise Vault Agent](#)
- [About the Enterprise Vault Agent and the backup components](#)
- [Enterprise Vault agent features](#)
- [Enterprise Vault agent requirements](#)

About Enterprise Vault

Enterprise Vault is a Windows application that enables an organization to store messaging and file system data automatically in centrally-held archives. Using the Enterprise Vault application, clients and users can retrieve selected items easily and quickly when required.

Enterprise Vault can archive any of the following types of data:

- Items in Microsoft Exchange user mailboxes
- Items in Microsoft Exchange journal mailboxes
- Microsoft Exchange Public Folder contents
- Items in Domino mail files
- Items in Domino journal databases
- Files held on network file servers

- Documents held on Microsoft SharePoint servers
- Instant Messages and Bloomberg messages
- SMTP messages from other messaging servers

For more information about Enterprise Vault, refer to the following URL.

<http://www.symantec.com/docs/DOC4402>

What's new in Enterprise Vault Agent 7.5

Enterprise Vault agent 7.5 supports Enterprise Vault 10.0. Enterprise Vault indexes the items that are archived. Indexing is done for faster and efficient searching of archived data.

Enterprise Vault 10.0 has a new 64-bit search engine. The 64-bit search engine has been created for the items that are indexed using Enterprise Vault 10.0 or later. In the earlier release, indexes were created using the 32-bit search engine.

In the 10.0 release, when a search is performed on an archive that has both the 32-bit and the 64-bit indexes, Enterprise Vault automatically searches across both the indexes.

For successful index locations and vault store partitions backups, there are some files that you need to exclude. These files must be added to the list of all NBU clients where the Enterprise Vault server is present.

See [“Notes about Enterprise Vault 10.0 backups”](#) on page 101.

See [“Excluding files from the exclude list”](#) on page 102.

About the NetBackup Enterprise Vault Agent

The NetBackup Enterprise Vault agent consists of the components that enable you to protect the Enterprise Vault configuration information and data that Enterprise Vault has archived. The agent supports Enterprise Vault 7.5, 8.0, 9.0, and 10 configurations. Thus, you should install all of the Enterprise Vault agent components on each of the systems that comprise an Enterprise Vault environment.

See [“Verifying Enterprise Vault agent operating system compatibility”](#) on page 22.

The Enterprise Vault agent enables you to back up and restore the Enterprise Vault file system data and the Enterprise Vault SQL data. These types of data can reside on different systems or devices, such as NTFS or NAS devices.

The Enterprise Vault agent can also serve as a disaster recovery solution for data that is archived with Enterprise Vault. Recovery of the archived data is not dependent on the archive source, such as Exchange Server or a specific file system.

The NetBackup Enterprise Vault agent and its capabilities are provided as add-ons to the NetBackup Windows client software. This agent is tightly integrated with NetBackup and the Backup, Archive, and Restore interface. Thus, this manual provides an overview of the Enterprise Vault agent functionality as it pertains to NetBackup and the Backup, Archive, and Restore interface. Back up and restore operations for the Enterprise Vault agent are identical to other NetBackup file operations, except where noted.

About the Enterprise Vault Agent and the backup components

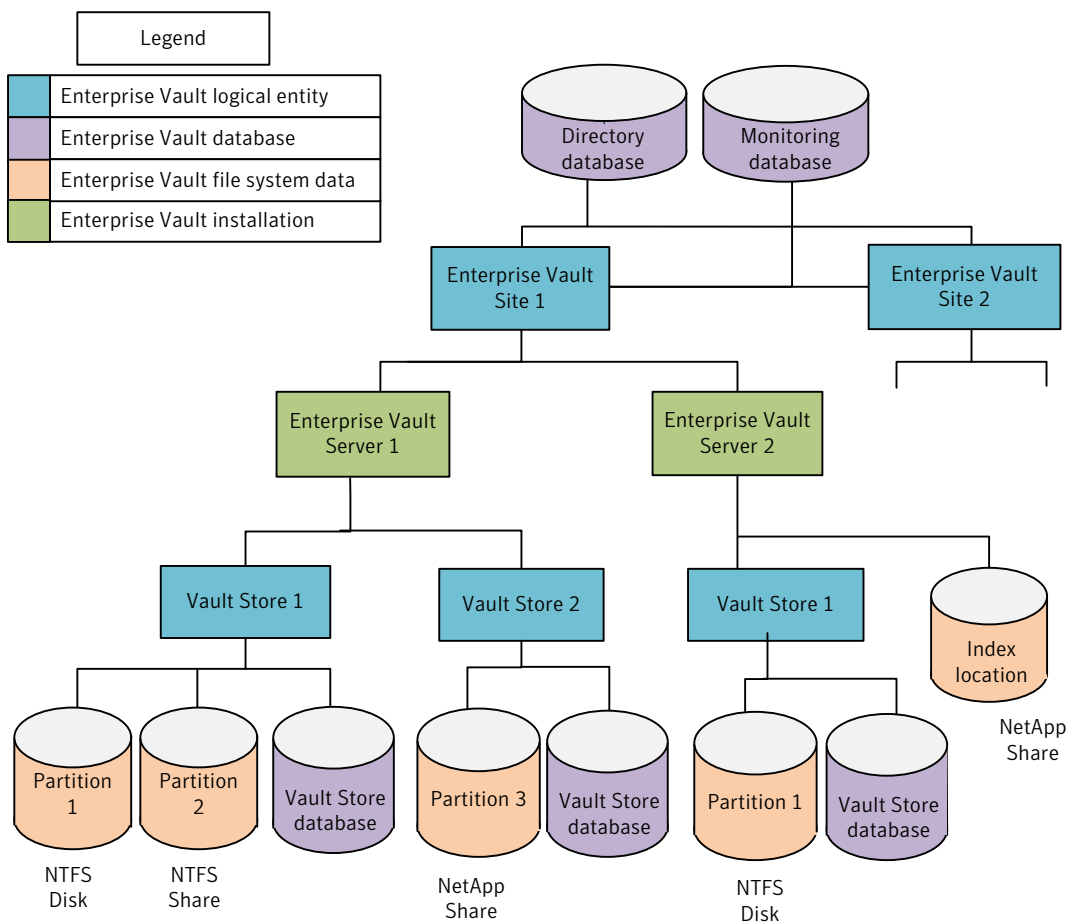
The NetBackup Enterprise Vault agent determines the configuration of an Enterprise Vault environment when an Enterprise Vault backup is run. This information is provided to the NetBackup master server to instantiate the appropriate NetBackup components on the clients for backup.

The Enterprise Vault agent enables you to back up and restore the following Enterprise Vault 7.5 components:

- Enterprise Vault directory database
- Enterprise Vault monitoring database
- Enterprise Vault archives (such as open and closed partitions)
For this release, the Enterprise Vault agent does not support any Enterprise Vault partitions that are based on a mapped drive.
See [“Enterprise Vault agent functionality and support for EV 7.5 and later”](#) on page 109.
- Enterprise Vault, vault store database
- Enterprise Vault index location
For this release, Enterprise Vault agent does not support the Enterprise Vault index locations that are based on a mapped drive.
See [“Enterprise Vault agent functionality and support for EV 7.5 and later”](#) on page 109.

[Figure 1-1](#) demonstrates how the Enterprise Vault 7.5 application components can be configured in the following hierarchical view. The types of data that are backed up depend on the directive that you choose when you create your policy.

Figure 1-1 Enterprise Vault 7.5 hierarchy



The Enterprise Vault agent enables you to back up and restore the following Enterprise Vault 8.0 or later components:

- Enterprise Vault directory database
- Enterprise Vault monitoring database
- Enterprise Vault FSA Reporting database
- Enterprise Vault auditing database
- Enterprise Vault index location

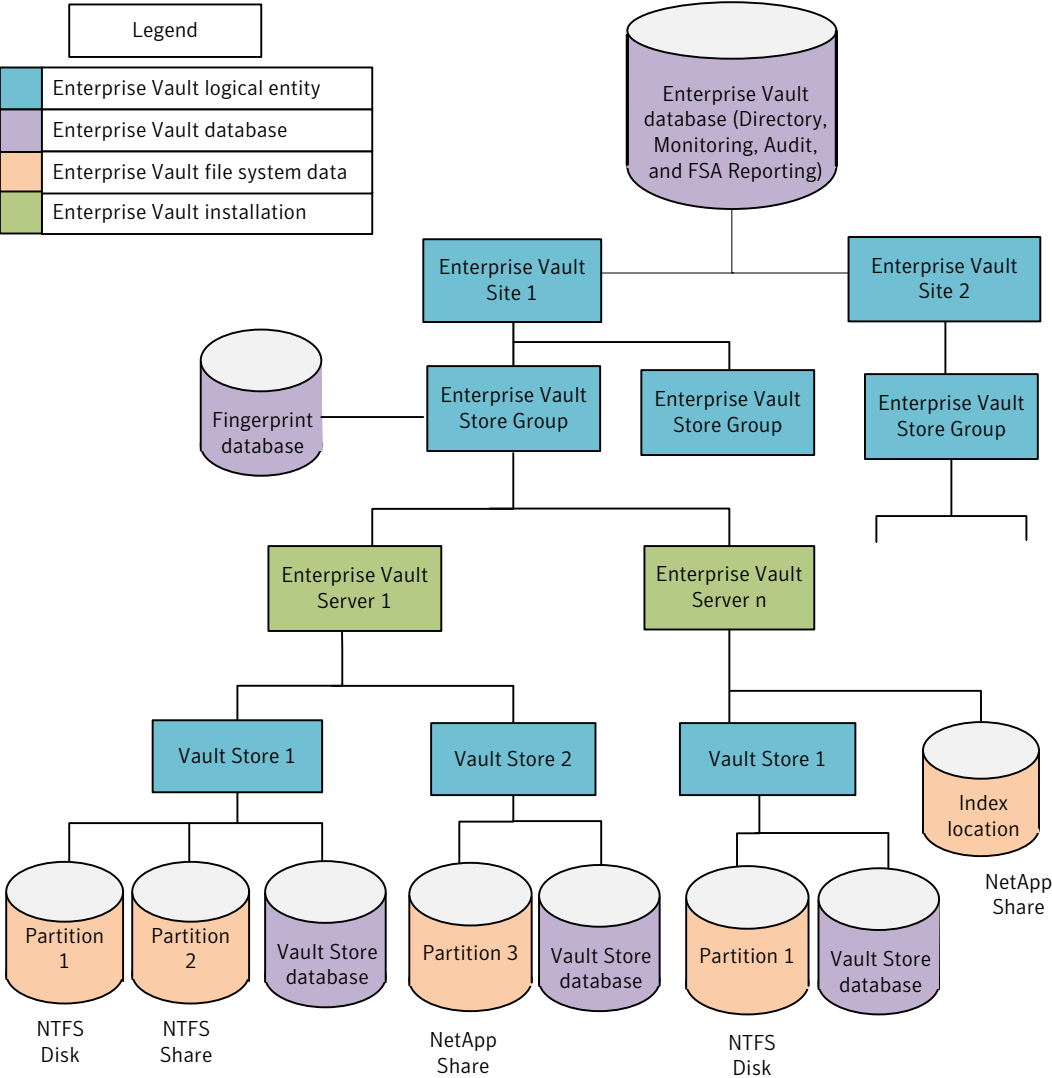
For this release, NetBackup does not support any Enterprise Vault index locations that are based on a mapped drive. If any index location in an

Enterprise Vault site is based on a mapped drive then there should not be any backup selection that uses the `EV_INDEX_LOCATION=EVSite Name` directive.

- Enterprise Vault archives (such as the open, closed, and ready partitions)
For this release, NetBackup does not support any Enterprise Vault partitions that are based on a mapped drive. That applies to open, closed, and ready partition components.
 - If an open partition is based on a mapped drive then there should not be any backup selection that uses the `EV_OPEN_PARTITION=Vault Store Name` (which contains that open partition) directive.
 - If a closed partition is based on a mapped drive then there should not be any backup selection that uses the `EV_CLOSED_PARTITION=VaultStoreName` (which contains that closed partition) directive.
 - If a ready partition is based on a mapped drive then there should not be any backup selection that uses the `EV_READY_PARTITION=VaultStoreName` (which contains that ready partition) directive.
- Enterprise Vault vault store database
- Enterprise Vault fingerprint database
- Enterprise Vault 9.0 or later supports streamer based open, closed, and ready partitions.

[Figure 1-2](#) demonstrates how the Enterprise Vault 8.0 and higher application components can be configured in the following hierarchical view.

Figure 1-2 Enterprise Vault 8.0 or later hierarchy



Enterprise Vault agent features

The Enterprise Vault agent is tightly integrated with NetBackup. For example, it provides you with the ability to perform online backups, save data to a variety of storage devices, automated backups, and so forth.

Table 1-1 lists the Enterprise Vault agent features.

Table 1-1 NetBackup Enterprise Vault agent features

Feature	Description
Online backup	<p>Certain online backups require NetBackup to put Enterprise Vault or specific Enterprise Vault components in read-only mode. When your backup involves an Open partition or an Index location component, NetBackup must put Enterprise Vault into read-only mode before the backup takes place. The following rules apply for Enterprise Vault 7.5, and 8.0 or later.</p> <ul style="list-style-type: none">■ When this particular backup occurs in an Enterprise Vault 7.5 environment, NetBackup places the entire Enterprise Vault server into read-only mode. The Enterprise Vault services and data are available during the backup.■ In an Enterprise Vault 8.0 or later environment, only the particular vault store or index location is placed into read-only mode. All other Enterprise Vault components are not placed in read-only mode.
Enterprise Vault backup schedules	<p>The NetBackup Enterprise Vault agent supports full, differential-incremental, and cumulative-incremental backups. These types of backups are configured in an Enterprise Vault policy that the user creates through the NetBackup Administration Console. The user can then specify which Enterprise Vault components to backup by selecting predefined directives in the backup policy.</p>
Tight NetBackup integration	<p>Tight integration with NetBackup means the following:</p> <ul style="list-style-type: none">■ An administrator already familiar with NetBackup procedures and software can easily configure and use NetBackup Enterprise Vault agent to perform backup and restore operations.■ Features and strengths of the NetBackup product suite are available to the user of the NetBackup Enterprise Vault agent. These features include scheduled operations. These features are described in detail in the <i>NetBackup Administrator's Guide, Volume I</i>.
Data management	<p>Enterprise Vault agent backups are saved to a wide variety of storage devices that NetBackup supports.</p>

Table 1-1 NetBackup Enterprise Vault agent features (*continued*)

Feature	Description
Automated backups	<p>Administrators can configure policies and schedule automatic, unattended backups for local or remote clients across the network. These backups are managed entirely by the NetBackup server from a central location.</p> <p>In addition, the administrator can manually back up Enterprise Vault archived data and Enterprise Vault configuration data (database) that is stored on different locations.</p>
Restore operations	An administrator who uses the Backup, Archive, and Restore interface can browse Enterprise Vault backups and select the ones to restore.
Redirected restore	The Enterprise Vault agent supports redirected (alternate) restore for the file system data and the SQL databases. This feature enables you to rename or redirect the backup objects for the file system data. For SQL objects, this feature supports redirected restores and it supports the renaming of an Enterprise Vault SQL database name. However, this feature does not support the renaming of the physical files that are associated with an SQL database.
Local media server	<p>The Enterprise Vault agent supports the use of a local media server as the primary media server during a backup. However, the configuration of the local media server for Enterprise Vault agent is different than what a NetBackup configuration uses.</p> <p>See “Configuring the local media server for Enterprise Vault backup” on page 36.</p>

Enterprise Vault agent requirements

Review the following requirements before you use the Enterprise Vault agent:

- Ensure that the Microsoft Core XML Services (MSXML 6.0 or later) is installed on the Enterprise Vault server. You can download and install MSXML from Microsoft Corporation's Web site.
- Install the NetBackup client (which includes the Enterprise Vault agent) on the client that runs the Enterprise Vault Storage Service and Enterprise Vault index service. If Enterprise Vault uses a storage device such as NetApp to store

archived data, the Enterprise Vault agent uses Microsoft's Common Internet File System (CIFS) protocol to access the data.

- Because this agent is installed with the NetBackup client software, you must also install the client on any system that hosts an Enterprise Vault SQL database.
- Verify that Enterprise Vault is supported on your operating system.
- At the time of this release, this version of the Enterprise Vault agent supports Enterprise Vault 7.5 and later. Contact Support for information about supporting future versions of Enterprise Vault.
See “ [Verifying Enterprise Vault agent operating system compatibility](#)” on page 22.

About NetBackup Enterprise Vault agent installation requirements

This chapter includes the following topics:

- [Installation requirements for NetBackup Enterprise Vault agent](#)
- [Verifying Enterprise Vault agent operating system compatibility](#)
- [NetBackup server and client software requirements](#)
- [Enterprise Vault support for Enterprise Vault Agent](#)
- [About Enterprise Vault agent installation requirements in a cluster](#)
- [Configuring Enterprise Vault Agent to protect Enterprise Vault databases](#)
- [Adding the Enterprise Vault agent license key](#)
- [Configuration requirements for upgrading the Enterprise Vault agent](#)

Installation requirements for NetBackup Enterprise Vault agent

Every NetBackup server includes the NetBackup client software by default. Therefore, you can use Enterprise Vault agent software on a NetBackup server or client (if the Enterprise Vault agent is supported on that platform).

Before you install the software, review the following requirements and ensure operating system compatibility:

- See “[Verifying Enterprise Vault agent operating system compatibility](#)” on page 22.
- See “[NetBackup server and client software requirements](#)” on page 22.
- See “[About Enterprise Vault agent installation requirements in a cluster](#)” on page 23.

Verifying Enterprise Vault agent operating system compatibility

Verify that Enterprise Vault agent is supported on your operating system before you install the software. The NetBackup Enterprise Vault Agent supports Enterprise Vault 7.5 and 8.0 SP2 and later versions. In addition, you can view the NetBackup database agent compatibility list on the Symantec Support Web site to determine operating system compatibility along with the versions of SQL that the Enterprise Vault Agent supports.

To verify operating system and compatibility

- 1 Open the following URL from your Internet browser:

`www.symantec.com/business/support`
- 2 Select the **NetBackup Enterprise Server** link under the **Support for Top Products** title on the Web page .
- 3 Select **Master Compatibility List** under the **Compatibility** title on the Web page .

The Web page refreshes and shows a list of compatibility documents. You can refine your search to find a link to the appropriate document. (The compatibility list documents are in PDF format. You must have Adobe Acrobat Reader to view these documents.)

- 4 In the list of documents, click on the following link:
NetBackup (tm) x.x Database Agent compatibility.
For x.x, look for the most current release of NetBackup.

NetBackup server and client software requirements

Verify that the following requirements are met for the NetBackup server and client software for the Enterprise Vault agent:

- The Enterprise Vault agent is automatically installed as part of the NetBackup client software. No custom installation is necessary. The NetBackup server

platform can be any Windows platform that NetBackup supports. For more information, see the *NetBackup Installation Guide*.

- The Enterprise Vault agent is a part of the NetBackup client software. The NetBackup client software must be installed on every system that either hosts Enterprise Vault SQL data or is an Enterprise Vault server. (If the Enterprise Vault server is also a NetBackup server, the client software is installed along with the NetBackup server software.)
- Verify that you have the supported Windows and Enterprise Vault version.

Enterprise Vault support for Enterprise Vault Agent

The following list helps you to know about the Enterprise Vault support for Enterprise Vault agent.

- NetBackup 6.5.4, 6.5.5, and 6.5.6 Enterprise Vault Agent is supported when used with a Enterprise Vault 7.5 or 8 that is configured in a Microsoft Cluster Server (MSCS).
- NetBackup 6.5.4, 6.5.5, and 6.5.6 Enterprise Vault Agent is not supported when used with a Enterprise Vault 7.5 or 8 that is configured in a Veritas Cluster Services (VCS) environment. However, this environment can be protected using legacy methods to back up the Enterprise Vault environment.
- NetBackup 7.0.x Enterprise Vault agent supports both MSCS and VCS clustered environments of Enterprise Vault.
The NetBackup 7.5 Enterprise Vault agent is not supported when used with the Enterprise Vault 10 and a SQL server configured in VCS.

About Enterprise Vault agent installation requirements in a cluster

You must verify that the Enterprise Vault agent software is installed and operational on each Enterprise Vault node in the cluster to ensure failover capabilities.

See “[Verifying Enterprise Vault agent operating system compatibility](#)” on page 22.

The NetBackup 6.5.4, 6.5.5, and 6.5.6 Enterprise Vault Agent supports Enterprise Vault that is clustered in the following Microsoft Cluster Server (MSCS) configurations:

- Enterprise Vault 7.5 on Windows 2003, 2008 (x86, AMD64)

- Enterprise Vault 8.0 SP2 or higher on Windows 2003, 2008 (x86, AMD64) with Windows registry changes applied.

To enable the NetBackup 6.5.4, 6.5.5, and 6.5.6 Enterprise Vault agent to detect an MSCS clustered Enterprise Vault 8 SP2 server, add the following Windows registry keys and String Values (type REG_SZ) on each cluster node:

- For x86 MSCS clusters: If a key does not exist, create the following one:

HKEY_LOCAL_MACHINE\Software\KVS\Enterprise Vault\Admin**ConfigState**

- For x64 MSCS clusters: If a key does not exist, create the following one:

HKEY_LOCAL_MACHINE\Software\Wow6432Node\KVS\Enterprise Vault\Admin**ConfigState**

When the key is created, add the following string values:

- "ClusVirtualServer"="virtual node name"
- "ClusResourceGroup"="EV Resource Group name"

Configuring Enterprise Vault Agent to protect Enterprise Vault databases

You must configure the Enterprise Vault Agent to protect the Enterprise Vault databases, hosted by an MSCS clustered server. You must make some changes to all the nodes in the clustered environment, to configure the NetBackup 6.5.4, 6.5.5 or 7.0 Enterprise Vault Agent. The changes to the nodes ensure that the Enterprise Vault databases are protected when hosted by an MSCS clustered Microsoft SQL Server . Refer to the following section.

To configure the NetBackup 6.5.4, 6.5.5 or 7.0 Enterprise Vault Agent

- 1 Select **Start > Symantec NetBackup > Backup, Archive, and Restore**.
- 2 From the **File** menu, select **NetBackup Properties**.
The NetBackup Client Properties dialog box is displayed. By default, the **General** tab is displayed.
- 3 Enter the Virtual SQL server name as the client name in the **Client name** text box.
- 4 A warning is displayed, click **OK**.
- 5 Click **OK** to exit the NetBackup Client Properties dialog box.

Once the Virtual SQL server name is added as the client name, you must add each node and the virtual cluster to the NetBackup client list. You can then configure

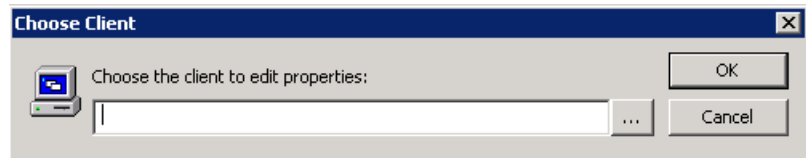
the nodes and virtual SQL server for the Enterprise Vault - NetBackup Master Admin Console.

To add and configure the nodes and virtual SQL server

- 1 On the NetBackup Administration Console , expand Host Properties.
- 2 From the **Actions** menu, select **Configure Client** or click the Configure Client icon.

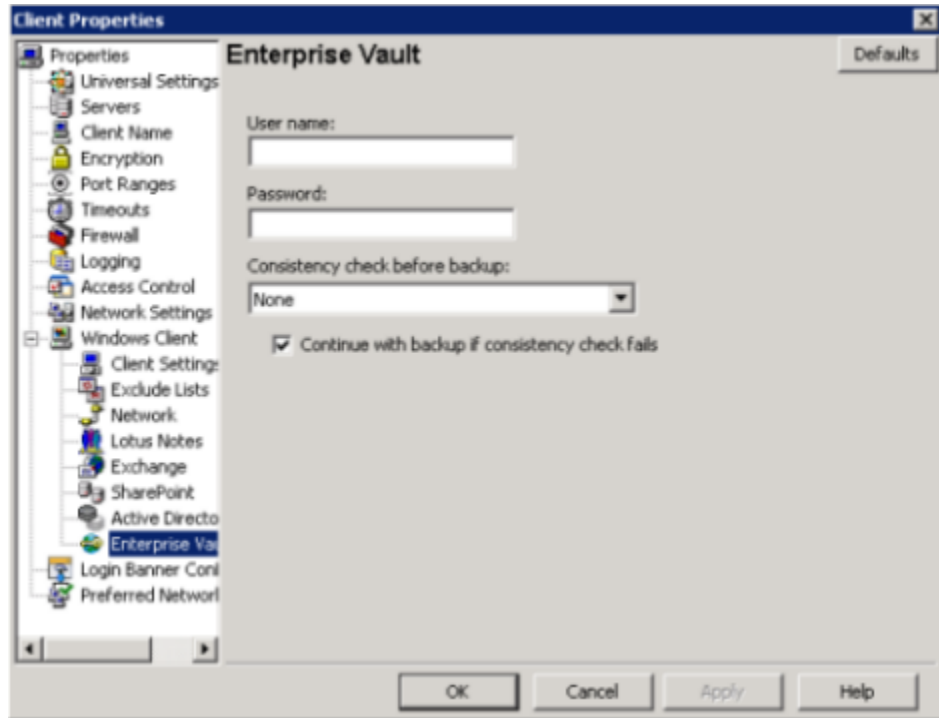


The Choose Client dialog box is displayed as shown in the following figure:



- 3 Click Browse and select the required computer and click OK.
- 4 Click OK to exit the Choose Client dialog box.

- 5 From the Host Properties list, select **Clients**. The available clients are displayed.
- 6 Right-click the required client and select Properties. The Client Properties dialog box is displayed as shown in the following figure:



For each node and cluster, configure the log on account to be the Enterprise Vault Admin user.

Adding the Enterprise Vault agent license key

The Enterprise Vault agent license is used similarly to how other database agents use their license keys. To use the Enterprise Vault agent, add a valid license key for it on the master server.

For information on how to add license keys, see the *NetBackup Administrator's Guide, Volume I*.

