Enterprise Vault™ Backup and Recovery

14.4

VERITAS™

Enterprise Vault™: Backup and Recovery

Last updated: 2023-03-06.

Legal Notice

Veritas Technologies LLC, 2625 Augustine Drive, Santa Clara, CA 95054

https://www.veritas.com

Technical Support

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

https://www.veritas.com/support

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

https://my.veritas.com

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

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

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

https://www.veritas.com/support/en_US/vqa

Documentation

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

https://www.veritas.com/docs/100040095

Documentation feedback

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

evdocs@veritas.com

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

https://www.veritas.com/community

Contents

Chapter 1

About this guide

This chapter includes the following topics:

About backup and recovery

This guide provides the information you need to be able to back up Enterprise Vault, and procedures to help you recover your Enterprise Vault environment in event of disaster.

Where to get more information about Enterprise Vault

Table 1-1 lists the documentation that accompanies Enterprise Vault. This documentation is also available in PDF and HTML format in the Veritas Documentation Library.

Table 1-1 Enterprise Vault documentation set

Document	Comments
Veritas Enterprise Vault Documentation Library	Includes all the following documents in Windows Help (`.chm`) format so that you can search across them all. It also includes links to the guides in Acrobat (`.pdf`) format. You can access the library in several ways, including the following: ■ In Windows Explorer, browse to the `Documentation\`*`language`*`\Administration Guides` subfolder of the Enterprise Vault installation folder, and then open the `EV_Help.chm` file. ■ On the **Help** menu in the Administration Console, click **Help on Enterprise Vault**.
Introduction and Planning	Provides an overview of Enterprise Vault functionality.
Deployment Scanner	Describes how to check the required software and settings before you install Enterprise Vault.
Installing and Configuring	Provides detailed information on setting up Enterprise Vault.
Upgrade Instructions	Describes how to upgrade an existing Enterprise Vault installation to the latest version.
Setting up Domino Server Archiving	Describes how to archive items from Domino mail files and journal databases.
Setting up Exchange Server Archiving	Describes how to archive items from Microsoft Exchange user mailboxes, journal mailboxes, and public folders.
Setting up File System Archiving	Describes how to archive files that are held on network file servers.
Setting up IMAP	Describes how to configure IMAP client access to Exchange archives and Internet Mail archives.
Setting up SharePoint Server Archiving	Describes how to archive documents from Microsoft SharePoint servers.
Setting up Skype for Business Archiving	Describes how to archive Skype for Business sessions.
Setting up SMTP Archiving	Describes how to archive SMTP messages from other messaging servers.
Setting up Microsoft Teams Archiving	Describes how to archive Microsoft Teams data.

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

Document	Comments
Classification using the Microsoft File Classification Infrastructure	Describes how to use the classification engine that is built into recent Windows Server editions to classify all new and existing archived content.
Classification using the Veritas Information Classifier	Describes how to use the Veritas Information Classifier to evaluate all new and archived content against a comprehensive set of industry-standard classification policies. If you are new to classification with Enterprise Vault, we recommend that you use the Veritas Information Classifier rather than the older and less intuitive File Classification Infrastructure engine.
Administrator's Guide	Describes how to perform day-to-day administration procedures.
PowerShell Cmdlets	Describes how to perform various administrative tasks by running the Enterprise Vault PowerShell cmdlets.
Auditing	Describes how to collect auditing information for events on Enterprise Vault servers.
Backup and Recovery	Describes how to implement an effective backup strategy to prevent data loss, and how to provide a means for recovery in the event of a system failure.
Reporting	Describes how to implement Enterprise Vault Reporting, which provides reports on the status of Enterprise Vault servers, archives, and archived items. If you configure FSA Reporting, additional reports are available for file servers and their volumes.
NSF Migration	Describes how to import content from Domino and Notes NSF files into Enterprise Vault archives.
PST Migration	Describes how to migrate content from Outlook PST files into Enterprise Vault archives.
Utilities	Describes Enterprise Vault tools and utilities.
Registry Values	A reference document that lists the registry values with which you can modify many aspects of Enterprise Vault behavior.
Help for Administration Console	The online Help for the Enterprise Vault Administration Console.

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

Document	Comments
Help for Enterprise Vault Operations Manager	The online Help for Enterprise Vault Operations Manager.

For the latest information on supported devices and versions of software, see the Enterprise Vault Compatibility Charts.

Enterprise Vault training modules

Veritas Education Services provides comprehensive training for Enterprise Vault, from basic administration to advanced topics and troubleshooting. Training is available in a variety of formats, including classroom-based and virtual training.

For more information on Enterprise Vault training, curriculum paths, and certification options, see https://www.veritas.com/services/education-services.

Chapter 2

Backing up Enterprise Vault

This chapter includes the following topics:

About Enterprise Vault backups

Enterprise Vault requires an effective backup strategy to prevent data loss, and to provide a means for recovery in the event of a system failure. When you plan this strategy, remember that Enterprise Vault components can be distributed across multiple systems. The resources on which Enterprise Vault depends may be remote from Enterprise Vault services and tasks.

Note: Enterprise Vault 14.2 and later introduces Elastisearch as the new indexing engine. The only reliable and supported way to back up the index data is by taking a snapshot. Refer to the associated KB articles for snapshot and restore below for more details:

How to backup indexes in Enterprise Vault 14.2 and later

How to restore Elasticsearch index data in Enterprise Vault 14.2 and later

---

This section describes:

- Enterprise Vault's backup mode which lets you place vault stores, index locations, and index snapshot locations in backup mode while you take backups.
- The databases you must back up.
- The data locations and index locations you must back up.
- The use of Enterprise Vault's backup mode PowerShell cmdlets in your backup scripts.

For additional information about Enterprise Vault backups, see the following article on the Veritas Support website:

- https://www.veritas.com/docs/100006827
- https://www.veritas.com/docs/100051323

About Enterprise Vault backup mode

Enterprise Vault lets you place vault stores, index locations, and index snapshot locations in backup mode for the duration of a data backup. Enterprise Vault does not write any data into vault store partitions or index locations or index snapshot locations while they are in backup mode. However, services to users are maintained while vault stores and index locations are in backup mode. For example, users can continue to search their archives and restore items from them.

You can set backup mode on vault stores and index locations in the Enterprise Vault administration console. When your backup is complete, you can use the administration console to clear backup mode.

You can also use PowerShell cmdlets in the Enterprise Vault Management Shell to set, clear, and report on vault store, index location, and index snapshot location backup mode. When you use the PowerShell cmdlets to set and clear backup mode, Enterprise Vault maintains a count of the number of requests for each vault store, index location, and index snapshot location to support the use of concurrent backup scripts.

