NetBackup™ for Enterprise Vault Agent Administrator's Guide

for Windows

Release 11.2

VERITAS
now part of Cohesity

NetBackup™ for Enterprise Vault™ Agent Administrator's Guide

Last updated: 2026-05-28

Legal Notice

Cohesity Support

Reach Cohesity Support

There are several ways to create a Cohesity support case.

- Go to Cohesity Support, to search in our knowledge base; or contact us by phone - United States and Canada: 1-855-9CO-HESI (926-4374), option 2.
- Log in to the Cohesity Support Portal to create a new case.
- Click the (**?**) icon on the Cohesity UI and select Support Portal.

Support/Service Assistance

First, contact the Service Provider that you have contracted for service and support. If you work directly with Cohesity and have a product warranty/entitlement, repair pricing, or technical support-related question, see your options below:

- To find solutions to your product issues or for suggestions or best practices, visit the Cohesity Knowledge Base.
- Log in to the Cohesity Support Portal to create a new case.
- To monitor your open cases, log in to the portal and click the **Cases** tab on the home page. This page should have all the case statuses and updates. You can also view individual case status.

Cohesity Software Running on Partner Hardware

For Cohesity software running on qualified third-party hardware, the following support workflow applies:

1. The customer may contact Cohesity Support first if the issue cannot be determined as a hardware issue.

   Note: Cohesity cannot process hardware replacement requests for partner hardware.

2. Cohesity Support triages the issue. If it is a software issue, Cohesity Support continues to work on it.
3. If it is a hardware/firmware issue or is suspected to be a hardware/firmware issue, Cohesity provides information about the issue to the customer and requests that the customer open a support ticket with the appropriate partner.
4. If needed, Cohesity Support can join a three-way call with the partner and the customer.
5. The customer informs Cohesity Support on the progress of the partner's case.

Contents

Chapter 1 Introduction to NetBackup Enterprise Vault 8

About Enterprise Vault 8
About the NetBackup Enterprise Vault Agent 9
About the Enterprise Vault Agent and the backup components 9
Enterprise Vault agent features 11
Enterprise Vault agent requirements 13

Chapter 2 Installing NetBackup for Enterprise Vault 14

Planning the installation of NetBackup for Enterprise Vault 14
Verifying the operating system and platform compatibility 15
NetBackup server and client requirements 15
About Enterprise Vault agent installation requirements in a cluster 16
Configuring Enterprise Vault Agent to protect Enterprise Vault databases 17
License for NetBackup for Enterprise Vault 18

Chapter 3 Configuration 19

Specifying a logon account for the Enterprise Vault server 19
About VSS-based snapshot configuration 21
Configuring the local media server for Enterprise Vault backup 23
Configuration requirements for an Enterprise Vault backup policy 24
Adding an Enterprise Vault policy 25
Enterprise Vault backup policy attributes 25
Adding schedules to an Enterprise Vault policy 26
About the types of Enterprise Vault backups 27
Creating a backup selections list 28
Adding a client to a policy 30

Chapter 4 About features provided by Enterprise Vault for a backup provider 31

About Enterprise Vault quiescence before a backup 31
About granular quiescence 32
About managing safety copies and backups 32

About the partition secure notification file 33
About the archive bit 33

Chapter 5 Performing backups of Enterprise Vault 35

About Enterprise Vault directives and what data they back up 35
Manually backing up Enterprise Vault resources 39
Canceling an Enterprise Vault backup job from the Activity monitor 39

Chapter 6 Performing restores of Enterprise Vault 41

Important notes about Enterprise Vault data restore 41
Stopping the administrative services on Enterprise Vault servers 43
About the Backup, Archive, and Restore interface 43
Viewing backup data using the Microsoft SQL Server Management Studio 44
Restoring Enterprise Vault data 45
About the Enterprise Vault restore options on the General tab 48
About the Enterprise Vault Database Settings tab 49
Specifying the server, clients, and policy type for restores 52
About restoring Enterprise Vault file system data 54
Restoring an Enterprise Vault file system component 55
About restoring Enterprise Vault SQL databases 57
About backup image restore sets 58
Restoring Enterprise Vault SQL database components 61

Chapter 7 Disaster recovery 64

Disaster recovery requirements for Enterprise Vault server 64
About disaster recovery of an Enterprise Vault site 65
Recovering a directory database 66
Recovering an auditing database 66
Recovering an FSA Reporting database 67
Recovering a Monitoring database 67
Recovering index locations 68
Recovering an Enterprise Vault vault store group 69
Recovering a fingerprint database 70
Recovering a vault store database 71
Recovering vault store partition 72
Recovering Enterprise Vault partitions 72
Recovering an Enterprise Vault server 73
Recovering an Enterprise Vault server on a different system 74

Chapter 8 Enterprise Vault Agent support for Enterprise Vault 77

Policy configuration for Enterprise Vault 77
Open partition, vault store database, and fingerprint database consistencies 78
Closed and ready partition consistencies 78
Index location consistencies 79
Directory database consistencies 79
Notes about Enterprise Vault 10.0 backups 79
Exclude file list for index locations 79
Exclude file list for vault partitions 80
Excluding files from the exclude list 80
About planning backup schedules 81
About hosts for Enterprise Vault policies 81
About Enterprise Vault tools 82
About Enterprise Vault agent backups 82
Privileges for Enterprise Vault backup 83
About Enterprise Vault agent restores 83
Changing the socket buffer size for large restores 84
Useful tips about Enterprise Vault agent 84
Enterprise Vault agent functionality and support for Enterprise Vault 85
Differential incremental backup taken after a restore fails for Enterprise Vault 86

Chapter 9 Troubleshooting 87

About troubleshooting 87
About debug logging 87
How to enable debug logging 88
Setting the debug level 89
About status reports 90
About operational reports 90
About progress reports 91
About NetBackup status-related troubleshooting information 91
NetBackup status code 2 91
NetBackup status code 13 92
NetBackup status code 39 92
NetBackup status code 59 93
NetBackup status code 69 93
NetBackup status code 156 94
NetBackup status code 1800 96

Appendix A NetBackup Enterprise Vault Migrator 98

About the Enterprise Vault Migrator 98
Configuring a backup policy for migration 99
About configuring Enterprise Vault for collection and migration 100
Testing the Enterprise Vault migrator configuration 101
Setting the recommended DCOM settings 102
Restoring Enterprise Vault migrated data from NetBackup 103
Restoring migrated data using the command line interface 104
Restoring migrated data using a Backup, Archive, and Restore user interface 104
Troubleshooting the Enterprise Vault migrator 105
Enterprise Vault migrator version information 106
About troubleshooting issues with the migrator 106
About Log Collection 108

Chapter 1

Introduction to NetBackup Enterprise Vault

This chapter includes the following topics:

- About Enterprise Vault
- 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 that are held on network file servers
- Documents that are 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.

https://support.cohesity.com/s/article/article-100040135

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 Enterprise Vault agent enables you to back up and restore the Enterprise Vault file system data and the Enterprise Vault SQL Server 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 the 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. 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 primary server to instantiate the appropriate NetBackup components on the clients for backup.