Note: In a NetBackup cluster, add the key on each node where the NetBackup server is installed.

To add an Enterprise Vault agent license key

- 1 On the master server, open the NetBackup Administration Console.
- 2 Click **Help > License Keys**.
- 3 Click **New**.
- 4 Type the license key and click **Add**.

Configuration requirements for upgrading the Enterprise Vault agent

NetBackup 7.5 and later versions support the newly added functionality and the new policy directives that make it a much more robust agent than the previous versions. Symantec suggests that you upgrade to the latest version of Enterprise Vault to take advantage of the new features.

If you elect to upgrade to NetBackup 7.5, you should understand the following configuration requirements:

- The NetBackup version on all of the Enterprise Vault servers (in one Enterprise Vault site deployment) must be the same.
- The NetBackup version on all of the SQL servers in the configuration must be the same as, or higher than the NetBackup version of the Enterprise Vault server in an Enterprise vault site.
For example, if a SQL server is a part of an Enterprise Vault site that contains the Enterprise Vault servers that are running NetBackup 7.5, then the SQL servers must run the same version level (or higher) as the Enterprise Vault servers.
- If an Enterprise Vault server is also used as a SQL server, the version of SQL on that server must be equal to or higher than the NetBackup version of the Enterprise Server.
- The NetBackup version on the master server and media servers must be same or higher than the NetBackup client version. For example, a NetBackup 7.5 master server can support a mixed environment of NetBackup 6.5.4 and 7.0 client servers.
- The only way that a NetBackup master server can communicate with the NetBackup 6.5.4 client and a NetBackup 7.5 client is with two or more Enterprise Vault sites. One site would contain NetBackup 6.5.4 Enterprise

Vault servers and the other site would contain NetBackup 7.5 Enterprise Vault servers. If these two sites share a SQL server, then that server must run must a version that is equal to or greater than NetBackup 7.5.

After you have finished the upgrade, more changes to the Enterprise Vault configuration may be required. For example, if you upgraded the master, media, and client servers to version 7.0 and you upgraded Enterprise Vault to version 8.0, then you must modify your backup policy to use Enterprise Vault 8.0 directives.

Table 2-1 shows the different versions of software that can be run within your Enterprise Vault environment. The table also shows which variation of software requires you to make additional changes after the upgrade completes.

Table 2-1

Upgrade scenarios after an upgrade to NetBackup 7.1 or later versions

NetBackup master and media version	NetBackup client version	Enterprise Vault version	What changes are required after an upgrade?
7.0	7.0	7.5	No additional changes are required.
7.0	6.5.4	7.5	No additional changes are required.
7.0	7.0	8.0	You must modify all current NetBackup Enterprise Vault policies to use the Enterprise Vault 8.0 or later directive set. See “ Configuration changes required after Enterprise Vault upgrade ” on page 28.
7.0	6.5.4	8.0	No additional changes are required. For more information on data protection of Enterprise Vault 8.0 or later components using NetBackup 6.5.4, see, Technote 323945. The technote, <i>Enterprise Vault 8.0 support using NetBackup 6.5.4</i> , is available on the Symantec Support Web site at the following URL: http://entsupport.symantec.com/docs/323945

Configuration changes required after Enterprise Vault upgrade

After you upgrade all servers to NetBackup 7.1 and Enterprise Vault to version 8.0, you must change the configuration of the NetBackup policies.

To change the Enterprise Vault directive set

- 1 Disable the Microsoft SQL Server policy type (**MS-SQL-server**) to protect the fingerprint, auditing, and FSA Reporting databases when using the Enterprise -Vault policy to protect these databases. If you do not disable these policies, you can encounter issues with incremental backups.

If you use the NetBackup SQL Agent to perform a backup then it can only be restored with the NetBackup SQL Agent. Refer to the *Enterprise Vault 8.0 support using NetBackup 6.5.4* white paper for more information.

- 2 Change the Enterprise Vault policy directives to include the Enterprise Vault 8.0 directive set.

See [“Configuring the policy directives after upgrading NetBackup and Enterprise Vault ”](#) on page 29.

- 3 Perform a full backup of all components in the Enterprise Vault site.

Configuring the policy directives after upgrading NetBackup and Enterprise Vault

After the upgrade, you must change the policy directives. You must remove all of the Enterprise Vault 7.5 directives and replace them with the Enterprise Vault 8.0 directive set. If you do not make this change the Enterprise Vault policy backups can fail. The following procedure explains how to remove and add policy directives.

To change the Enterprise Vault 7.5 directives to directives for Enterprise Vault versions 8.0 and later

- 1 Modify the policy directive list to use the Enterprise Vault directive set. Double-click on an existing policy to see the current configuration of that policy.
- 2 Open the **Backup Selections** tab. From this tab, you can now remove the old directives and add the directives of Enterprise Vault versions 8.0 and later.
- 3 Use the following table to determine which Enterprise Vault 8.0 and later version directive corresponds the previous Enterprise Vault 7.5 directive.

Directives in Enterprise Vault 7.5

EV_DIR_DB

Corresponding directives in Enterprise Vault versions 8.0 and later

EV_DIR_DB

This directive remains the same from Enterprise Vault 7.5 to Enterprise Vault 8.0 and later versions.

Directives in Enterprise Vault 7.5	Corresponding directives in Enterprise Vault versions 8.0 and later
EV_MONITORING_DB	<div>EV_MONITORING_DB</div> <div>This directive remains the same from Enterprise Vault 7.5 to Enterprise Vault 8.0 and later versions.</div>
EV_OPEN_PARTITIONS	<div>Specify EV_OPEN_PARTITION=<i>Vault Store name</i> for all vault stores that correspond to the Enterprise Vault server that is listed in the policy client.</div>
EV_CLOSED_PARTITIONS	<div>Specify EV_CLOSED_PARTITIONS=<i>Vault Store name</i> for all vault stores that correspond to the Enterprise Vault server that is listed in the policy client.</div>
EV_VAULT_STORE_DB	<div>Specify the EV_VAULT_STORE_DB=<i>EV Vault Store name</i> directive for all of the vault stores that correspond to the Enterprise Vault server that is listed in the policy client.</div>
EV_VAULT_STORE_DB= <i>EV Vault Store name</i>	<div>EV_VAULT_STORE_DB=<i>EV Vault Store name</i></div> <div>This directive remains the same from Enterprise Vault 7.5 to Enterprise Vault 8.0 and later versions.</div>
EV_VAULT_STORE= <i>EV Vault Store name</i>	<div>Based on the partitions available in the vault store use the following:</div> <div><div>■ EV_OPEN_PARTITION=<i>Vault Store name</i></div><div>■ EV_CLOSED_PARTITIONS=<i>Vault Store name</i></div><div>■ EV_READY_PARTITIONS=<i>Vault Store name</i></div></div> <div>If there is no open partition specify EV_VAULT_STORE_DB=<i>Vault Store name</i></div>
EV_VAULT_STORE	<div>Specify the open, closed, and ready partitions for all of the vault stores that correspond to the Enterprise Vault server.</div>

Directives in Enterprise Vault 7.5	Corresponding directives in Enterprise Vault versions 8.0 and later
EV_INDEX_LOCATION	An Enterprise Vault, server-level backup of Index locations is not supported for EV8.0. You can use EV_INDEX_LOCATION= <i>site name</i> to back up all Index locations in the site.
EV_SERVER	Enterprise Vault 8.0 and the later versions do not support server-level backups. You must separate the policy into multiple policies to protect the Enterprise Vault components.
EV_SITE	Enterprise Vault 8.0 and the later versions do not support site-level backups. You must separate the policy into multiple policies to protect the Enterprise Vault components.

About additional new directives of Enterprise Vault 8.0 and later versions

The Enterprise Vault agent supports the following new Enterprise Vault directives for 8.0 and later versions:

- EV_FINGERPRINT_DB
You can use this directive to backup the fingerprint database component.
- EV_FSAREPORTING_DB
You can use this directive to backup the FSA Reporting database component.
- EV_AUDIT_DB
You can use this directive to backup the auditing database component.

Upgrading to Enterprise Vault 9.0

To upgrade to Enterprise Vault 9.0 from Enterprise Vault 8.0, no modifications are required to be made in the backup policy.

Upgrading to Enterprise Vault 10.0

To upgrade to Enterprise Vault 10.0 from Enterprise Vault 8.0, no modifications are required to be made in the backup policy.

Configuration

This chapter includes the following topics:

- [About the Windows and Java user interfaces](#)
- [Specifying a logon account for the Enterprise Vault server](#)
- [About VSS-based snapshot configuration](#)
- [Configuring the local media server for Enterprise Vault backup](#)
- [Configuration requirements for an Enterprise Vault backup policy](#)
- [Adding a new Enterprise Vault policy](#)
- [Enterprise Vault backup policy attributes](#)
- [Adding schedules to an Enterprise Vault policy](#)
- [About the types of Enterprise Vault backups](#)
- [Creating a backup selections list](#)
- [Adding a client to a policy](#)

About the Windows and Java user interfaces

You can perform many of the configuration steps in this topic from the NetBackup Administration Console on the master server. The type of console available depends on your master server's platform. NetBackup supports a Windows and Java interface on Windows master servers.

The Java and Windows interfaces are nearly identical. If interface differences exist in the configuration procedures, the term “Windows interface” or “Java interface” appears in the procedure to differentiate between the two interfaces.

Specifying a logon account for the Enterprise Vault server

To perform backups and restores, NetBackup must know the user name and password for the account that is used to logon to the Enterprise Vault server and to interact with the Enterprise Vault SQL database. The user must set the logon account for every NetBackup client that runs backup and restore operations for Enterprise Vault components.

The Enterprise Vault agent user should have the following user-credential privileges:

- The ability to back up and restore SQL databases
- The ability to communicate with the Enterprise Vault services and to put Enterprise Vault into backup mode
- Permissions to read and write from the Enterprise Vault file system paths such as the Enterprise Vault partitions, and index locations. The file paths can be on the UNC or the local drive

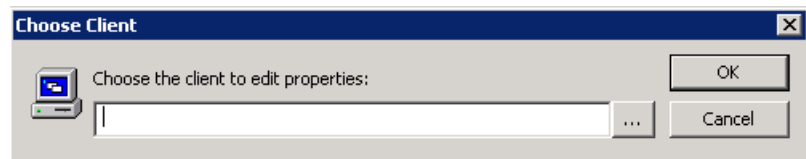
Note: You must perform the following procedure for all of the Enterprise Vault servers and the SQL servers in an Enterprise Vault site configuration.

To specify the logon account for the Enterprise Vault server

- 1 Open the NetBackup Administration Console.
- 2 Expand **NetBackup Management > Host Properties > Clients**.
- 3 If the client does not appear in the client list, click the **Configure client** icon.

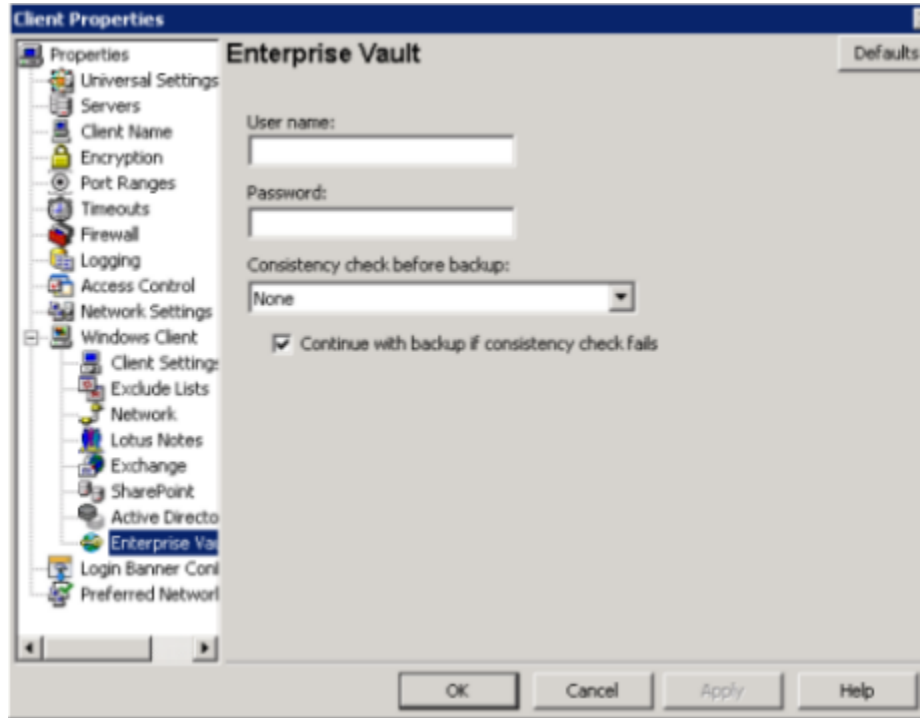


Enter a client name in the **Choose Client** dialog box as shown in the following figure and click **OK**.



- 4 In the right pane, right-click on the client and click **Properties**.

- 5 In the left pane, expand **Windows Client** and click **Enterprise Vault**. The **Client Properties** dialog box is displayed as shown in the following figure.



- 6 In the **User name** box, specify the user ID for the account that is used to log on to Enterprise Vault (DOMAIN\user name).
- 7 In the **Password** box, specify the password for the account.
- 8 Click **OK** to save your changes.

About VSS-based snapshot configuration

In NetBackup 7.1 and later, the Enterprise Vault agent provides support for VSS copy-on-write snapshots, but the user is not allowed to configure it. In the Enterprise Vault policy type, the Snapshot check box is disabled because Snapshots have been automated to run under certain conditions.

The Enterprise Vault agent uses the snapshot mechanism in following scenarios:

- An Enterprise Vault SQL database backup using a FULL schedule.

- An Enterprise Vault File System data backup for a non-UNC (Universal Naming Convention) location.

Table 3-1 illustrates when snapshot is used.

Table 3-1 Conditions of when snapshot is used

Data type	Schedule type	Is a snapshot used?
Enterprise Vault SQL database	FULL	Yes
Enterprise Vault SQL database	Incremental	No
Enterprise Vault File System data is exposed as a UNC path (For example: \\server\share\data_path)	Any	No
Enterprise Vault File System data is exposed as a non-UNC path	Any	Yes

The following list contains the additional notes that relate to a VSS-based snapshot configuration:

- The Enterprise Vault agent internally uses the VSS-based snapshot. Therefore, every drive that has the Enterprise Vault data must have an ample amount of free space for a VSS snapshot to be taken. A snapshot can fail if the amount of free space on the selected drive is insufficient.
See [“About the VSS_E_INSUFFICIENT_STORAGE snapshot error”](#) on page 120.
- With NetBackup 7.1 and later, the Enterprise Vault agent attempts to take as many snapshots per snapshot job as possible. The maximum number of snapshots that can occur during a single snapshot job is 64 which, is also the default value. You can lower this value by adjusting the maximum number of snapshots that can occur during a single snapshot job. The registry DWORD value, *MaxSnapshotPerJob* controls the maximum number of snapshots. This registry value is located under the registry key,
Software\VERITAS\NetBackup\CurrentVersion\Agents\EnterpriseVault\.
The default for the *MaxSnapshotPerJob* value is 64 snapshots per snapshot job.

Configuring the local media server for Enterprise Vault backup

The NetBackup Enterprise Vault agent is designed to use the local media server as often as possible during a backup. For example, if the Enterprise Vault server or Enterprise Vault-SQL server is also a NetBackup media server, then the

Enterprise Vault backup tries to use the media that is attached to the local system as much as possible. However, because of parameters such as, **resource inheritance from the parent job**, it is possible that the Enterprise Vault backup may not use the local media server.

For the Enterprise Vault agent, local media server support is implicit and no external setting can disable it. The NetBackup master server configuration for local media server support does not have any effect on the Enterprise Vault backups that use or do not use the local media.

For an Enterprise Vault backup to use the local media server, you need to make some configuration changes. Refer to the following procedure for these changes.

To configure the local media for Enterprise Vault backup

- 1 First, configure the Enterprise Vault policy's storage unit. To configure the policy, open the existing Enterprise Vault policy.
- 2 From the Attributes tab, choose the Any Available option from the **Policy storage unit/lifecycle policy** drop-down list.
- 3 Next, configure the storage units that belong to the local media server. To configure the storage unit, open the **Change Storage Unit** dialog box and ensure that the **On Demand Only** check box is deselected for the storage unit.
- 4 Finally ensure that the following media server entries exist in the Server Properties of a host:
 - The master server must have entries for all media servers in Enterprise Vault site.
 - Each media server in the Enterprise Vault site should have entries in their properties for other media servers in the Enterprise Vault site.
 - All NetBackup clients (Enterprise Vault servers or Enterprise Vault-SQL servers) should have entries in their properties for all the media servers in the Enterprise Vault site.

Configuration requirements for an Enterprise Vault backup policy

A backup policy for an Enterprise Vault agent defines the backup criteria for a specific group of one or more clients. The criteria includes the following:

- Storage unit and media to use
- Policy attributes
- Backup schedules

- Clients to be backed up
- Backup selection

Before you create and run a backup policy, ensure that you set the value for the following items in the Administration Console:

Before you create and run a backup policy, ensure that you set the value for **Maximum concurrent jobs** and **Maximum jobs per client** options from the Administration console.

The **Maximum concurrent jobs** option is available in the **Storage Unit Settings** dialog box. The value under this option indicates the number of concurrent backup jobs that can use a storage unit and directly affect the performance of the backup. Symantec recommends that you change the value of this setting based on the following:

- Your Enterprise Vault configurations
- Policy clients
- Policy backup selections
- Capability of the storage unit

The **Maximum jobs per client** option is available under the master server Host properties (Global Settings). Symantec recommends that you change the value based on your Enterprise Vault configuration and backup selections.

To back up an Enterprise Vault environment, create at least one Enterprise Vault policy with the appropriate schedules. A configuration can have a single policy that includes all clients or many policies, some of which include only one client.

See the *NetBackup Administrator's Guide, Volume I*.

See [“Adding a new Enterprise Vault policy”](#) on page 38.

See [“Adding schedules to an Enterprise Vault policy”](#) on page 41.

See [“Adding a client to a policy”](#) on page 46.

Adding a new Enterprise Vault policy

This topic describes how to add a new Enterprise Vault backup policy.

Note the following before you add a new Enterprise Vault backup policy:

- If you use the command-line interface (CLI) to create the new policy, the identifying number for an Enterprise Vault agent policy type is 39.
- Multistream backups and restores are not supported at this time.

To add a new policy

- 1 Log on to the master server as administrator (Windows) and start the NetBackup Administration Console.
- 2 If your site has more than one master server, select the one where you want to add the policy.
- 3 Add a new policy by making the appropriate selection:
 - In the left pane, right-click **Policies**. Select **New Policy** (Windows interface).
 - In the left pane, click **Policies**. In the **All Policies** pane, right-click the master server and click **New Policy** (Java interface).
- 4 In the **Add a New Policy** dialog box, in the **Policy name** field, type a unique name for the new policy.
- 5 Uncheck the **Use Backup Policy Configuration Wizard** check box.

Note: By default, this option is checked. Uncheck this check box if you want to manually create a new policy. If this check box is not unchecked, the **Backup Policy Configuration** wizard appears and guides you through the backup policy creation process.

- 6 Click **OK**.
- 7 On the **Attribute** tab of the **Add a New Policy** dialog box, select the **Enterprise-Vault** policy type from the **Policy type** drop-down list.

The Enterprise Vault database agent policy type does not appear in the drop-down list unless the master server has a license key for this database agent.
- 8 Complete the entries on the **Attributes** tab.
- 9 Continue by adding additional policy information as follows:
 - Add schedules
See [“Adding schedules to an Enterprise Vault policy”](#) on page 41.
 - Add clients
See [“Adding a client to a policy”](#) on page 46.
 - Add Enterprise Vault directives to the backup selections list

See [“Creating a backup selections list”](#) on page 43.

10 When you finish all of the schedule, client, and backup selections click, **OK**.

The policy is validated and created if it found to be valid. If the policy is not valid the policy validation fails with a status 69 or 1800 error.

For more information about how to correct your policy or for more information about the status errors, refer to the following sections.

See [“Creating a backup selections list”](#) on page 43.

See [“Adding a client to a policy”](#) on page 46.

Enterprise Vault backup policy attributes

Policy attributes vary according to your specific backup strategy and system configuration.

For more information on policy attributes, see the *NetBackup Administrator’s Guide, Volume I*.

[Table 3-2](#) shows the policy attributes that are available for Enterprise Vault backups.

Table 3-2 Policy attribute descriptions

Attribute	Description
Policy type	Determines the types of clients that can be in the policy. In some cases policy type determines the types of backups that NetBackup can perform on those clients. To use the Enterprise Vault agent, you must define at least one policy of type that is <i>Enterprise-Vault</i> . Note: If you use the command-line interface (CLI), the identifying number for an Enterprise Vault agent policy type is 39.
Limit jobs per policy	Limits the number of jobs that NetBackup performs concurrently with this policy. Set this option to a number that is determined by the backup selection and your Enterprise Vault configuration. A single policy can result in multiple jobs. In addition, you can run backups without using this option.

Table 3-2 Policy attribute descriptions (*continued*)

Attribute	Description
Allow multiple data streams	<p>This attribute is enabled when the user creates an Enterprise Vault policy. However, Enterprise Vault agent does not support the multiple data streams feature.</p> <p>This attribute specifies that NetBackup can divide automatic backups for each client into multiple jobs. Each job backs up only a part of the list of backup selections. The jobs are in separate data streams and can occur concurrently. The number of available storage units, multiplex settings, and the maximum jobs parameters determine the total number of streams and how many can run concurrently.</p>
Keyword phrase	A textual description of a backup. Useful for browsing backups and restores.

Adding schedules to an Enterprise Vault policy

Each policy has its own set of schedules. These schedules control the initiation of automatic backups and also specify when the user operations can be initiated.

To add a schedule

- 1 In the **Policy** dialog box, click the **Schedules** tab.
To access the **Policy** dialog box, double-click the required policy name under the **Policies** list in the NetBackup Administration Console.
- 2 Click **New**.
- 3 Specify a unique name for the schedule.
- 4 Select the **Type of backup**.
- 5 Specify the other properties for the schedule.
- 6 Click the **Start Window** tab if you want to define the period of time during which the backup starts and ends.
- 7 Click the **Exclude Dates** tab if you want to exclude specific dates from the schedule.
- 8 Click **OK**.

About the types of Enterprise Vault backups

Table 3-3 describes the type of backups available with the Enterprise Vault agent.

See [“About Enterprise Vault directives and what data they back up”](#) on page 55. for additional information on what types of data is backed up.

Table 3-3 Description of types of backups

Backup Type	Description
Full Backup	Select this back up type to back up any Enterprise Vault component. All Enterprise Vault directives support full backups.
User Backup	This type of backup is not supported for Enterprise Vault.
User Archive	This type of backup is not supported for Enterprise Vault.
Cumulative Incremental backup	<p>This backup type backs up the files that are specified in the backup selections list that has changed since the last full backup. All files are backed up if no previous Full backup has been done. Cumulative incremental backups occur automatically according to schedule criteria. A complete restore requires the last full backup and the last, cumulative incremental backup.</p> <p>Note the following about Cumulative Incremental backups:</p> <ul style="list-style-type: none">■ For an SQL database, a cumulative backup is a database differential backup.■ A cumulative incremental backup does not reset the archive bit of an object that is included for backup. See “About the archive bit ” on page 53.■ Do not combine incremental backups (differential and cumulative) within the same Enterprise Vault policy if the incremental backups are based on the archive bit.

Table 3-3 Description of types of backups (continued)

Backup Type	Description
Differential Incremental backup	<p>Select this backup type to only back up the changes that are made to the data since the last full backup or previous incremental backup.</p> <p>For an SQL database, a differential incremental backup backs up the transaction log which also truncates the logs. This schedule type is available for all Enterprise Vault components.</p> <p>Warning: Confirm that the regular differential incremental backups are performed against all EV databases to ensure that the Transaction Logs are backed up and truncated. This applies to Open Partitions as well since the Vault Store Database is automatically backed up with an Open Partition backup.</p> <p>Note: Enterprise Vault creates different SQL databases with the transaction log mode set as FULL. Symantec recommends that this mode remains set as FULL, otherwise the Enterprise Vault SQL differential backup cannot be used.</p> <p>NetBackup enables you to backup files system files using the timestamp or the archive bit . See the "Client Settings (Windows) properties" topic in the <i>NetBackup Administrator's Guide, Volume I</i> for information on how to configure the Incremental backups to be based on the timestamp or the archive bit .</p> <p>Differential Incremental backups based on the archive bit include a file in a backup only if the archive bit of that file is set. A differential-incremental backup clears the archive bit if the files are successfully backed up.</p> <p>Note: Do not combine incremental backups (differential and cumulative) within the same Enterprise Vault policy if the incremental backups are based on the archive bit.</p>

Creating a backup selections list

From the **Backup Selections** tab you can specify Enterprise Vault components to back up Enterprise Vault sites, servers, databases, indexes, or Enterprise Vault partitions. You determine which Enterprise Vault entity to back up by adding directives to the **Backup Selections** list. Each directive specifies the Enterprise Vault component(s) to back up.

Note: The Enterprise Vault entity names cannot begin with a space or end with a space. Any Enterprise Vault entity name that uses this format is not supported.

NetBackup uses the same backup selection list for all of the clients that are backed up according to the policy.

To create a backup selections list

- 1 In the **Policy** dialog box, click the **Backup Selections** tab.
- 2 Click **New**.
- 3 Click the directive icon that appears on the right in the **Backup Selections** field.
- 4 From the **Directive** drop-down list in the **Select Directive** dialog box, select the Enterprise Vault version that you have installed. The list of directives that appear correspond to the version of Enterprise Vault you have installed.

The following is a list of naming conventions that apply to Enterprise Vault directives:

- NetBackup does not support the use of blank spaces either before or after a component name. Directives that contain an equals sign have a variable field that you can modify with a component name, such as *EV site* name or *EV vault store* name. This component name cannot start with or end with a blank space. The Enterprise Vault agent removes these spaces from the backup selection.
- Enterprise Vault supports blank spaces anywhere in the component name. The Enterprise Vault agent cannot back up an Enterprise Vault component whose name begins or ends with a blank space.
- Enterprise Vault enables you to configure multiple vault store groups or vault stores with the same name. However, NetBackup does not support vault store groups or vault stores using the same name, if they share the same directory database.