For more information, see How to Check, Set or Clear backup mode on Enterprise Vault Stores, Indexes and Index Snapshot Locations in version 14.2 and later

See "About backup mode cmdlets" on page 17.

To manage backup mode on vault stores, your user account must be assigned the storage administrator role. To manage backup mode on index locations, your user account must be assigned the power administrator role.

See "Roles-based administration" in the *Administrator's Guide*.

In the administration console, you can set and clear vault store backup mode in the following places:

- The context menu on the Enterprise Vault site
- The context menu on any vault store group
- The context menu on any vault store

You can set and clear index location backup mode in the following places:

- The context menu on the Enterprise Vault site
- The context menu on any Enterprise Vault server
- The index service properties page

When you set and clear backup mode on index locations and vault stores, events are written to the Enterprise Vault event log. The indexing service also writes an event when it starts, if any index locations are in backup mode. This event lists all the index locations that are in backup mode.

The following examples show how to use backup mode in the administration console. The first example is a procedure to set backup mode on all the vault stores in a vault store group. The second example is a procedure to find the current backup mode settings for index locations on a server called EVServer.domain1.local.

To set backup mode on all the vault stores in a vault store group

1. In the left pane of the administration console, expand the **Vault Store Group** container.
2. Right-click the vault store group whose vault stores you want to place in backup mode, and click **Set State** > **Set Backup Mode on all Vault Stores**.

The **Backup Mode** column in the right pane now shows that backup mode is set on all the vault stores in the vault store group.

To see the current backup mode settings for index locations, and to change these settings

1. In the left pane of the administration console, browse to **Enterprise Vault Servers** > **EVServer.domain1.local** > **Services**.
2. In the right pane, right-click **Enterprise Vault Indexing Service** and click **Properties**.
3. Click the **Index Locations** tab.
4. The **Backup Mode** column shows the current backup mode settings for all the index locations on the server. You can change the setting for any of these locations.

Backup of Enterprise Vault data

You must back up the following Enterprise Vault data and databases:

- Enterprise Vault system databases backup
- Fingerprint databases backup
- Vault store partitions and vault store databases backup
- Backing up index locations
- Backing up the classification policy folder
- Backing up index snapshot locations

Enterprise Vault system databases backup

To make a complete Enterprise Vault system backup, you must back up the following system databases:

- `EnterpriseVaultDirectory`. You must back up this database immediately after you back up one or more vault store databases.
  See "Vault store partitions and vault store databases backup" on page 14.
- `EnterpriseVaultMonitoring`
- `EnterpriseVaultAudit`, if you have enabled Enterprise Vault auditing.
- Each FSA Reporting database you have set up, if you use FSA Reporting.

The following document on the Veritas Support website describes procedures which you can use to back up your Enterprise Vault SQL databases if you do not use a third party SQL backup tool:

https://www.veritas.com/docs/100022023

Note: Every Enterprise Vault server must also have a complete system and file backup. This backup must include the registry because all Enterprise Vault services store information in the registry. You should consider taking this system and file backup at the same time you back up the Enterprise Vault system databases.

Fingerprint databases backup

Each vault store group usually has a fingerprint database which holds the data that enables Enterprise Vault single instance storage.

Each fingerprint database is called `EVVSG_vaultstoregroup_n_m`, where *vaultstoregroup* is the name of the vault store group with its spaces removed. *n* and *m* are internally generated integers.

You should also set backup mode on the corresponding vault store group, and back up all its vault stores at the same time you back up the fingerprint database.

See "About Enterprise Vault backup mode" on page 11.

The following document on the Veritas Support website describes procedures which you can use to back up your Enterprise Vault SQL databases if you do not use a third party SQL backup tool:

https://www.veritas.com/docs/100022023

Vault store partitions and vault store databases backup

Each vault store has a database which is called `EVvaultstore_n`, where *vaultstore* is the name of the vault store with its spaces removed, and *n* is an internally generated integer.

Back up the vault store databases at the same you back up the vault store partitions.

Note: After you back up a vault store database or back up a group of vault store databases, immediately back up the directory database (`EnterpriseVaultDirectory`).

Before you back up the vault store databases and vault store partitions, place the vault stores in backup mode.

See "About Enterprise Vault backup mode" on page 11.

Removal of Enterprise Vault safety copies after backup

When Enterprise Vault detects that a vault store partition has been backed up, it is free to remove the safety copies of the items it archived previously. Enterprise Vault can detect that partitions have been backed up by inspecting the archive attribute on individual files if your backup software clears the archive attribute after backup. Alternatively, you can use a trigger file mechanism.

For more information about the relationship between backup software and the detection of partition backups, see "About Enterprise Vault safety copies" in *Installing and Configuring*.

Backing up index locations

Note: Enterprise Vault version 14.2 onwards, Elasticsearch is the new indexing engine. The index data backup strategy has changed. For all the Elasticsearch index locations, you must now take snapshots of the index data on the Enterprise Vault index server, instead of taking filesystem-level backup of the index data. The backup strategy for all the non-Elasticsearch index locations in your environment continues to be the same as prior to release 14.2 and supports only filesystem-level backup.

Each Enterprise Vault indexing service can store its indexes in multiple locations, and you must back up all these locations. On each Enterprise Vault server, the index locations are listed on the **Index Locations** tab of the **Enterprise Vault Indexing Service** properties page.

The following procedure shows how to find the index locations you need to back up on a server called EVServer.domain1.local.

Note: To find a complete list of all the index locations to back up, you must complete this procedure on all the Enterprise Vault servers that run an indexing service.

To find a complete list of the index locations you must back up

1. In the left pane of the administration console, browse to **Enterprise Vault Servers** > **EVServer.domain1.local** > **Services**.
2. In the right pane, right-click **Enterprise Vault Indexing Service** and click **Properties**.
3. Click the **Index Locations** tab and note the index locations that you must back up.

Before you back up index locations, you must place them in backup mode.

See “About Enterprise Vault backup mode” on page 11.

Note: For Enterprise Vault 10.0 and later, you must ensure that all the indexing services in your environment are running before you set backup mode on index locations.

While index locations are in backup mode, users can continue to search their archives. In environments where it is not necessary to maintain this functionality during the backup window, you can stop all the indexing services while you take backups. If you do this, you do not have to set backup mode on index locations.

Note: Enterprise Vault 14.2 or later, uses Elastisearch for indexing. So, Enterprise Vault 14.2 onwards, the only reliable and supported way to back up the index data is by taking a snapshot. For more information, see How to backup indexes in Enterprise Vault 14.2 and late

Backing up the classification policy folder

The classification feature in Enterprise Vault 12.2 and later stores its policy files in a folder on a shared network drive. You specify the path to this folder when you run the `Initialize-EVClassificationVIC` cmdlet to set up the feature. The folder stores any new classification policies that you define and any changes that you make to the built-in policies, such as enabling or disabling those policies.