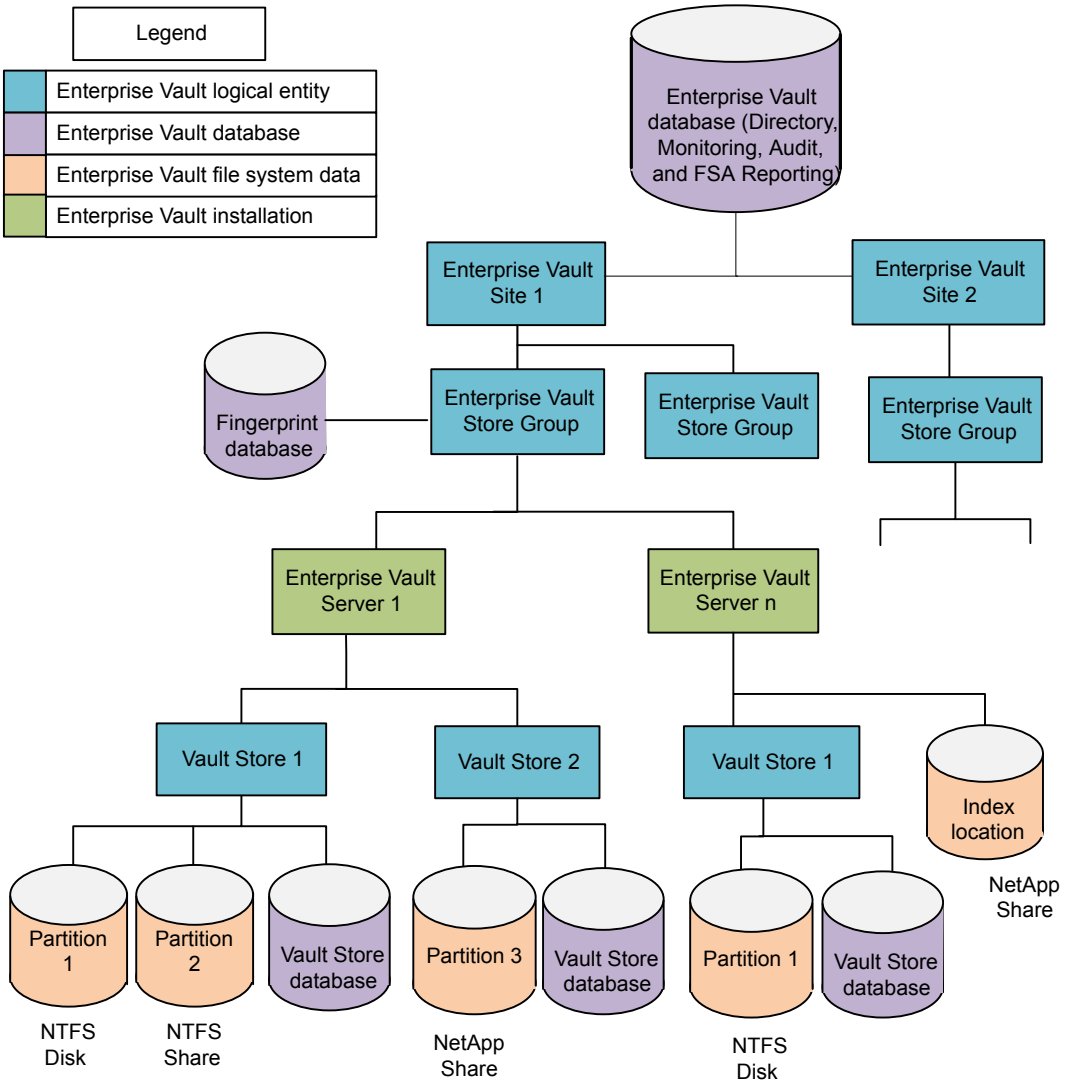
The Enterprise Vault agent enables you to back up and restore the following Enterprise Vault components:

- 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=*EV Site 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 supports streamer based open, closed, and ready partitions.

Figure 1-1 demonstrates how the Enterprise Vault components can be configured in the following hierarchical view.

Figure 1-1 Enterprise Vault 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	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. 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	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.
Tight NetBackup integration	Tight integration with NetBackup means the following: ■ 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 NetBackup Administrator's Guide, Volume I.
Data management	Enterprise Vault agent backups are saved to a wide variety of storage devices that NetBackup supports.
Automated backups	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. In addition, the administrator can manually back up Enterprise Vault archived data and Enterprise Vault configuration data (database) that is stored on different locations.

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

Feature	Description
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 Server databases. This feature enables you to rename or redirect the backup objects for the file system data. For SQL Server objects, this feature supports redirected restores and it supports the renaming of an Enterprise Vault SQL Server database name. However, this feature does not support the renaming of the physical files that are associated with an SQL Server database.
Local media server	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. See "Configuring the local media server for Enterprise Vault backup" on page 23.

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) are installed on the Enterprise Vault server. You can download and install MSXML from Microsoft Corporation's website.
- 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 EV 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.

Chapter 2

Installing NetBackup for Enterprise Vault

This chapter includes the following topics:

- Planning the installation of NetBackup for Enterprise Vault
- Verifying the operating system and platform compatibility
- NetBackup server and client requirements
- About Enterprise Vault agent installation requirements in a cluster
- Configuring Enterprise Vault Agent to protect Enterprise Vault databases
- License for NetBackup for Enterprise Vault

Planning the installation of NetBackup for Enterprise Vault

Perform the following tasks before you use NetBackup for Enterprise Vault.