Enterprise Vault 7.5 or later, directive sets enable you to select one or more directives. For example, you can select the EV_DIR_DB directive and the EV_MONITORING_DB directive in a single backup policy.

Note: With Enterprise Vault 8.0 or later, you cannot use the EV_DIR_DB directive with the EV_INDEX_LOCATION= and the EV_OPEN_PARTITION= directives.

See [“About Enterprise Vault directives and what data they back up”](#) on page 55.

The available Enterprise Vault 7.5 directives are as follows:

- EV_DIR_DB
- EV_MONITORING_DB
- EV_SERVER
- EV_SITE
- EV_VAULT_STORE
- EV_VAULT_STORE=*EV vault store name*
- EV_VAULT_STORE_DB
- EV_VAULT_STORE_DB=*EV vault store name*
- EV_INDEX_LOCATION
- EV_OPEN_PARTITIONS
- EV_CLOSED_PARTITIONS

The available Enterprise Vault 8.0 or later directives are as follows:

- EV_DIR_DB
- EV_MONITORING_DB
- EV_FSAREPORTING_DB
- EV_AUDIT_DB
- EV_INDEX_LOCATION=*site name*
- EV_OPEN_PARTITION=*vault store name*
- EV_CLOSED_PARTITIONS=*vault store name*
- EV_READY_PARTITIONS=*vault store name*
- EV_VAULT_STORE_DB=*vault store name*
- EV_FINGERPRINT_DB=*vault store group name*

- 5 Click **OK**.
- 6 You can rename any directive by selecting the directive and clicking **Rename**.
- 7 Click **OK** when you have finished adding directives to the **Backup Selections** list.

Adding a client to a policy

The clients list contains a list of the clients that are backed up during an automatic backup. In addition, a client that is specified in the policy should be an Enterprise Vault server.

Note: You can add only one client to a policy, multiple clients are not supported in the same policy.

NetBackup client software must be installed on each system that hosts an Enterprise Vault database or is an Enterprise Vault server .

To add a client to a policy

- 1
- In the **Policy** dialog box, click the **Clients** tab.
- To access the **Policy** dialog box, double-click the policy name in the **Policies** list in the NetBackup Administration Console.
- 2
- Click **New** and enter the client name in the interface.
- See “[About hosts for Enterprise Vault policies](#)” on page 105. for policy client name recommendations
- For more information about Enterprise Vault site and server aliases, see the *Symantec Enterprise Vault Administrator's Guide*.
- 3
- (Windows interface) Type the name of the client and press Enter.
- If NetBackup cannot detect the hardware and the operating system, a dialog box appears so you can specify this information.
- If the Enterprise Vault server is part of an Enterprise Vault cluster, then you must specify the virtual name of the Enterprise Vault server as the policy client.
- 4
- (Java interface) Type the name of the client you want to add.
- If the Enterprise Vault server is part of an Enterprise Vault cluster, then you must specify the virtual name of the Enterprise Vault server as the policy client.

The following options are available when you add a client:

Client name	Type the name of the client you want to add.
Hardware and operating system	Choose the applicable hardware and operating system of the client.

5 (Java interface) Click **Add**.

The following directives do not allow multiple clients:

- EV_INDEX_LOCATION=
- EV_OPEN_PARTITION=
- EV_READY_PARTITIONS=
- EV_CLOSED_PARTITIONS=
- EV_FINGERPRINT_DB=
- EV_VAULT_STORE_DB=

6 If this client is the last client, click **OK**.

Adding a client is the last step in creating a new Enterprise Vault policy.

About features provided by Enterprise Vault for a backup provider

This chapter includes the following topics:

- [About Enterprise Vault quiescence before a backup](#)
- [About quiescing and unquiescing Enterprise Vault services](#)
- [About granular quiescence](#)
- [About managing safety copies and backups](#)
- [About the partition secure notification file](#)
- [About the archive bit](#)

About Enterprise Vault quiescence before a backup

To back up an Open partition or Index location, Enterprise Vault needs to be quiesced before the backup job starts. The way quiescence is achieved in Enterprise Vault 7.5 is different from how it is achieved in Enterprise Vault 8.0 and later.

Note: Enterprise Vault uses three terms to define quiescence. Those three terms are read-only mode, backup mode, and quiescence. These terms are used interchangeably in reference to Enterprise Vault.

For Enterprise Vault 7.5, the following applies when NetBackup quiesces Enterprise Vault:

- Quiescence always happens at the Enterprise Vault server level. For example, if only one vault store needs to be backed up, the entire Enterprise Vault server is put into read-only mode.
- Whenever an Enterprise Vault server is put into read-only mode, there are four services that are put into read-only mode. The following list shows the names of the Enterprise Vault services that are quiesced:
 - The Task Controller Service
 - The Storage Service
 - The Indexing Service
 - The Shopping Service
- When an Enterprise Vault server is put into read-only mode, you can access the data, however you cannot archive any data. Even if only one open partition is backed up the archiving cannot not happen in any of the vault stores in the Enterprise Vault server.

See [“About quiescing and unquiescing Enterprise Vault services”](#) on page 50.

In Enterprise Vault 8.0 or later a more granular method to quiesce Enterprise Vault components is used.

See [“About granular quiescence”](#) on page 51.

About quiescing and unquiescing Enterprise Vault services

In Enterprise Vault 8.0 or later, quiescing and unquiescing is done at the component level.

See [“About granular quiescence”](#) on page 51.

In Enterprise Vault 7.5, the mechanism to quiesce and unquiesce is performed at the Enterprise Vault server level through the following Enterprise Vault registry keys:

- EnableArchive
- EnableCrawler
- EnableExpiry
- EnableFileWatch
- EnablePSTMigrations
- EnableReplayIndex

■ EnableRestore

The locations of the Enterprise Vault registry keys are as follows:

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

The following lists provide a high-level overview of how to quiesce or unquiesce the Enterprise Vault services.

- To quiesce the Enterprise Vault services, stop the Enterprise Vault services, create the special Enterprise Vault registry keys, and restart the services. Make sure that you create the Enterprise Vault registry keys with a value of zero.
- To unquiesce the Enterprise Vault services, stop the Enterprise Vault services, delete the special Enterprise Vault registry keys, and restart the services.

Multiple quiescent and unquiescent jobs can run on the same Enterprise Vault server. Therefore, NetBackup uses a registry counter (NBU_EV_QSE_LEVEL) to track the number of times the Enterprise Vault services are put into read-only mode. If the value of this counter is zero, the Enterprise Vault services are running in a read-write mode. If value of this counter is non-zero, then the Enterprise Vault services are running in a read-only mode.

Note: Incorrect use of the Windows registry editor may prevent the operating system from functioning properly. You should be very careful when making changes to a Windows registry. Only those who have experience with the registry editor application should attempt to modify the registry. Symantec recommends that you make a complete backup of the registry and workstation before you make any registry changes.

The location of this registry counter is one of the following addresses:

- HKEY_LOCAL_MACHINE\SOFTWARE\KVS\Enterprise Vault\NetBackup
- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KVS\Enterprise Vault\NetBackup

About granular quiescence

Enterprise Vault 8.0 or later supports the ability to set the backup mode at all levels. However, NetBackup 7.1 or the later version sets the backup mode only at the vault store and the Index location level.

The ability to set the backup mode at the vault store and Index location level ensures that the following happens during a backup:

- While one vault store is put into a backup mode, any other vault store in the Enterprise Vault site can continue to archive. When the backup mode is set on a vault store its content can be retrieved. However, the vault store cannot archive new content until the backup mode is cleared.
- When the backup mode is set for an index location backup, no new indexes are created on that index location until the backup mode is cleared.
- When NetBackup sets the backup mode, Enterprise Vault uses three services internally. These services need to remain up on all Enterprise Vault servers in the Enterprise Vault site during the backup. The following is a list of the three Enterprise Vault services that must remain running during the backup:
 - Directory service
 - Storage service
 - Index service

If a backup job fails and the vault store or index location continues to be in backup mode, you can use the Enterprise Vault Administration Console or the PowerShell `cmdlets` to set and clear the backup mode for the following:

- Vault stores
See the *Symantec Enterprise Vault Administrator's Guide* for additional information.
- Index locations
If you use the Enterprise Vault Administration Console, remember to refresh the console before and after you set or clear the backup mode.
See the *Symantec Enterprise Vault Administrator's Guide* for additional information.

Note: The Enterprise Vault 9.0 and later versions supports atomicity for quiescence.

About managing safety copies and backups

Enterprise Vault manages safety copies based on partition backups. After a partition backup finishes, the backup product informs Enterprise Vault that the backup has completed successfully. Enterprise Vault then deletes the safety copy. Enterprise Vault accepts notification from the backup product through the partition secure notification file or by the archive bit of the files in the partition.

You can configure Enterprise Vault to accept either method of notification to determine if the files in the partition have been backed up.

See [“About the partition secure notification file”](#) on page 53.

See [“About the archive bit ”](#) on page 53.

About the partition secure notification file

Enterprise Vault 8.0 or greater supports a trigger file mechanism for managing safety copies by enabling the Check for a trigger file option. Enterprise Vault determines whether the archived data in a vault store partition has been backed up. It checks for a trigger file in the partition root directory.

- See, "Using the trigger file mechanism" in the *Symantec Enterprise Vault Administrator's Guide*.
- See, "Managing safety copies " in the *Symantec Enterprise Vault Administrator's Guide*.

After a successful backup of an Enterprise Vault 8.0 or greater partition (open, closed, or ready partition), NetBackup creates a `PartitionSecuredNotification.xml` file and stores it in that partition's root directory. The creation of the `PartitionSecuredNotification.xml` file is not dependent on how Enterprise Vault is configured. NetBackup always creates the file.

The `PartitionSecuredNotification.xml` file contains a vendor name, vendor application type, and a timestamp. Timestamp written in the trigger file is for the following:

- Snapshot-based backups: The time before the snapshot is created.
- Non-snapshot-based backups: The time before the backup (backup part of the entire job) job is started.

The backup creates the `PartitionSecuredNotification.xml` the file that is then backed up in subsequent backups.

When preparing to restore an open, closed, or ready partition, you should ensure that you do not select the `PartitionSecuredNotification.xml` file to be restored.

About the archive bit

The Enterprise Vault 7.5 and later versions use the archive attribute option as a way to support managing safety copies. When the bit is cleared, Enterprise Vault considers the file to be backed up and any corresponding safety copies are removed.

The NetBackup Enterprise Vault agent resets the archive bit on the files that were backed up in FULL and DIFFERENTIAL schedules.

A cumulative incremental backup does not reset the archive bit of an object that is included for backup. In addition, if a cumulative-incremental backup is run after a differential-incremental backup completes (and the archive bit is reset), the cumulative-incremental backup does not include the files that were backed up in the differential-incremental backup.

If the Enterprise Vault vault store is configured with the, **Remove safety copies after backup**, option set, and the Enterprise Vault partition that is configured with the **Use the archive attribute** setting for a backup, then the archive file (safety copy) delete does not occur after a cumulative-incremental backup.

Performing backups of Enterprise Vault

This chapter includes the following topics:

- [About Enterprise Vault directives and what data they back up](#)
- [Manually backing up Enterprise Vault resources](#)
- [Canceling an Enterprise Vault backup job from the Activity Monitor](#)

About Enterprise Vault directives and what data they back up

When you create a policy to back up Enterprise Vault data, you choose the directive based on the data that you want to back up. In addition, the data that you back up also depends on the client(s) that you select in the policy. The following tables identify each of the available Enterprise Vault directives for Enterprise Vault 7.5 and Enterprise Vault 8.0 or later versions. Finally, a brief summary is provided that describes the data that is backed up when that particular directive is selected.

Note: Symantec recommends that you create Enterprise Vault policies with the directives that do not back up the same Enterprise Vault data. For example, an Enterprise Vault 7.5 backup policy with the EV_SITE directive can back up the same data as a backup policy with the EV_SERVER directive. In this case, running the Enterprise Vault backup policy that is configured with the EV_SERVER directive is not necessary.

[Table 5-1](#) shows the Enterprise Vault 7.5 directives. With each of these directives you can assume that a policy client is specified and each directive applies to full,

differential, and cumulative backups. In addition, Enterprise Vault 7.5 supports multiple policy clients (except for the EV_VAULT_STORE_DB= directive).

Table 5-1 Enterprise Vault 7.5 directives and what they back up

Directive (backup selection)	Description
EV_DIR_DB (directory database)	<p>The directory database is an SQL database that contains configuration information.</p> <ul style="list-style-type: none"> ■ Use this directive to back up the directory database of the Enterprise Vault site that the policy client belongs to. ■ The directory database does not need to be hosted on the policy client. ■ This database is known as a site-level database.
EV_MONITORING_DB (monitoring database)	<p>The monitoring database is an SQL database that is associated with the Enterprise Vault monitoring service. This database typically contains performance and trend information about Enterprise Vault activities.</p> <ul style="list-style-type: none"> ■ Use this directive to back up the monitoring database of the Enterprise Vault site that the policy client belongs to. ■ The monitoring database does not need to be hosted on the policy client. ■ This database is known as a site-level database.
EV_INDEX_LOCATION (Enterprise Vault index locations)	<p>Use this directive to backup Enterprise Vault index locations. You can use any backup schedule with this directive.</p> <ul style="list-style-type: none"> ■ Use this directive to back up the index locations that are specific to the Enterprise Vault server alias.
EV_VAULT_STORE (Enterprise Vault, vault store)	<p>An Enterprise Vault, vault store consists of one or more Partitions and the vault store database. The EV_VAULT_STORE directive enables you to backup data of all vault stores that are specific to the Enterprise Vault server alias.</p> <ul style="list-style-type: none"> ■ Use this directive to back up the data that belongs to each vault store. That includes all partitions and their corresponding vault store databases. ■ The vault store database can be hosted on a different system.
EV_VAULT_STORE= <i>EV Vault Store name</i> (Enterprise Vault, vault store)	<p>An Enterprise Vault, vault store consists of one or more Partitions and the vault store database. Use this directive to back up a particular vault store for a specific Enterprise Vault server that you defined in the policy.</p> <ul style="list-style-type: none"> ■ Use this directive to back up all Enterprise Vault partitions in a particular vault store along with a corresponding vault store database. ■ If <i>EV Vault Store name</i> is not specified, the job fails. ■ The vault store database can be hosted on a different system.

Table 5-1

Enterprise Vault 7.5 directives and what they back up *(continued)*

Directive (backup selection)	Description
EV_OPEN_PARTITIONS (open partition) and EV_CLOSED_PARTITIONS (closed partition)	<p>Open and closed partitions store Enterprise Vault archives. They can be present on NTFS file system or NAS devices. Each partition is in either an open state or a closed state. Use the closed partition directive to back up all closed partitions present on the Enterprise Vault server alias. Use the open partition directive to back up all open partitions present on Enterprise Vault server A. In addition, when an open partition is backed up, the corresponding vault store database is also backed up.</p> <p>You can use any backup schedule with either of these directives.</p> <p>For open partitions:</p> <ul style="list-style-type: none"> ■ All open partitions that are hosted on the policy client along with the corresponding vault store database are backed up. ■ Each backed up open partition is part of one vault store that is hosted on the policy client. <p>For closed partitions:</p> <ul style="list-style-type: none"> ■ All closed partitions that are hosted on the policy client are backed up. ■ Each backed up closed partition is part of one vault store that is hosted on the policy client.
EV_VAULT_STORE_DB (Enterprise Vault, vault store database)	<p>The Enterprise Vault, vault store database is an SQL database that can contain metadata about the vault store and archived data.</p> <p>The EV_VAULT_STORE_DB directive enables you to back up all vault store databases for a specific Enterprise Vault server that you defined in the policy.</p> <p>You can use any backup schedule with this directive.</p> <ul style="list-style-type: none"> ■ All of the vault store databases that correspond to the vault stores that the policy client hosts are backed up. ■ The vault store databases can be hosted on a different system.

Table 5-1 Enterprise Vault 7.5 directives and what they back up (*continued*)

Directive (backup selection)	Description
EV_VAULT_STORE_DB= <i>EV Vault Store name</i> (Enterprise Vault, vault store)	<p>The Enterprise Vault, vault store database is an SQL database that can contain metadata about the vault store and archived data.</p> <p>Use this directive to back up a vault store database of a particular vault store for an Enterprise Vault server that you defined in the policy.</p> <p>You can use any backup schedule with this directive.</p> <ul style="list-style-type: none"> ■ The Enterprise Vault vault store database of the specified <i>Vault Store name</i> that is hosted on the policy client is backed up. ■ The vault store databases can be hosted on a different system. ■ This directive does not support multiple policy clients in the client list. ■ If <i>Vault Store name</i> is not specified, the job fails. <p>Note: The <i>vault store name</i> is the vault store name and not the vault store database name.</p>
EV_SERVER (Enterprise Vault server)	<p>An Enterprise Vault server can consist of multiple Vault stores, multiple index locations. Select this directive when you want to back up all of the Enterprise Vault data that is a part of a particular Enterprise Vault server . You can use any backup schedule with this directive.</p> <ul style="list-style-type: none"> ■ All index locations and vault stores (similar to EV_VAULT_STORE) that are hosted on the policy client get backed up.
EV_SITE (Enterprise Vault site)	<p>An Enterprise Vault site can contain multiple Enterprise Vault servers. Select this directive when you want to back up multiple pieces of data from various locations. You can use any backup schedule with this directive.</p> <ul style="list-style-type: none"> ■ Use this directive to back up all index locations and vault stores (similar to EV_VAULT_STORE) that any Enterprise Vault server hosts in the Enterprise Vault site that the policy client belongs to.

[Table 5-2](#) shows the Enterprise Vault 8.0 or later directives. In the following table a policy client has been specified and each directive applies to full, differential, and cumulative backups. In addition, Enterprise Vault 8.0 supports multiple policy clients (except for the EV_VAULT_STORE_DB=, EV_OPEN_PARTITION=, EV_READY_PARTITIONS=, EV_CLOSED_PARTITIONS=, EV_FINGERPRINT_DB=, and EV_VAULT_STORE_DB= directives).

Table 5-2 Enterprise Vault 8.0 or later directives and what they back up

Directive (backup selection)	Description
EV_DIR_DB	<p>The directory database is an SQL database that contains configuration information.</p> <ul style="list-style-type: none"> ■ Use this directive to back up the directory database of the Enterprise Vault site that the policy client belongs to. ■ The directory database does not need to be hosted on the policy client. ■ This database is known as a site-level database. ■ This directive supports multiple policy clients in the client list. You should add multiple clients when multiple Enterprise Vault sites have their own directory database. ■ You cannot use this directive with the EV_INDEX_LOCATION= and the EV_OPEN_PARTITION= directives.
EV_MONITORING_DB	<p>The monitoring database is an SQL database that is associated with the Enterprise Vault monitoring service. This database typically contains performance and trend information about Enterprise Vault activities.</p> <ul style="list-style-type: none"> ■ Use this directive to back up the monitoring database of the Enterprise Vault site that the policy client belongs to. ■ The monitoring database does not need to be hosted on the policy client. ■ This database is known as a site-level database. ■ This directive supports multiple policy clients in the client list. You should add multiple clients when multiple Enterprise Vault sites have their own monitoring database.
EV_AUDIT_DB	<p>The auditing database only exists if Enterprise Vault auditing is enabled. The audit database contains audit records of various configurable Enterprise Vault operations.</p> <p>Use this directive to back up the auditing database in the Enterprise Vault deployment if you have Audit enabled. This option is disabled by default.</p> <ul style="list-style-type: none"> ■ The auditing database does not need to be hosted on the policy client. ■ This directive supports multiple policy clients in the client list. You should add multiple clients when multiple Enterprise Vault sites have their own auditing database.

Table 5-2 Enterprise Vault 8.0 or later directives and what they back up
(continued)

Directive (backup selection)	Description
EV_FSAREPORTING_DB	<p>The FSA Reporting database only exists if FSA Reporting has been configured. The FSA Reporting database contains a history of the active and the archived files on the file servers. This data is used to track trends and as a summary of the archived files and active files on file servers.</p> <p>Use this directive to back up the FSA Reporting database in the Enterprise Vault deployment if you have FSA Reporting enabled. This option is disabled by default.</p> <ul style="list-style-type: none"> ■ The FSA Reporting database does not need to be hosted on the policy client. ■ This directive supports multiple policy clients in the client list. You should add multiple clients when multiple Enterprise Vault sites have their own FSA Reporting database.
EV_INDEX_LOCATION= <i>Site name</i>	<p>Use this directive to back up all index locations in the Enterprise Vault site, that the <i>Site name</i> variable specifies. You can use any backup schedule with this directive.</p> <ul style="list-style-type: none"> ■ You cannot use this directive with the EV_DIR_DB directive. ■ This directive does not support multiple policy clients in the client list. ■ If <i>Site name</i> is not specified, the job fails.
EV_OPEN_PARTITION= <i>Vault Store name</i>	<p>The open partition directive backs up the open partition and Vault Store database of the Vault Store that you specify when you define the <i>Vault Store name</i>. The partition can be present on NTFS file system or NAS devices.</p> <p>You can use any backup schedule with this directive.</p> <p>For open partitions:</p> <ul style="list-style-type: none"> ■ You cannot use this directive with the EV_DIR_DB directive. ■ This directive does not support multiple policy clients in the client list. ■ If <i>Vault Store name</i> is not specified, the job fails. <p>Note: For the streamer-based open partitions, do not use this directive as the backup would succeed partially. Instead, use the EV_VAULT_STORE_DB directive.</p>

Table 5-2 Enterprise Vault 8.0 or later directives and what they back up
(continued)

Directive (backup selection)	Description
EV_CLOSED_PARTITIONS= <i>Vault Store name</i>	<p>The closed partitions directive backs up any closed partitions of the Vault Store that you specify when you define the <i>Vault Store name</i>. The partitions can be present on NTFS file system or NAS devices.</p> <p>You can use any backup schedule with this directive.</p> <p>For closed partitions:</p> <ul style="list-style-type: none"> ■ This directive does not support multiple policy clients in the client list. ■ If <i>Vault Store name</i> is not specified, the job fails. <p>Note: Do not use this directive for streamer based closed partitions. If some closed partitions are streamer-based , the job is completed, but the data is not backed up by NBU. If all close partitions are streamer-based the job fails.</p>
EV_READY_PARTITIONS= <i>Vault Store name</i>	<p>The ready partitions directive backs up the ready partitions of the Vault Store that you specify when you define the <i>Vault Store name</i>. The partitions can be present on NTFS file system or NAS devices.</p> <p>You can use any backup schedule with this directive.</p> <p>For ready partitions:</p> <ul style="list-style-type: none"> ■ This directive does not support multiple policy clients in the client list. ■ If <i>Vault Store name</i> is not specified, the job fails. <p>Note: Do not use this directive for the streamer-based ready partitions. If some ready partitions are streamer-based , the job is completed but the data is not backed up by NBU. If all ready partitions are streamer-based the job fails.</p>
EV_VAULT_STORE_DB= <i>Vault Store name</i>	<p>The Enterprise Vault, vault store database is an SQL database that can contain metadata about the vault store and archived data.</p> <p>Use this directive to back up the vault store database that the <i>Vault Store name</i> variable specifies in the Enterprise Vault deployment.</p> <p>You can use any backup schedule with this directive.</p> <p>The following applies for this directive:</p> <ul style="list-style-type: none"> ■ The vault store databases can be hosted on a different system. ■ This directive does not support multiple policy clients in the client list. ■ If <i>Vault Store name</i> is not specified, the job fails. <p>Note: The <i>vault store name</i> is the vault store name and not the vault store database name.</p>

Table 5-2

Enterprise Vault 8.0 or later directives and what they back up

(continued)

Directive (backup selection)	Description
EV_FINGERPRINT_DB= Vault Store Group name	<p>The fingerprint database contains information about archived data in Vault Store Partitions. Use this directive to back up the fingerprint database that is associated with the supplied Vault Store Group. The Enterprise Vault agent can discover multiple fingerprint databases when a Vault Store Group is configured to support multiple fingerprint databases.</p> <p>You can use any backup schedule with this directive.</p> <p>The following applies for this directive:</p> <ul style="list-style-type: none">■ The fingerprint database can be hosted on a different system.■ The job fails if the Vault Store group name is not specified.■ This directive does not support multiple policy clients in the client list.

Manually backing up Enterprise Vault resources

Enterprise Vault backups can run automatically if you specify a time period within an Enterprise Vault backup policy. However, there are instances when you want to start a backup manually based on an existing Enterprise Vault backup policy. You can initiate a manual Enterprise Vault backup from the NetBackup Administration Console.

See [“To run an Enterprise Vault backup manually”](#) on page 62.

Note: User-directed backups are not supported.

To run an Enterprise Vault backup manually

- 1 Log onto the NetBackup server as Administrator.
- 2 Select, **Start > Programs > Symantec NetBackup > NetBackup Administration Console**.
- 3 Expand **Policies** in the left pane of the NetBackup Administration Console. Existing policies appear.
- 4 Select the policy that you want to run. The right pane displays the policy configuration information for the policy that you select.
- 5 Right-click on the policy and select the **Manual Backup** option, or click the **Manual Backup** icon on the toolbar at the top of the NetBackup Administration Console.

- 6 Select the schedule and one or more of the clients to start the backup from the **Manual Backup** dialog box.
- 7 Click **OK** to begin the backup.