We recommend that you regularly back up the contents of the policy folder so that you can recover them in the event of a system failure.

Backing up index snapshot locations

The Enterprise Vault Administrator may wish to make an independent backup of index snapshot repository or index snapshot location, so that a copy of its contents can be used to recreate the index repository to a point-in-time state later. The contents of index snapshot repository will be used to restore snapshots of index data for Elasticsearch indexes.

Enterprise Vault recommends regular backing up of index snapshot repository or index snapshot location.

Note: If you are already using any third-party backup software to take file-system backup and you want to add index snapshot location as a part of that, ensure that you perform the following actions:

Action 1: Set that index snapshot location in backup mode using the `Set-EVIndexSnapshotLocationBackupMode` PowerShell command as a part of the pre-backup script.

Action 2: Clear that backup mode of index snapshot location using the `Clear-EVIndexSnapshotLocationBackupMode` PowerShell command as a part of the post-backup script.

To find the complete list of the index snapshot locations you must backup:

Use the command `Get-EVIndexSnapshotLocation`. Refer to the *Enterprise Vault PowerShell Cmdlets* guide for more details about the same.

Before you back up index snapshot locations, you must place them in backup mode. See "About Enterprise Vault backup mode" on page 11.

About backup mode cmdlets

Enterprise Vault provides a set of PowerShell cmdlets which you can use to set and clear backup mode on the following:

- Vault stores
- Vault store groups
- Index locations
- Index snapshot locations

You can run these cmdlets directly in the Enterprise Vault Management Shell, and use them in your backup scripts. For example, use the cmdlets in a pre-backup script to set backup mode on index locations and vault stores before the backup is taken. After the backup has completed, use the cmdlets in a post-backup script to clear backup mode.

For each index location, index snapshot location, and vault store, Enterprise Vault maintains a count of the number of set requests and clear requests, to support the use of concurrent backup scripts. Enterprise Vault increments the count by 1 on each request to set backup mode, and decrements the count by 1 on each request to clear backup mode.

When you use concurrent backup scripts, Enterprise Vault does not clear backup mode from a vault store, an index location, or an index snapshot location, until all the scripts that have set backup mode, have also cleared backup mode.

Note: When you use the Administration Console to clear backup mode from an index location or vault store, Enterprise Vault ignores the backup mode count and forcibly clears backup mode.

To run PowerShell cmdlets directly, first run the Enterprise Vault Management Shell

- Start the Enterprise Vault Management Shell.

  PowerShell opens and loads the Enterprise Vault snap-in which makes the backup mode cmdlets available in the shell.

The Enterprise Vault Management Shell provides the following backup mode cmdlets:

`Get-IndexLocationBackupMode`	Reports the current backup mode settings on index locations.
`Set-IndexLocationBackupMode`	Increments the backup mode count on index locations.
`Clear-IndexLocationBackUpMode`	Decrements the backup mode count on index locations.
`Get-VaultStoreBackupMode`	Reports the current backup mode settings on vault stores.
`Set-VaultStoreBackupMode`	Increments the backup mode count on vault stores.
`Clear-VaultStoreBackupMode`	Decrements the backup mode count on vault stores.
`Set-EVIndexSnapshotLocationBackupMode`	Increments the backup mode count on index snapshot locations.
`Clear-EVIndexSnapshotLocationBackupMode`	Decrements the backup mode count on index snapshot locations.

Help is available for all the cmdlets. For example, the following command shows the detailed Help for `Clear-VaultStoreBackupMode`:

```
Get-Help Clear-VaultStoreBackupMode -detailed
```

You can also generate PowerShell backup mode commands that are based on the configuration of your environment and ready for use in your backup scripts.

See "Generating PowerShell backup commands for your environment" on page 22.

Index location backup mode cmdlet syntax

The syntax is the same for all three index location backup mode cmdlets. For example:

```
Set-IndexLocationBackupMode [-EVServerName] <String> [[-IndexRootPath]
<String>] [-EVSiteName <String>] [<CommonParameters>]
```

The following examples show how `Set-IndexLocationBackupMode` is used to increment the backup mode count on index locations:

- `Set-IndexLocationBackupMode EVServer`

  This command increments the backup mode count on all the index locations that are associated with server EVServer.

- `Set-IndexLocationBackupMode EVServer -IndexRootPath f:\indexing\index0`
  This command increments the backup mode count on index location `f:\indexing\index0`.
- `Set-IndexLocationBackupMode EVServer -EVSiteName Site1`
  This command increments the backup mode count on all the index locations in Site1.

In all cases, you must specify the name of the server that owns the index location or site so the cmdlet can find its ID.

If you know the ID of the index location, site or server, you can use the following syntax to increment the backup mode count:

```
Set-IndexLocationBackupMode [-EntryId <String>] [<CommonParameters>]
```

For example:

```
Set-IndexLocationBackupMode -EntryId
1F3C7910CD579234AB8EB207F0ECEBCE91210000EVServer.Domain1.local
```

This command increments the backup mode count on the object that has the specified ID. Specify the ID of an index location to increment the backup mode count on that index location. Specify the ID of a server or a site to increment the backup mode count on all its associated index locations.

`Clear-IndexLocationBackupMode` uses the same syntax to decrement the backup mode count on index locations. It also has an additional parameter which you can use to forcibly clear backup mode from index locations. For example:

```
Clear-IndexLocationBackupMode EV1 -ForceClearBackupMode 1
```

This command forcibly clears backup mode from all the index locations associated with server EV1. `Clear-IndexLocationBackupMode` ignores the existing backup mode count and sets it to 0.

`Get-IndexLocationBackupMode` also uses the same syntax to report current backup mode settings.

Vault store backup mode cmdlet syntax

The syntax is the same for all three vault store backup mode cmdlets. For example:

```
Clear-VaultStoreBackupMode [-Name] <String> [-EVServerName] <String>
[-EvObjectType] <EVObjectType> [<CommonParameters>]
```

The following examples show how `Clear-VaultStoreBackupMode` is used to decrement the backup mode count on vault stores and vault store groups:

- `Clear-VaultStoreBackupMode VS1 EVServer VaultStore`
  This command decrements the backup mode count on vault store VS1.
- `Clear-VaultStoreBackupMode VSG1 EVServer VaultStoreGroup`
  This command decrements the backup mode count on all the vault stores in vault store group VSG1.
- `Clear-VaultStoreBackupMode Site1 EVServer Site`
  This command decrements the backup mode count on all the vault stores in Site1.

In all cases you must provide the name of the server that owns the vault stores or site, and specify the object type. These parameters allow the cmdlet to find the correct ID.

