Symantec.
Confidence in a connected world.

Backing Up Enterprise Vault

Evan Barrett
Enterprise Vault Technical Field Enablement

Last Update: November 3, 2010

Contents

If you have any comments on this Whitepaper please email EV-TFE-Feedback@Symantec.com

Overview

The purpose of this document is to provide a best practice approach to backing up the three main components of Enterprise Vault: The Microsoft SQL Server databases, Enterprise Vault indexes and Enterprise Vault Stores. This document will also provide specific examples of backup scripts, registry settings, and additional information for backing up Enterprise Vault with Symantec NetBackup using standard file level backups as well as using the new NetBackup Enterprise Vault backup agent.

Backing up the Database Component

The database component plays a crucial role for Enterprise Vault. All configuration data for a particular Enterprise Vault installation is stored in the EnterpriseVaultDirectory database. Besides the "EnterpriseVaultDirectory" database, Enterprise Vault has other databases related to vault stores, fingerprinting, reporting, and auditing. These databases start with "EV" and must be backed up to ensure proper recovery of Enterprise Vault.

It is highly recommended that SQL databases be backed up at or nearly the same time as other Enterprise Vault data such as vault store partitions and indexes. This will ensure the best data integrity if a full restore from backups is required for Enterprise Vault.

This section will document three recommended back up methods: flat files, using commercially available backup products such as Symantec's NetBackup or Backup Exec, and high availability. Attempting to back up the database by not using one of the following methods can lead to the following issues:
1) Fail completely as most backup products for Windows have a difficult time backing up open files
2) The backing up of the database while not in "backup mode" or "read-only mode" will lead to bad data being backed up usually resulting in failed restore attempts or restores with faulty data.

For the backing up of Vault Store Group databases (or fingerprint databases), please read section entitled "Timing of Backups".

The Flat File Method

The flat file method uses the native backup utility that is built into Microsoft SQL Server. The SQL backup utility will put the database(s) associated with Enterprise Vault into "backup mode" allowing for a clean backup of the database.   Microsoft SQL Server will dump the contents of the databases and transaction logs into flat files. In turn, these flat files can be backed up to tape or to disk.

Before starting the backing of the SQL databases, it is highly recommended that Enterprise Vault be put into Read-Only mode (Enterprise Vault 2007 and older) or Backup Mode (Enterprise Vault 8.0 or newer). This will ensure that Enterprise Vault is not attempted to update the database.

If copying these flat files to disk, it is highly recommended that the disk be on a different system, preferably at a remote site. As this might not be possible for all situations, it is recommended at minimum that the files be copied to a physically different disk than where the database data and transaction logs are stored. Thus, in the event of a hard disk failure of the database data and logs, the backup will still be available.

If backing up to tape, it is recommended that backup tapes be stored in a safe location preferably at an offsite location for a period of time after the backup. This will provide for data availability in the event of a site failure due to fire, flooding, or other events. Once again, this might not be suitable for all locations. A "tape vault" which is designed to protect tape media from fire and water can also be used for the safe storage of media.

The flat files, in turn, can also be backed up using Windows NT backup or a commercial backup product. These backup products can be configured to back up the flat files straight to tape or a remote disk.

For more information on using the built-in Microsoft SQL Server backup, please refer to the Microsoft SQL Server documentation.

Using Commercially Available Backup Software
There is a wide range of commercially available backup software suites and can take advantage of the Microsoft SQL's backup API. These backup products will work directly with the SQL backup API to back up databases and transaction logs by putting the databases into "backup mode" to ensure data integrity that can be used to restore the data properly.

If backing up to disk is the preferred method, it is highly recommended that the backed up data be migrated to disk at a remote location in the event of a site failure due to fire, flooding, or other events or be migrated to tape in the long run.

If backing up directly to tape, it is recommended that a tape rotation policy be implemented that allows for tape media to be sent offsite for safe keeping in the event of location disaster such as fire, flooding, or other events. This may not always be a feasible solution. Thus, it is minimally recommended that backup media be store in a "tape vault" that will safe guard media from fire or flooding.

Symantec Backup Exec and NetBackup both have additionally licensed add-ons that will back up Microsoft SQL databases and transaction logs which work directly with the SQL backup API.

Using High Availability
Using High Availability, also known as clustering, can allow the Enterprise Vault database components to stay online in the event of a hardware or site failure. Using Microsoft Cluster Server or Symantec Storage Foundation for Windows with High Availability (SFW-HA), a cluster can be configured to host the Enterprise Vault database at the primary location on one or more systems and can be configured to host the database at a remote location for the purposes of failover in the event of a site disaster of the primary location. It should be noted that using a high availability solution should still incorporate a backup solution as outlined in the "Setting and Clearing Backup Mode in the Enterprise Vault Administration Console" and "Setting and Clearing Backup Mode in the Enterprise Vault Management Shell" sections.

Newer versions of Microsoft SQL offer various log shipping methods that can assist with disaster recovery as well. For more information, please refer to the Microsoft SQL documentation.

It should be noted that using a high availability or log shipping solution should still incorporate a backup solution as outlined in the previous sections.

Backing up Enterprise Vault Index and Vault Store Partition Locations
Developing a reliable backup solution for Enterprise Vault Indexes and Stores is crucial for safe guarding valuable data that has been archived. In the event of a hardware failure or site disaster, a good backup will make recovering Enterprise Vault archived data quicker and easier.   This section will document basic requirements for backing up archived content.

When using Safety Copies, items archived by Enterprise Vault will not be deleted from the target until a good backup of the vault store partitions have been completed. This provides a safety net in the event of a hardware failure of the vault store partition(s).

Starting with Enterprise Vault 8.0, a new backup mechanism allows the Enterprise Vault administrator an easier way to back up data. Using the Enterprise Vault Administration Console or Enterprise Vault Management Shell (based on Powershell), the administrator can easily put Enterprise Vault indexes or Vault Stores in to Backup Mode. Once an index or vault store is in Backup Mode, it can be safely backed up as the index or vault store is in read-only mode for the purposes of backup. Additional content may not be added or modified while in Backup Mode. Once a backup has completed, indexes or vault stores can be taken out of Backup Mode in order for normal operations to resume.   It should be noted that end users can still search and retrieve data from Enterprise Vault while an index or Vault Store is in Backup Mode.

Setting and Clearing Backup Mode in the Enterprise Vault Administration Console
The VAC allows the administrator to set Backup Mode for vault stores and/or indexes at a site or
Enterprise Vault server level.