Canceling an Enterprise Vault backup job from the Activity Monitor

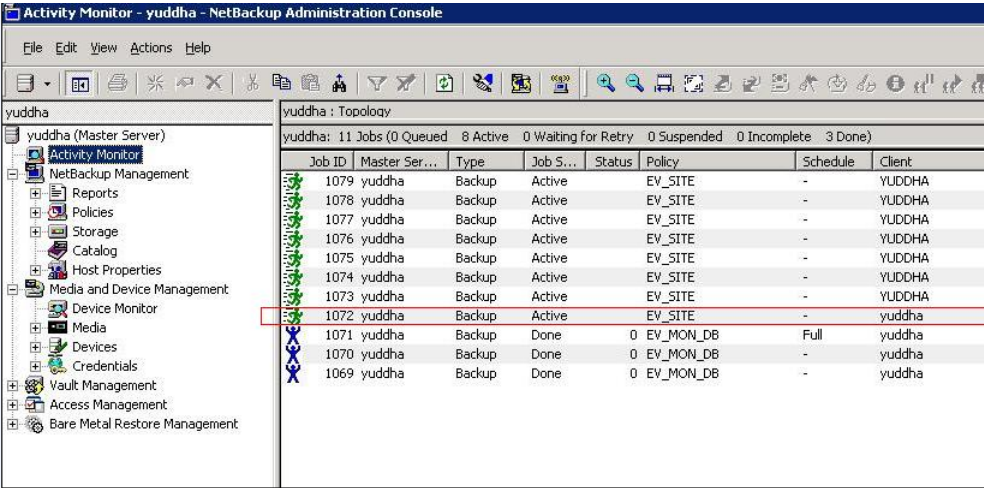
You can cancel an Enterprise Vault backup from the NetBackup Activity Monitor. If you choose to cancel a backup job, you should understand that the following applies:

- When you choose to cancel an Enterprise Vault agent job, all child jobs are canceled. The selected job is canceled along with any sibling, active or queued job. If a parent job exists, it waits for all of the children jobs to get canceled and then the status of the parent becomes canceled. The status of the sibling jobs that completed before the cancel request does not change and you can use their image for a restore.
- If you choose to cancel a full backup that involves an Enterprise Vault SQL database (such as a directory database), then you must make sure that you exit that back up. Then you must make sure that you take a full backup before you start the next cumulative backup.

To cancel an Enterprise Vault backup job from the Activity Monitor

- 1 Log on to the master server as administrator. Start the NetBackup Administration Console.
- 2 Click **Activity Monitor**.
- 3 Select the first job of the backup that you want to cancel
[Figure 5-1](#) shows a job that has been selected to be canceled.
- 4 Right-click on the selected job and select **Cancel Job**.

Figure 5-1 Job selection in the Activity Monitor for job cancellation



Performing restores of Enterprise Vault

This chapter includes the following topics:

- [Important notes about Enterprise Vault data restore](#)
- [Stopping the administrative services on Enterprise Vault servers](#)
- [About the Backup, Archive, and Restore interface](#)
- [Viewing backup data using the Microsoft SQL Server Management Studio](#)
- [Restoring Enterprise Vault data](#)
- [About the Enterprise Vault restore options on the General tab](#)
- [About the Enterprise Vault Database Settings tab](#)
- [Specifying the server, clients, and policy type for restores](#)
- [About restoring Enterprise Vault file system data](#)
- [Restoring an Enterprise Vault file system component](#)
- [About restoring Enterprise Vault SQL databases](#)
- [Restoring Enterprise Vault SQL database components](#)

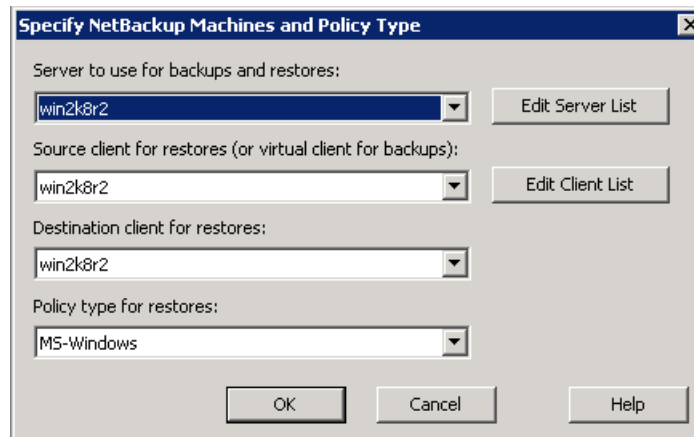
Important notes about Enterprise Vault data restore

The Backup, Archive, and Restore user interface is used to restore Enterprise Vault data. You can restore any type of Enterprise Vault data from the Backup, Archive, and Restore user interface whose backup was taken from Enterprise Vault agent policy.

Review the following before you begin an Enterprise Vault restore:

- The destination client for Enterprise Vault file system data restore should have the same version of Enterprise Vault installed as the client from where Enterprise Vault was backed up.

From the Backup, Archive, and Restore interface, you can change the destination client and policy type. Select **File > Specify NetBackup Machine and Policy Type** and make the necessary adjustments to the options in this dialog box as shown in the following image.



- When you perform a disaster recovery of Enterprise Vault data, restore the directory database first. After you successfully restore the directory database, you can restore other Enterprise Vault components and partitions.
- Symantec recommends that you restore the vault store database when you attempt to restore an open partition. In addition, you should restore the open partition when you attempt to restore the vault store database.
- Symantec recommends that you restore individual components of Enterprise Vault one at a time.
- For Enterprise Vault 7.5 or later, you must stop all Enterprise Vault services on Enterprise Vault servers when performing a restore.

See [“Stopping the administrative services on Enterprise Vault servers”](#) on page 67.

When you restore Enterprise Vault data you select the backup images that are displayed in the Backup, Archive, and Restore interface. These images are for Enterprise Vault file system data or Enterprise Vault SQL databases.

See [“About the Backup, Archive, and Restore interface”](#) on page 67.

See [“Restoring Enterprise Vault SQL database components”](#) on page 82.

See [“Restoring an Enterprise Vault file system component”](#) on page 77.

Stopping the administrative services on Enterprise Vault servers

The following describes how to stop the Administrative services on Enterprise Vault servers before you attempt a restore:

To stop the administrative services on Enterprise Vault servers

- 1 Click **Start > Programs > Administrative Tools > Services**
- 2 From the **Services** page, select and stop each Enterprise Vault service.

About the Backup, Archive, and Restore interface

The Backup, Archive, and Restore interface consists of three primary panes that enable you to select the images that you want to restore. The three panes are the **NetBackup History** pane, the **All Folders** pane, and the **Contents** pane. The **NetBackup History** pane displays the backup images that are available for restore, the type of backup that was performed, and the policy name. The **All Folders** pane displays a hierarchal view of the items that are available to restore. This pane updates after you select an image in the **NetBackup History** pane. The **Contents** pane displays the file(s) that correspond to the selection that you make in the **All Folders** pane.

In the **NetBackup Administration Console**, in the toolbar, select **File > Backup, Archive, and Restore** to open the Backup, Archive, and Restore interface. Click the **Select for Restore** option to view the contents.

The interface also displays information about the backups that have been run. You can then select the backup images that you want to restore. However, it can be difficult to locate a particular restore set for the SQL images and the number of associated images for each restore set. One reason is because the interface does not show the database names. You would have to look at each image in the interface and expand each one to see the database name. This method is cumbersome, time consuming, and often confusing for the user.

The Backup, Archive, and Restore interface contains a search feature that enables you to search for an object in the backup images to restore. To begin a search, select some images from the **History** pane and click on the search (binocular) icon in the interface. A **Search Backups** dialog box appears with the Start and End dates updated to match the dates that you chose. Enter a keyword in a regular expression format in the **Search Folder** field. For example, enter `*All Partitions*` to search for images with "All Partitions" as an object name. You can also enter a word or phrase in the Keyword Phrase field. After you enter the appropriate information, click **Search**.

If the images that you selected contain an object that matches the keyword you entered, then the interface displays the content of that image.

Note: You can also begin a search using the Search for Items to Restore (binocular) icon. When the **Search Backups** dialog box opens, enter a search folder, a keyword, and a Start and an End date.

Viewing backup data using the Microsoft SQL Server Management Studio

By using the **Microsoft SQL Server Management Studio** and a specific query, you can view various SQL backup image information from the output of the query. The output contains database names, the backup start and finish date, and the backup type (FULL, CUMULATIVE, and DIFFERENTIAL). This query enables you to easily determine the backups for a database and then use the BAR user interface to select and restore those images.

Figure 6-1 shows a sample output of a backup set.

Figure 6-1 Sample output of a backup set

Results		Messages			
	Server	database_name	backup_start_date	backup_finish_date	backup_type
1	RON\NITINDB	EnterpriseVaultDirectory	2008-10-10 15:07:08.000	2008-10-10 15:07:10.000	Database
2	RON\NITINDB	EnterpriseVaultDirectory	2008-10-10 15:09:23.000	2008-10-10 15:09:23.000	Database
3	RON\NITINDB	EnterpriseVaultDirectory	2008-10-11 16:39:41.000	2008-10-11 16:39:42.000	Database
4	RON\NITINDB	EnterpriseVaultDirectory	2008-10-12 00:20:35.000	2008-10-12 00:20:35.000	Log
5	RON\NITINDB	EnterpriseVaultDirectory	2008-10-22 19:35:33.000	2008-10-22 19:35:34.000	Database
6	RON\NITINDB	EnterpriseVaultDirectory	2008-11-05 12:09:39.000	2008-11-05 12:09:40.000	Database
7	RON\NITINDB	EnterpriseVaultDirectory	2008-11-05 12:14:58.000	2008-11-05 12:14:59.000	Database
8	RON\NITINDB	EnterpriseVaultDirectory	2008-11-05 13:55:05.000	2008-11-05 13:55:05.000	Database
9	RON\NITINDB	EnterpriseVaultDirectory	2008-11-05 14:11:54.000	2008-11-05 14:11:55.000	Database
10	RON\NITINDB	EnterpriseVaultDirectory	2008-11-05 14:44:54.000	2008-11-05 14:44:54.000	Database
11	RON\NITINDB	EnterpriseVaultDirectory	2008-11-05 19:38:29.000	2008-11-05 19:38:30.000	Database
Query executed successfully.			RON\NITINDB (9.0 RTM)	RON\Administrator (75)	master 00:00:01 352 rows

To view backup information using the Microsoft SQL Server Management Studio.

- 1 Open the **Microsoft SQL Server Management Studio**.
- 2 Click **New Query**.

3 Enter the following query

```
Select

    CONVERT (CHAR (100), SERVERPROPERTY ('Servername')) AS Server,

    msdb.dbo.backupset.database_name,

    msdb.dbo.backupset.backup_start_date,

    msdb.dbo.backupset.backup_finish_date,

    CASE msdb..backupset.type

        WHEN 'D' THEN 'Database'

        WHEN 'L' THEN 'Log'

        WHEN 'I' THEN 'Differential'

    END AS backup_type

FROM    msdb.dbo.backupmediafamily

        INNER JOIN msdb.dbo.backupset ON

msdb.dbo.backupmediafamily.media_set_id =

msdb.dbo.backupset.media_set_id

ORDER BY

    msdb.dbo.backupset.database_name,

    msdb.dbo.backupset.backup_start_date
```

4 Click **Execute**.

Restoring Enterprise Vault data

Enterprise Vault is a distributed application that can store archived data at different locations. When you restore Enterprise Vault data, you can restore Enterprise Vault file system data or Enterprise Vault SQL databases. Enterprise Vault file system data consists of Enterprise Vault indexes, open partition, closed partitions, or ready partitions. Examples of Enterprise Vault SQL database information are Enterprise Vault directory database, a monitoring database, or a vault store database. The following procedure describes how to restore Enterprise Vault data.

To restore Enterprise Vault data

- 1 Open the Backup, Archive, and Restore interface and log on as Administrator.
- 2 Select **File > Specify NetBackup Machines and Policy Type**.
- 3 Select the **Enterprise-Vault** policy type in the **Policy type for restores** drop-down list.
- 4 Click **OK**. NetBackup browses for Enterprise Vault backup images.
- 5 From the **NetBackup History** pane, select the image(s) that contain the objects you want to restore.
- 6 In the **All Folders** pane, expand **Enterprise Vault Resources**.
- 7 Select the object(s) to restore.
- 8 Choose **Actions > Restore**.
- 9 In the **Restore Marked Files** dialog box, make selections on the two tabbed pages depending on what you want to restore.
 - If you want to restore Enterprise Vault file system data, update the **General** tab.
See [“About the Enterprise Vault restore options on the General tab”](#) on page 70.
 - If you want to restore Enterprise Vault SQL database, update the **Enterprise Vault Database Settings** tab.
See [“About the Enterprise Vault Database Settings tab”](#) on page 71.
- 10 Click **Start Restore**.

About the Enterprise Vault restore options on the General tab

The **General** tab is used to specify options during a restore or a redirect operation of Enterprise Vault File System (FS) components. You first select the components that you want to restore from the Enterprise Vault restore user interface. You can then restore these selections to the same location from where the backup was performed, or to a different location that you designate.

[Table 6-1](#) describes the restore options, including the restore destination options on the **General** tab.

Table 6-1 Lists the restore options on the **General** tab

Option	Description
Restore everything to its original location	Restores the selected items to the same location from which they were backed up. This option is the default option.
Restore everything to a different location	This option is disabled.
Restore individual folders and files to different locations	<p>Select this option to restore any selected Enterprise Vault file system data to different locations.</p> <p>The items you mark for restore appear in the Restore individual folders and files to different locations list box. When you select a folder for restore, that folder name appears in the list box (not the individual files in that folder). To restore individual files to different locations, select files individually.</p> <p>When you double-click on the source list, you see that content already exists. You should remove all of the existing content and then enter a physical path of a new destination in the Enter New Destination dialog box. You can also use the browse feature to browse for a new destination.</p> <p>Note: If you type a new destination in the Destination field, you must enter a valid physical path.</p> <p>NetBackup browses the local computer where the Backup, Archive, and Restore interface is running. NetBackup only browses the local computer, even if you chose to redirect a restore to a different client.</p> <p>You must provide or select a file name as the destination if you change the destination location of the file. For folders, the destination name is used as the folder name.</p> <p>See “About restoring Enterprise Vault file system data” on page 76.</p>
Create virtual disks and redirect to them	This option is disabled.
Overwrite existing file	Overwrites the existing files and folders. The default is not to overwrite.
Restore the file using a temporary file name	This option is disabled.
If the file exists, do not restore it	The default.

About the Enterprise Vault Database Settings tab

On Enterprise Vault **Database Settings** tab you can choose how you want to leave the Enterprise Vault SQL database after a restore job completes. You have the

option to leave the database operational, non-operational, or in a read-only state that enables you to still restore additional transaction logs. Also, you can perform an alternate SQL restore, a Point in time (PIT) restore, or a consistency check of the database after the restore completes.

Table 6-2 lists the restore options on the Enterprise Vault **Database Setting** tab.

Table 6-2 Enterprise Vault **Database Setting** tab options

Restore option	Description
Restore completion state	<p>After a restore completes, you can leave an SQL database in any of the following states:</p> <ul style="list-style-type: none">■ Operational■ Read-only■ Non-operational <p>To bring the Enterprise Vault SQL database to the required Point in time (PIT) or end-of-log (EOL), the SQL database restore consists of a set of restores. An example set of restores consists of the following:</p> <ul style="list-style-type: none">■ A FULL database restore■ The last CUMMULATIVE (database differential) restore■ One or more DIFFERENTIAL (transaction log) backups that were taken after the last cumulative backup <p>In other scenarios, the set of restores would require a subset of restores, such as a FULL or a FULL and cumulative restore. If the set contains incremental restores, the initial restores should leave the database in a “Restore pending” state so future restores append to the database. Thus, you should use the Leave database operational option only in the last restore job of the restore set. Once the database is brought online, the user cannot make any further cumulative or differential (database differential or transaction log) restores on that database. If you want to perform any further restores, you must start from a FULL database restore.</p> <p>Note: Given a PIT or EOL, the NetBackup SQL Agent has the capacity to find the SQL restore set (FULL, database differential, and transaction logs). However, the Enterprise Vault agent does not have this capability; therefore, the user must find and sequence the SQL restore set manually.</p>

Table 6-2 Enterprise Vault **Database Setting** tab options (*continued*)

Restore option	Description
Consistency check after restore	<p>You can check the consistency of the database after restores are complete.</p> <p>To check the consistency of the database, select one of the following consistency checks when you select the Leave database operational option:</p> <ul style="list-style-type: none"> ■ Full check, excluding indexes Select this option to exclude indexes from the consistency check. If indexes are not checked, the consistency check runs significantly faster but is not as thorough. Only the data pages and clustered index pages for each user table are included in the consistency check. The consistency of the nonclustered index pages is not checked. ■ Full check, including indexes Select this option to include indexes in the consistency check. Any errors are logged. This option is selected by default. ■ Physical check only (SQL 2000 only) Select this option to perform a low overhead check of the physical consistency of the SQL Server 2000 database. This option only checks the following: <ul style="list-style-type: none"> ■ The integrity of the physical structure of the page and record headers ■ The consistency between the pages' object ID and index ID ■ The allocation structures ■ None Select this option to ensure that no consistency check occurs after a restore. <p>Note: Any option other than None is effective only in the restore job that brings the database to an operational state.</p>
Point-in-time recovery	<p>To recover the Enterprise Vault SQL database to a PIT, select a restore set that includes the immediate DIFFERENTIAL (transaction log) backup after the PIT. In addition, while restoring this backup you must select the "PIT" option and specify the PIT.</p> <p>You must ensure that you use the PIT option only with the last differential backup restore. You must select the Leave database operational option in the user interface to enable you to select the PIT option.</p>
Redirected restore	<p>Select this option and specify the new <SQL INSTANCE\SQL database name > to restore to an alternate client, alternate SQL instance, or alternate SQL database. You must do that for each restore in the restore set. The destination SQL database should not be present. If it is present, a chance of data loss in the destination database is possible.</p> <p>Note: You can change the <i>SQL INSTANCE</i> name, however do not change the <i>SQL database name</i>. If you change the <i>SQL database name</i> Enterprise Vault does not automatically recognize the new name. If you chose to change the <i>SQL database name</i> then you must also update your Enterprise Vault configuration.</p> <p>Note: A redirected restore of an auditing database must be made to the same SQL instance where the directory database resides.</p>

Table 6-2 Enterprise Vault **Database Setting** tab options (continued)

Restore option	Description
Take database offline	Select this option to disconnect all the connections to the destination SQL database (including Enterprise Vault connections) before it is restored. You should use this option only with the full restore .

Specifying the server, clients, and policy type for restores

To restore Enterprise Vault data, use the **Backup, Archive, and Restore** user interface. You must specify the NetBackup server along with the source client and the destination client to perform the restore operation.

A restore of Enterprise Vault data generally involves redirected restores. Similarly to how SQL backups occur, Enterprise Vault backups are cataloged against the Enterprise Vault server and should be restored to the SQL host. In addition, there can be other Enterprise Vault components that are cataloged against an Enterprise Vault server but the restore should happen to a different Enterprise Vault server. How to interpret the destination client from the backup view is explained later in this chapter. To perform redirected restores NetBackup requires additional steps then those in this topic. refer to the "To allow all clients to perform redirected restores" topic in the *NetBackup Administrator's Guide for Windows, Volume I*.

Note: To browse the Enterprise Vault Administration Console for a destination client, the Enterprise Vault services must be up and running. You should know the destination client name before you start a restore because you must stop those services on all Enterprise Vault servers for a restore.

To specify the server, source client, destination client, and policy type for a restore operation

- 1 Log on as Administrator.
- 2 Open the Backup, Archive, and Restore user interface.
- 3 Click **File > Select Files and Folders to Restore > from Normal Backup**.
- 4 Click **File > Specify NetBackup Machines and Policy Type**.
- 5 In the **Specify NetBackup Machines and Policy Type** dialog box, select the server that you want to use for restores from the **Server to use for backups and restores** list.

- 6 From the **Source client for restores** list, select the source client. The source client is the policy client in the backup policy from where the backup happened.
- 7 From the **Destination client for restores** list, select the client that you want. The destination client is the name of the system where you want the images to be restored. You can determine the name of the destination client from either the NetBackup Backup, Archive, and Restore user interface or the Enterprise Vault Administration Console.

You interpret the destination client based on the version of Enterprise Vault and the data type that you want to restore. The following explains how to determine the destination client of a file system or SQL data type on either Enterprise Vault 7.5 or 8.0 and later.

- Interpreting the destination client for Enterprise Vault 7.5
 - File system data type, such as an Index location or an open or a closed partition
From the NetBackup Backup, Archive, and Restore user interface, expand the selected image to see the hierarchy of the Enterprise Vault resources so you can view the Enterprise Vault server. The destination client is displayed within the parenthesis along side the Enterprise Vault server. For example, a destination client named `CLIENT ONE`, is displayed as **EV server (CLIENT ONE)** in the hierarchy.
 - SQL data type, such as directory, monitoring, or vault store databases
The database name contains the system name in a format similar to `System name\SQL instance\SQL DB name`. For example, a vault store database on `CLIENT TWO`, would appear as **Vault Store DB (CLIENT TWO\SQLINST\database)**. The destination client name in this example is `CLIENT TWO`.
- Interpreting the destination client for Enterprise Vault 8.0 or later
 - File system data type in a local drive, such as an Index location or an open, closed, or ready partition
The root path of the partition that you want to restore contains the system name that you use as the destination client name. From the NetBackup Backup, Archive, and Restore user interface, you can view the partition or the index location that you want to restore. The root path of a partition or index location is shown within parenthesis along side the partition or the index location name. This root path uses the format, `\\system name\Drive$\partition name`. For example, a destination client named `VMWIN-X64` for a closed partition named `VS1 Ptn1` would appear as **VS1 Ptn1(\\VMWIN-X64\Drive\$\VS1 Ptn1)**.

- File system data type in a UNC path, such as an Index location or an open, closed, or ready partition
The UNC restore can use any Enterprise Vault server in an Enterprise Vault site as the destination client. That is possible because the data is automatically restored to its original location because the source path is embedded in the file path. You must make sure that the Enterprise Vault user name credentials for this Enterprise Vault server, has write permissions for this UNC path. The user name credentials are specified in the NetBackup client properties.
- SQL data type, such as directory, monitoring, auditing, FSA Reporting, fingerprint, or vault store databases
The database name contains the system name in a format similar to `System name\SQL instance\SQL DB name`. For example, a vault store database on `CLIENT TWO`, would appear as **Vault Store DB (CLIENT TWO\SQLINST(database))**. The destination client name in this example is `CLIENT TWO`.

- 8 From the **Policy type for restores** list, click **Enterprise-Vault**.
- 9 Click **OK**.

About restoring Enterprise Vault file system data

An Enterprise Vault file system component can be categorized as an Enterprise Vault index, an open partition, a closed partition, or a ready partition.

Review the following notes before you attempt to restore a file system component:

- The destination client for an Enterprise Vault file system data restore should have the same or higher version of Enterprise Vault installed as the client from where Enterprise Vault was backed up.
- The Backup, Archive, and Restore user interface does not prohibit you from selecting more than one component to restore. However, selecting more than one file system component for restore can result in a failed restore operation.
- When you restore Enterprise Vault file system data from one backup image, you can use any option in **Restore destination choices** field.
- When you restore Enterprise Vault file system data that consists of multiple images, the following applies:
 - You can restore data to the original location.
 - To restore data to an alternate location, you must use the **Restore individual folder and files** option.

- In the **Alternate restore options** dialog box, provide a physical path. However, the user interface displays an Enterprise Vault logical path representation. You must manually update this path to reflect the correct physical path of the alternate location.
- In the Backup, Archive, and Restore user interface, you can select one or more folders under the Index location; however you cannot select individual files inside an index folder. In addition, if you deselect an index location, all of the files that are contained within that location are also deselected.
- When you restore an open partition, you should also restore the vault store database if it is available.

Restoring an Enterprise Vault file system component

You can use the same procedure to restore an Enterprise Vault file system component such as an index location, an open partition, a closed partition, or a ready partition. When you restore an index location, you restore the index folders that reside in the hierarchy of that location. When you restore an open partition, you restore the selected physical store for the Enterprise Vault archives. An open partition can be an NTFS directory or an NAS device share and only one open partition can exist in a vault store. In addition, a vault store can contain one or more closed partitions that you can select to restore.

Use any of the following methods to restore Enterprise Vault file system data:

- Run the restore from the NetBackup master server.
- Run the restore from the system that hosted the Enterprise Vault file system data and also the NetBackup policy client for the Enterprise Vault file system data backup images.
- Run the restore from the system that hosted the Enterprise Vault file system data. However, this system was not the NetBackup policy client for the Enterprise Vault file system data backup images.

By default, a NetBackup client is not allowed to show the backup images where the policy client for those images is some other NetBackup client. In this case, you may have to add a **No Restriction File** on the NetBackup master server. That allows this NetBackup client to show and restore the backup images of Enterprise Vault file system data that were taken through another NetBackup client.

See the *NetBackup Administrator's Guide for Windows, Volume I* for more information about the **No Restriction File**.

To restore an Enterprise Vault component

- 1 Log on as administrator.
- 2 Stop the Enterprise Vault administrative services on all Enterprise Vault systems.

See [“Important notes about Enterprise Vault data restore”](#) on page 65.
- 3 Open the Backup, Archive, and Restore interface.
- 4 Click **File > Select Files and Folders to Restore > from Normal Backup**.
- 5 In the **Restore** window, select the **Enterprise-Vault** policy type (click **File > Specify NetBackup Machines and Policy Type**).
- 6 Click **OK**.
- 7 From the **NetBackup History** pane, select the image(s) that contain the objects that you want to restore and restore them in the following sequence:
 - The full backup image
 - The last cumulative image
 - The series of differential images that were taken after the last cumulative backup
- 8 In the **All Folders** pane, expand **Enterprise Vault Resources**.
- 9 Expand the Enterprise Vault file system components that you want to restore.
The following list provides examples of what you expand and select:
 - Expand **Index Locations** and select the Index folders that you want to restore.
 - Expand **EV Vault Store > All Partitions** and select the open partition that you want to restore.
 - Expand **EV Vault Store > All Partitions** and select the closed partition(s) that you want to restore.
 - Expand **EV Vault Store > All Partitions** and select the ready partition(s) that you want to restore.
- 10 Click **Actions > Restore**.
- 11 In the **Enterprise Vault Restore** dialog box, click the **General** tab and configure the various settings for your restore.
- 12 Click **Start Restore**.