You must provide the parameters in the order that is shown if you omit the parameter names. However, if you provide parameter names, you can use them in any order. For example:

```
Clear-VaultStoreBackupMode -EVServerName EVServer -EVObjectType
VaultStore -Name VS1
```

If you know the ID of the vault store, vault store group or site, you can use the following syntax to decrement the backup mode count:

```
Clear-VaultStoreBackupMode -EntryId <String> [<CommonParameters>]
```

For example:

```
Clear-VaultStoreBackupMode -EntryId
1F3C7910CD579234AB8EB207F0ECEBCE91210000EVServer.Domain1.local
```

This command decrements the backup mode count on the object that has the specified ID. Specify the ID of a vault store to decrement the backup mode count on that vault store. Specify the ID of a vault store group or a site to decrement the backup mode count on all its associated vault stores.

`Clear-VaultStoreBackupMode` uses the same syntax to decrement the backup mode count on vault stores. It also has an additional parameter which you can use to forcibly clear backup mode from vault stores. For example:

```
Clear-VaultStoreBackupMode EV1 -ForceClearBackupMode 1
```

This command forcibly clears backup mode from all the vault stores associated with server EV1. `Clear-VaultStoreBackupMode` ignores the existing backup mode count and sets it to 0.

`Get-VaultStoreBackupMode` also uses the same syntax to report current backup mode settings.

Index snapshot location backup mode cmdlet syntax

The syntax is the same for all three index snapshot location backup mode cmdlets. For example:

```
Set-EVIndexSnapshotLocationBackupMode [-SiteId <String>]
[-EVServerName <String>] [-Path <String>] [<CommonParameters>]
```

The following examples show how `Set- EVIndexSnapshotLocationBackupMode` is used to increment the backup mode count on index snapshot locations:

```
Set- EVIndexSnapshotLocationBackupMode EVServer
```

This command increments the backup mode count on all the index snapshot locations that are associated with server `EVServer`.

```
Set-IndexLocationBackupMode EVServer -Path e:\indexsnapshotlocation
```

This command increments the backup mode count on index snapshot location `e:\indexsnapshotlocation`

```
Set-EVIndexSnapshotLocationBackupMode -SiteId
17EEC4C7A9E1E4540AE93FC7B20C6A7311d10000evserver.earth.local
-EVServerName EVServer
```

Increments the backup mode count of all index snapshot locations configured on the Enterprise Vault index server `EVServer` in the Enterprise Vault site `17EEC4C7A9E1E4540AE93FC7B20C6A7311d10000evserver.earth.local`.

`Clear- EVIndexSnapshotLocationBackupMode` uses the same syntax to decrement the backup mode count on index snapshot locations. It also has an additional parameter which you can use to forcibly clear backup mode from index snapshot locations. For example:

```
Clear-EVIndexSnapshotLocationBackupMode -EVServerName
evserver.earth.local -ForceClearBackupMode
```

This command forcibly clears backup mode from all the index snapshot locations configured on the Enterprise Vault index server `evserver.earth.local`. `Clear-EVIndexSnapshotLocationBackupMode` ignores the existing backup mode count and sets it to 0.

`Get- EVIndexSnapshotLocationBackupMode` also uses the same syntax to report current backup mode settings.

Note: Enterprise Vault recommends that you set up and clear the backup mode at the Enterprise Vault site level.

Generating PowerShell backup commands for your environment

Enterprise Vault includes a PowerShell script called `Transform-Backup.ps1`, which you can use to generate PowerShell backup mode commands for your environment.

`Transform-Backup.ps1` generates an HTML file that contains a set backup mode command, and a clear backup mode command for each of the following entities in your environment:

- Enterprise Vault site (all vault stores)
- Vault store group
- Vault store
- Enterprise Vault site (all index locations)
- Enterprise Vault site (all index snapshot locations)

Note: Enterprise Vault version 14.2 onwards, Elasticsearch is the new indexing engine. The index data backup strategy has changed. For all the Elasticsearch index locations, you must now take snapshots of the index data on the Enterprise Vault index server, instead of taking filesystem-level backup of index data.

The backup strategy for all the non-Elasticsearch index locations in your environment continues to be the same as before 14.2 and supports only filesystem-level backup.

To protect your data from accidental loss, it is strongly recommended that you:

- Take a snapshot of the index data for all the Elasticsearch index locations. For more information, refer to the following article on how to backup indexes in Enterprise Vault 14.2 and later:
  https://www.veritas.com/content/support/en_US/article.100051446
- Take a backup of the index snapshot location where index snapshots are stored.
  See "Backing up index locations" on page 15.

You can use any of the commands from the HTML file that are appropriate to your backup regime.

For example, if you back up all the data associated with an entire Enterprise Vault site in one operation, your pre-backup script should include the command to set backup mode on the site's vault stores, the command to set backup mode on the site's index locations, and the command to set backup mode on the site's index snapshot locations.

When the backup operation is complete, your post-backup script should include the command to clear backup mode from the site's vault stores, the command to clear backup mode from the site's index locations, and the command to clear backup mode from the site's index snapshot locations.

`Transform-Backup.ps1` is in the `Templates` folder beneath the Enterprise Vault installation folder (for example, `C:\Program Files (x86)\Enterprise Vault\Reports\Templates`).

Before you run the script, you must set the PowerShell script execution policy, to allow only signed scripts to run. You only have to do this once.

To set the PowerShell script execution policy

1. Start the Enterprise Vault Management Shell.
2. Run the following command:

```
Set-ExecutionPolicy -executionPolicy AllSigned
```

When you have set the PowerShell script execution policy, you can run `Transform-Backup.ps1` to generate the backup mode commands for your environment.

To run the script

1. Start the Enterprise Vault Management Shell.
2. Change directory to the `Reports\Templates` folder beneath the Enterprise Vault installation folder.
3. Enter the following command to run the script:

```
.\Transform-Backup.ps1
```

4. At the following prompt:

```
Do you want to run software from this untrusted publisher?
```

   Choose `R` to run the script once.

At the end of the script, the HTML file generated by `Transform-Backup.ps1` opens automatically in your default web browser.

Using PowerShell cmdlets in backup scripts

Enterprise Vault's backup mode PowerShell cmdlets are designed to be used in your backup scripts to control backup mode. For example, you can set backup mode on vault stores, index locations, and index snapshot locations before you take a backup, and clear backup mode again after the backup is complete.

This section describes how to use Enterprise Vault's backup mode PowerShell cmdlets in your backup scripts.