Table 2-1 Installation steps for NetBackup for Enterprise Vault

Step	Action	Description
Step 1	Verify the operating system and platform compatibility.	See "Verifying the operating system and platform compatibility " on page 15.
Step 2	Verify the NetBackup software requirements for NetBackup for Enterprise Vault.	See "NetBackup server and client requirements" on page 15.

Table 2-1 Installation steps for NetBackup for Enterprise Vault *(continued)*

Step	Action	Description
Step 3	Verify that primary server has a valid license for NetBackup for Enterprise Vault and any NetBackup options.	See "License for NetBackup for Enterprise Vault" on page 18.

Verifying the operating system and platform compatibility

Verify that the NetBackup for Enterprise Vault agent is supported on your operating system or platform.

To verify operating system and compatibility

1. Go to the NetBackup compatibility list site.

   https://support.cohesity.com/s/article/article-100040093

2. Select the link for the following document:

   Application/Database Agent Compatibility List

NetBackup server and client requirements

Before you install NetBackup, review the requirements for the NetBackup server and the NetBackup clients.

NetBackup server requirements

Verify that the following requirements are met for the NetBackup server:

- The NetBackup server software is installed and operational on the NetBackup server.
  See the NetBackup Installation Guide.
- Make sure that you configure any backup media that the storage unit uses. The number of media volumes that are required depends on several things:
  - The devices that are used and the storage capacity of the media.
  - The sizes of the databases that you want to back up.
  - The amount of data that you want to archive.
  - The size of your backups.
  - The frequency of backups or archives.

- The length of retention of the backup images.

See the NetBackup Administrator's Guide, Volume I.

NetBackup client requirements

Verify that the following requirements are met for the NetBackup clients:

- To use the new features that are included in NetBackup for Enterprise Vault in NetBackup 11.2, you must upgrade your NetBackup for Enterprise Vault clients to NetBackup 11.2. The NetBackup media server must use the same version as the NetBackup for Enterprise Vault client or a higher version than the client.

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 the operating system and platform compatibility " on page 15.

For more information about the NetBackup Enterprise Vault Agent support for Enterprise Vault that is clustered in WSFC configurations, refer to the NetBackup Software Compatibility List.

To enable the NetBackup Enterprise Vault agent to detect a WSFC clustered server, you must make some changes on each cluster node. Add the following Windows registry keys and String Values (type REG_SZ) on each cluster node:

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

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

- For x64 WSFC 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 a WSFC clustered server. You must make some changes to all the nodes in the clustered environment, to configure the NetBackup Enterprise Vault Agent. The changes to the nodes ensure that the Enterprise Vault databases are protected when hosted by a WSFC clustered Microsoft SQL Server. The following section contains configuration information:

To configure the NetBackup Enterprise Vault Agent

1. Select **Start** > **Veritas NetBackup** > **Backup, Archive, and Restore**.
2. From the **File** menu, select **NetBackup Client 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 message is displayed.
5. Click **OK**.
6. Click **OK** to exit the NetBackup Client Properties dialog box.

You must now 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.
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.

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

License for NetBackup for Enterprise Vault

The NetBackup for Enterprise Vault agent is installed with the NetBackup client software. No separate installation is required. A valid license for the agent must exist on the primary server.

More information is available on how to add licenses.

See the NetBackup Web UI Administrator's Guide.

For a NetBackup cluster, a valid license for NetBackup for Enterprise Vault must exist on each node where NetBackup server resides.

Chapter 3

Configuration

This chapter includes the following topics:

- 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 an 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

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 log on 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

---

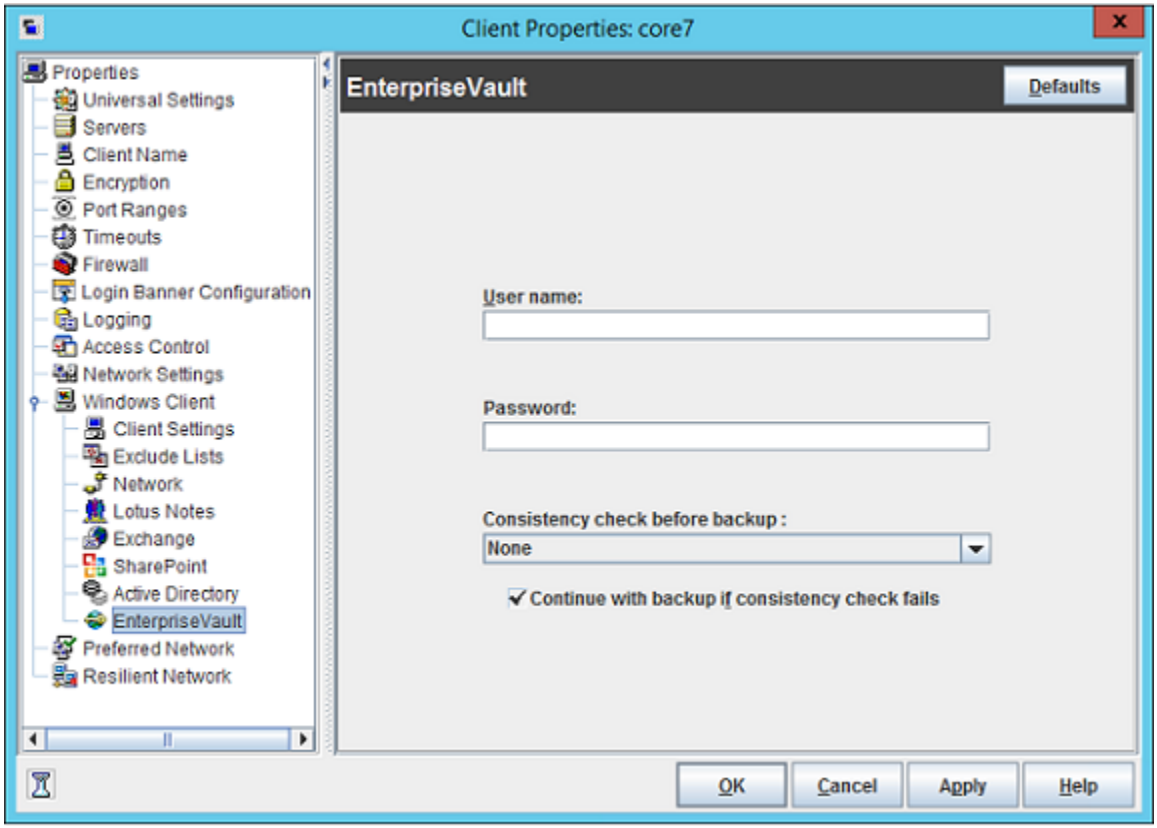
Note: You must perform the following procedure for all of the Enterprise Vault servers and the SQL servers in an Enterprise Vault site configuration.