- 13 Repeat steps 7 through 12 for each image that you select to restore.
- 14 After the restore, return to the Enterprise Vault servers that manages the restored Enterprise Vault file system data. Click **Start > Programs > Administrative Tools > Services** and restart the Enterprise Vault services on each of the Enterprise Vault servers.

About restoring Enterprise Vault SQL databases

You can categorize an Enterprise Vault SQL database component as one of the following databases:

- A directory database
- A monitoring database
- An FSA Reporting database
- An auditing database
- A fingerprint database
- A .NDF datafile
- A vault store database

Note: Restoring multiple Enterprise Vault images in one restore operation is not supported in this release. Symantec recommends that you restore one backup image at a time. Selecting multiple backup images in a single restore job may give unpredictable results.

Review the following notes before you attempt to restore an Enterprise Vault SQL database:

- Restore full and incremental backups one at a time.
- When you do a redirected restore, you must select the Redirected restore option and specify the alternate SQL instance name and database name. (This requirement applies to each restore in the restore set.) The SQL instance name always contains the system name. (For default instances, the system name is the instance name.)
- The Enterprise Vault agent cannot restore data and log files (.MDF and .LDF files) of an Enterprise Vault SQL database to a physical path that is different from the original physical path. As a result, the Enterprise Vault SQL restore is affected as follows:

- The drive (C:/ or D:/) used by these files at backup time is available at the restore time (in the destination client).
- In the redirected restore, if a new path (SQL instance or database name) already exists and it is associated with some other physical files. The database becomes associated with the new physical files after the restore completes. The physical files of the old database become dangling files and are no longer associated with a database.
- In the redirected restore, if the physical files to be restored are present and associated with some other database, manually take the database offline. If you do not take the database offline, the restore cannot overwrite those files.

About backup image restore sets

Backup images are displayed in the Backup, Archive, and Restore interface. These images correspond to Enterprise Vault file system data or Enterprise Vault SQL databases. The images that you select comprise a backup image restore set.

To perform an Enterprise Vault SQL database restore or a recovery with Point in time (PIT), first determine the time to which you want to restore or recover the database. Next, decide upon the group of backup images that need to be restored in a sequence to restore or recover the database. This group of backup images is called a backup image restore set. A backup image restore set consists of the following images:

Note: Recovery is only possible with SQL differential (transaction log) backup images.

- Full backup image: A restore set starts with a full backup image.
- Cumulative backup image: Add the last, cumulative backup image to the set. Add this image if it occurred between when the full backup image was taken and the time you decided to perform the restore or recovery.
- Differential backup images: Add the differential backup images that occurred between the last cumulative backup (or full backup if no cumulative backup happened) and the time that you decided to perform the restore or recovery. If you want to perform a recovery with PIT, then include the immediate differential image after the PIT in the restore set.

The following example demonstrates how to determine a backup image restore set in different use cases.

Figure 6-2 shows a variety of backup images that were taken and the time instance that it occurred.

Figure 6-2 Backup images taken over time

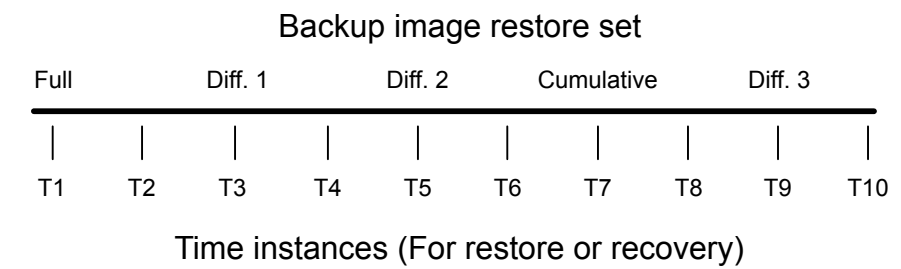


Table 6-3 demonstrates which backup images you would select to comprise a backup image restore set at any given time instance. Depending on the time you want to restore or recover the database, determines which backup images you must include in the backup image restore set.

Table 6-3 Understanding which back up images to select for a restore

Time instance	The backup images that comprise the backup image restore set
t1	Full backup
t2	Full + Differential 1 (PIT)
t3	Full + Differential 1
t4	Full + Differential 1 + Differential 2 (PIT)
t5	Full + Differential 1 + Differential 2
t6	Full + Differential 1 + Differential 2 + Differential 3 (PIT)
t7	Full + Cumulative
t8	Full + Cumulative + Differential 3 (PIT)
t9	Full + Cumulative + Differential 3
t10	Full + Cumulative + Differential 3 (SQL tail-log backup)

The following examples explain which backup images you must select in the Backup, Archive, and Restore interface:

■ Example 1:

To restore an SQL database to time instance t3, your backup image restore set must consist of the following backup images:

- The full backup image with the options **Take database offline** and **Leave database Non-operational** or **Leave database Read-only** enabled.
- The first differential backup image with the option **Leave database operational** enabled.

■ Example 2:

To recover an SQL database with PIT at time instance t8, your backup image restore set must consist of the following backup images:

- The full backup image with the options **Take database offline** and **Leave database Non-operational** or **Leave database Read-only** enabled.
- The last cumulative-backup image with the option **Leave database Non-operational** or **Leave database Read-only** enabled.
- The third differential backup image with the option **Leave database operational** and **Point-in-time recovery** enabled.

■ Example 3:

To recover an SQL database at time instance t10 which is after the last differential backup, you must use Microsoft's SQL tail-log mechanism. For more information about performing a tail-log backup, visit Microsoft's Web site and search for more information on this topic.

In this example the backup image restore set would include the following images:

- The full backup image with the options **Take database offline** and **Leave database Non-operational** or **Leave database Read-only** enabled.
- The last cumulative-backup image with the option **Leave database Non-operational** or **Leave database Read-only** enabled.
- The third differential backup image with the option **Leave database operational** and **Point-in-time recovery** enabled.
- Perform a tail-log backup. See Microsoft's Web site for instructions on how to perform this type of backup.

Restoring Enterprise Vault SQL database components

You can use the same procedure to restore the following Enterprise Vault SQL database components:

- An Enterprise Vault directory database

- An Enterprise Vault monitoring database
- An Enterprise Vault FSA Reporting database
- An Enterprise Vault auditing database
- An Enterprise Vault vault store database

Note: If you restore a vault store database, Symantec recommends that you also restore the corresponding open partition if it is available.

- An Enterprise Vault fingerprint database

You can restore an Enterprise Vault SQL database from any of the following systems:

- Run the restore from the NetBackup master server.
- Run the restore from the system that hosted the Enterprise Vault SQL database and also the policy host for the policy that was used to take the backup of this SQL database.
- Run the restore from the system that hosted the Enterprise Vault SQL database and was not the NetBackup policy client for the Enterprise Vault SQL database backup images.

Note: By default, a NetBackup client is not allowed to show the backup images for which a policy client is some other NetBackup client. You may need to add a **No Restriction File** on the NetBackup master server. That enables the NetBackup client to show and restore the backup images of the Enterprise Vault SQL database that were taken through some other NetBackup client.

See the *NetBackup Administrator's Guide for Windows, Volume I* for more information about the **No Restriction File**.

To restore Enterprise Vault SQL database components

- 1 Log on as administrator.
- 2 Stop the Enterprise Vault administrative services on all of the Enterprise Vault systems.
 See [“Important notes about Enterprise Vault data restore”](#) on page 65.
- 3 Open the Backup, Archive, and Restore interface.
- 4 Click **File > Select Files and Folders to Restore > from Normal Backup**.

- 5 In the **Restore** window, select the **Enterprise-Vault** policy type (choose **File > Specify NetBackup Machines and Policy Type**).
- 6 Click **OK**.
- 7 In the **NetBackup History** pane, determine which backup images to restore. See [“About backup image restore sets”](#) on page 80.
- 8 Select the backup images from the backup image restore set in the proper sequence, then restore one image at a time. Start with the full backup image.
- 9 In the **All Folders** pane, expand **Enterprise Vault Resources**.
- 10 Select the folder(s) of the Enterprise Vault SQL components to restore. (For example, you can restore the Enterprise Vault directory database, the Enterprise Vault monitoring database, or the vault store database.)
- 11 Click **Actions > Restore**.
- 12 In the **Enterprise Vault Restore** dialog box, click the **Database Settings** tab.
- 13 Configure the Recovery completion state, consistency check, and other settings for your restore.
- 14 Click **Start Restore**.
- 15 Repeat steps 8 through 14 for each image that you select to restore.
- 16 After the restore completes, start the Enterprise Vault services on all of the Enterprise Vault systems. Select **Start > Programs > Administrative Tools > Services**.

Disaster recovery

This chapter includes the following topics:

- Disaster recovery requirements for Enterprise Vault server
- About disaster recovery of an Enterprise Vault site
- Recovering a directory database
- Recovering an auditing database
- Recovering an FSA Reporting database
- Recovering a Monitoring database
- Recovering index locations
- Recovering a Enterprise Vault vault store group
- Recovering a fingerprint database
- Recovering a vault store database
- Recovering vault store partition
- Recovering Enterprise Vault partitions
- Recovering an Enterprise Vault server
- Recovering an Enterprise Vault server on a different system

Disaster recovery requirements for Enterprise Vault server

Disaster recovery requirements include the following:

- A copy of NetBackup for Windows with a license for the Enterprise Vault agent that is added on the master server
- The latest backup of the Enterprise Vault server that you want to recover
- Any service packs that have been applied to the original installation

For additional information about Enterprise Vault disaster recovery requirements, see the *Symantec Enterprise Vault Administrator's Guide*.

About disaster recovery of an Enterprise Vault site

If a disaster occurs, the system should have ability to recover your Enterprise Vault environment. This environment can consist of Enterprise Vault components, such as a directory database, a monitoring database, vault store databases, and Enterprise Vault index locations. The system should also have the ability to recover an Enterprise Vault server on the same system or to another system.

Note: Unless otherwise stated, do not start any Enterprise Vault service until you complete all the steps of a recovery procedure. If you start the Enterprise vault service to browse the Enterprise vault configuration, stop the Enterprise vault service before you move to the next step of recovery. If you chose to not run the Enterprise Vault recovery tools to repair consistency after the restore is complete, a data loss can occur. In addition, Symantec recommends that you run Enterprise Vault tools with the guidance of Enterprise Vault Support.

When a disaster occurs, there is a logical order that you should use to recover your Enterprise Vault environment. The following list provides a high-level summary of the process you should follow to successfully recover your data:

- First, identify the SQL server that hosted the directory database.
- Install the operating system and any other required applications on the SQL server that you identified and then begin to restore the directory database.
- Restore the directory database.
See [“Recovering a directory database”](#) on page 87.
- Install Enterprise Vault server on one of the systems and direct Enterprise Vault to the appropriate directory database.
- Finally, start the admin and the directory services and open the Enterprise Vault Administration Console. With the Enterprise Vault Administration Console open, determine which Enterprise Vault server and SQL server to use as the destination client for other entities.

Note: If you use the Enterprise Vault Administration Console to browse for the destination client, remember to stop the Enterprise Vault services before starting a recovery. You must stop all Enterprise Vault services on all Enterprise Vault servers before attempting a restore or recovery.

See [“Recovering a Monitoring database”](#) on page 89.

See [“Recovering an auditing database”](#) on page 87.

See [“Recovering an FSA Reporting database”](#) on page 88.

See [“Recovering index locations”](#) on page 89.

See [“Recovering a Enterprise Vault vault store group”](#) on page 90.

See [“Recovering an Enterprise Vault server”](#) on page 94.

See [“Recovering an Enterprise Vault server on a different system”](#) on page 96.

Recovering a directory database

Use the following procedure to recover a directory database in Enterprise Vault 7.5 and later.

Note: Before starting the recovery process, see the *Recovery* chapter, in the *Symantec Enterprise Vault™ Administrator's Guide for Windows*.

To recover a directory database

- 1 Start with the system that hosted the Enterprise Vault directory database.
- 2 Prepare this system for restore by installing the operating system and any other required applications.
- 3 Install the SQL Server on this system if it is not installed on this system already.
- 4 Install the NetBackup client on this system.
- 5 Restore the Enterprise Vault directory database.

See [“Restoring Enterprise Vault SQL database components”](#) on page 82.

Recovering an auditing database

Use the following procedure to recover an auditing database in Enterprise Vault 8.0 or later.

Note: Before starting the recovery process, see the *Recovery* chapter, in the *Symantec Enterprise Vault™ Administrator's Guide for Windows*.

To recover an auditing database

- 1 Start with the system that hosted the Enterprise Vault auditing database. This server should be the same server that currently hosts the directory database.

The auditing database can only exist in the SQL instance that hosts the directory database. It cannot exist in a separate SQL instance.
- 2 Prepare this system for restore by installing the operating system and any other required applications.
- 3 Install the SQL Server on this system if it is not installed on this system already.
- 4 Install the NetBackup client on this system.
- 5 Restore the Enterprise Vault auditing database back to the SQL server where the directory database resides.

See [“Restoring Enterprise Vault SQL database components”](#) on page 82.

Recovering an FSA Reporting database

Use the following procedure to recover an FSA Reporting database in Enterprise Vault 8.0 or later.

Note: Before starting the recovery process, see the *Recovery* chapter, in the *Symantec Enterprise Vault™ Administrator's Guide for Windows*.

To recover an FSA Reporting database

- 1 Start with the system that hosted the Enterprise Vault FSA Reporting database.
- 2 Prepare this system for restore by installing the operating system and any other required applications.
- 3 Install the SQL Server on this system if it is not installed on this system already.
- 4 Install the NetBackup client on this system.
- 5 Restore the Enterprise Vault FSA Reporting database.

See [“Restoring Enterprise Vault SQL database components”](#) on page 82.

Recovering a Monitoring database

Use the following procedure to recover a Monitoring database in Enterprise Vault 7.5 or later.

Note: Before starting the recovery process, see the *Recovery* chapter, in the *Symantec Enterprise Vault™ Administrator's Guide for Windows*.

To recover a Monitoring database

- 1 Start with the system that hosted the Enterprise Vault Monitoring database.
- 2 Prepare this system for restore by installing the operating system and any other required applications.
- 3 Install the SQL server on this system if it is not installed on this system already.
- 4 Install the NetBackup client on this system if it is not installed on this system already.
- 5 Restore the Enterprise Vault Monitoring database.

See [“Restoring Enterprise Vault SQL database components”](#) on page 82.

Recovering index locations

The following procedure describes how to recover Index locations in Enterprise Vault 7.5 or later.

Note: Symantec recommends that you run the Enterprise Vault tools to verify the consistency of Enterprise Vault indexes and database. If inconsistency exists, rebuild the Enterprise Vault indexes. In addition, Symantec recommends that you run Enterprise Vault tools with the guidance of Enterprise Vault Support.

To recover Enterprise Vault Index locations

- 1 Start with the first Enterprise Vault server in the Enterprise Vault site.
- 2 Prepare this system for restore by installing the operating system and any other required applications.
- 3 Install Enterprise Vault application on this system if it is not installed already.

- 4 Configure the Enterprise Vault server to the Enterprise Vault directory database in the Enterprise Vault configuration.

It may benefit you to know the Enterprise Vault topology on this Enterprise Vault server when it is time to select the Enterprise Vault backup images.

- 5 Install the NetBackup client on this system if it is not installed already.
- 6 Restore the index location data for all index locations that was part of this Enterprise Vault server.

See [“Restoring an Enterprise Vault file system component”](#) on page 77.

- 7 Repeat Step 1 through Step 6 for each Enterprise Vault server that was a part of this Enterprise Vault site.

Recovering a Enterprise Vault vault store group

A Enterprise Vault vault store group consists of vault stores and fingerprint databases. Use the following procedure to recover a vault store group in Enterprise Vault 8.0 or later.

To restore a Enterprise Vault vault store group

- 1 Identify the vault stores in a vault store group. You can use the Vault administration console to identify the vault stores.
- 2 Identify the fingerprint database for that vault store group.
- 3 Because a vault store group involves multiple Enterprise Vault servers, stop the Enterprise Vault services on all required servers.
- 4 Restore the first vault store that is a part of this Enterprise Vault Store group. Use the following steps to understand which are the components that you must restore:

- Restore the vault store database.
See [“Recovering a vault store database”](#) on page 92.
- Restore all of the vault store partitions.
Restore the first vault store partition.
See [“Recovering vault store partition”](#) on page 93.
Repeat this step for all partitions in the vault store.

- 5 Repeat step 4 for all of the remaining vault stores, which are a part of this Enterprise Vault Store group.
- 6 Restore the fingerprint database.

See [“Recovering a fingerprint database”](#) on page 91.

- 7 After the restore is complete, run the Enterprise Vault recovery tools.
If you chose to not run the Enterprise Vault recovery tools to repair consistency after the restore is complete, data loss can occur. In addition, Symantec recommends that you run Enterprise Vault tools with the guidance of Enterprise Vault Support.
- 8 Start the Enterprise Vault services on all Enterprise Vault servers.

Recovering a fingerprint database

To recover a fingerprint database, you must be aware of the following:

- The destination client for the fingerprint database restores
- The timestamp to perform a point-in-time recovery of the fingerprint database

Use the following procedure to recover a fingerprint database in Enterprise Vault 8.0 or later.

To recover the fingerprint database

- 1 Identify the name of vault store group whose fingerprint database needs to be restored.
- 2 Identify the vault stores in the chosen vault store group. You can obtain this information by browsing Vault Administration Console.
- 3 Identify the Enterprise Vault servers that are a part of the vault store group whose fingerprint database you want to restore.
- 4 Install the operating system and any other required applications (including the Enterprise Vault application) on the all Enterprise Vault servers within the vault store group.
- 5 Stop the Enterprise Vault services that are running on the Enterprise Vault servers that host the vault stores in a vault store group. The fingerprint database to be restored is associated with that vault store group. The Enterprise Vault server is seen as a **Computer** in the properties of a vault store in the Vault Administration Console.

- 6 Before restoring the fingerprint database, get the latest backup time of the open, closed, and ready partitions, and the vault store databases that comprise the vault store group of the fingerprint database you want to restore. (This backup timestamp is referred to as the timestamp of the vault store backup. This timestamp is the backup time of the images that were restored using the Enterprise Vault agent.) All partitions and vault store database images may not have same backup time. Therefore, you should use the most recent backup time as the vault store backup timestamp and then start the restore of the fingerprint database.

See [“Restoring Enterprise Vault SQL database components”](#) on page 82.

If there are multiple fingerprint databases, then you should repeat this step for each fingerprint database.

- 7 Run the Enterprise Vault recovery tools to repair the consistency of the entire vault store group. That helps to bring the partitions, the vault store database, and the fingerprint database to a consistent state.

Note: Symantec recommends that you run Enterprise Vault tools with the guidance of Enterprise Vault Support.

- 8 If there is no fingerprint database backup after a vault store backup timestamp, restore all of the available fingerprint database backups from the last full backup and any incremental backups. Run the Enterprise Vault recovery tools to recover any missing entries of the fingerprint database. If you do not add the missing entries, you can encounter a data loss if the items are expired or deleted from Enterprise Vault archives.
- 9 Restart the services on the Enterprise Vault servers.

Recovering a vault store database

The following procedure describes how to recover a vault store database. Use the following procedure to recover a vault store database in Enterprise Vault 7.5 or later.

To restore a vault store database

- 1 Prepare the system that was used to host the vault store database for this vault store. Install the operating system and any other required applications to prepare the system.
- 2 Install the SQL Server on this system if it is not installed on this system already.

- 3 Install the NetBackup client on this system if it is not installed on this system already.
- 4 Restore the vault store database that is associated with this vault store.
See [“Restoring Enterprise Vault SQL database components”](#) on page 82.
- 5 Run the Enterprise Vault recovery tools to repair the consistency of the vault store. This step helps to bring the partitions, the vault store databases to a consistent state.

If you chose to not run the Enterprise Vault recovery tools to repair any inconsistency, data loss can occur.

Symantec recommends that you run Enterprise Vault tools with the guidance of Enterprise Vault Support.

Recovering vault store partition

The following procedure describes how to recover a vault store partition in Enterprise Vault 7.5 or later. The following procedure is applicable for open, closed, and ready partitions.

To recover a vault store partition

- 1 Prepare to restore the system that you used to host this vault store.
- 2 Install the operating system and any other required applications.
- 3 Install the Enterprise Vault application on this system if it is not installed already.
- 4 Configure the Enterprise Vault server to the Enterprise Vault directory database in the Enterprise Vault configuration.

It may benefit you to know the Enterprise Vault topology on this Enterprise Vault server when it is time to select the Enterprise Vault backup images.

- 5 Install the NetBackup client on this system if it is not installed already.
- 6 Restore the vault store partition data.
See [“Restoring an Enterprise Vault file system component”](#) on page 77.
- 7 Run the Enterprise Vault recovery tools to repair the consistency of the vault store. This step helps to bring the partitions and the vault store databases to a consistent state.

If you chose to not run the Enterprise Vault recovery tools to repair any inconsistency, data loss can occur. Symantec recommends that you run Enterprise Vault tools with the guidance of Enterprise Vault Support.

Recovering Enterprise Vault partitions

The following procedure describes how to recover Enterprise Vault partitions within an Enterprise Vault site.

To recover Enterprise Vault partitions

- 1 Start with the first Enterprise Vault server in the Enterprise Vault site.
- 2 Prepare this system for restore by installing the operating system and any other required applications.
- 3 Install the Enterprise Vault application on this system if it is not installed already.

It may benefit you to know the Enterprise Vault topology on this Enterprise Vault server when it is time to select the Enterprise Vault backup images. (This application is not necessary for disaster recovery.)

- 4 Configure the Enterprise Vault server to the Enterprise Vault directory database in the Enterprise Vault configuration.
- 5 Install the NetBackup client on this system if it is not installed already.
- 6 Restore the data for all of the Enterprise Vault partitions that are a part of this Enterprise Vault server.

See [“Restoring an Enterprise Vault file system component”](#) on page 77.

- 7 Repeat Step 1 through Step 6 for each Enterprise Vault server that was a part of this Enterprise Vault site.

Recovering an Enterprise Vault server

The following procedure describes how to recover an Enterprise Vault server. Use the following procedure to recover an Enterprise Vault server in Enterprise Vault 7.5 or later.

Note: Symantec recommends that you run the Enterprise Vault tools to verify the consistency of the Enterprise Vault indexes and database. If an inconsistency exists, rebuild the Enterprise Vault indexes. In addition, Symantec recommends that you run Enterprise Vault tools with the guidance of Enterprise Vault Support.

To recover an Enterprise Vault server

- 1 Install the operating system and any other required applications to prepare the Enterprise Vault server for restore.
- 2 Install the Enterprise Vault application on this system if it is not installed already.

It may benefit you to know the Enterprise Vault topology on this Enterprise Vault server when it is time to select the Enterprise Vault backup images.

- 3 Restore the Enterprise Vault directory database if this Enterprise Vault server hosted the Enterprise Vault directory database.

See [“Restoring Enterprise Vault SQL database components”](#) on page 82.

- 4 Configure the Enterprise Vault server to the Enterprise Vault directory database in the Enterprise Vault configuration.
- 5 Install the NetBackup client on this system if it is not installed already.
- 6 Restore the Enterprise Vault monitoring database if this Enterprise Vault server hosted the Enterprise Vault monitoring database.
See [“Restoring Enterprise Vault SQL database components”](#) on page 82.
- 7 Restore the Enterprise Vault auditing database if this Enterprise Vault server hosted the Enterprise Vault auditing database.
See [“Recovering an auditing database”](#) on page 87.
- 8 Restore the Enterprise Vault FSA Reporting database if this Enterprise Vault server hosted the Enterprise Vault FSA Reporting database.
See [“Recovering an FSA Reporting database”](#) on page 88.
- 9 Restore the Enterprise Vault fingerprint database if the Enterprise Vault hosted a vault store group.
See [“Recovering a fingerprint database”](#) on page 91.
- 10 Restore the first vault store that is a part of this Enterprise Vault server . Use the following steps to understand which are the components that you must restore:

- Restore the vault store database.
See [“Recovering a vault store database”](#) on page 92.
- Restore all of the vault store partitions.
Restore the first vault store partition.
See [“Recovering vault store partition”](#) on page 93.
Repeat this step for all partitions in the vault store.

- Run the Enterprise Vault recovery tools to repair the consistency of the vault store. That helps to bring the partitions, and the vault store database, to a consistent state. Symantec recommends that you run Enterprise Vault tools with the guidance of Enterprise Vault Support.
- 11 Repeat Step 10 for the remaining vault stores that are a part of this Enterprise Vault server.
 - 12 Restore the index location data for all index locations that were a part of this Enterprise Vault server.

See [“Restoring an Enterprise Vault file system component”](#) on page 77.

Recovering an Enterprise Vault server on a different system

The following procedure describes how to recover an Enterprise Vault server that is located on a different system in Enterprise Vault 7.5 or later.

To recover an Enterprise Vault server on a different system

- 1 Prepare the Enterprise Vault server for restore by installing the operating system and any other required applications.
- 2 Install Enterprise Vault application on this system if it is not installed already.
It may benefit you to know the Enterprise Vault topology on this Enterprise Vault server when it is time to select the Enterprise Vault backup images.
- 3 Configure the Enterprise Vault server to the Enterprise Vault directory database in the Enterprise Vault configuration.
- 4 Install the NetBackup client on this system if it is not installed already.
- 5 Restore the Enterprise Vault directory database (EV_DIR_DB) if this Enterprise Vault server hosted the Enterprise Vault directory database.

See [“Restoring Enterprise Vault SQL database components”](#) on page 82.

- 6 Update the Enterprise Vault directory database for the new system.

You can update the Enterprise Vault directory database by running a query that Enterprise Vault provides on the new system by using the SQL server Management Studio. The query updates any information about the previous Enterprise Vault server with the new Enterprise Vault server.

See the *Symantec Enterprise Vault Administration Guide* for more information about this query.