In your backup scripts, you can use a single command to:

- Run a new instance of Windows PowerShell
- Load the Enterprise Vault PowerShell snap-in
- Run the appropriate cmdlet to control backup mode

On 64-bit Windows operating systems, you must run the Enterprise Vault PowerShell snap-in under the 32-bit version of PowerShell. The 32-bit version of PowerShell is installed in `%SystemRoot%\SysWow64\WindowsPowerShell\v1.0`.

For example, you can use the following command at the start of your backup script, or in a pre-backup script, to set backup mode before you take a backup. This command runs PowerShell and loads the Enterprise Vault PowerShell snap-in, then runs the `set-vaultstorebackupmode` cmdlet, to set backup mode on the vault store group called Express Vault Store Group:

```
%SystemRoot%\SysWow64\WindowsPowerShell\v1.0\powershell -psconsolefile
"C:\Program Files (x86)\Enterprise Vault\EVShell.psc1" -command "&
{set-vaultstorebackupmode -name 'Express Vault Store Group'
-evservername EVserver -evobjecttype vaultstoregroup}"
```

After your backup is complete, you should run a similar command in your script to clear backup mode. For example:

```
%SystemRoot%\SysWow64\WindowsPowerShell\v1.0\powershell -psconsolefile
"C:\Program Files (x86)\Enterprise Vault\EVShell.psc1" -command "&
{clear-vaultstorebackupmode -name 'Express Vault Store Group'
-evservername EVserver -evobjecttype vaultstoregroup}"
```

Chapter 3

Enterprise Vault recovery procedures

This chapter includes the following topics:

About using EVSVR as part of the recovery procedure

Enterprise Vault comes with a command-line utility, EVSVR, with which you can verify the consistency of the information in your vault store partitions and databases, and repair any errors. As part of any recovery procedure, we strongly recommend that you run EVSVR on multiple occasions to identify and resolve any issues:

- Before you undertake the recovery procedure, run EVSVR to identify the issues.
- When either of the following situations arises, run EVSVR again to verify that you have resolved the issues:
  - You have completed the recovery procedure.
  - The recovery procedure requires you to put your environment into normal operation (for example, in order to archive or rearchive items).

You may need to use EVSVR to make your environment consistent before you can resume normal operations.

For guidelines on how to run EVSVR, see the *Utilities* guide.

Recovering Enterprise Vault using full system backups

If you have chosen to make an application backup of your complete Enterprise Vault environment (systems, services, and tasks), you can restore it by following the steps below.

To recover Enterprise Vault using full system backups

1. Restore your full system backups.
2. If services are missing from the service control panel, use one of the following procedures to run the Enterprise Vault Configuration wizard to reconstruct the service information.
   - If you are recovering all the Enterprise Vault servers that run a Directory service and you are restoring the first one of these servers, use *Recovery procedure 6*.
     See "Recovery procedure 6: Recreating services and tasks on the first Directory service computer" on page 33.
   - When you recover subsequent servers including other servers that run a Directory service, use *Recovery procedure 7*.
     See "Recovery procedure 7: Recreating services and tasks on Enterprise Vault servers" on page 34.

Carrying out an environment recovery procedure

If a disaster occurs, follow these steps to recover an Enterprise Vault environment.

Note: Unless otherwise stated, do not start any Enterprise Vault service until all the steps of this recovery procedure have been completed.

To recover an Enterprise Vault environment

1. Restore file system backups.
2. Restore the following Enterprise Vault databases:
   - `EnterpriseVaultDirectory`
   - `EnterpriseVaultMonitoring`

- `EnterpriseVaultAudit`
- Each FSA Reporting database you have set up, if you use FSA Reporting.
- Each fingerprint database
- Each vault store database

3. Restore vault store partitions to their original locations.
4. Restore index volumes to their original locations.
5. Restore index snapshot locations to their original locations.
6. Restore the indexing data snapshot using the `Restore-EVIndexSnapshot` command. Refer to the *Enterprise Vault PowerShell Cmdlets* guide for more details.

   For more information, see How to restore Elasticsearch index data in Enterprise Vault 14.2 and later.
7. Repeat archiving operations that took place after your last backup completed.
8. Cancel all pending items from mailboxes.
9. Add any SharePoint targets that are missing. For each missing target, select the same vault store that was previously used.

   For more information on adding web applications or site collections as targets, see the *Setting up SharePoint Server Archiving* guide.

Recovering Enterprise Vault using data-only backups

Use the following recovery procedures when you have backed up only Enterprise Vault data, including the registry, and have not backed up the system disks on your Enterprise Vault servers.

The procedures described in this section require backups of the following Enterprise Vault databases:

- `EnterpriseVaultDirectory`
- `EnterpriseVaultMonitoring`
- `EnterpriseVaultAudit`
- Each FSA Reporting database you have set up, if you use FSA Reporting.
- Fingerprint databases
- Vault store databases

You must also have backups of the following Enterprise Vault data:

- Vault store partitions
- Index locations
- Index snpashot locations

You can use these procedures when you need to recover only one Enterprise Vault server, or to recover multiple servers.

To recover each server, you need to know which Enterprise Vault services it was running before the disaster occurred. If you are unsure which Enterprise Vault services were running on each server, run the SQL script `ServiceLocations.sql`, which is installed in the Enterprise Vault installation folder, for example `C:\Program Files (x86)\Enterprise Vault`.

Note: Before you can run the script you must first restore your Enterprise Vault Directory database.

Recovery procedure 1: Installing software on the servers

All the data relating to your previous Enterprise Vault installation needs to be recovered onto new servers. For each server that has failed you need to set up a new computer. Ideally, set up each computer with the same name as the original computer that it is replacing.

Note: If this is not possible the recovery steps tell you what to do to accommodate a change in computer name.

Build each new system, starting with the installation of Windows and then all the prerequisites for Enterprise Vault. Refer to the Enterprise Vault documentation if you are not sure which prerequisite software you must install on each computer.

When you have set up the correct prerequisite software on each server, install Enterprise Vault on the server.

Note the following:

- Install Enterprise Vault on each new server, into the same folder as on the original server.
- Install the same version of Enterprise Vault as is being used in your current environment.

Do not run the Enterprise Vault Configuration wizard at the end of completing the installation of the Enterprise Vault software.

Recovery procedure 2: Restoring Enterprise Vault system databases

Restore the following Enterprise Vault databases:

- `EnterpriseVaultDirectory`
- `EnterpriseVaultMonitoring`
- `EnterpriseVaultAudit`
- Each FSA Reporting database you have set up, if you use FSA Reporting.
- Fingerprint databases
- Vault store databases

If you have restored `EnterpriseVaultMonitoring` or the FSA Reporting databases to a SQL server other than the one that previously hosted them, you must update the Directory database.