Setting Backup Mode for an Enterprise Vault Site
To set Backup Mode for an entire site, bring up the Enterprise Vault Administration Console (VAC), right-
click on the site name, and then click on Set State:
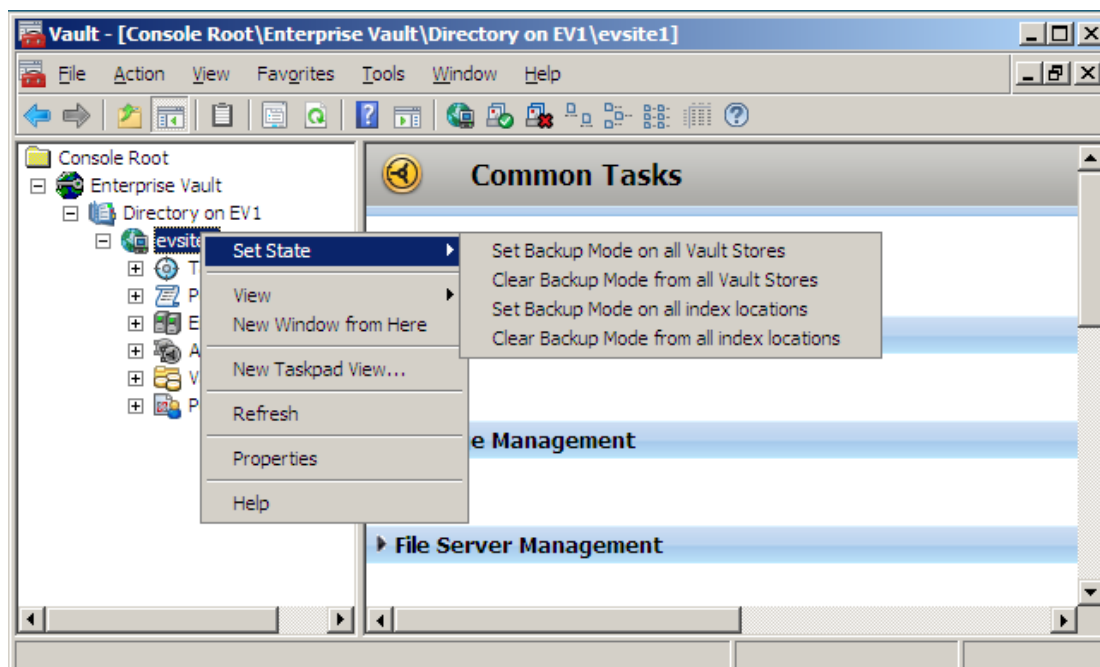
There are four different options once Set State has been selected: Set Backup Mode on all Vault Stores,
Clear Backup Mode from all Vault Stores, Set Backup Mode on all index locations, and Clear Backup Mode
from all index locations.

When selecting "Set Backup Mode" on Vault Stores or index locations at the site level (as shown in the
previous screenshot), all Vault Stores and/or indexes in that particular Enterprise Vault site will be put into
Backup Mode. A confirmation screen will appear asking the user to confirm Backup Mode. Once clicking
yes, Enterprise Vault will put the selected items in Backup Mode and a pop up window will appear letting
the user know when this process has been completed.

When selecting "Clear Backup Mode" on Vault Stores or index locations, Backup Mode will be cleared. A
confirmation screen will appear asking the user to confirm the clearing of Backup Mode. Once clicking yes,
Enterprise Vault will take the selected items out of Backup Mode and window pop up will appear once the
process has been finished.