- 7 Restore the Enterprise Vault monitoring database (EV_MONITORING_DB) if this Enterprise Vault server hosted the Enterprise Vault monitoring database.
See [“Restoring Enterprise Vault SQL database components”](#) on page 82.
- 8 Restore the Enterprise Vault auditing database if this Enterprise Vault server hosted the Enterprise Vault auditing database.
See [“Recovering an auditing database”](#) on page 87.
- 9 Restore the Enterprise Vault FSA Reporting database if this Enterprise Vault server hosted the Enterprise Vault FSA Reporting database.
See [“Recovering an FSA Reporting database”](#) on page 88.
- 10 Restore the Enterprise Vault fingerprint database if the Enterprise Vault hosted a vault store group.
See [“Recovering a fingerprint database”](#) on page 91.
- 11 Restore the first vault store that is a part of this Enterprise Vault server. Use the following steps to understand which are the components that you must restore:
 - Restore the vault store database.
See [“Recovering a vault store database”](#) on page 92.
 - Restore all of the vault store partitions.
Restore the first vault store partition.
See [“Recovering vault store partition”](#) on page 93.
Repeat this step for all partitions in the vault store.
 - Run the Enterprise Vault recovery tools to repair the consistency of the vault store. That helps to bring the partitions, and the vault store database, to a consistent state. Symantec recommends that you run Enterprise Vault tools with the guidance of Enterprise Vault Support.
- 12 Repeat Step 11 for the remaining vault stores that are a part of this Enterprise Vault server.
- 13 Restore the index location data for all index locations that were a part of this Enterprise Vault server.
See [“Restoring an Enterprise Vault file system component”](#) on page 77.

Note: Symantec recommends that you run the Enterprise Vault tools to verify the consistency of Enterprise Vault indexes and database. If an inconsistency exists in Enterprise Vault Indexes rebuild them. In addition, Symantec recommends that you run Enterprise Vault tools with the guidance of Enterprise Vault Support.

Enterprise Vault Agent support for EV 7.5, 8.0 and later

This chapter includes the following topics:

- [Policy configuration for Enterprise Vault 8.0 and later versions](#)
- [Notes about Enterprise Vault 10.0 backups](#)
- [Excluding files from the exclude list](#)
- [Directives for Enterprise Vault 7.5 policy creation](#)
- [About planning backup schedules](#)
- [About hosts for Enterprise Vault policies](#)
- [About Enterprise Vault tools](#)
- [About Enterprise Vault agent backups](#)
- [About Enterprise Vault agent restores](#)
- [Useful tips about Enterprise Vault agent](#)
- [Enterprise Vault agent functionality and support for EV 7.5 and later](#)

Policy configuration for Enterprise Vault 8.0 and later versions

The following topics contain the information that pertains to policy creation for Enterprise Vault 8.0 or later.

See [“Open partition, vault store database, and fingerprint database consistencies”](#) on page 100.

See [“Closed and ready partition consistencies”](#) on page 100.

See [“Index location consistencies”](#) on page 101.

See [“Directory database consistencies”](#) on page 101.

Open partition, vault store database, and fingerprint database consistencies

To ensure consistency when backing up a fingerprint database, you should add all open partitions of the vault store group and the fingerprint database in the same policy. By grouping these components into a single policy, you can ensure that the specified Vault Stores remain in backup mode until all snapshots are taken or the backup finishes. Configuring a policy in this way also means that the vault stores spend less time in backup mode.

The following is an example of how you would configure a new policy that includes a fingerprint database:

- EV_OPEN_PARTITION=vs1
- EV_OPEN_PARTITION=vs2
- EV_OPEN_PARTITION=vs3
- EV_FINGERPRINT_DB=vsg1

Where vsg1 is a vault store group and vs1, vs2, and vs3 are all the vault stores under vsg1.

Closed and ready partition consistencies

The following points help you to maintain a consistency for the closed and the ready partitions backup.

- You should back up the closed partitions and the ready partitions of a Vault Store in separate policies. In addition, these partitions do not need to be backed up daily. You can schedule these backups to occur less frequently than a directory database, for example.

- If the amount of data is small enough, you can combine the closed and the ready partitions of multiple Vault Store's in a single policy. However, if the amount of data is large, Symantec recommends that you back up the closed and the ready partitions in separate policies.

Index location consistencies

You should protect index locations in an Enterprise Vault site with a separate policy to maintain consistency. In addition, it is recommended that you schedule a daily backup of the index locations because the archival process creates indexes regularly.

Directory database consistencies

The following points help you to maintain the directory database consistency.

- You should back up the directory database frequently. Symantec recommends that you back up this database daily.
- You can protect all of the site-level databases (directory, monitoring, FSAReporting, and auditing databases) in a single policy.
- With Enterprise Vault 8.0 or later, you cannot select the EV_DIR_DB directive with the EV_INDEX_LOCATION= and the EV_OPEN_PARTITION= directives. In addition, you should not schedule a directory database policy backup to run at the same time as an index location backup policy or an open partition backup policy.
- Before you make any change in the Enterprise Vault configuration, Symantec recommends that you back up the directory database first. Then after you change the Enterprise Vault configuration, back up the directory database again. Next, perform a full backup of the Enterprise Vault components that the configuration changes affected.

Notes about Enterprise Vault 10.0 backups

In Enterprise Vault 10.0, before you configure the index locations and vault partitions backup, there is a list of files that you must exclude from the exclude list. An exclude list names the files and directories to be excluded from backups of the selected Windows clients. The following sections identify the files that need to be excluded for a successful backup.

Exclude file list for index locations

The following list specifies the files that need to be excluded from the exclude list for index locations backup.

- `crawler-fatal-error`
- `crawler-read-only`
- `crawler.log`
- `crawler-service.pipe`
- `indexer-fatal-error`
- `indexer-read-only`
- `indexer.log`
- `indexer-service.pipe`

Exclude file list for vault partitions

The following list specifies the files that need to be excluded from the exclude list for vault partitions backup.

- `.ARCH`
- `.lock`

Note: File name must be enclosed with wild characters. For example, the file `*crawler-fatal-error*` or `*.ARCH*`.

See [“Excluding files from the exclude list”](#) on page 102.

Excluding files from the exclude list

An exclude list names the files and directories to be excluded from backups of the selected Windows clients.

For UNIX clients, use the `bpgetconfig` and `bpsetconfig` commands to gather and modify the exclude list files from the `/usr/opensv/netbackup` directory on each client.

For more information, see the *Symantec NetBackup™ Administrator's Guide*.

To exclude files from the exclude list

- 1 In the **NetBackup Administration Console**, expand **NetBackup Management** > **Host Properties** > **Clients**. Double-click on a client, the **Client Properties** dialog box opens.
- 2 Under **Exclude Lists**, click **Add**. The **Add to Exclude List** dialog box opens.
- 3 In the **Policy** field, select **All Policies**. The **Policy** field contains a list of all the policies that contain the files and the directories that you want to exclude.
- 4 In the **Schedule** field, select **All Schedules**. The **Schedules** field contains a list of the schedules associated with the policies that you select to be excluded from the backup.
- 5 In the **Files/Directories** field, enter the files or directories that need to be excluded from the exclude list based on the selected policy and schedule.
- 6 Click **Add** to add the selected files to the exclude list.
- 7 Click **Apply** and then click **OK**.

See [“Notes about Enterprise Vault 10.0 backups”](#) on page 101.

Directives for Enterprise Vault 7.5 policy creation

This topic contains information about Enterprise Vault 7.5 directives. It also contains suggestions about which directive you should use and when you should use it in a policy.

[Table 8-1](#) provides recommendations of when you should use the various Enterprise Vault 7.5 directives.

Table 8-1 Understanding which directive to use and when

Backup selection	Recommendations
EV_INDEX_LOCATION and EV_OPEN_PARTITIONS	Symantec recommends that you use these directives more frequently than the other directives. In fact, you should schedule these directives to run daily backups. These directives take the backup to a more granular level to protect Enterprise Vault. These directives should be the most preferred backup selections when you want to protect large deployments of Enterprise Vault.

Table 8-1 Understanding which directive to use and when *(continued)*

Backup selection	Recommendations
EV_CLOSED_PARTITIONS	Closed partitions can be backed up by a policy that uses the EV_SITE or EV_SERVER directives. However, if these policies are not scheduled, then you can use the EV_CLOSED_PARTITIONS directive in a policy to back up the closed partitions. Closed partitions do not typically change often, so you can schedule a backup with this directive to occur less frequently.
EV_VAULT_STORE_DB and EV_VAULT_STORE_DB=	The EV_OPEN_PARTITIONS directive implicitly backs up the Vault Store database so you would not need to back up the vault store separately. However, if Enterprise Vault collection is enabled, then you should plan to use these directives to back up the vault store database regularly. If collection is not enabled, then you can plan to use these directives before you do any maintenance on the SQL server that hosts these databases. In addition, you should also plan to back up the directory (EV_DIR_DB) and monitoring (EV_MONITORING_DB) databases in the maintenance case.
EV_VAULT_STORE and EV_VAULT_STORE=	Using this directive means data that is not modified regularly is backed up more frequently than it needs to be. Symantec recommends that you use these directives when you want to repair a particular Vault Store or multiple Vault Stores.
EV_SERVER	Using this directive means data that is not modified regularly is backed up more frequently than it needs to be. Symantec recommends that you use this directive for planned maintenance on an Enterprise Vault server.
EV_SITE	Using this directive means data that is not modified regularly is backed up more frequently than it needs to be. Symantec recommends that you use this directive only for small Enterprise Vault setups and if the backup window and media usage is acceptable.

About planning backup schedules

This topic provides information to help you configure backup schedules. More specifically, it helps you understand how frequently you should perform full, incremental, and cumulative backups when backing up Enterprise Vault

components. In addition, this information reminds you that there are certain backups that you should not schedule to run at the same time.

See [“Configuration requirements for an Enterprise Vault backup policy”](#) on page 37.

Symantec has the following recommendations when you plan your backup schedules:

- You should perform at least one weekly full backup and daily incremental backups for all Enterprise Vault components. In addition, Symantec recommends that you perform one or two cumulative backups each week. You can monitor the size of the incremental backups to help you decide how many cumulative backups you should schedule. The greater the size of the incremental backups, the greater the need to perform two cumulative backups.
- As you determine the schedules of your backups, you should be careful that you do not overlap certain backups. For example, do not allow a directory database backup window to overlap with the backup window of an open partition or index locations backup.

About hosts for Enterprise Vault policies

When you add a client to a policy the client must be an Enterprise Vault server. For all Enterprise Vault 8.0 or later backup selection types, the recommended client name is Enterprise Vault Site alias or Any Enterprise Vault server alias.

[Table 8-2](#) shows the Enterprise Vault 7.5 client name recommendations for a policy client.

Table 8-2 Enterprise Vault 7.5 client name recommendations

Backup selection	Recommendation for Client name
EV_SITE	Enterprise Vault Site alias
EV_SERVER	Enterprise Vault Server alias
EV_DIR_DB	Enterprise Vault Site alias or Enterprise Vault Server alias
EV_MON_DB	Enterprise Vault Site alias or Enterprise Vault Server alias
Others	Enterprise Vault Server alias

Note: For Enterprise Vault 8.0 the same client name is used across all of the policies to protect an Enterprise Vault site.

For more information about Enterprise Vault site and server aliases, see the *Symantec Enterprise Vault Administrator's Guide*.

About Enterprise Vault tools

Enterprise Vault provides a number of utilities to test and verify the Enterprise Vault performance. One such utility is the EVSVR tool. The EVSVR tool is a Windows command-line utility for Enterprise Vault storage reporting and verification. The tool can report on, verify, and repair the Enterprise Vault storage.

NetBackup recommends that you use the EVSVR tool to check any inconsistency after a successful restore of partitions, a vault store database, or a Fingerprint database. This tool can also help you to repair these components.

See the Enterprise Vault Administrator's Guide for more details about the tool.

About Enterprise Vault agent backups

Review the following information about the Enterprise Vault agent backups before planning the SQL database backup:

When you attempt to back up an SQL database, Symantec recommends that you run a full backup before any incremental backup. If you perform scheduled incremental backups when no full backup exists the following occurs:

- The first scheduled Cumulative incremental backup is a streamed-base backup and is treated as a full backup . However, the Backup, Archive, and Restore user interface displays the backup as a Cumulative backup. As a result, any following scheduled Cumulative incremental backups are “cumulative” in nature.
- The first scheduled Differential incremental backup is a streamed-base backup and is treated as a full backup . However, the Backup, Archive, and Restore user interface displays the backup as a Differential backup. As a result, any following scheduled Differential incremental backups are “differential” in nature.

If a full backup for an Enterprise Vault SQL database fails, manually initiate a second full backup and ensure that it finishes successfully before a Cumulative Incremental schedule backup starts. If the full backup for an Enterprise Vault SQL database fails, the following occurs:

- Any Cumulative incremental backups that were run after the failure and before the next, successful full backup cannot be restored. This issue only affects Cumulative backups after a failed full backup . Differential incremental backups are not affected, even after a failed full backup.

- An attempt to restore these Cumulative Incremental backup images fails with a status 5 error, and this failure can result in a data loss. The tar log file contains the following message: `SQL Error Description: This differential backup cannot be restored because the database has not been restored to the correct earlier state.`
- You can however, restore the data from the Differential backup images. You must restore all of the Differential backup images after the restore of the last full-backup image.
To avoid this issue, Symantec recommends that you make sure the full backup is successful before you begin a Cumulative incremental backup. Ensuring a successful full backup before you attempt Cumulative backup guards against a data loss scenario.

Finally, check whether you have the required privileges to create backups using the Enterprise Vault agent.

Privileges for Enterprise Vault backup

You require certain privileges to create Enterprise Vault agent backups. The privileges are :

- SeBackupPrivilege
- SeRestorePrivilege
- SeSecurityPrivilege
- SeTakeOwnershipPrivilege
- SeDebugPrivilege

These privileges are required to create a backup. To assign these specific privileges to the Enterprise Vault administrator account, you need to add them to the following locations in the Local Security Policy. If Enterprise Vault is clustered, add these privileges on all nodes of the cluster.

- Backup files and directories = SeBackupPrivilege.
- Restore files and directories = SeRestorePrivilege..
- Manage auditing and security log = SeSecurityPrivilege
- Take ownership of files or other objects = SeTakeOwnershipPrivilege.
- Debug programs = SeDebugPrivilege.

About Enterprise Vault agent restores

Refer to the following points for information and tips about Enterprise Vault agent restores:

- Do not restore PSN files while restoring a partition.
- A restore (or an alternate restore) of multiple SQL objects in a single restore job is not supported.
To perform an alternate restore of Enterprise Vault SQL data, pick the SQL object from a single backup image. Do not mix the SQL object selection from one backup image with file system objects or other SQL objects from another backup image.
- A restore gets slow when you attempt to restore a large number of files or a large amount of data. For better results, change the socket buffer size.
See “[Changing the socket buffer size for large restores](#)” on page 108.

Changing the socket buffer size for large restores

When you attempt to restore a large number of files or a large amount of data, the restore may run very slow. If you encounter this sort of behavior, you should change the socket buffer size on the NetBackup media server and the NetBackup destination client. The following procedures explain how to set this socket buffer size.

For more information about changing the socket buffer size, see the *NetBackup Tuning Guide for UNIX, Windows, and Linux*.

To change the socket buffer size on a NetBackup media server

- 1 Go to `<NetBackup Install Path>\Veritas\NetBackup`.
- 2 Create a file with name `NET_BUFFER_SZ`.
- 3 Put a number in this file that is: 65536.
- 4 Save the file.

To change the socket buffer size on a NetBackup destination client

- 1 Go to the NetBackup master server and start the NetBackup Activity Monitor.
- 2 Select, Host Properties > Clients.
- 3 Open the **Host Properties** window for the NetBackup destination client.
- 4 Select, Windows Client > Client Settings.
- 5 Change the **Communication buffer size** to 64 kilobytes.

Useful tips about Enterprise Vault agent

Understand the following items for useful tips about the Enterprise Vault agent:

- You should run an Enterprise Vault backup when there is no configuration change happening for Enterprise Vault.
An Enterprise Vault configuration can change automatically like an Enterprise Vault partition roll-over. That can change the state of some partitions (open to closed and ready to open). As part of Enterprise Vault backup, NetBackup queries Enterprise Vault for its configuration. That happens in the first job (known as the discovery job) of the compound backup job.
If an Enterprise Vault configuration change and NetBackup's discovery job happens at the same time then any one of the following can occur:
 - Fail with a status code 2
 - Partially succeed with a status code 1 (Some Enterprise Vault objects may not be backed up.)
 - Success without any error (Some Enterprise Vault objects may not be backed up.)
- Across multiple Enterprise Vault sites, Enterprise Vault enables you to configure multiple Enterprise Vault vault store groups or vault stores with the same name. However, NetBackup does not support multiple vault store groups or multiple vault store configurations with the same name across Enterprise Vault sites. In addition, NetBackup does not support these types of configurations within the same Enterprise Vault site. If you attempt this type of configuration using the NetBackup Enterprise Vault agent, you can encounter unexpected behavior from the agent that can cause a data loss.

Enterprise Vault agent functionality and support for EV 7.5 and later

This topic contains the notes that are applicable to the functionality of the NetBackup Enterprise Vault agent and how it supports Enterprise Vault 7.5 or later:

- For this release, the Enterprise Vault agent does not support any Enterprise Vault partitions that are based on a mapped drive. That applies to open and closed partition components.
 - If an open partition is based on a mapped drive then there should not be any backup selection that uses the EV_OPEN_PARTITIONS directive for the Enterprise Vault server that contains that open partition.

- If a closed partition is based on a mapped drive then there should not be any backup selection that uses the EV_CLOSED_PARTITIONS directive for the Enterprise Vault server that contains the closed partition.
- For this release, Enterprise Vault agent does not support the Enterprise Vault index locations that are based on a mapped drive. If any index location in an Enterprise Vault site is based on a mapped drive then you should ensure that no backup selection uses the EV_INDEX_LOCATION directive.
- Information on supported cluster environments for Enterprise Vault is available.
See the, *Symantec Enterprise Vault™ Administrator's Guide* document.

Differential incremental backup taken after a restore fails for EV 7.5 and later versions

Run a full backup and perform a restore of the backup image. Then, run a differential incremental backup, the backup fails with error 13.

The reason for the backup failure is that the NetBackup Enterprise Vault Agent's use of the Backup Exec SQL Agent code change (for DB backups) does not allow incremental backups until a new full backup is complete after the restore. So when a differential incremental backup is run, the backup is treated as a new database, wherein you are required to first run a full backup and then the differential incremental backup. A restore should not be done before the incremental backup.

Note: An incremental backup after a full restore was allowed in the earlier versions of NetBackup. The failure of the incremental backup failure after a full restore has been observed in the NetBackup 7.5.

Troubleshooting

This chapter includes the following topics:

- [About troubleshooting](#)
- [About debug logging](#)
- [How to enable debug logging](#)
- [Setting the debug level](#)
- [About status reports](#)
- [About operational reports](#)
- [About progress reports](#)
- [About NetBackup status-related troubleshooting information](#)

About troubleshooting

This chapter explains the processes and resources that can help you troubleshoot the NetBackup Enterprise Vault agent. These resources include the debug logs and status reports for NetBackup and for the database agent to help troubleshoot the backup and restore operations. These reports are useful for finding the errors that are associated with those applications.

About debug logging

The NetBackup master, media, and client software offer a comprehensive set of debug logs for troubleshooting any problems that may occur during NetBackup operations.

You can control the amount of information that is written to the debug logs.

See [“To set the debug level”](#) on page 113.

After you determine the cause of a problem, you can disable the debug logging by removing the previously created debug logging directories.

For details on the contents of these debug logs, refer to the *NetBackup Troubleshooting Guide*. For additional NetBackup master server logs, media server logs, and client logs, see the NetBackup Backup, Archive, and Restore user interface online Help and the *NetBackup Administrator’s Guide for Windows, Volume I*.

Note: When debug logging is enabled, the files can become large and can adversely affect other backups that use the same files.

To create all debug logs, run the following batch file:

```
install_path\NetBackup\logs\mklogdir.bat
```

How to enable debug logging

To enable debug logging for standard backup operations, you need to create directories on the client system. The following tables give information about the type of directories that are required.

[Table 9-1](#) lists the directories to create to capture various backup, restore, and snapshot data.

[Table 9-2](#) lists the Windows event logs to create on the NetBackup media server.

[Table 9-3](#) lists the Windows event logs to create on the NetBackup master server.

Table 9-1 List of the directories to create to capture various backup, restore, and snapshot data

Directories to create	Data logged
install_path\Netbackup\logs\bpbkar	all backups
install_path\Netbackup\logs\tar	all restores
install_path\Netbackup\logs\bpresolver	Enterprise Vault configuration discovery, Enterprise Vault [un]quiescence
install_path\NetBackup\logs\bpfis	Snapshot information
C:\Program Files\Common Files\Symantec Shared\VxFl\4\Logs	See the <i>VxFl Administrator's Guide</i> on the Symantec Support Web site.

Table 9-1 List of the directories to create to capture various backup, restore, and snapshot data (*continued*)

Directories to create	Data logged
<code>install_path\NetBackup\logs\nbwin</code>	Backup, Archive, and Restore user interface information
<code>install_path\NetBackup\logs\AltPath</code>	Alternate restore information

Table 9-2 Lists the directories to create to capture various backup, restore, and snapshot data on the NetBackup media server

Directories to create	Enterprise Vault operation information
<code>install_path\Netbackup\logs\bpbrm (Windows)</code>	Back up and Restore Manager
<code>usr/opensv/netbackup/logs/bpbrm(UNIX)</code>	Back up and Restore Manager

Table 9-3 Lists the VxUL logs for NetBackup Policy Execution Manager and NetBackup Job Manager

Directories to create	Enterprise Vault operation information
<code>install_path\Netbackup\logs (Windows)</code>	NetBackup Job Manager
<code>usr/opensv/netbackup/logs(UNIX)</code>	NetBackup Policy Execution Manager
Refer to the "Unified logging" topic in the <i>NetBackup Troubleshooting Guide for UNIX, Windows, Linux</i> .	

After you create these directories all debug logging information is placed in the separate files that are created on a date basis.

Setting the debug level

You can control the amount of information that is written to the debug logs by changing the **General** debug level. The higher the value, the more information is logged. For most operations, the default value of 0 is sufficient. However, technical support may ask you to change the value to a higher level while a problem is analyzed. The following procedure helps you to change the debug level.

To set the debug level

- 1 Click **Start > Programs > Symantec NetBackup > Backup, Archive, and Restore**.
- 2 Click **File > NetBackup Client Properties**.

- 3 Click the **Troubleshooting** tab. By default, the **Debug Levels** settings are zero.
- 4 From the **General Debug Level** drop-down list, set the debug level as required.
- 5 Click **OK** to save your changes.

About status reports

NetBackup provides a variety of status reports to verify the completion of backup and restore operations. In addition, users and the administrator can set up additional reports if a site requires them.

About operational reports

The administrator has access to operational progress reports through the NetBackup Administration Console.

You can generate the following reports for a specific time frame, client, or master server:

- Status of Backups
- Client Backups
- Problems
- All Log Entries
- Media Lists
- Media Contents
- Images on Media
- Media Logs
- Media Summary
- Media Written

Refer to *NetBackup Administrator's Guide, Volume I* for details.

About progress reports

Progress reports on the client allow easy monitoring of user operations. Administrators can monitor operations and detect any problems that occur for any restore operation. To view the status of an operation, select **File > Status**, click the task for which you want to check the progress, and click **Refresh**.

When the requested operation's *successfully completed* message appears, the NetBackup operation is finished. (See your *NetBackup Backup, Archive, and Restore Getting Started Guide* for further information on the progress report and the meanings of the messages.)

About NetBackup status-related troubleshooting information

This section describes the status codes that pertain directly to the Enterprise Vault agent.

See [“NetBackup status code 2”](#) on page 115.

See [“NetBackup status code 13”](#) on page 116.

See [“NetBackup status code 39”](#) on page 116.

See [“NetBackup status code 59”](#) on page 117.

See [“NetBackup status code 69”](#) on page 117.

See [“NetBackup status code 156”](#) on page 118.

See [“NetBackup status code 1800”](#) on page 120.

NetBackup status code 2

- Verify if the Enterprise Vault services are running on the related Enterprise Vault servers.

Enterprise Vault services could be stopped automatically if any disk volume in the system is full. In addition, the Enterprise Vault services could stop if the client is also a media server and if a disk storage unit is full. In this situation, you would start the Enterprise Vault services and re-run the backup.

- Verify whether the Enterprise Vault user name credentials that are given in the client host properties are correct or not.

- Ensure that MSXML is installed.

If MSXML 6 is not installed, the client's `sbpresolver` log contains the following error message:

```
registry key for MSXML6 not found. Seems that MSXML6 is not
installed...Exiting
```

You should install MSXML 6 and run the backup again.

- Look at the Event Viewer of the policy client and related Enterprise Vault servers.

- For Enterprise Vault 8.0, quiescence can fail if the Enterprise Vault component (Vault store or Index location) or its parent component (such as, vault store group or site) is already quiesced. The backups fail with a status 2. You should clear the backup mode and attempt to run the backup again.
- A backup can fail with a status 2 if the backup runs within a few minutes from when an Enterprise Vault directory database was restored. You should browse the Enterprise Vault configuration from Vault Administration Console and attempt to run the backup again.