To update the monitoring settings in the Directory database

- On the SQL server that hosts the Directory database, run the following SQL script:

```
USE EnterpriseVaultDirectory
UPDATE MonitoringSettings
SET SQLServer = 'SQL_server_name'
```

  Where *SQL_server_name* is the name of the new SQL server.

To update the FSA reporting settings in the Directory database

1. On the SQL server that hosts the Directory database, run the following SQL script to determine which SQL server hosted each FSA Reporting database:

```
USE EnterpriseVaultDirectory
Select SQLServer,DatabaseName From FSAReportingDatabase
```

2. Run the following SQL script:

```
USE EnterpriseVaultDirectory
UPDATE FSAReportingDatabase
SET SQLServer = 'SQL_server_name'
WHERE DatabaseName = 'FSA_reporting_database_name'
```

   Where:

   - *SQL_server_name* is the name of the new SQL server.
   - *FSA_reporting_database_name* is the name of the FSA Reporting database that you restored.

Recovery procedure 3: Renaming servers

Ideally, you should set up each server with the same name as the original server that it is replacing. However, if this is not the case, you must perform the following extra procedure.

Warning: If you are running Enterprise Vault in a clustered environment, do not perform this operation unless Veritas Support advises you to do so.

To set up a server with a different name than the old server

1. Repeat the following steps for each server that you are recovering:
   - Run SQL Query Analyzer and connect to the server that is running the Enterprise Vault Directory service.
   - Enter and run the following SQL command:

     ```
     USE EnterpriseVaultDirectory
     UPDATE ComputerEntry
     SET ComputerNameAlternate = 'Name of new server'
     WHERE ComputerNameAlternate = 'Name of old server'
     ```

2. Check that the DNS alias you set up for the old server points to the name of the new server. If you are unsure what the DNS alias is, run the following SQL query against the EnterpriseVaultDirectory database.

   ```
   USE EnterpriseVaultDirectory
   SELECT ComputerName FROM ComputerEntry
   ```

3. If you are recovering the system that provided the vault site alias (usually the first server that was added to the site), then you need to update the vault site alias to point to the new server. To do this, perform the following steps in the order listed:
   - Run SQL Query Analyzer and connect to the server running the Enterprise Vault Directory service.
   - Enter and run the following SQL command:

     ```
     USE EnterpriseVaultDirectory
     SELECT SiteEntryId
     FROM SiteEntry
     ```

     The value returned contain the vault site alias at the end of a long string of numbers. For example, if the command returns the following then the vault site alias is `sitealias`:

```
10354B15D38FE5B41BAAC212490EBA5351d10000sitealias
```

- In DNS, change the DNS alias entry so that it points at the new server.

Recovery procedure 4: Copy or move the Enterprise Vault data files

Copy or move the Enterprise Vault Elasticsearch index locations

You now need to restore the backups of the Enterprise Vault index snapshot locations to their locations on the Enterprise Vault servers.

Enterprise Vault 14.2 uses Elastisearch for indexing. So, Enterprise Vault 14.2 onwards, the only reliable and supported way to restore the index data is by restoring a snapshot.

For more information, see How to restore Elasticsearch index data in Enterprise Vault 14.2 and later.

Copy or move the Enterprise Vault Non-Elasticsearch index locations

You now need to restore the backups of the Enterprise Vault data files to their locations on the Enterprise Vault servers.

Depending on the original Enterprise Vault components that existed on the servers you are recovering you must restore only the following data files:

- If you are restoring a server that used to run a Storage service, or a server that is configured in a cluster, you need to restore onto this server the saveset files for any vault stores managed by the original Storage service.
- If you are restoring a server that used to run an Indexing service, or a server that is configured in a cluster, you need to restore onto this server the indexing data files managed by the original Indexing service.
- If you are restoring a server that used to run a Shopping service, or a server that is configured in a cluster, you need to restore onto this server the shopping files managed by the original Shopping service.

The Enterprise Vault data should be restored to the locations where they existed on the original servers. For example, if you are recovering the server running the Indexing service and the indexing data was originally stored in the following location:

```
I:\Indexing
```

then this indexing data should be restored to the same location on the new server.

To reorganize and move any SQL database devices on the disks, you can perform the procedures as listed in the following Microsoft Knowledge Base article:

http://support.microsoft.com/?kbid=181602

This must be correct before you start any of the Enterprise Vault services, otherwise some cleanup operations may occur, resulting in information loss.

Recovery procedure 5: Clearing the directory database entries

You can clear the directory database entries for all of the Enterprise Vault servers in your environment, or for selected servers.

The SQL query that is provided in this section clears the entries in the database for all the Enterprise Vault servers. If you have multiple Enterprise Vault servers in your environment, you may want to recover only some of the servers. The following technical note provides alternative SQL scripts that let you specify the servers for which you want to clear directory entries:

https://www.veritas.com/docs/100001173

To clear the directory database entries for all of the Enterprise Vault servers

1. Run SQL Query Analyzer and connect to the server running the Enterprise Vault Directory service.
2. Enter and run the following SQL command:

```
USE EnterpriseVaultDirectory
UPDATE StorageServiceEntry
SET StorageArchive = '', StorageRestore = '',
StorageReplayIndex = '', StorageSpool = ''
UPDATE RetrievalTask
SET RetrievalSpoolQueue = ''
UPDATE ArchivingRetrievalTask
SET MessageQueue = ''
UPDATE RetrievalTask
SET MessageQueue = ''
UPDATE JournalTask
SET MessageQueue = ''
UPDATE PublicFolderTask
SET MessageQueue = ''
```

Recovery procedure 6: Recreating services and tasks on the first Directory service computer

If you are recovering all the Enterprise Vault servers that run a Directory service, you must use this procedure when you recover the first of these servers. When you recover the subsequent servers including other servers that run a Directory service, use the procedure described in *Recovery procedure 7*.

See "Recovery procedure 7: Recreating services and tasks on Enterprise Vault servers" on page 34.

The Enterprise Vault Configuration wizard is able to detect missing services and tasks provided that the server name is identical to that in the original installation, or you have correctly followed *Recovery procedure 3*.

See "Recovery procedure 3: Renaming servers" on page 30.

To recreate services and tasks on the first Directory service computer

1. Start the Enterprise Vault Configuration wizard.
2. Select **Yes** to create a new Directory service, and then click **Next**.
3. Enter the details of the Vault Service account, and then click **Next**.