Setting and Clearing Backup Mode for a Specific Vault Store
Enterprise Vault 8.0 also offers the ability to put a particular Vault Store into Back Mode. This is easily
done by selecting the desired Vault Store, right-clicking on it and selecting Set Backup Mode as illustrated
in the following screenshot:
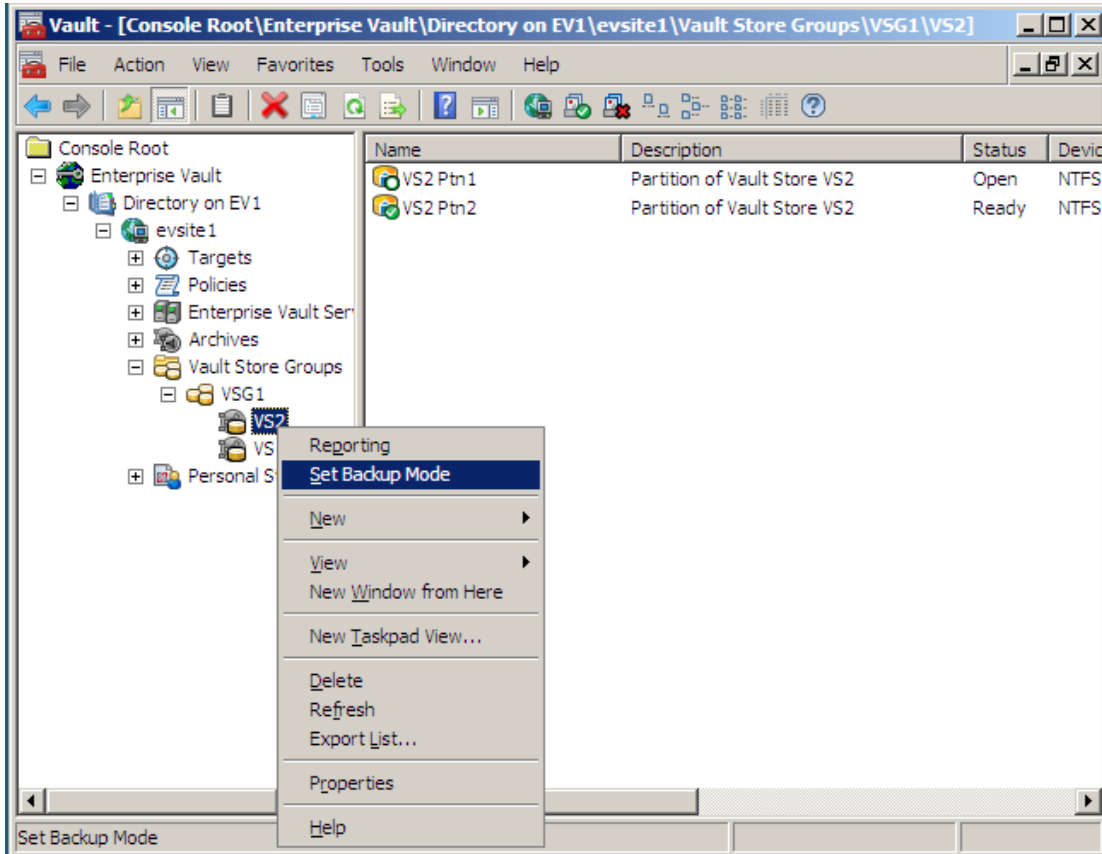
Clearing Backup Mode uses the same process as setting Backup Mode. It should be noted that when setting or clearing Backup Mode on a specific Vault Store, you will only have the option to either Set or Clear Backup Mode depending on the state of the Vault Store. To clear Backup Mode, simply select Clear Backup Mode:
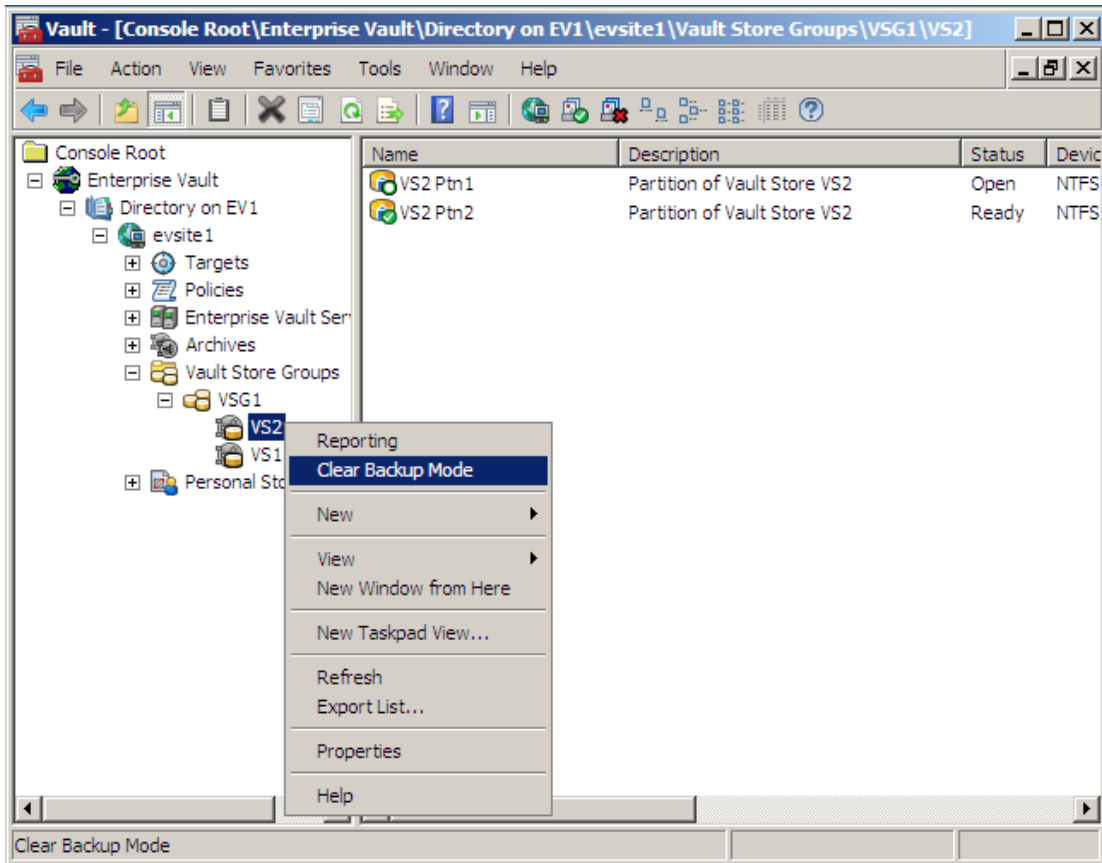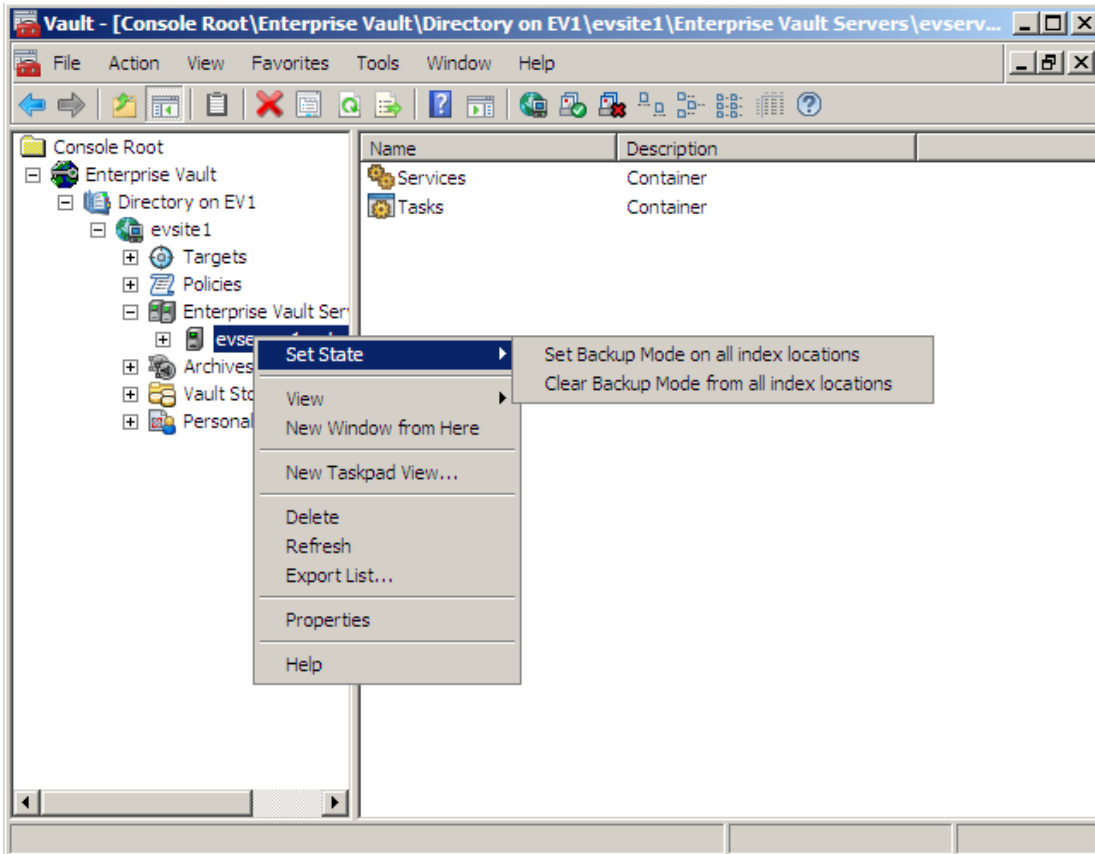
Setting and Clearing Backup Mode for All Indexes on an Enterprise Vault Server