NetBackup status code 13

Explanation: file read failed

After a NetBackup installation, it is possible for the first EV-SQL backup policy to fail with a status 13 error. If an EV-SQL backup fails with a status 13, do the following:

- Make sure that the SQL version that is installed is at least SQL 2005 SP2 or greater.
- Create the following registry DWORD value in the particular SQL client.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Veritas\NetBackup\BEDS\Engine\NTFS\FsUseAsyncIo
```

- Set the registry DWORD value to 1.
If this registry DWORD value already exists and the value is set to something other than 1, change the value to 1.

NetBackup status code 39

Explanation: Microsoft Cluster Server (MSCS) clustered Enterprise Vault database backup is not accepted in NetBackup.

You must configure NetBackup 6.5.4, 6.5.5, or 7.0 Enterprise Vault Agent to protect the Enterprise Vault databases that are hosted by an MSCS clustered Microsoft SQL Server . You need to configure the host name. Add the name of the Virtual SQL server as the client name for each server node.

To add virtual SQL server name for each cluster node

- 1 Select **Start > Symantec NetBackup > Backup, Archive, and Restore**.
- 2 From the **File** menu, select **NetBackup Properties**. The NetBackup Client Properties dialog box is displayed.
- 3 Enter the Virtual SQL server name as the client name in the **Client name** text box.

- 4 A warning is displayed, click **OK**.
- 5 Click **OK** to exit the NetBackup Client Properties dialog box.

After you add the virtual SQL server name for each cluster node, configure the cluster nodes and the virtual SQL server for Enterprise Vault.

To configure cluster nodes and virtual SQL server for Enterprise Vault

- 1 On the NetBackup Administration Console , expand **Host Properties**.
- 2 From the **Actions** menu, select **Configure Client**.
- 3 Browse and select the required computer and click **OK**.
- 4 Click **OK** to exit the Choose Client dialog box.
- 5 From the Host Properties list, select **Clients**. The available clients are displayed.
- 6 Right-click the required client and select **Properties**. The Client Properties dialog box is displayed.

For each node and cluster, configure the log on account to be the Enterprise Vault Admin user.

NetBackup status code 59

Explanation: access to the client was not allowed

If you have multiple NetBackup media servers, you should specify all these media servers in the client. You can specify them during the client configuration or from the host properties of the client. If the client is also a media server, you must explicitly add it as media server.

If you encounter error, check whether the names of all of the media servers among the Enterprise Vault servers are specified in the client configuration. You can obtain the media server name from the job details page in Activity Monitor, of the NetBackup Administration Console.

NetBackup status code 69

Explanation: invalid directives within the same policy

If a policy contains the directives that cannot be specified together in the same policy then the policy creation and modification fails with a status code 69.

Recommended action: From the backup selection remove any one of the directive that cannot be specified together.

See [“About Enterprise Vault directives and what data they back up”](#) on page 55.

NetBackup status code 156

NetBackup status code 156 is displayed when a snapshot fails. The `VSS_E_BAD_STATE` and `VSS_E_INSUFFICIENT_STORAGE` error messages are displayed.

The `VSS_E_BAD_STATE` message is displayed when the VSS writer is in a bad state, as in if it is not stable. Reset the VSS state to fix this error.

The `VSS_E_INSUFFICIENT_STORAGE` message is displayed when there is insufficient space on the drive to create snapshots. Pre-configure a shadow storage area on a drive to fix this issue.

About the `VSS_E_BAD_STATE` snapshot error

Explanation: A snapshot job has failed with an error `VSS_E_BAD_STATE` error.

The Enterprise Vault agent can cause a snapshot job to fail with a status code 156 error. This status code indicates that a snapshot job has failed with an error `VSS_E_BAD_STATE` and if it is not corrected, subsequent snapshot jobs fail.

If the `VSS_E_BAD_STATE` error occurs a message similar to the following appears in the `bpfis` log file:

```
onlfi_vfms_logf: snapshot services: vss:
"IVssBackupComponents::DoSnapshotSet" failed with error
"VSS_E_BAD_STATE:(error value=0x80042301)" while trying to commit
snapshot set {AF8C691F-4111-46B2-A538-DE7F2670915A}
```

Perform the following to reset the Microsoft Volume Shadow Copy Service (VSS) writer states and to ensure that future snapshot jobs are successful.

To reset the Microsoft Volume Shadow Copy Service (VSS) writer states

- 1 Run `services.msc`.
- 2 Ensure that the **MS Software Shadow Copy Provider service's Startup** type is set to **Manual**.
- 3 Ensure that the **Volume Shadow Copy service's Startup** type is set to **Manual**.
- 4 Run `cmd.exe`.
- 5 From the command line, run `vssadmin list writers`.

This command shows you the state of the VSS writers. If any of them are in a bad state (a state other than Stable) then you must manually reset the writer's state.

- 6** Reset the VSS writer states by running the following commands from the command line:

```
net stop swprv

cd %SystemRoot%\system32

regsvr32 ole32.dll

net stop vss

regsvr32 oleaut32.dll

regsvr32 vss_ps.dll

vssvc /Register

regsvr32 /I swprv.dll

regsvr32 /I eventcls.dll

regsvr32 es.dll

regsvr32 stdprov.dll

regsvr32 msxml.dll

regsvr32 msxml2.dll

regsvr32 msxml3.dll

regsvr32 msxml6.dll

net start "COM + Event System"
```

Note: Verify that the msxml6.dll or msxml6r.dll files are in the system32 directory. If they are not present in the directory, then run the Windows update to get the .dll files. Finally, run the `regsvr32` command again for these DLLs after you have verified that they are in your system32 directory.

- 7** If you are on a Windows 2003 system, run the command, `regsvr32 vssui.dll` from the command line. If your computer is not running Windows 2003, then you can skip this step.
- 8** Restart your computer.

After you restart the computer you should run the following commands:

- `C:\> vssadmin list writers`
- To make sure that all VSS writers are in stable state.
- `C:\> vssadmin list shadows`

The result of this command should show no existing shadow copies.

About the VSS_E_INSUFFICIENT_STORAGE snapshot error

During a snapshot, if VSS finds that no shadow storage area is configured for the requested drive it attempts to create a storage area. An attempt is made to create the shadow storage area on the same drive first. For example, if the `D:\` drive is the requested drive, it attempts to create the shadow storage area on the `D:\` drive. If it cannot create a shadow storage area on the requested drive, it tries to create a shadow storage area on some other drive.

If there is not enough room on the selected drive where the storage area is created, the snapshot fails with a `VSS_E_INSUFFICIENT_STORAGE` error.

Preconfigure a shadow storage area on a drive to avoid this issue. However, if that storage area is not large enough it can cause the snapshot to fail with the same error.

Another way to resolve this issue is to remove any stale snapshots that are present on the drive.

For more information about Microsoft's VSS, refer to the Microsoft Web site. You can use the error names as keywords when searching the Microsoft Web site.

NetBackup status code 1800

Explanation: invalid client list

For Enterprise Vault-type policies, please verify that multiple clients are not added to the list of clients if you specify any of the following Enterprise Vault 8.0 directives in the backup selection:

- `EV_INDEX_LOCATION=`
- `EV_VAULT_STORE_DB=`
- `EV_OPEN_PARTITION=`
- `EV_CLOSED_PARTITIONS=`
- `EV_FINGERPRINT_DB=`
- `EV_READY_PARTITIONS=`

Specify only one client in the policy or from backup selection remove the directive that does not support multiple client.

See [“About Enterprise Vault directives and what data they back up”](#) on page 55.

The NetBackup Enterprise Vault Agent portal is a good place for more information about the NetBackup 6.5.x and 7.0.x Enterprise Vault Agents. See the following URL for more information.

<http://www.symantec.com/business/support/index?page=content&id=TECH126523>

NetBackup Enterprise Vault Migrator

This appendix includes the following topics:

- [About the Enterprise Vault Migrator](#)
- [About configuring a backup policy for migration](#)
- [About configuring Enterprise Vault for collection and migration](#)
- [About NetBackup Enterprise Vault migrator registration](#)
- [Register NetBackup Enterprise Vault migrator](#)
- [Testing the Enterprise Vault migrator configuration](#)
- [Setting the recommended DCOM settings](#)
- [Restoring Enterprise Vault migrated data from NetBackup](#)
- [Troubleshooting the Enterprise Vault migrator](#)

About the Enterprise Vault Migrator

As the amount of data that companies store continues to grow, they must find ways to scale their storage environments to accommodate the growth. More importantly, companies continue to scrutinize how their data is managed and retained in the most cost-effective ways as possible.

Enterprise Vault migrator enables you to automatically migrate data from primary disk storage locations to more cost-effective secondary disk storage locations. You can now define automatic, policy-based migration strategies to move archived data from Enterprise Vault-managed disks to NetBackup-managed media types.

When you use NetBackup with Enterprise Vault, archived items from Enterprise Vault can be automatically stored and retrieved on the storage devices that NetBackup manages. All archived items are first stored within a vault store partition within Enterprise Vault. After Enterprise Vault archives the item, a collection process is run and that result it is placed into a CAB file. Once the CAB file is created, it is now ready to be migrated from Enterprise Vault to NetBackup using a migration process. The Enterprise Vault migration process calls the NetBackup migration process, which starts a backup of the CAB files by a NetBackup policy. Once the backup is complete, Enterprise Vault truncates the vault store partition copy of the CAB file. That reduces the Enterprise Vault disk storage space and leverages the investments that were made in the NetBackup infrastructure.

During the NetBackup migration process multiple copies can be made using inline tape copies. Disk storage units (DSUs) and disk storage staging units (DSUs) are also supported for the NetBackup-controlled migrations that are direct to disk. However, Symantec recommends that you keep traditional backups separate from Enterprise Vault data because the retention requirements are likely to be very different.

About configuring a backup policy for migration

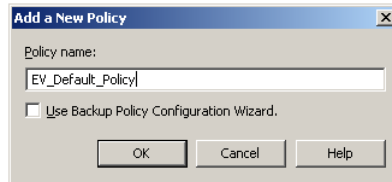
You must create a NetBackup backup policy through which the Enterprise Vault migration can take place. The following procedure describes how to create the backup policy.

To create a NetBackup backup policy for an Enterprise Vault migration

- 1 Log on to the master server as administrator. Start the NetBackup Administration Console .
- 2 If your site has more than one master server, select the one where you want to add the policy.
- 3 Add a new policy by making the appropriate selection:
 - In the left pane, right-click **Policies**. Select **New Policy** (Windows interface).
 - In the left pane, click **Policies**. In the **All Policies** pane, right-click the master server and click **New Policy** (Java interface).

- 4 In the **Add a New Policy** dialog box, in the **Policy name** field, type a unique name for the new policy.

You can specify any name that you want. However, make a note of this name because you may use it again when you configure Enterprise Vault in a later step.

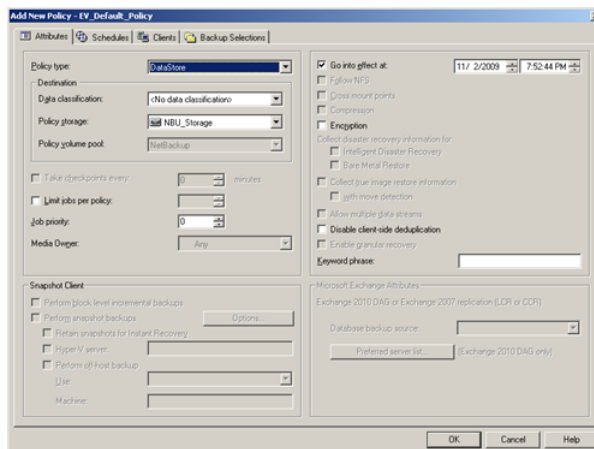


- 5 Uncheck the **Use Backup Policy Configuration Wizard** check box.

By default, this option is checked. When this check box is checked, the **Backup Policy Configuration** wizard appears and guides you through the backup policy creation process. To manually create a new policy, uncheck this check box.

- 6 Click **OK**.

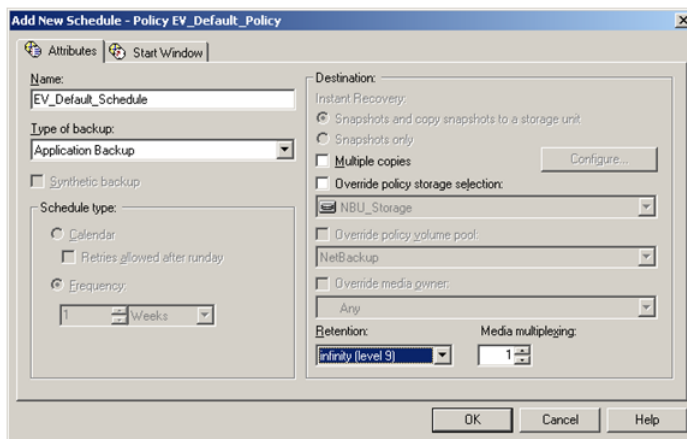
- 7 On the **Attribute** tab of the **Add a New Policy** dialog box, select the **DataStore** policy type from the **Policy type** drop-down list.



- 8 Complete the entries on the **Attributes** tab.
- 9 Continue by creating a schedule for the policy with the following attributes:
 - Enter the name of the schedule. The name must be `EV_Default_Schedule`.

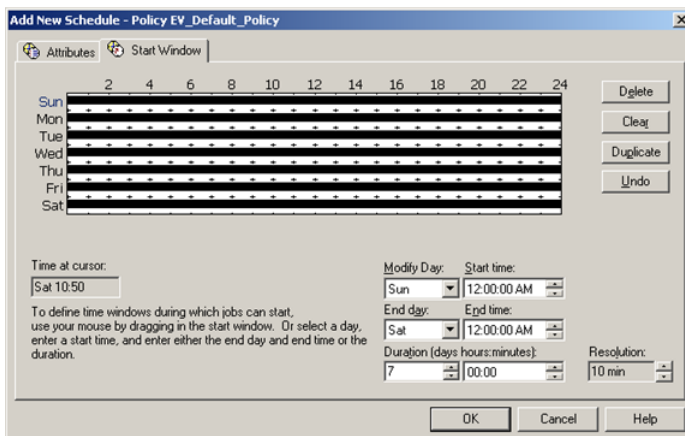
The name of the schedule is not configurable and is expected to be EV_Default_Schedule.

- Set the type of backup to **Application Backup**.
- Set the retention period to **infinity (level 9)**.
 When you specify the retention level as **infinity (level 9)**, you allow Enterprise Vault to have full control on the life cycle of migrated data. When Enterprise Vault wants to delete a migrated file, NetBackup is explicitly notified to delete it.



- 10 Specify backup window of schedule. Click the **Start Window** tab to define the period of time during which the backup starts and ends.

The schedules should be set to allow backups and restores to happen at any time. The Vault Store Partition configuration controls the Enterprise Vault migration (backup) times.

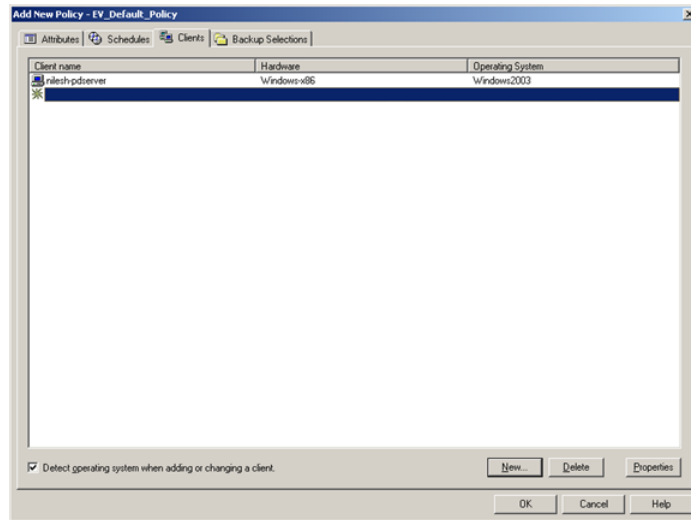


- 11 Click **OK**.

- 12 Specify a NetBackup client for the policy. In the **Policy** dialog box, click the **Clients** tab.

You should use the name of the Enterprise Vault server whose data is to be migrated in the NetBackup client for the policy.

To access the **Policy** dialog box, double-click the policy name in the client list in the NetBackup Administration Console.



- 13 Click **OK**.

You do not need to specify policy directives because the file names are passed automatically between Enterprise Vault and NetBackup.

NetBackup administrators may find the following notes helpful when configuring a NetBackup policy for the Enterprise Vault migrator:

- You should take additional tape drives and storage slots into consideration when you use the NetBackup migrator feature to store Enterprise Vault data.
- If tapes are removed from the library, timeouts can occur and you may not be able to automatically retrieve your data.
- Timeouts can occur if all tape drives are in use when an Enterprise Vault user or application accesses the data that resides in a library.
- Timeouts can occur if a migration occurs (writing to the tape) while data on the same tape is accessed for a retrieval.

About configuring Enterprise Vault for collection and migration

You must configure every Enterprise Vault partition, whose data is to be migrated, for collection and migration. The following procedure explains how to configure Enterprise Vault for collection and migration.

To configure Enterprise Vault for collection and migration

- 1 Specify the collection criteria. From the Enterprise Vault user interface, select the **Collections** tab within the **Vault Store Partition Properties** dialog box.

Define the schedule for when you want the collections to run by setting the attributes on this tabbed page. Symantec recommends that you configure quiet times when archiving and backups are not scheduled.

The collection process enables you to specify how old the DVS files need to be before they are collected. A typical setting is 30, 60, or more days after a DVS file has been archived before it is collected into a CAB file.

- 2 Specify the migration criteria. Select the **Migration** tab within the **Vault Store Partition Properties** dialog box. Set the following attributes on this tabbed page:

- Select the **Migrate files** check box.
- Specify the age after which the collected files become eligible for migration.
- Specify the **Remove collection files from primary storage** settings.
This value sets the amount of time the ARCHCAB files stay in the Vault Storage Partition after the collection is copied to tertiary storage.

- 3 Configure the migration properties. Select the **Advanced** tab within the **Vault Store Partition Properties** dialog box. Set the following attributes on this tabbed page:

- **NBU policy**
The name of the NetBackup policy through which migration is expected to take place.
- **NBU server**
The name of the NetBackup master server.
- You can modify the default values of the other settings if you deem it is necessary.

About NetBackup Enterprise Vault migrator registration

The NetBackup Enterprise Vault migrator is a COM server that is shipped with the NetBackup 7.1 or later versions. In addition, the NetBackup Enterprise Vault migrator also ships with all Enterprise Vault releases before 7.1, including Enterprise Vault 8.0 SP2 or later. However, from the Enterprise Vault 8.0 SP3 release, the NetBackup Enterprise Vault migrator ships only with NetBackup.

When NetBackup 7.5 is installed, there is a possibility that the NetBackup Enterprise Vault Migrator gets installed twice in some customer's configuration. The migrator can get installed during NetBackup 7.5 installation and also during the Enterprise Vault installation (version EV 8 SP2 or an earlier version).

The following list describes the different scenarios that can arise depending on whether NetBackup is installed before Enterprise Vault or vice versa:

- NetBackup 7.1 or later is installed after Enterprise Vault (8.0 SP2 or an earlier version).

In this scenario Enterprise Vault is already installed and a version of the NetBackup Enterprise Vault migrator was installed with it. When the NetBackup installation starts, the NetBackup 7.1 or later version of the Enterprise Vault migrator is installed. When that happens Enterprise Vault uses the NetBackup Enterprise Vault migrator that is installed with NetBackup 7.1 or later. You do not need to do anything to register the migrator; it is done automatically.

- Enterprise Vault (8.0 SP2 or earlier releases) is installed after NetBackup 7.1. In this scenario, the NetBackup 7.1 or later version of the NetBackup Enterprise Vault migrator was installed when NetBackup 7.1 or later was installed. When Enterprise Vault is installed, an earlier version of the Enterprise Vault migrator is installed and registered. This version of the migrator is not as new as the version that is installed with NetBackup 7.1 and later and it is not the appropriate version for Enterprise Vault to use. Again, it is important that Enterprise Vault use the migrator that NetBackup 7.1 or later is registered with.

You should ensure that Enterprise Vault uses the Enterprise Vault migrator that was installed with NetBackup. To register the correct version, you must manually register the NetBackup Enterprise Vault migrator that is installed with NetBackup 7.1 or later after the Enterprise Vault installation completes.

See [“Register NetBackup Enterprise Vault migrator”](#) on page 131.

Register NetBackup Enterprise Vault migrator

To manually register the NetBackup Enterprise Vault migrator installed by NetBackup

- 1 Stop all Enterprise Vault services on all systems where Enterprise Vault is installed.
 - Start the service **Control Manager**.
 - Make a note of all of the Enterprise Vault services that are currently running. The names of the Enterprise Vault services begin with *Enterprise Vault*.
 - Stop all of the Enterprise Vault services.
- 2 Register the new NetBackup 7.1 Enterprise Vault migrator module.
 - Open a Command prompt window.
 - Go to the `NetBackup\bin` directory.
 - Type the following command to register the NetBackup 7.1 Enterprise Vault migrator module, `NBUMigrator.exe`.
NBUMigrator.exe /RegServer
- 3 Start the Enterprise Vault services that were stopped in Step 1.

After you have registered the Enterprise Vault migrator, Symantec recommends that you do the following:

 - Test your migrator configuration.
See [“Testing the Enterprise Vault migrator configuration”](#) on page 131.
 - Set the recommended DCOM settings so the migrator runs under the proper user identity.
See [“Setting the recommended DCOM settings”](#) on page 134.
Symantec recommends that you review this topic irrespective of whether you have performed a manual registration or not.

Testing the Enterprise Vault migrator configuration

After you have installed and registered the Enterprise Vault migrator, Symantec recommends that you test the configuration, especially if you manually registered the migrator. If you choose to not register the migrator, then you can skip this section.

Registration can occur automatically by the NetBackup installation process or it you can do it manually. Manual registration may be required after NetBackup 7.0

is installed for versions of Enterprise Vault that are earlier than Enterprise Vault 8.0 SP2.

See “[About NetBackup Enterprise Vault migrator registration](#)” on page 130.

This procedure helps you identify any issues in the registration of the new component. The following procedure steps you through this process.

To test the Enterprise Vault migrator configuration

- 1 Determine if any Enterprise Vault partitions exist. If previously configured partitions exist, proceed to Step 2.

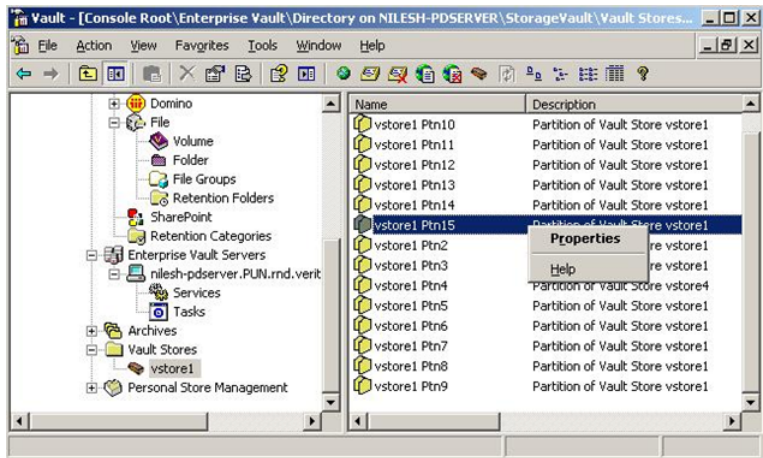
If no Enterprise Vault partitions have been configured for migration, then Symantec recommends that you download the following white paper on Enterprise Vault integration. This paper contains information on archiving and migration, and how to configure Enterprise Vault with NetBackup. (Symantec recommends that you focus your attention on the NetBackup Configuration and Enterprise Vault Configuration sections.) After you have finished configuring the migrator, you can proceed to Step 2.

See the following document for more information:

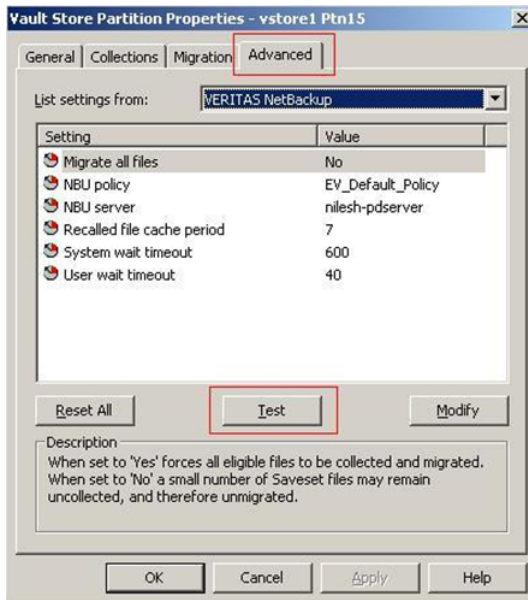
http://eval.symantec.com/mktginfo/products/White_Papers/Data_Protection/ent-whitepaper_veritas_nbup_and_veritas_ev_integration_02-2006.en-us.pdf

- 2 Open the Enterprise Vault Administration Console.
- 3 Select a partition that has been configured for migration.

- 4 Right-click on the partition and select **Properties**.



- 5 Select the **Advanced** tab in the **Vault Store Partition Properties** dialog box and click the **Test** option.



If the test is successful, a dialog appears that states the Migrator Configuration Test was successful.

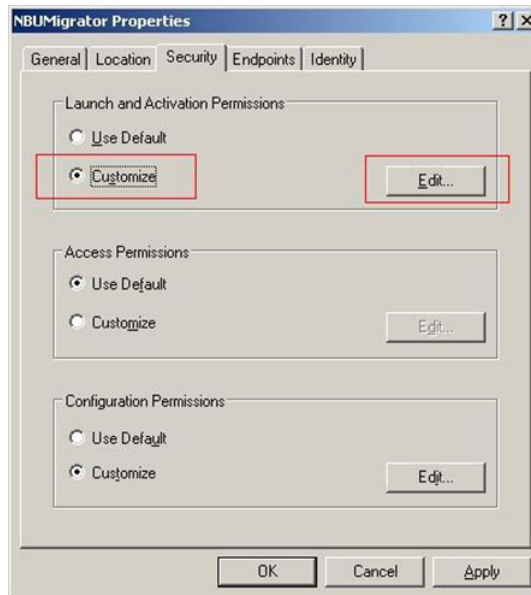
Setting the recommended DCOM settings

You should configure the DCOM settings so that the migrator runs under the identity of the user who launched it. In addition, you should configure the DCOM settings to allow members of the local administrator's group and the SYSTEM group to perform the following:

- Launch the Enterprise Vault migrator locally and remotely.
- Activate and access the Enterprise Vault migrator locally and remotely.

To apply the recommended DCOM settings

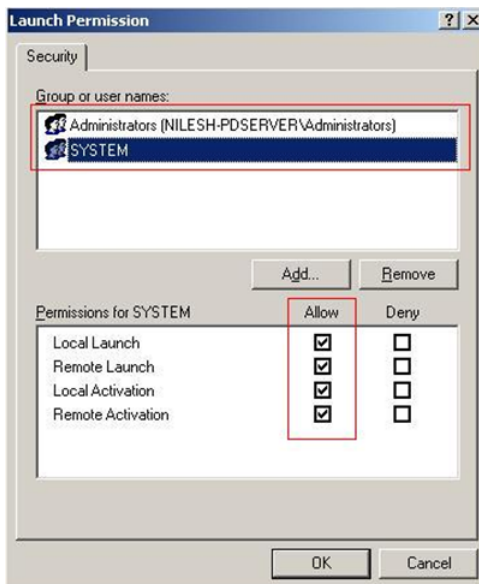
- 1 Start the application dcomcnfg.exe.
- 2 Search for **NBUMigrator** under, Component Services > **Computers** > **My Computer** > **DCOMConfig**.
- 3 Right-click **NBUMigrator** and select **Properties**.
- 4 Select the **Securities** tab.
- 5 In the **Launch and Activation Permissions** field, select the **Customize** option and then click **Edit**.



- 6 From the **Launch Permission** dialog box make sure that only the following groups are in the Group or user names field:
 - Local administrator's group

- **SYSTEM** group

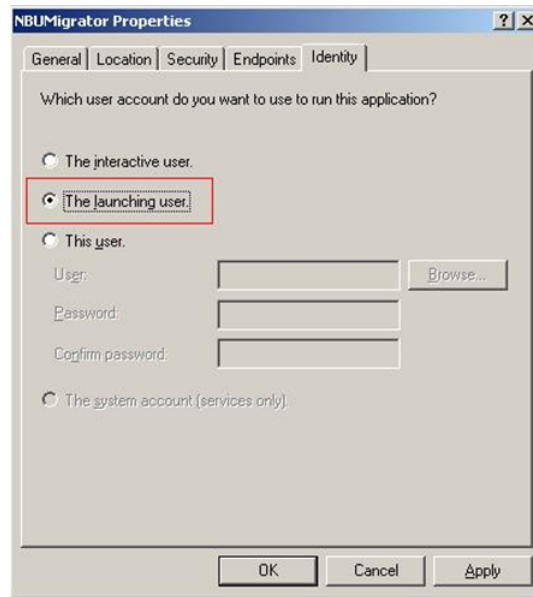
In the **Permissions for SYSTEM** field, ensure that both groups are given full permissions and click **OK**.



- 7 On the **Securities** tab, select the **Customize** option in the **AccessPermissions** field, then click **Edit**.
- 8 From the **Access Permission** dialog box make sure that only the following groups are in the Group or user names field:
 - Local administrator's group
 - **SYSTEM** group

In the **Permissions** field, ensure that both groups are given full permissions and click **OK**.
- 9 Select the **Identity** tab.

10 Select **The launching user** option.



11 Click **OK**. The DCOM configurations settings have been applied.

Restoring Enterprise Vault migrated data from NetBackup

Enterprise Vault enables you to seamlessly access archived data. More importantly, you can seamlessly access archived data that has been migrated from Enterprise Vault secondary storage to NetBackup tertiary storage. When you access archived data that has been migrated, Enterprise Vault automatically restores the data from the NetBackup tertiary storage to the Enterprise Vault secondary storage. Enterprise Vault then restores the data from the Enterprise Vault secondary storage to a destination client of your choosing.

However, in certain scenarios it may be more convenient and effective to manually invoke the restore of migrated data from the NetBackup tertiary storage to the Enterprise Vault secondary storage. The following list shows some examples of when it may be more beneficial to manually perform the restore:

- To rebuild an index
- To rebuild an offline vault
- To export an archive

- For disaster recovery

NetBackup enables you to manually restore migrated data onto the Enterprise Vault secondary storage using one of the following methods:

- The command line interface
- The Backup, Archive, and Restore user interface

Restoring migrated data using the command line interface

The `bprestore` command contains a new parameter that is designed to migrate NetBackup data. For restoring the data that has been migrated from Enterprise Vault, you must pass a new parameter `-ev_migrated_data` to the `bprestore` command line. If the `-ev_migrated_data` parameter is passed to `bprestore`, NetBackup expects that the data being restored is data that has been migrated from Enterprise Vault. The restore is then performed accordingly.

Note: Other required parameters of the command line interface need to be passed appropriately for the restore operation to complete successfully.

If the `-ev_migrated_data` parameter is passed to `bprestore`, the data being restored must be Enterprise Vault-migrated data. Attempting to use this parameter to restore the data that is not Enterprise Vault-migrated data can result in unpredictable behavior, and is not supported.

The following is an example of how you can use the `bprestore` command to restore Enterprise Vault-migrated data.