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 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.



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

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 **Perform snapshot backups** 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 96.
- 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 primary 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 primary 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. Veritas 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 primary server Host properties (Global Settings). Veritas 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 an Enterprise Vault policy" on page 25.

See "Adding schedules to an Enterprise Vault policy" on page 26.

See "Adding a client to a policy" on page 30.

Adding an Enterprise Vault policy

This topic describes how to add an Enterprise Vault backup policy.

To add a new policy

1. Open the NetBackup web UI and sign into the primary server.
2. On the left, select **Protection > Policies**.
3. Select the **Add** button.
4. On the **Attributes** tab, do the following:
   - In the **Policy name** field, type a unique name for the policy.
   - From the **Policy type** list, select **Enterprise-Vault**.
     The Enterprise Vault database agent policy type displays if the primary server has a license for this database agent.
5. Continue by adding additional policy information as follows:
   - Add schedules.
     See "Adding schedules to an Enterprise Vault policy" on page 26.
   - Add clients.
     See "Adding a client to a policy" on page 30.
   - Add Enterprise Vault directives to the backup selections list.
     See "Creating a backup selections list" on page 28.
6. When you finish configuring the schedule, client, and backup selections, select the **Create** button.

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 *Enterprise-Vault*. **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.
Allow multiple data streams	This attribute is enabled when the user creates an Enterprise Vault policy. However, Enterprise Vault agent does not support the multiple data streams feature. 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.
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. Open the policy and select the **Schedules** tab.
2. Select the **Add** button.
3. Specify a unique name for the schedule.
4. Select the **Type of backup**.
5. Specify the other properties for the schedule.

6 Select the **Start window** tab if you want to define the period of time during which the backup starts and ends.

7 Select the **Exclude Dates** tab if you want to exclude specific dates from the schedule.

8 Select **Add**.

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 35. for additional information on the types of data that 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	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. Note the following about Cumulative Incremental backups: ■ 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 33. ■ 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	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. 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. **Warning:** Confirm that regular differential incremental backups are performed against all EV databases to ensure that the transaction logs are backed up and truncated. Confirm this for Open Partitions as well since the Vault Store Database is automatically backed up with an Open Partition backup. **Note:** Enterprise Vault creates different SQL databases with the transaction log mode set as FULL. Veritas recommends that this mode remains set as FULL, otherwise the Enterprise Vault SQL differential backup cannot be used. NetBackup enables you to backup files system files using the timestamp or the archive bit. See the NetBackup Administrator's Guide, Volume I for information on how to configure the Incremental backups to be based on the timestamp or the archive bit. 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. **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.

Creating a backup selections list

On the **Backup selections** tab you specify the Enterprise Vault components to back up Enterprise Vault sites, servers, databases, indexes, or Enterprise Vault partitions. You use directives to specify the Enterprise Vault components 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, select the **Backup selections** tab.
2. Select the **Add** button.
3. From the **Pathname or directive** list, select the directive. The directives that display depend on the version of Enterprise Vault that you installed.

   See the section called “Naming conventions for Enterprise Vault directives” on page 29.

   See “About Enterprise Vault directives and what data they back up” on page 35.
4. Select the **Add to list** button.

   You can rename any directive by clicking in the list and directly editing the line.
5. Select the **Add** button when you finish adding directives.

Naming conventions for Enterprise Vault directives

The following naming conventions 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 and later directive sets enable you to select one or more directives. For example, you can add 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.

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 the following requirements for clients in an Enterprise Vault policy:

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

To add a client to a policy

1. In the policy, select the **Clients** tab.
2. Select the **Add** button.
3. 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.

   For policy client name recommendations, see the following topic:

   See "About hosts for Enterprise Vault policies" on page 81.

   For more information about Enterprise Vault site and server aliases, see the *Enterprise Vault Administrator's Guide*.
4. Select the **Add** button.
5. If this client is the last client, select **Create** or **Save** to save the policy.

Chapter 4

About features provided by Enterprise Vault for a backup provider

This chapter includes the following topics:

- About Enterprise Vault quiescence before a backup
- 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.

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.

See “About granular quiescence” on page 32.

About granular quiescence

Enterprise Vault 8.0 or later supports the ability to set the backup mode at all levels. However, NetBackup 7.1 and later versions set 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 *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 *Enterprise Vault Administrator's Guide* for additional information.

Note: Enterprise Vault 9.0 and later versions support 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 33.

See “About the archive bit ” on page 33.

About the partition secure notification file

Enterprise Vault 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 *Enterprise Vault Administrator's Guide*.
- See, "Managing safety copies " in the *Enterprise Vault Administrator's Guide*.

After a successful backup of a 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

Enterprise Vault uses 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.

Chapter 5

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 is backed up also depends on the client(s) that you select in the policy. The following table identifies each of the available Enterprise Vault directives along with a brief summary of the data that is backed up when that particular directive is selected.

Note: Veritas 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 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 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 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 5-1 Enterprise Vault directives and what they back up

Directive (backup selection)	Description
EV_DIR_DB	The directory database is an SQL database that contains configuration information. ■ 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	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. ■ 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	The auditing database only exists if Enterprise Vault auditing is enabled. The audit database contains audit records of various configurable Enterprise Vault operations. 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. ■ 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 5-1 Enterprise Vault directives and what they back up *(continued)*

Directive (backup selection)	Description
EV_FSAREPORTING_DB	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. 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. ■ 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=*Site name*	Use this directive to back up all index locations in the Enterprise Vault site, that the *Site name* variable specifies. You can use any backup schedule with this directive. ■ You cannot use this directive with the EV_DIR_DB directive. ■ This directive does not support multiple policy clients in the client list. ■ If *Site name* is not specified, the job fails.
EV_OPEN_PARTITION=*Vault Store name*	The open partition directive backs up the open partition and Vault Store database of the Vault Store that you specify when you define the *Vault Store name*. The partition can be present on NTFS file system or NAS devices. You can use any backup schedule with this directive. For open partitions: ■ You cannot use this directive with the EV_DIR_DB directive. ■ This directive does not support multiple policy clients in the client list. ■ If *Vault Store name* is not specified, the job fails. **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.