Setting and Clearing Backup Mode on all indexes on a particular Enterprise Vault Server is also a simple task when using the VAC. The administrator can simply expand out the VAC to Enterprise Vault Servers, right-click on the desired Enterprise Vault server, click on Set State and select "Set Backup Mode on all index locations" or "Clear Backup Mode from all index locations" as shown in the following screenshot:
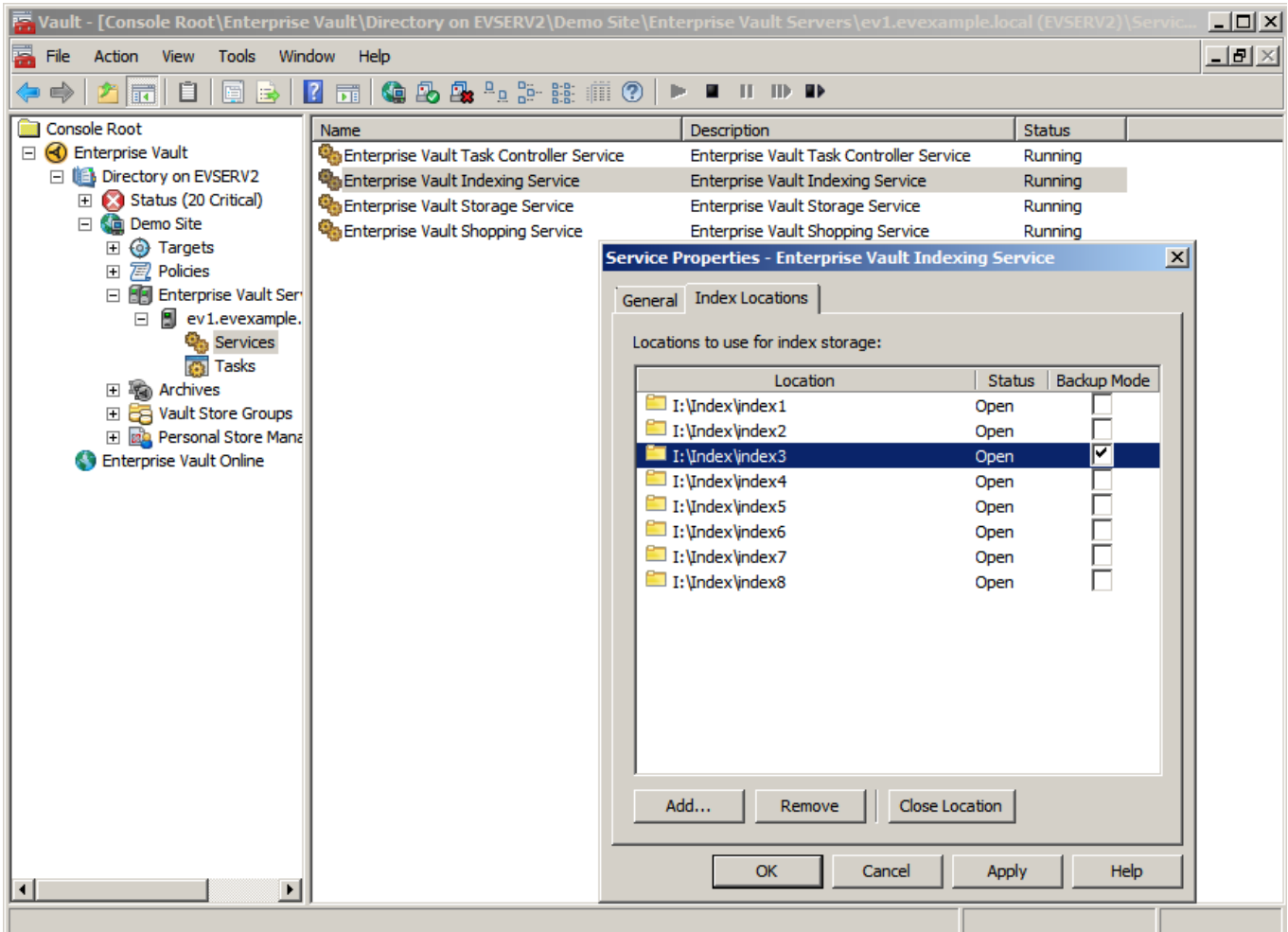
Setting and Clearing Backup Mode for a Specific Index on an Enterprise Vault Server

If a particular index location needs to be put into or out of Backup Mode, the administrator can simply use the VAC. In the VAC, expand out to Enterprise Vault Servers, expanding the desired server, click on Services, double-clicking on the Enterprise Vault Index Service (to bring up its properties), and selecting the Index Locations tab. Setting or clearing Backup Mode for a particular index is as simple as checking or clearing the "Backup Mode" checkbox for the particular index location as detailed in the following screenshot:

Setting and Clearing Backup Mode Using the Enterprise Vault Management Shell
Enterprise Vault 8.0 offers a new PowerShell tool that allows the administrator to put Enterprise Vault into and out of Backup Mode. Using the management shell allows the administrator to control Backup Mode using a script. This is particularly useful for unattended backups of Microsoft SQL databases, Vault Store partitions, and index locations. To use the shell, Windows PowerShell MUST be installed.

Using Enterprise Vault Management Shell for the First Time
If the Enterprise Vault Management Shell has not been previously used, it must be manually initialized (only once) by running it from the Windows Start Menu. Simply click on Start->Programs->Enterprise Vault->Enterprise Vault Management Shell. If PowerShell has not been enabled, a pop up window will appear asking the user if PowerShell should be enabled. Click on Yes. The initialization process may take a few moments to complete.