```
bprestore -S NBU Master Server Name -C Enterprise Vault Server Name
-t 24 -ev_migrated_data Files_to_Be_Restored
```

Restoring migrated data using a Backup, Archive, and Restore user interface

You can use the Backup, Archive and Restore user interface on a Windows, UNIX, or Linux platform to restore Enterprise Vault-migrated data. Perform the following procedure to restore migrated data from NetBackup no matter what system you run the Backup, Archive, and Restore user interface from.

To restore Enterprise Vault migrated data using the Backup, Archive, and Restore user interface

- 1 Start the Backup, Archive, and Restore user interface.
- 2 Open the **Specify NetBackup Machines and Policy Type** dialog box.

- Select **File > Specify NetBackup Machines and Policy Type**. (Windows interface)
 - Select **Actions > Specify NetBackup Machines and Policy Type**. (Java interface)
- 3 From the **Specify NetBackup Machines and Policy Type** dialog, perform the following:
- Select the server to use for backups and restores.
 - Designate the source client for the restore.
 - Designate the destination client for the restore.
 - Select **DataStore** in the **Policy type for restores** field.
- 4 Select the list of backups to be restored in the **NetBackup History** field of the user interface and then click the **Restore** icon.
- Make sure that you have selected only Enterprise Vault migrated backups to be restored.
- 5 From the **Restore Marked Files** dialog box, select the **Restore as Enterprise Vault migrated data** check box.
- 6 Click **Start Restore**.

Troubleshooting the Enterprise Vault migrator

This topic provides some useful instruction that can help you troubleshoot the NetBackup Enterprise Vault migrator. Also included is Enterprise Vault migrator version information and detailed instructions on how to collect Enterprise Vault and NetBackup debug logs.

Enterprise Vault migrator version information

The following table shows the Enterprise Vault migrator version compatibility information for the different NetBackup releases.

File name	NetBackup release compatibility	Description
NBUMigrator.dll	Pre-NetBackup 6.5.2 releases	This Enterprise Vault migrator was shipped with Enterprise Vault.

File name	NetBackup release compatibility	Description
NBUMigrator.exe	NetBackup 6.5.2 through 6.5.4	This version of the Enterprise Vault migrator was made available as a download on the Symantec Support Web site. See http://entsupport.symantec.com/docs/327571 .
NBUMigrator.exe	NetBackup 7.1	This version of the Enterprise Vault migrator is shipped with NetBackup 7.1.

About troubleshooting issues with the migrator

The following topics explain the steps to take if you encounter a problem while you use the Enterprise Vault migrator.

Is the data being archived?

To verify that data is archived, ensure that the `.dvs` and the `.dvh` files are created in the partition for the archived files.

Is the data being collected?

You should verify following collection criteria:

■ Collection age

From the **Vault Store Partition Properties** dialog box, you should verify the setting that you configured for the **Collect files older than** field. This field is located on the **Collections** tab. Make sure that you specify the age appropriately.

■ Minimum files in collection criteria

You can override the default minimum file value by creating a registry key `HKEY_LOCAL_MACHINE\SOFTWARE\KVS\Enterprise Vault\Storage\MinimumFilesInCollection`. That is a **DWORD** value and the data should specify the minimum number of files that can be present in a collection file.

To verify that the data is collected, ensure that the `.dvs` and the `.dvh` files in the partition are converted to `CAB` files.

Is the migration being configured appropriately?

From the **Advanced** tab on the **Vault Store Partition Properties** dialog box, you can configure a partition for migration. Make sure that you enter the value of **NBU Policy** and **NBU Server** correctly.

To verify that you configured the migration properly, click **Test**.

If the test fails, and the **NBU Policy** and **NBU Server** configurations are correct, the issue could be due to one of the following reasons:

- The `xbsa` (Datastore) license is not installed in NetBackup.

If the Datastore license is not installed in NetBackup, the test fails. The user interface does not provide any notification that a licensing issue is the cause of the failure.

If it is a licensing issue, the following message (or something similar) appears in the `exten_client` logs.

```
InvalididParameterHandler bsa_checkfeatureID: None of the features
are licensed.
```

This string may also appear in the `Dtrace` logs.

```
Failed to initialize xBSA. Make sure NetBackup client is installed
and configured.
```

To resolve this issue, perform the following:

- Install the required NetBackup license.
- Restart the NetBackup services. Do that only if it is required.
- NBUMigrator is not registered.

In certain scenarios you must manually install and register the migrator. In this case, if you have not followed the registration steps then the following error appears as an Enterprise Vault pop-up dialog box.

```
The selected file migration software is not registered or
installed. Reason: Class not registered
```

To resolve this issue, register the Enterprise Vault migrator.

See [“Register NetBackup Enterprise Vault migrator”](#) on page 131.

- The `xbsa.dll` is not present in the system path.

In the first version of the Enterprise Vault migrator (`NBUMigrator.dll`), the path of the file `xbsa.dll` needed to be present in the `PATH` environment variable. That is no longer the case with the later releases of the Enterprise Vault migrator. The path is now configured programmatically.

If the `xbsa.dll` is not present in the system path, then the following message is logged on the `Dtrace` logs.

Failed to load xbsa library. Check the Net Backup client installation, ensuring that xbsa.dll is installed.

To resolve this issue perform the following:

- Add the path of `xbsa.dll` to the `PATH` environment variable. The `xbsa.dll` is present under `NBU_INSTALL_DIRECTORY\bin`.
- Restart the Enterprise Vault Admin Service . Restarting this service restarts all of the Enterprise Vault services. You need to restart all of the Enterprise Vault processes because certain processes may use the migrator (`NBUMigrator.dll`). Restarting them enables them to locate and load the `xbsa.dll`.

Is the data being migrated?

From the **Migration** tab on the **VaultStorePartitionProperties** dialog box, there is an age after which the files satisfy the migration criteria. Make sure that this age is specified appropriately. To verify that the item migration to NetBackup is in progress, ensure that the backup tasks (for the migration policy) appear in NetBackup.

About Log Collection

The NetBackup Enterprise Vault migrator generates logs on Enterprise Vault and NetBackup. The following topics describe how to collect the required logs.

About Enterprise Vault logs

The NetBackup Enterprise Vault migrator uses the `Dtrace.exe` application to generate Enterprise Vault logs.

To run the `Dtrace.exe` application and collect Enterprise Vault logs

- 1 Begin this procedure on the computer where you installed the Enterprise Storage Service.

Typically the 'Storage Service' is installed on and runs on the machine on which the Enterprise Vault Server has been installed. However it is possible for customers to have an environment where the 'Storage Service' is installed on and runs on a machine other than the Enterprise Vault Server.

- 2 Open a command prompt and go to the directory under which Enterprise Vault is installed.

This directory (for example, `C:\Program Files\Enterprise Vault`) contains the `Dtrace.exe` file.

3 Run `Dtrace.exe`.

4 Set verbose logging on the required processes.

Set verbose logging on the following processes when you want to collect migrator logs:

- `StorageFileWatch`
- `EVStgOfflineOpns`
- `StorageManagement`

This process is required to analyze logs when you want to test the Enterprise Vault Configuration.

- `StorageDelete`

This process is required when you want to analyze the logs after you delete a partition whose data has been migrated.

Execute the following commands to set the verbose logging:

- `set StorageFileWatch verbose`
- `set EVStgOfflineOpns verbose`
- `set StorageManagement verbose`
- `set StorageDelete verbose`

```

C:\Program Files\Enterprise Vault>DTrace.exe
DTrace Version <7.5.2.1862>
? for help
DT>set StorageFileWatch verbose
Set Trace Options

Id      Name                Detail    Include Events
-      -
-      - StorageFileWatch  Verbose   Yes

DT>set EVStgOfflineOpns verbose
Set Trace Options

Id      Name                Detail    Include Events
-      -
-      - EVStgOfflineOpns   Verbose   Yes

DT>

```

Enter the command, `view`, to see a list of processes for which you can enable verbose logging.

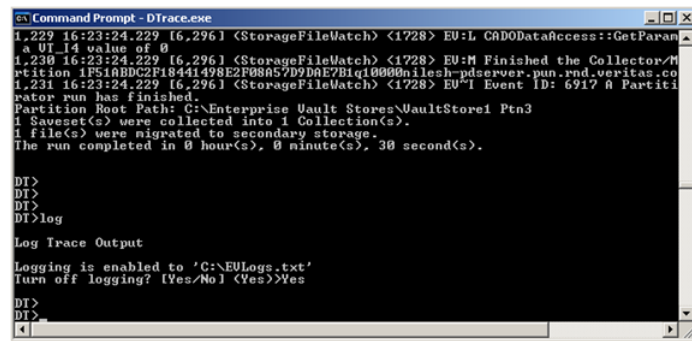
5 Set the log file. From the Command Prompt window, you can execute the command, `log log_file_name`, to set the log file.

As an example, you enter the `log EVLogs.txt` to set the log file to `C:\EVLogs.txt`.

- 6 Enable monitoring. From the Command prompt window, you can execute the command, `mon`, to set monitoring.
- 7 Execute the migrator tasks for which logs are required.
 Execute the tasks (Migration/Retrieval/Deletion) for which logs are required. The Dtrace screen displays the various logs that are generated for the task.
- 8 Press Control-C to exit from the monitoring phase.
- 9 Disable logging.

You must disable the logging to ensure that all log entries are stored in the log file. You can use the command, `log`, to disable logging.

After you type the `log` command, you are prompted to confirm that you want to disable logging. Type, `Yes`.



```

C:\> Command Prompt - DTrace.exe
1.229 16:23:24.229 [6.296] <StorageFileWatch> <1728> EU:l, GADODataAccess::GetParam
a UI_I4 value of 0
1.230 16:23:24.229 [6.296] <StorageFileWatch> <1728> EU:M Finished the Collector/M
Partition 1E5A0D02F1B441498E2F68A57D9DAE7B1q10000nilesh-pdsrver-run-and-veritas.co
1.231 16:23:24.229 [6.296] <StorageFileWatch> <1728> EU:l Event ID: 6917 A Partiti
rator run has finished.
Partition Root Path: C:\Enterprise Vault Stores\VaultStore1 Ptn3
1 SaveSet(s) were collected into 1 Collection(s).
1 file(s) were migrated to secondary storage.
The run completed in 0 hour(s), 0 minute(s), 30 second(s).

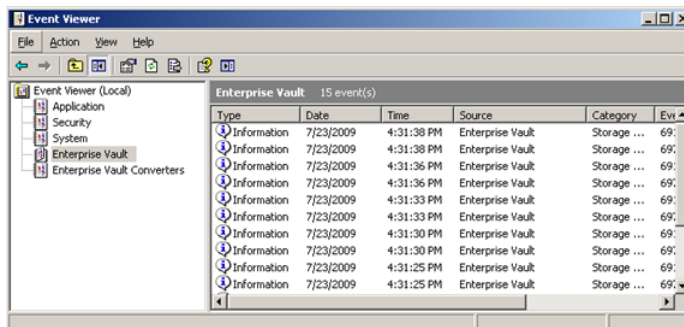
DI>
DI>
DI>
DI>log

Log Trace Output
Logging is enabled to 'C:\EVLogs.txt'
Turn off logging? [Yes/No] <Yes>>Yes
DI>
DI>
    
```

- 10 Collect the log file.
 The log file that was configured in Steps 4 and 5 (`C:\EVLogs.txt`) now contains all of the required logs.

About Enterprise Vault events

The NetBackup Enterprise Vault migrator generates events that specifies the status of most of the tasks that it executes. These events also provide useful information for troubleshooting purposes. From the Event Viewer, you see the events under the header, **Enterprise Vault**. You should view the events on the machine where you installed the Enterprise Vault Storage Service.



About NetBackup logs

The NetBackup Enterprise Vault migrator communicates to NetBackup through the VxBSA module, and the VxBSA logs are the logs that you must collect from NetBackup. Each NetBackup backup takes place through the `bpbkar` process. The restore takes place through a tar process. Thus, it is important that you collect the logs for both these processes.

Note: Use the following procedure as a guideline only. Even though the objectives that are stated within the procedure remain the same, the steps to achieve them may vary with different versions of NetBackup. The same principle also applies to the screen shots provided.

In case of any believed discrepancy, see the *Symantec NetBackup Troubleshooting Guide UNIX, Windows, Linux* for more information.

To collect the Enterprise Vault logs that were migrated to the NetBackup logs

- 1 Go to the NetBackup logs directory.

A *logs* directory resides under the NetBackup installed directory. For example, if NetBackup is installed under the directory, `C:\Program Files\Veritas\NetBackup\`, then the following *logs* directory also exists:

`C:\Program Files\Veritas\NetBackup\logs`

- 2 Create the required directories under the NetBackup logs folder.

You should refer to the following logs as your first point of reference when you investigate the details of any failure:

- vxbsa logs
- bpbkar logs
- tar logs

To enable the creation of these log files you must create the following directories under the NetBackup logs folder (if they do not already exist):

- `exten_client`

Executing `mklogdir.bat` creates several log directories. However, this command does not create the directory, `exten_client`.

- `bpbkar`

- `tar`

The migration can fail because of any failure in the workings of NetBackup. Therefore, even though the first point of investigation should start with the mentioned logs, it is safest to collect all of the logs by executing the command, `mklogdir.bat`.

3 Set the NetBackup logging level to the required level.

You should update the logging level of the NetBackup client through which the migration takes place. Ideally, you should set the logging level to the highest level. You configure the client in the profile through which the migration takes place (for example, `EV_Default_Profile`).

You can update the logging level using the **Client Properties** dialog on either the NetBackup Administration Console or the Backup, Archive, and Restore user interface.

From the **Client Properties** dialog on the Backup, Archive, and Restore user interface, you can configure the Debug logging levels on the **Troubleshooting** tab. Use the following recommended values:

- General: 2
- Verbose: 5

4 Execute the migrator tasks for which logs are required.

5 Collect log files.

Collect the latest files under the following directories:

- `exten_client`

- `bpbkar`

- `tar`

You should collect all the logs files by either creating a .zip file of the NetBackup logs folder, or copying the latest file under every directory under the NetBackup logs folder.

Index

A

- Add clients to a policy 128
- Add new policy 38, 125
- Adding a policy
 - client name 46
- Allowing multiple clients 47
- alternate SQL restore 72
- Archive bit attribute option 53

B

- Backup image restore sets 80–82
- Backup policy
 - Backup schedules
 - Backup selection 37
- Backup Policy Configuration Wizard 39, 125
- Backup schedules 37, 104
- Backup, Archive, and Restore user interface 65, 77, 80, 113, 137
 - All Folders pane
 - NetBackup History pane 67
- Backups
 - Cumulative incremental backups 42
 - Differential Incremental backups 43
 - full backups 42
- backups
 - back up types 42
- Best practices
 - Enterprise Vault agent backups 106
 - Enterprise Vault agent restores 108
- bpbklog 112
- bpfi log 112
- bppfi log 112

C

- client name 46
- Closed partition 57
- closed partitions directive 61
- Collecting migrated Enterprise Vault logs 144
- compatibility information 22

Configuring

- Local media server 36

- Configuring Enterprise Vault
 - for collection
 - for migration 129

consistencies

- closed and ready partitions 100
- database
 - fingerprint databases 100
 - open partition databases 100
 - vault store databases 100
- directory database 101
- Index location 101

- Consistency check 73

- consistency check 72

- Cummulative backup 72

- Cumulative backup 80

D

- Datastore license 140
- debug logging 111
- Differential backup 72, 80
- differential-incremental backups 43
- Disaster recovery requirements 85
- DVS files 129

E

- enable debug logging 112
- Enterprise Vault
 - client name 105
- Enterprise Vault 7.5 directives 45, 103
- Enterprise Vault 8.0 directives 45
- Enterprise Vault Agent
 - components
 - archives 13
- Enterprise Vault agent functionality and support for EV 7.5 and later 109
- Enterprise Vault Agent policy
 - Backup Selections tab 43
- Enterprise Vault agent user-credentials 34
- Enterprise Vault auditing database 59

- Enterprise Vault backup
 - backup manually 62
 - from NetBackup Activity Monitor 63
- Enterprise Vault backup policy
 - policy type 38
- Enterprise Vault data restore 65
- Enterprise Vault directives 55
 - 7.5 directives
 - 8.0 directives 29
 - what they back up 56
 - 8.0 directives
 - what they back up 58
- Enterprise Vault disaster recovery 66
- Enterprise Vault events 143
- Enterprise Vault file system component
 - closed partition 76
 - Enterprise Vault index 76
 - open partition 76
 - ready partition 76
- Enterprise Vault file system components 70
- Enterprise Vault file system data 66, 69
- Enterprise Vault index locations 56, 60
- Enterprise Vault index service 18
- Enterprise Vault logs
 - for Enterprise Vault migrator
 - Dtrace.exe application 141
- Enterprise Vault Migrator
 - Configure backup policy 124
 - log collection 141
- Enterprise Vault restore options
 - Database Settings tab 71
 - General tab 70
- Enterprise Vault secondary storage 136
- Enterprise Vault server directive 58
- Enterprise Vault Server Log On account 35
- Enterprise Vault services
 - Indexing Service 50
 - Shopping Service 50
 - Storage Service 50
 - Task Controller Service 50
- Enterprise Vault site directive 58
- Enterprise Vault SQL databases 66, 69
- Enterprise Vault Storage Service 18
- Enterprise Vault tools 89, 97, 106
- Enterprise Vault, vault store 56
- Enterprise Vault, vault store database 61
- Enterprise-Vault policy type 39
- EV_AUDIT_DB 31
- EV_FINGERPRINT_DB 31

- EV_FSAREPORTING_DB 31
- Event Viewer 143

F

- fingerprint database 62
- FSA Reporting database 60
- Full backup 72, 80

G

- Granular quiescence
 - backup mode 51

I

- installation
 - adding a license key 26
 - platform compatibility 22
- Installation requirements 22

J

- Java interface 33

L

- license keys, adding 27

M

- maximum jobs parameters 41
- Microsoft Core XML Services 18
- Microsoft's Common Internet File System 18
- Migrator communication to NetBackup
 - VxBSA module
 - VxBSA logs 144
- Migrator registration 130
 - manual registration 131
- Migrator troubleshooting techniques 139
 - data archiving 139
 - data collection 139
 - data migration 141
 - migration configuration 140
- Migrator version information 138
- multiple clients 47

N

- NetBackup logs 144
- NetBackup troubleshooting status codes 115
 - status code 13 116
 - status code 156 118

NetBackup troubleshooting status codes *(continued)*
 status code 1800 120
 status code 2 115
 status code 59 117
 status code 69 117
 Netbackup troubleshooting status codes
 status code 39 116

O

Open partition 57
 open partition directive 60
 Operational reports 114

P

Partition secure notification file 53
 PartitionSecuredNotification.xml file 53
 platform compatibility 22
 Point in time (PIT) restore 72
 Point-in-time recovery 73
 Policy
 Schedule 41
 Policy attributes 37
 Policy configuration
 Enterprise Vault 8.0 100
 policy configuration
 attributes 40
 Policy creation
 Enterprise Vault 7.5 103
 policy type 40
 policy validation 40
 progress reports 114

Q

quiescing Enterprise Vault 8.0 50

R

ready partitions directive 61
 Recovering a auditing database 87
 Recovering a directory database 87
 Recovering a fingerprint database 91
 Recovering a FSA Reporting database 88
 Recovering a Monitoring database 89
 Recovering a vault store database 92
 Recovering a vault store group 90
 Recovering a vault store partition 93
 Recovering an Enterprise Vault server 94
 Recovering an Enterprise Vault server on a different
 system 96

Recovering an Enterprise Vault site 86
 Recovering Enterprise Vault partitions 94
 Recovering index locations 89
 Redirected restore 73
 Restore completion state 72
 restores
 Enterprise Vault Resources 70, 83
 Restoring Enterprise Vault auditing database 79
 Restoring Enterprise Vault data 69
 Restoring Enterprise Vault directory database 79
 Restoring Enterprise Vault file system component 77
 Restoring Enterprise Vault file system data 76
 Restoring Enterprise Vault fingerprint database 79
 Restoring Enterprise Vault FSA Reporting
 database 79
 Restoring Enterprise Vault migrated data 136
 Restoring Enterprise Vault monitoring database 79
 Restoring Enterprise Vault SQL database components
 auditing database 83
 directory database 82
 fingerprint database 83
 FSA Reporting database 83
 monitoring database 83
 vault store database 83
 Restoring Enterprise Vault SQL databases 79
 auditing database 79
 directory database 79
 fingerprint database 79
 FSA Reporting database 79
 monitoring database 79
 vault store database 79
 Restoring Enterprise Vault vault store database 79
 Restoring migrated data
 using a Backup, Archive, and Restore user
 interface 137
 using the command line interface 137

S

safety copies, managing 53
 Schedule
 adding 41
 Setting the debug level 113
 Snapshots 35
 maximum number
 MaxSnapshotPerJob 36
 Socket buffer size
 change buffer size
 set buffer size 108
 Specify collection criteria 129

- Specify migration criteria 129
- Specifying a backup window in a schedule 127
- Specifying the server for restore
 - clients
 - policy type 74
- SQL database
 - directory database 56, 59
 - Enterprise Vault, vault store database 57
 - monitoring database 56, 59

T

- Troubleshooting Enterprise Vault Agent
 - debug logs
 - status reports 111
- Troubleshooting the Enterprise Vault migrator 138

U

- Upgrade scenarios 27
- Useful tips 109

V

- Viewing backup data
 - via Backup, Archive, and Restore interface 67
 - via Microsoft SQL Server Management Studio 68

W

- Windows interface 33