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

Directive (backup selection)	Description
EV_CLOSED_PARTITIONS=*Vault Store name*	The closed partitions directive backs up any closed partitions of the Vault Store that you specify when you define the *Vault Store name*. The partitions can be present on NTFS file system or NAS devices. You can use any backup schedule with this directive. For closed partitions: ■ This directive does not support multiple policy clients in the client list. ■ If *Vault Store name* is not specified, the job fails. **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 NetBackup. If all close partitions are streamer-based the job fails.
EV_READY_PARTITIONS=*Vault Store name*	The ready partitions directive backs up the ready partitions of the Vault Store that you specify when you define the *Vault Store name*. The partitions can be present on NTFS file system or NAS devices. You can use any backup schedule with this directive. For ready partitions: ■ This directive does not support multiple policy clients in the client list. ■ If *Vault Store name* is not specified, the job fails. **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 NetBackup. If all ready partitions are streamer-based the job fails.
EV_VAULT_STORE_DB=*Vault Store name*	The Enterprise Vault, vault store database is an SQL database that can contain metadata about the vault store and archived data. Use this directive to back up the vault store database that the *Vault Store name* variable specifies in the Enterprise Vault deployment. You can use any backup schedule with this directive. The following applies for this directive: ■ The vault store databases can be hosted on a different system. ■ This directive does not support multiple policy clients in the client list. ■ If *Vault Store name* is not specified, the job fails. **Note:** The *vault store name* is the vault store name and not the vault store database name.

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

Directive (backup selection)	Description
EV_FINGERPRINT_DB=*Vault Store Group name*	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. You can use any backup schedule with this directive. The following applies for this directive: ■ 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.

See "To run an Enterprise Vault backup manually" on page 39.

Note: User-directed backups are not supported.

To run an Enterprise Vault backup manually

1. Open the NetBackup web UI.
2. On the left, select **Protection > Policies**.
3. Select the check box for the policy that you want to run.
4. Select **Manual backup**.
5. Select the schedule and one or more of the clients.
6. Select the **Backup** button to begin the backup.

Canceling an Enterprise Vault backup job from the Activity monitor

You can cancel an Enterprise Vault backup from the 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 job that is active or queued. 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 you canceled the job does not change and you can use their images for a restore.
- If you choose to cancel a full backup that involves an Enterprise Vault SQL Server database (such as a directory database), then you must make sure that you exit that backup. 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. Open the NetBackup web UI.
2. On the left, select **Activity monitor**. The select the **Jobs** tab.
3. Select the check box for the first job of the backup that you want to cancel.
4. Select **Cancel**.

Chapter 6

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

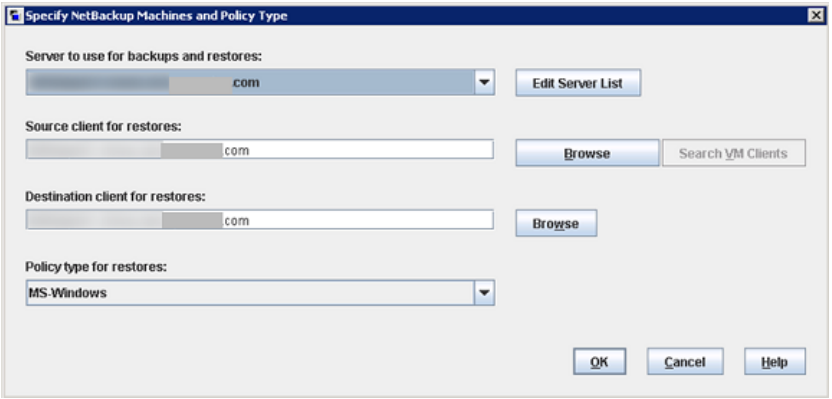
Important notes about Enterprise Vault data restore

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.
- Veritas 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.
- Veritas recommends that you restore individual components of Enterprise Vault one at a time.
- 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 43.
  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 43.
  See "Restoring Enterprise Vault SQL database components" on page 61.

See "Restoring an Enterprise Vault file system component" on page 55.

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 hierarchical 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 files that correspond to the selection that you make in the **All Folders** pane.

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 Server 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 following procedure describes how to use these interfaces search for an object to restore in the backup images.

To search backup images in the Backup, Archive, and Restore interface

1. Select the images from the **History** pane and click on the search (binoculars) icon in the interface.
2. Enter a keyword **Search Folder** field.

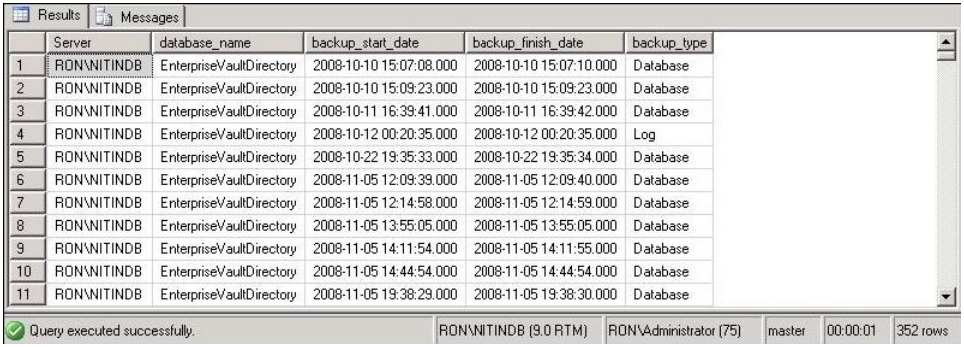
   Use a regular expression format. For example, enter `*All Partitions*` to search for images with "All Partitions" as an object name. You can also enter a word or phrase in the **Keyword phrase** field.
3. Select the **Search** button.

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 Backup, Archive, and Restore 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 the Enterprise Vault directory database, a monitoring database, or a vault store database. The following procedures describes how to restore Enterprise Vault data.

See the section called “Restore Enterprise Vault migrated data (NetBackup web UI)” on page 46.