Enterprise Vault 8.0SP3 Changes
Starting with Enterprise Vault 8.0SP3, a new PowerShell script to help generate backup mode commands specific to the environment. The script (%PROGRAMFILES%\Enterprise Vault\Reports\Templates\Transform-Backup.ps1) generates the PowerShell backup commands which you can use to place your Enterprise Vault environment in Backup Mode. The PowerShell commands are

specific to your environment can be used directly in your backup scripts. For more information, please review the following technical note:

http://www.symantec.com/business/support/index?page=content&id=TECH75694

Before running this script for the first time, you must grant permissions for the script to be run by executing the following command in PowerShell: *Set-ExecutionPolicy –ExecutionPolicy Allsigned*.

Running the Transform-Backup.ps1 script will generate an HTML file which will be opened by the default browser:
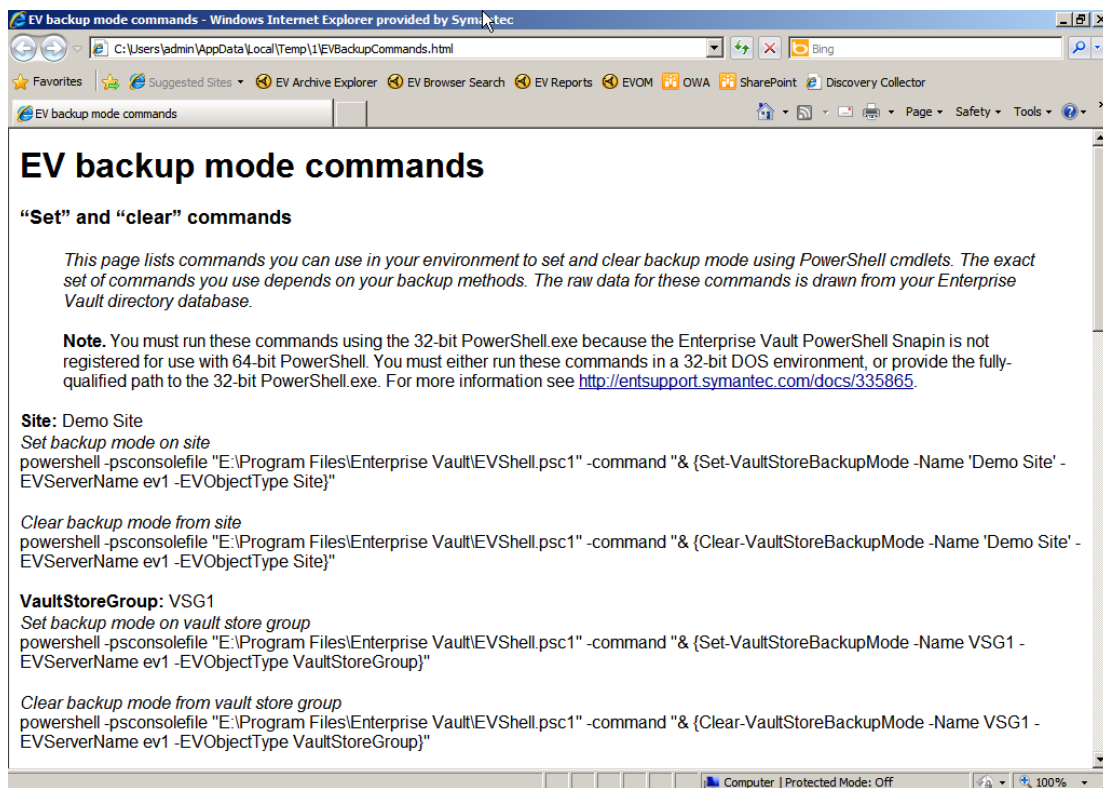
PowerShell Usage for Vault Stores

Start Enterprise Vault Management Shell from the Windows Start menu: Start->Programs->Enterprise Vault->Enterprise Vault Management Shell.

The basic command structure for setting and clearing a Vault Store into and out of backup mode:

```
Set-VaultStoreBackupMode [-EVServerName] <string> [-Name] <string> -
EVObjectType <EVObjectType> [<CommonParameters>]

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

Example (setting Backup Mode at a site level) where LiveSite is the site name, EVServer1 is the server, and Site is specified for site-wide backup mode:

```
Set-VaultStoreBackupMode LiveSite EVServer1 Site
```

Example (setting Backup Mode on a particular Vault Store) where Store1 is the Vault Store Name, EVServer1 is the EV server, and VaultStore is specified to indicate Backup Mode for a Vault Store:

```
Set-VaultStoreBackupMode Store1 EVServer1 VaultStore
```

Example (clearing Backup Mode at the vault store group level) where MyGroup1 is the Vault Store Group name, EVServer1 is the EV server name, and VaultStoreGroup is specified to indicate backup mode for a Vault Store Group:

```
Clear-VaultStoreBackupMode MyGroup1 EVServer01 VaultStoreGroup
```

Example (clearing Backup Mode using an Entry ID):

```
Clear-VaultStoreBackupMode –EntryID <Entry ID>
```

PowerShell Usage for Indexes

Start Enterprise Vault Management Shell from the Windows Start menu: Start->Programs->Enterprise Vault->Enterprise Vault Management Shell.

The basic command line structure for setting and clearing an Index location in and out of Backup Mode:

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

```
Clear-IndexLocationBackupMode [-EVServerName] <string> -EVSiteName <string>
-IndexRootPath <string> [<CommonParameters>]
```

```
Set-IndexLocationBackupMode – EntryId <string> [<CommonParameters>]
```

```
Clear-IndexLocationBackupMode – EntryId <string> [<CommonParameters>]
```

Example (setting backup mode for the site) where EVserver1 is the name of the EV server and LiveSite is the name of the EV site:

```
Set-IndexLocationBackupMode EVServer1 LiveSite
```

Example (setting backup mode for one Index location) where EVServer1 is the name of the EV server and "F:\indexes\index5" is the direct path to an index location:

```
Set-IndexLocationBackupMode EVServer1 F:\indexes\index5
```

Example (clearing backup mode for an EV server) where EVServer1 is the EV server name:

```
Clear-IndexLocationBackupMode EVServer1
```

Example (clearing the backup mode using an Entry ID):

```
Clear-IndexLocationBackupMode <EntryID>
```

Scripting out PowerShell Commands

Often times a backup application will allow the administrator to run pre and post backup script files from a .bat or .cmd file. The following examples demonstrate how to put Enterprise Vault into and out of Backup Mode for all Vault Store and Indexes in an EV site using a batch file. The example assumes that Enterprise Vault is installed on the C: drive, EVServer1 is the EV server name, and "life line" is the name of the Enterprise Vault site.

Pre-Backup.bat:

```
powershell.exe –PSConsole "C:\Program Files\Enterprise Vault\evshell.psc1"
set-indexlocationbackupmode EVServer1 'life line'

powershell.exe –PSConsole "C:\Program Files\Enterprise Vault\evshell.psc1"
set-vaultstorebackupmode 'life line' EVServer1 Site
```

Post-Backup.bat:

```
powershell.exe –PSConsole "C:\Program Files\Enterprise Vault\evshell.psc1"
clear-indexlocationbackupmode EVServer1 'life line'

powershell.exe –PSConsole "C:\Program Files\Enterprise Vault\evshell.psc1"
clear-vaultstorebackupmode 'life line' EVServer1 Site
```

Considerations When Upgrading from Older Versions of Enterprise Vault

Versions of Enterprise Vault prior to version 8.0 relied on Windows Registry modifications and the stopping and starting certain EV services. When upgrading to Enterprise Vault 8.0, the previous backup methods will still work. Warning messages will be generated in the Event Viewer logs stating that EV is set up to work with the older backup methods when the Enterprise Vault Admin service starts and, as such, the new Backup Mode will be disabled.

To use the new Backup Mode method in Enterprise Vault 8.0 after an upgrade, the following Windows Registry values will need to be removed from HKEY_LOCAL_MACHINE\Software\KVS\Enterprise Vault\Storage:

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

Advanced Backup Strategies

Vault Store Partition Sizes

When using Enterprise Vault 8.0 or later with Optimized Single Instance Storage (OSIS), keep Vault Store partition sizes smaller. Smaller partitions close faster and also backup faster. Using the partition rollover feature (available with Enterprise Vault 8.0 and later) will automatically open the next "ready" partition when configured properly.

Utilizing Snapshots for Backing up Enterprise Vault

Using snapshot technology (such as using Storage Foundation for Windows or hardware snapshots) to back up Enterprise Vault index and storage volumes can decrease the amount of time required in Backup Mode. Here are the recommended steps:

- Snap back existing snapshot volumes to their original counterparts (if volumes have already in a snapshot state)
- Put index and/or Vault Stores in Backup Mode (or Read-Only Mode with older versions of Enterprise Vault)
- Perform snapshot operation
- Clear Backup Mode for indexes and/or Vault Stores.
- Perform backup of the snapshot volumes

Note: When using snapshots for backups and using Enterprise Vault Safety Copies, the Vault Store partition backup mode must be set to "Check for a trigger file". The following screenshot shows how set up a Vault Store partition to use a trigger file with Enterprise Vault 9.0:
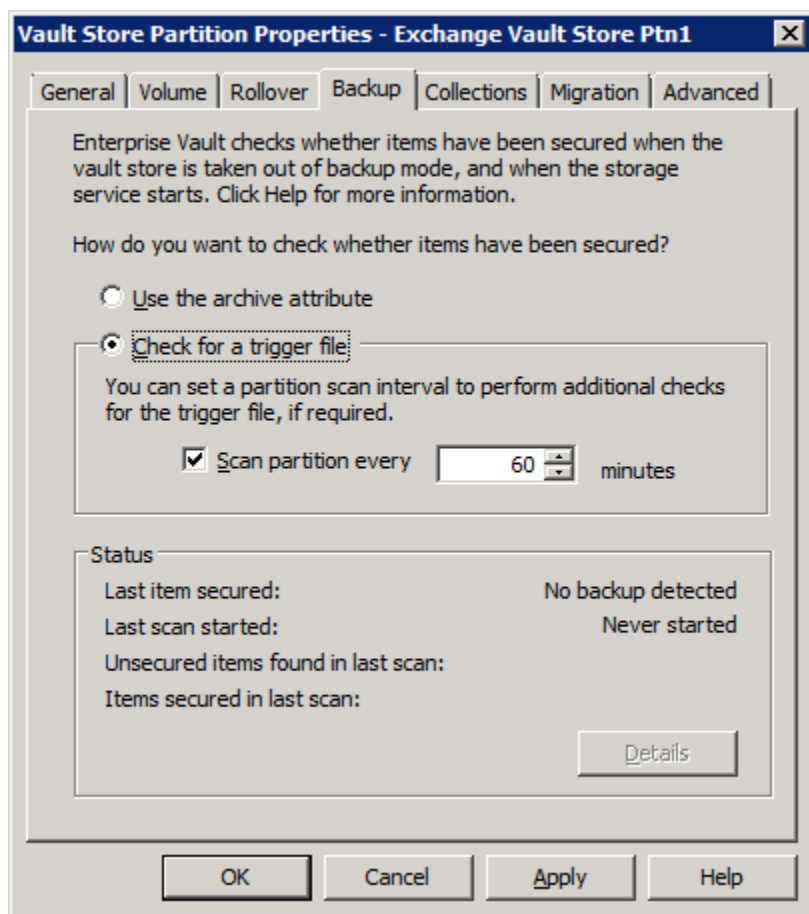
Backup the Whole Enterprise Vault Server in One Backup Job?
If a separate backup job cannot be used to back up just the Enterprise Vault indexes and Vault Store partitions, then developing scripts as outlined in the "Backing up Enterprise Vault Index and Vault Store Partition Locations" section should be used. However, if a separate job can be created just for the purposes of backing up Enterprise Vault data, the following requirements should be followed when performing regular system backups:

For a regular system backup that does not include Enterprise Vault Indexes and Store data, the following locations should be *excluded* from the system backup:

- Index locations (such as l:\index)
- Vault store locations (such as s:\storage)
- Shopping service data (such as C:\Program Files\Enterprise Vault\Shopping)