   The Enterprise Vault Configuration wizard does the following:

   - Converts the login for the Enterprise Vault Admin service so that it runs under the Vault Service account.
   - Adds the Vault Service account to the Local Administrators group on the computer.
   - Grants the user rights **Log on as a service** and **Debug programs** to the Vault Service account.
   - Creates and starts the Enterprise Vault Directory service.
4. When prompted for the name of the SQL Server that will host the directory database, enter the name of SQL Server used to host the directory database for the original configuration of Enterprise Vault, and then click **Next**.
5. The Enterprise Vault Configuration wizard checks that the SQL Server exists and can connect to it. As long as you have recovered the Directory database, the Enterprise Vault Configuration wizard now recreates the services and tasks installed on the Directory service computer.
6. To recreate the Enterprise Vault services on the Directory service computer, enter the password of the Vault Service account.

7 When the repair has finished, a success message is displayed.

8 If the Enterprise Vault Configuration wizard does not display a message, do not continue to run the wizard. Close the wizard and do the following:

- Check that all previous steps have been successful, repeat any missed steps, and then run the Enterprise Vault Configuration wizard again.
- Create a String registry value called UseLanManNameForSCM under the following registry key:

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

- Give UseLanManNameForSCM a value of 1.
- Run the Enterprise Vault Configuration wizard again.
- If the problem persists, contact Enterprise Vault Support for further assistance.

Recovery procedure 7: Recreating services and tasks on Enterprise Vault servers

If you are recovering all the Enterprise Vault servers that run a Directory service, for the first one you must use *Recovery procedure 6*.

See "Recovery procedure 6: Recreating services and tasks on the first Directory service computer" on page 33.

When you recover the subsequent servers including other servers that run a Directory service, use the procedure described in this section.

The Enterprise Vault Configuration wizard is able to detect missing services and tasks provided that the server name is identical to that in the original installation, or you have correctly followed *Recovery procedure 3*.

See "Recovery procedure 3: Renaming servers" on page 30.

To recreate services on other Enterprise Vault servers

1 Make sure the server running the Directory service is available on the network and the Directory service is started.

2 Make sure the Admin service is started on the local computer.

3. Start the Enterprise Vault Configuration wizard on the server.
4. When asked whether you want to create a directory or use an existing one, select **No, use existing remote Vault Directory** and enter the name of the server running the Directory service.
5. Enter the password of the Vault Service account. This is necessary to recreate the Enterprise Vault services on the computer.
6. The Enterprise Vault Configuration wizard recreates the Enterprise Vault services and tasks that used to run on the server and displays a message to indicate success.
7. If the Enterprise Vault Configuration wizard does not display a success message, do not continue to run the wizard. Close the wizard and then do the following:
   - Check that all previous steps have been successful, repeat any missed steps, and then run the Enterprise Vault Configuration wizard again.
   - Create a String registry value called UseLanManNameForSCM under the following registry key:

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

   - Give UseLanManNameForSCM a value of 1.
   - Run the Enterprise Vault Configuration wizard again

- If you are sure you have followed all steps correctly and setting the registry key does also not help, contact your Enterprise Vault Support Representative for further assistance.

8 Start all the Enterprise Vault services.

The message queues should automatically be recreated on the new server. If the Storage service is configured to start multiple processes, it may stop during message queue creation. This is because of a conflict between the processes creating the queues. To fix the problem, restart the Storage service.

If the Indexing service finds any inconsistency in the index metadata, it automatically synchronizes the metadata. You may see the following events:

```
Event 41395 Index Volume metadata upgrade required
Event 41372 Index Volume metadata synchronization started
```

During the synchronization the Indexing service logs progress events every 10 minutes. At the end of the synchronization, one of the following events is logged:

```
Event 41373 Index Volume metadata synchronization completed
Event 41377 Index Volume metadata synchronization completed
```

The index synchronization may take some time. For example, an Enterprise Vault recommended specification server takes approximately 10 minutes to process 5,000 index volumes.

If any other index housekeeping is required there will be other progress messages every few minutes.

Recovery procedure 8: Checking the Web Access application settings

You must now ensure that the port and protocol settings for the Web Access application are correct.

To check the Web Access application settings

1 Open the Administration Console.

2 Expand the **Enterprise Vault** and **Directory** containers.

3 Right-click the **Site** entry, and then select **Properties**.

4 View the General page. Check that the port and protocol set for accessing the Web Access application virtual directory, **/EnterpriseVault**, match the settings on the Default Web Site in IIS.

Recovery procedure 9: Checking registry entries

Check that the Enterprise Vault registry entries are all set correctly on the newly-recovered servers.

The main registry entries are under the following key:

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

Additionally, you may have set registry entries under HKEY_CURRENT_USER when logged in as the Vault Service account. If so, restore these entries on each server too, under the following key:

```
HKEY_CURRENT_USER
 \Software
  \KVS
   \Enterprise Vault
```

Recovery of an Enterprise Vault component

Table 3-1 describes how to restore individual Enterprise Vault components.

Caution: Only perform this operation if you are advised to do so by Veritas support.

Table 3-1 How to recover Enterprise Vault components

To recover this component	Do this
Directory database	**1** Ensure that the Enterprise Vault Admin services on all computers are stopped. To do this, use Windows Manager to stop the Enterprise Vault Admin service on each computer. **2** Restore the databases. **3** Start the Directory service.
Directory service computer	**1** Restore the system backup, and the Directory service database. **2** Restore the backups of any other Enterprise Vault services that run on this computer.
Index snapshot locations	Restore the backup of index snapshot location to its original location.

Table 3-1 How to recover Enterprise Vault components *(continued)*

To recover this component	Do this

Index locations	**1** Restore the system backup of the computer running the Indexing service.
	2 Ensure that the service is stopped.
	3 Restore all the Indexing files to their original locations; ensure that all the backed-up files are restored, and that no other files remain in the indexing folders. Do not try to restore individual files because this leads to inconsistent indexes that may be unusable.
	4 Restore the backups of any other Enterprise Vault services that run on this computer.
	When correctly restored, the Indexing service can use the restored indexes. However, there may be indexing entries lost from archive operations carried out since the last backup. The Storage service will automatically reconstruct the affected indexes.
	If the Indexing service finds any inconsistency in the index metadata, it automatically synchronizes the metadata. You may see the following events:
	`Event 41395 Index Volume metadata upgrade required`
	`Event 41372 Index Volume metadata synchronization started`
	During the synchronization the Indexing service logs progress events every 10 minutes. At the end of the synchronization, one of the following events is logged:
	`Event 41373 Index Volume metadata synchronization completed`
	`Event 41377 Index Volume metadata synchronization completed`
	The index synchronization may take some time. For example, an Enterprise Vault recommended specification server takes approximately 10 minutes to process 5,000 index volumes.
	If any other index housekeeping is required there will be other progress messages every few minutes.
	Note: Enterprise Vault 14.2 uses Elastisearch for indexing. So, Enterprise Vault 14.2 onwards, the only reliable and supported way to restore the index data is by restoring a snapshot.
	For more information, see How to restore Elasticsearch index data in Enterprise Vault 14.2 and later.