See the section called “Restore Enterprise Vault data (Backup, Archive, and Restore interface)” on page 47.

Restore Enterprise Vault migrated data (NetBackup web UI)

The following procedure describes how to restore Enterprise Vault data with the NetBackup web UI.

To restore Enterprise Vault migrated data (NetBackup web UI)

1. Open the NetBackup web UI and sign into the server that you want to perform the restore.
2. On the left, select **Recovery**.
3. Go to the **Regular recovery** card and select the **Start recovery** button.
4. From the **Policy type** list, select **Datastore**.
5. From the **Source client** list, select the source client. The source client is the policy client in the backup policy from where the backup happened.
6. By default the **Destination client**, is the same source client you have selected to restore the images. You can determine the name of the destination client from either the NetBackup web UI or the Enterprise Vault Administration Console.
7. Click **Next**.
8. If necessary, edit the date range to locate the images that contain the objects that you want to restore.
9. Select the objects to restore.
10. Click **Next**.
11. From the **Restore target** list, select the target location where you want to restore the Enterprise Vault migrated data.
12. From the **Recovery options** list, select the **Restore as Enterprise Vault migrated data** to restore the Enterprise Vault migrated data.

    Note: The options to **Create and restore to a new virtual hard disk file** and to **Restore directories without crossing mount points** is displayed in theNetBackup web UI or the Enterprise Vault Administration Console but is not supported for NetBackup Enterprise Vault data recovery using Datastore policy.

13. In the **Media server**, do any of the following:

- Select the **Default** option to select the default media server.
- Select the **Select** option to select the media server that you want for the Enterprise Vault data migration.

14 Set the job priority number for backup storage.

15 Review or edit the recovery job summary.

16 Click **Start recovery**.

Restore Enterprise Vault data (Backup, Archive, and Restore interface)

The following procedure describes how to restore Enterprise Vault data with the Backup, Archive, and Restore interface.

To restore Enterprise Vault data (Backup, Archive, and Restore interface)

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** list.

4 Click **OK**. NetBackup browses for Enterprise Vault backup images.

5 From the **NetBackup History** pane, select the images that contain the objects you want to restore.

6 In the **All Folders** pane, expand **Enterprise Vault Resources**.

7 Select the objects to restore.

8 Choose **Actions** > **Restore**.

9 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 48.
- 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 49.

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	Restores the selected items to the different location from which they were backed up.
Restore individual folders and files to different locations	Select this option to restore any selected Enterprise Vault file system data to different locations. 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. 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. **Note:** If you type a new destination in the **Destination** field, you must enter a valid physical path. 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. 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. See “About restoring Enterprise Vault file system data” on page 54.

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

Option	Description
Create and restore to a new virtual hard disk file	Creates and restores the selected items to a new virtual hard disk file. This option is displayed in the NetBackup Administration Console but is not supported for the Enterprise Vault policy.
Create virtual disks and redirect to them	This option is disabled.
Restore directories without crossing mount points	Restores the directories without crossing mount points. This option is displayed in the NetBackup Administration Console but is not supported for the Enterprise Vault policy.
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	After a restore completes, you can leave an SQL database in any of the following states: ■ Operational ■ Read-only ■ Non-operational 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: ■ A FULL database restore ■ The last CUMULATIVE (database differential) restore ■ One or more DIFFERENTIAL (transaction log) backups that were taken after the last cumulative backup 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. **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.

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

Restore option	Description
Consistency check after restore	You can check the consistency of the database after restores are complete. To check the consistency of the database, select one of the following consistency checks when you select the **Leave database operational** option: ■ **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)** This option only applies to SQL Server 2000. ■ **None** Select this option to ensure that no consistency check occurs after a restore. **Note:** Any option other than **None** is effective only in the restore job that brings the database to an operational state.
Point-in-time recovery	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. 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.
Redirected restore	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. **Note:** You can change the *SQL INSTANCE* name, however do not change the *SQL database name*. If you change the *SQL database name* Enterprise Vault does not automatically recognize the new name. If you chose to change the *SQL database name* then you must also update your Enterprise Vault configuration. **Note:** A redirected restore of an auditing database must be made to the same SQL instance where the directory database resides.
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

A restore of Enterprise Vault data generally involves redirected restores. Similarly to how SQL Server backups occur, Enterprise Vault backups are cataloged against the Enterprise Vault server and should be restored to the SQL Server 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. See the NetBackup Administrator's Guide, Volume I for details.

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.

See the section called "Specify the server, source client, destination client, and policy type for a restore operation (NetBackup web UI)" on page 52.

See the section called "Specify the server, source client, destination client, and policy type for a restore operation (Backup, Archive, and Restore interface)" on page 53.

Specify the server, source client, destination client, and policy type for a restore operation (NetBackup web UI)

When you use the **NetBackup web UI** to restore Enterprise Vault data, you sign into the server that you want to perform the restore and specify the source client and the destination client. You must have the RBAC Administrator role or a role with permissions to perform restores from the the **Recovery** node.

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

1. Open the NetBackup web UI and sign into the primary server that you want to perform the restore.
2. On the left, select **Recovery**.
3. Go to the **Regular recovery** card and select the **Start recovery** button.
4. From the **Policy type** list, select **Datastore**.
5. From the **Source client** list, select the source client. The source client is the policy client in the backup policy from where the backup happened.

6 From the **Destination client** list, select the name of the client where you want to restore the images. You can determine the name of the destination client from either the NetBackup web UI or the Enterprise Vault Administration Console.

See the section called “Determining the destination client for Enterprise Vault” on page 54.

7 Click **Next** and continue with restore.

Specify the server, source client, destination client, and policy type for a restore operation (Backup, Archive, and Restore interface)

When you use the **Backup, Archive, and Restore** interface to restore Enterprise Vault data, you must specify the NetBackup server along with the source client and the destination client.

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.

See the section called “Determining the destination client for Enterprise Vault” on page 54.

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

9 Click **OK**.

Determining the destination client for Enterprise Vault

You determine 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 Enterprise Vault:

- 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 username credentials for this Enterprise Vault server, has write permissions for this UNC path. The username 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`.