If using remote storage for indexes or Vault Store partitions, it is recommended that system backups for those remote systems exclude the Enterprise Vault data locations.

Backup Frequency for Index and Vault Store Partitions
For the ease of recovering Enterprise Vault indexes and stores, it is recommended that full backups be used for each backup. Backups for active indexes and open vault store partitions should be done on a daily basis in order to backup newly archived data. As a daily full backup may not always be feasible, a weekly full backup and daily incremental backup may be more practical.

To reduce the amount of data being backed up, Enterprise Vault indexes and store partitions that have been closed can be backed up less frequently. Since no additional data will be added to a closed vault store partition, a backup can be performed once a month or quarter or even once year. The retention period for a backup image of closed partitions should be set to the frequency of the backup or longer.

Timing of Backups
In order to provide the best consistency for backups of Enterprise Vault databases, indexes, and storage, a backup methodology must be configured to so that backups of these items happen around the same time. Otherwise, data discrepancies between the database, index and store volumes will be encountered.

For example, if the Enterprise Vault database backups are performed at 8:00 PM nightly, but the backup of the Enterprise Vault index and storage volumes are performed at midnight, there is a four hour discrepancy between what the database backup contains and what the index and storage volumes contain. In the event of a full restoration event, the database may not be up to date with the contents of index and storage volumes which can potentially cause a loss of archived content.

Thus is recommended that the backup of Enterprise Vault databases be started around the same time as the Enterprise Vault index and storage volumes for *all* Enterprise Vault servers to provide the best consistency.

Backing up the Enterprise Vault fingerprint databases should be treated slightly different. A full backup of the fingerprint databases should be completed before the backup of vault store partitions, indexes, and other SQL databases. Once the backup of the vault store partitions, indexes, and other databases is complete, it is **highly** recommended that a transaction log backup of the fingerprint databases be performed within a few hours.

Backing up Enterprise Vault with Symantec NetBackup
This section will discuss backing up Enterprise Vault with NetBackup using standard file level backups and using the new NetBackup Enterprise Vault backup agent.

The NetBackup Enterprise Vault Backup Agent
The Enterprise Vault agent was originally introduced in NetBackup 6.5.4 and provided full support for Enterprise Vault 2007 but only partial support for Enterprise Vault 8.0 (complete protection requires the agent to be used in conjunction with the MS-SQL agent).

The Enterprise Vault agent for NetBackup 7.0 improves upon the original NetBackup 6.5.4 agent by fully supporting Enterprise Vault 8.0 and 9.0 (with NetBackup 7.0.1) as well as providing the ability to back up additional Enterprise Vault SQL databases such as the fingerprint, audit, and FSA reporting databases. These databases contain valuable metadata for Enterprise Vault as well as auditing and reporting information. The agent now provides a full back up solution for Enterprise Vault 8.0 and 9.0 and utilizes the newer Backup Mode operations automatically without the use of pre and post backup scripts.