Table 3-1 How to recover Enterprise Vault components *(continued)*

To recover this component	Do this
Shopping service files	**1** Restore the system backup of the computer running the Shopping service. **2** Ensure that the Shopping service is stopped. **3** Restore the backup of the shopping data to its original location. **4** Restore the backups of any other Enterprise Vault services that run on this computer. **5** Start the Shopping service. Users should be able to use their existing shopping baskets and create new shopping baskets.
Vault store files	**1** Restore each system running a Storage service. **2** Restore the vault store files into their original locations. **3** Restore the vault store's database. **4** Restore the backups of any other Enterprise Vault services that run on the restored Storage service computer. **5** Run the EVSVR utility to verify the consistency of the information in your vault store partitions and databases, and repair any errors. See the *Utilities* guide for more information.
Vault store or fingerprint databases	**1** Restore the computer running the Storage service and replace the vault store files. **2** Restore the following databases: ■ Vault store or fingerprint databases ■ Directory database ■ Primary and msdb databases **3** Restore the backups of any other Enterprise Vault services that run on the restored Storage service computer. **4** Run the EVSVR utility to verify the consistency of the information in your vault store partitions and databases, and repair any errors. See the *Utilities* guide for more information.

Recovery of Enterprise Vault in a VCS cluster

This section outlines how to repair an Enterprise Vault VCS cluster in which one or all of the nodes needs rebuilding. See the *Installing and Configuring* guide and *Solutions Guide* for Veritas Storage Foundation and High Availability Solutions for more information on how to perform the following steps.

The *Installing and Configuring* guide also describes how to implement a disaster recovery solution using Veritas Storage Foundation HA with the Veritas Volume Replicator (VVR) and Global Cluster Option (GCO).

See "About using EVSVR as part of the recovery procedure" on page 25.

Recovery scenario 1: One of the cluster nodes needs rebuilding

If one of the Enterprise Vault nodes in the cluster needs rebuilding, the failover node should automatically take its place. Follow the steps below to rebuild the inoperable node and make it available again as the new failover node.

To repair a single node in the cluster

1. Install Windows and all other prerequisite software.
2. If necessary, install VCS and configure the node as part of the cluster.
3. If necessary, install Enterprise Vault.
4. Run the Enterprise Vault Cluster Setup wizard. You must modify the existing service group so that the node is a member of it.
5. Run the Enterprise Vault Configuration wizard on the failover node. You must choose to add the node as a failover node for an existing clustered server.

Recovery scenario 2: All the cluster nodes need rebuilding

If all the cluster nodes need rebuilding, but you have backup copies of the SQL Server databases and the Indexing and saveset data for Enterprise Vault, you can follow the steps below to rectify the situation.

To repair all the nodes in the cluster

1. Rebuild all the computers and restore the databases.

   See "Recovery procedure 2: Restoring Enterprise Vault system databases" on page 29.
2. Recreate the cluster in VCS with the same number of disks, and mount the shared disk with the same drive letters as before.
3. Restore the Indexing and Enterprise Vault store data to disks using the same drive letters as before.

   See "Recovery procedure 4: Copy or move the Enterprise Vault data files" on page 31.
4. Install Enterprise Vault on all the nodes in the cluster.
5. For each Enterprise Vault server in the cluster, perform the following steps in the order listed:

- Run the Enterprise Vault Cluster Setup wizard to recreate the service groups. Use the same virtual server names as before.
- Run the Enterprise Vault Configuration wizard on the primary node. Choose to configure a new Enterprise Vault server with cluster group.
  The wizard detects the existing virtual server name and performs a repair. When the repair is complete, a wizard page is displayed with which you can create the service resources. Do not bring the resources online when given the option to do so.
- Run the Enterprise Vault Configuration wizard on the failover node. Choose to add the node as a failover node for an existing clustered server.

6 Clear the Directory database entries.

See "Recovery procedure 5: Clearing the directory database entries" on page 32.

7 Check the Web Access application URL.

See "Recovery procedure 8: Checking the Web Access application settings" on page 36.

8 Bring the cluster resources online and test that failovers work as planned.

Recovery of Enterprise Vault in a Windows Server failover cluster

This section outlines how to repair Enterprise Vault in a Windows Server failover cluster when one or all of the nodes needs rebuilding. For detailed instructions on how to perform individual steps, see the *Installing and Configuring* guide.

Recovery scenario 1: One of the cluster nodes needs rebuilding

If one of the Enterprise Vault nodes in the cluster fails, the failover node should automatically take its place. The steps below outline how to rebuild the inoperable node and, assuming an any-to-any configuration, make it available as the new failover node.

To repair a single node in the cluster

1 Install Windows and all other prerequisite software.

2 Install Enterprise Vault.

3 Use Failover Cluster Manager to add the node to the cluster. Replace the old node with the new node as the following:

- A possible owner of each resource in the failed-over resource group.
- A preferred owner of the failed-over resource group.

4 Run the Enterprise Vault Configuration wizard on the new node, selecting the option to add the node as a failover node for an existing clustered server.

Recovery scenario 2: All the cluster nodes need rebuilding

If all the cluster nodes need rebuilding, but you have backup copies of the SQL Server databases and the Indexing and saveset data for Enterprise Vault, you can follow the steps below to rectify the situation.

To repair all the nodes in the cluster

1 Rebuild all the computers and restore the databases.

See "Recovery procedure 2: Restoring Enterprise Vault system databases" on page 29.

2 Recreate the cluster using Failover Cluster Manager. Use the same number of disks, and mount the shared disks with the same drive letters as before.

3 Restore the Indexing and Enterprise Vault store data to disks using the same drive letters as before.

See "Recovery procedure 4: Copy or move the Enterprise Vault data files" on page 31.

4 Recreate the resource groups, including the prerequisite resources, using the original virtual server names.

5 Install Enterprise Vault on all the nodes in the cluster.

6 Run the Enterprise Vault Configuration wizard on each primary node. Choose to configure a new Enterprise Vault server with cluster support. The wizard detects the existing virtual server name in the Enterprise Vault Directory database's ComputerEntry table, and performs a repair.

When the repair is complete, a wizard page is displayed, with which you can recreate the Enterprise Vault service resources and Server Instance resource. Do not bring the resources online when given the option to do so.

7 Run the Enterprise Vault Configuration wizard on each failover node. Choose to add the node as a failover node for an existing clustered server.

8 Clear the Directory database entries.

See "Recovery procedure 5: Clearing the directory database entries" on page 32.

9 Check the Web Access application URL.

See “Recovery procedure 8: Checking the Web Access application settings” on page 36.

10 Bring the cluster resources online and test that failovers work as planned.