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 primary 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 primary 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, 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 41.
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. Veritas 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

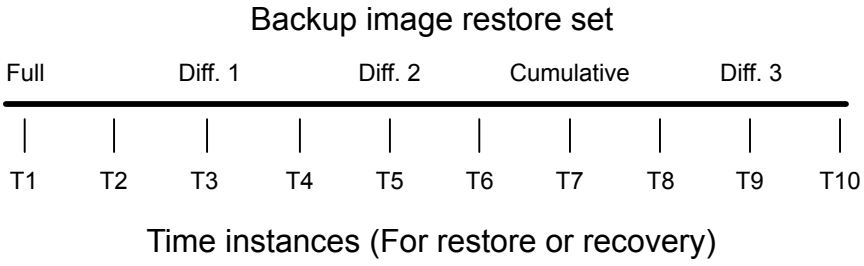


Table 6-3 demonstrates which backup images you would select to comprise a backup image restore set at any given time instance. Depending on the time you want to restore or recover the database, determines which backup images you must include in the backup image restore set.

Table 6-3 Understanding which backup 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)

Table 6-3 Understanding which backup images to select for a restore *(continued)*

Time instance	The backup images that comprise the backup image restore set
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 website 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 website 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, Veritas 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 primary 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 primary 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, 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 41.
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 58.
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**.

Chapter 7

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 an 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 primary 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 *Enterprise Vault Administrator's Guide* on the Veritas support website.

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, Veritas 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 66.
- 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 67.

See "Recovering an auditing database" on page 66.

See "Recovering an FSA Reporting database" on page 67.

See "Recovering index locations" on page 68.

See "Recovering an Enterprise Vault vault store group" on page 69.

See "Recovering an Enterprise Vault server" on page 73.

See "Recovering an Enterprise Vault server on a different system" on page 74.

Recovering a directory database

Use the following procedure to recover a directory database in Enterprise Vault:

Note: Before starting the recovery process, see the *Recovery* chapter, in the *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 61.

Recovering an auditing database

Use the following procedure to recover an auditing database in Enterprise Vault:

Note: Before starting the recovery process, see the *Recovery* chapter, in the *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 61.

Recovering an FSA Reporting database

Use the following procedure to recover an FSA Reporting database in Enterprise Vault:

Note: Before starting the recovery process, see the *Recovery* chapter, in the *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 61.

Recovering a Monitoring database

Use the following procedure to recover a Monitoring database in Enterprise Vault:

Note: Before starting the recovery process, see the *Recovery* chapter, in the *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 61.

Recovering index locations

The following procedure describes how to recover Index locations in Enterprise Vault:

Note: Veritas 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, Veritas 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 55.

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 vault store group

An 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:

To restore an 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 71.
- Restore all of the vault store partitions.
  Restore the first vault store partition.
  See “Recovering vault store partition” on page 72.
  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 70.

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, Veritas 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:

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 61.

   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: Veritas 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:

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 61.

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.

Veritas 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. 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 55.
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. Veritas 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 55.

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:

Note: Veritas 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, Veritas 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 61.

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 61.

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 66.

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 67.

9 Restore the Enterprise Vault fingerprint database if the Enterprise Vault hosted a vault store group.

See "Recovering a fingerprint database" on page 70.

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 71.
- Restore all of the vault store partitions.
  Restore the first vault store partition.
  See "Recovering vault store partition" on page 72.
  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. Veritas 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 55.

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:

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 61.
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 *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 61.
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 66.
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 67.
10. Restore the Enterprise Vault fingerprint database if the Enterprise Vault hosted a vault store group.

    See "Recovering a fingerprint database" on page 70.
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 71.

- Restore all of the vault store partitions.
  Restore the first vault store partition.
  See “Recovering vault store partition” on page 72.
  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. Veritas 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 55.

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

Chapter 8

Enterprise Vault Agent support for Enterprise Vault

This chapter includes the following topics:

- Policy configuration for Enterprise Vault
- Notes about Enterprise Vault 10.0 backups
- Excluding files from the exclude list
- 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 Enterprise Vault

Policy configuration for Enterprise Vault

The following topics contain the information that pertains to policy creation for Enterprise Vault:

See "Open partition, vault store database, and fingerprint database consistencies" on page 78.

See "Closed and ready partition consistencies" on page 78.

See "Index location consistencies" on page 79.

See "Directory database consistencies" on page 79.

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, Veritas 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. Veritas 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.
- 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, Veritas 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 sucessful 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 80.

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/openv/netbackup` directory on each client.

For more information, see the NetBackup Administrator's Guide, Volume 1.

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 of 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 79.

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 24.

Veritas 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, Veritas 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 backup selection types, the recommended client name is Enterprise Vault Site alias or Any Enterprise Vault server alias.

Note: The same client name is used across all policies to protect an Enterprise Vault site.

For more information about Enterprise Vault site and server aliases, see the *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 Enterprise Vault Storage Verify and Repair (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.

The tool also verifies the consistency of information of a vault store and finger print databases. This technology has been included in EV 9.0.4.

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, Veritas 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, Veritas 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 the following privileges to create Enterprise Vault agent backups:

- 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 84.

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.

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 primary server and start the 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 Enterprise Vault

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

- 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.
- The 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.

Differential incremental backup taken after a restore fails for Enterprise Vault

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.

Chapter 9

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 primary, 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 90.

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 primary 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, 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 and capture back up, 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 primary server.

Table 9-1 List of the directories to create and capture back up, 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 C:\Program Files\Common Files\Veritas Shared\VxFI\4\Logs	Snapshot information See the *VxFI Administrator's Guide* on the Veritas support site.

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

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

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

Directories to create	Enterprise Vault operation information
install_path\Netbackup\logs\bpbrm (Windows)	Back up and Restore Manager
usr/openv/netbackup/logs/bpbrm(UNIX)	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
install_path\Netbackup\logs (Windows)	NetBackup Job Manager
usr/openv/netbackup/logs(UNIX) Refer to the "Unified logging" topic in the NetBackup Troubleshooting Guide.	NetBackup Policy Execution Manager

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 > Veritas 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 primary 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 the 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 91.

See "NetBackup status code 13" on page 92.

See "NetBackup status code 39" on page 92.

See "NetBackup status code 59" on page 93.

See "NetBackup status code 69" on page 93.

See "NetBackup status code 156" on page 94.

See "NetBackup status code 1800" on page 96.

NetBackup status code 2

Message: none of the requested files were backed up

The following list can help determine the cause of the issue:

- 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 `bpresolver` 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.
- 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

Message: file read failed

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

1. On the SQL Server client, open the following registry key:

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

2. Create a new DWORD value named **FsUseAsyncIo**.
3. Set the DWORD value to **1**.

   If this registry DWORD value already exists and the value is not 1, change the value to 1.

NetBackup status code 39

Message: client name mismatch

You must configure NetBackup Enterprise Vault Agent to protect the Enterprise Vault databases that are hosted by a WSFC 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** > **Veritas 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

Message: 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

Message: invalid filelist specification

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 35.

NetBackup status code 156

Message: snapshot error encountered

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 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 website. You can use the error names as keywords when searching the Microsoft website.

NetBackup status code 1800

Message: invalid client list

For Enterprise Vault-type policies, verify that the 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 35.

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

https://www.veritas.com/docs/100001067

Appendix A

NetBackup Enterprise Vault Migrator

This appendix includes the following topics:

- About the Enterprise Vault Migrator
- Configuring a backup policy for migration
- About configuring Enterprise Vault for collection and migration
- 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 accomodate 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, Veritas recommends that you keep traditional backups separate from Enterprise Vault data because the retention requirements are likely to be very different.

Configuring a backup policy for migration

You must create a backup policy through which the Enterprise Vault migration can take place.

NetBackup administrators may find the following notes helpful when they configure 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, time-outs can occur and you may not be able to automatically retrieve your data.
- Time-outs can occur if all tape drives are in use when an Enterprise Vault user or application accesses the data that resides in a library.
- Time-outs can occur if a migration occurs (writing to the tape) while data on the same tape is accessed for a retrieval.

To add a backup policy for migration

1. Open the NetBackup web UI and sign into the primary server.
2. On the left, select **Protection > Policies**.
3. Select the **Add** button.
4. On the **Attributes** tab, do the following:
   - In the **Policy name** field, type a unique name for the 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.

- From the **Policy type** list, select **DataStore**.
  The Enterprise Vault database agent policy type displays if the primary server has a license for this database agent.

5 Create 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 **Infinite (Retention Level 9)**.
  When you specify the retention level as **Infinite (Retention 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.

6 Specify the backup window of the schedule. Select the **Start window** tab to define the period of time during which the backup starts and ends.

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

7 On the **Clients** tab, specify a NetBackup client for the policy.

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

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

9 When you finish configuring the policy, select the **Create** button.

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. Veritas 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 primary server.
   - You can modify the default values of the other settings if you deem it is necessary.

Testing the Enterprise Vault migrator configuration

After you have installed and registered the Enterprise Vault migrator, Veritas 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.

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 exist, first configure the partitions for migration. Then continue with Step 2.
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 the 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 is 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 the structure 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
```

Following are some examples of how to use the `bprestore`:

The following `bprestore` CLI format restores or recalls data of a particular partition (VS Ptn3) or all migrated files for a particular EV-Server.

```
..\Veritas\NetBackup\bin>bprestore -S hpesx4v5 -C hpesx4v7 -t 24
-ev_migrated_data "/E/Enterprise Vault Stores/VS Ptn3/*"
```

The following `bprestore` CLI format restores data of all partitions or migrated files for a particular EV-Server.

```
..\Veritas\NetBackup\bin>bprestore -S hpesx4v5 -C hpesx4v7 -t 24
-ev_migrated_data *
```

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**.

Note: While restoring Enterprise Vault migrated data using the Datastore policy, the options to **Create and restore to a new virtual hard disk file** and to **Restore directories without crossing mount points** are not supported.

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.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 `.dvf` 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 `.dvf` 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.
- 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 NetBackup 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 **Vault Store Partition Properties** 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`

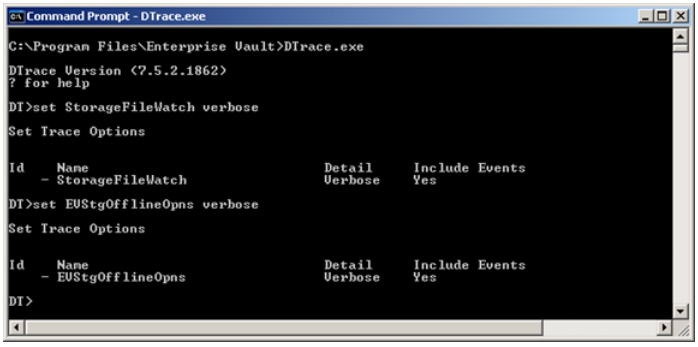
- `EVStgOffilineOpns`
- `StorageManagement`

  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`



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.

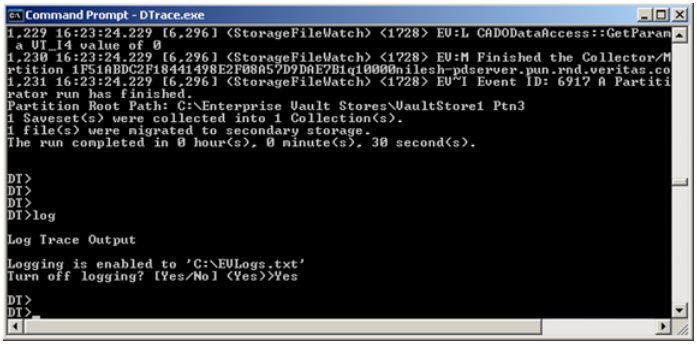
Execute the tasks (Migration/Retrieval/Deletion) for which logs are required. The Dtrace screen displays the various logs that are generated for the task.

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`.

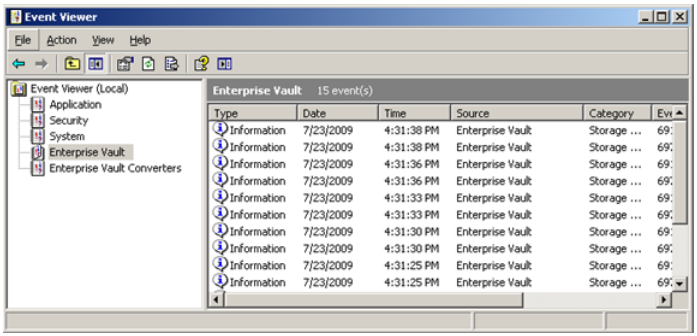


10 Collect the log file.

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 *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 the `mklogdir.bat` command 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.