The agent provides a new backup policy type entitled "Enterprise-Vault" and provides several backup directives that back up various aspects of Enterprise Vault. For more information on the agent, please read the "Symantec NetBackup for Enterprise Vault Agent Administrator's Guide".

Backup Scenario #1: Using file level backups
This environment contains one Enterprise Vault 8.0 server with one index location and two Vault Store partitions.

Sample Policy: EV
Attributes:

Backing up Enterprise Vault

Schedules:

Backing up Enterprise Vault

Clients:

Change Policy – EV

Attributes | Schedules | Clients | Backup Selections

Client name	Hardware	Operating System
evvista	PC	Windows Server 2003

☑ Detect operating system when adding or changing a client.

New... | Delete | Properties

OK | Cancel | Help
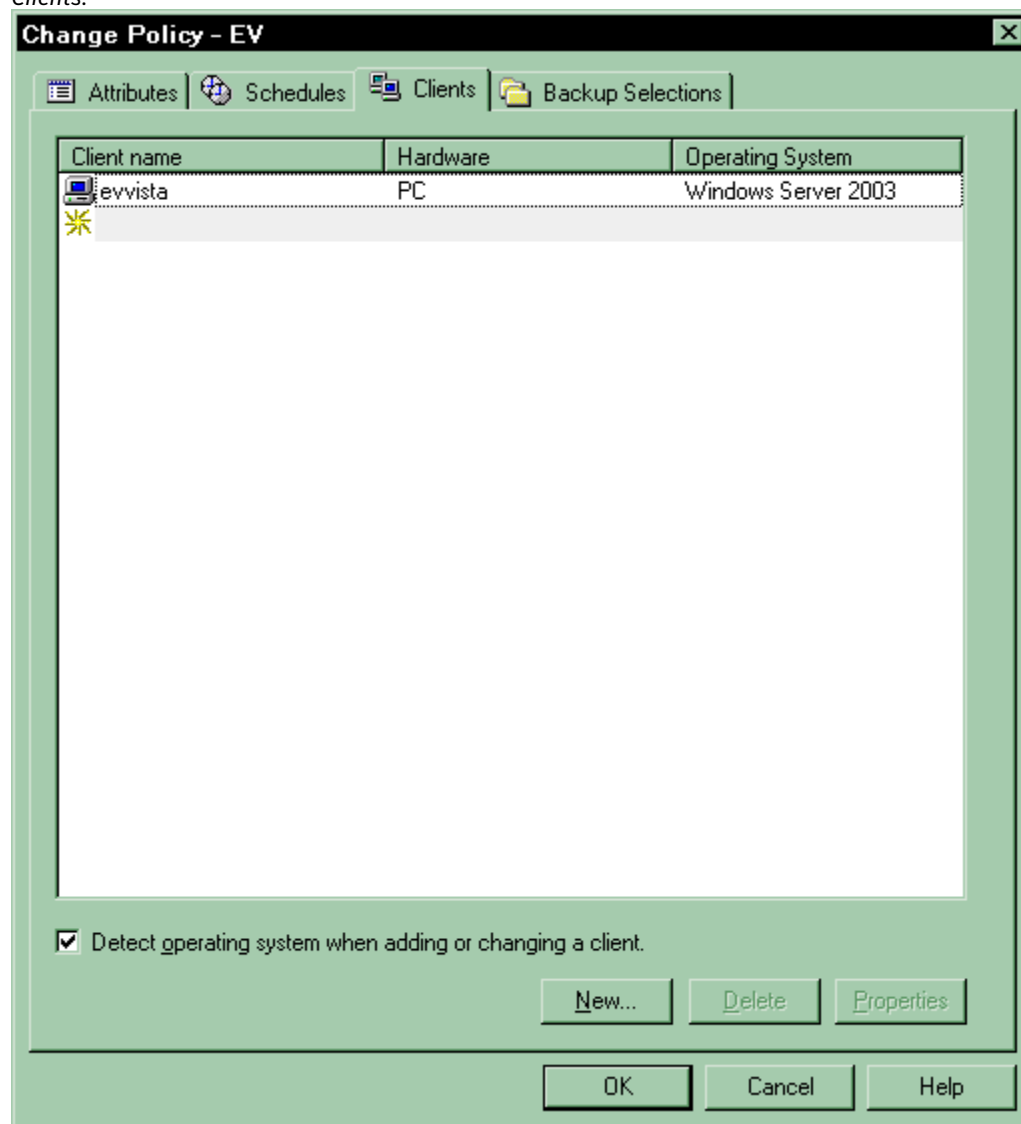
Backup Selections (this example shows local and remote index and Vault Store partition locations):

Change Policy – EV

| Attributes | Schedules | Clients | Backup Selections |

Backup Selections

- S:\
- I:\
- E:\Program Files\Enterprise Vault\Shopping
- \\vistafile\evstorage

[New...] [Delete] [Rename] [Up] [Down]

[OK] [Cancel] [Help]
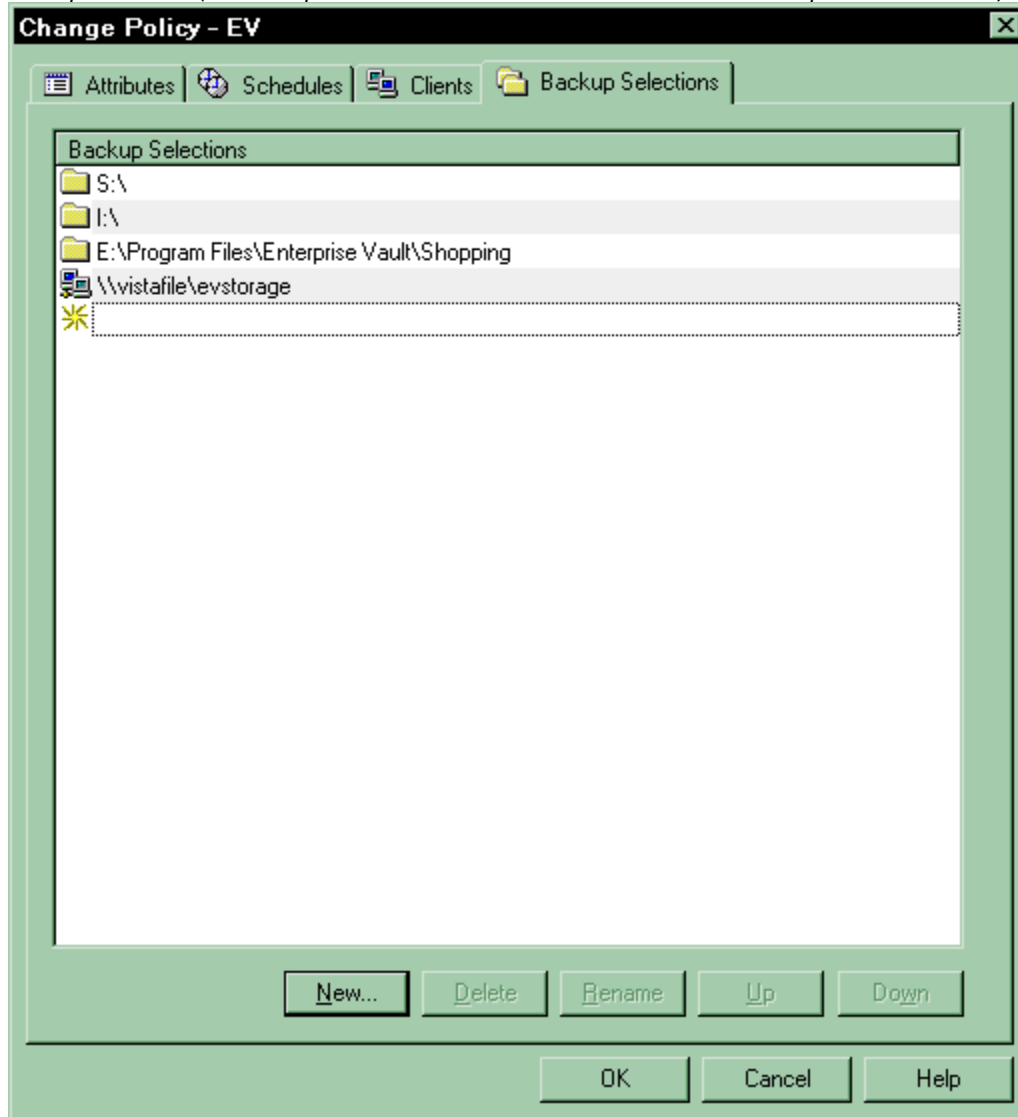
Notes:
The client name(s) should be the DNS alias for the Enterprise Vault Server(s).

It should be noted when backing up network based locations (such as the \\vistafile\evstorage in the example), the NetBackup Client Service should run with a service account that has read/write permissions on the share.

When the EV policy is kicked off (regardless of which schedule is used), the NetBackup client looks for bpstart_notify.bat and bpend_notify.bat (for post backup) and can also look for bpstart_notify.<policy_name>.bat and bpend_notify.<policy_name>.bat. If these batch files exist, they will be processed pre and post backup. Thus, EV can be put into and taken out of Backup Mode using these batch files. **For sample bpstart_notify.bat and bpend_notify.bat files, see the "Scripting out PowerShell Commands".**

For more information on bpstart_notify and bpend_notify files, please read the *NetBackup Administrators Guide*.

Notes for Scenario #1:

- If Vault Store partitions and index volumes are large with numerous small files, the backup can take considerable time
- If new Vault Store partition or index location is added, the backup policy must be manually updated to include these new locations
- At least one Microsoft SQL backup policy must be created to back up the EnterpriseVaultDirectory database, Vault Store database, monitoring database, and the fingerprint database. If FSA Reporting or auditing is enabled, these databases would also need to be backed up.

Scenario #2: Using the NetBackup Enterprise Vault Backup Agent

Sample Environment

- Three Enterprise Vault 9.0 servers each with their own indexes and Vault Stores
- One Vault Store Group (VSG1)
- Multiple Vault Store partitions in open, closed, and ready states. Vault Store names:
    o Exchange
    o ExchangeJournal
    o FSA
    o SharePoint
- One Microsoft SQL 2008 R2 server with the following databases:
    o Directory database
    o Vault Store databases
    o Fingerprint database for VSG1
    o Auditing database
    o FSA Reporting databases
    o Monitoring database

Proposed Backup Policies
This sample environment will have four backup policy configurations:

- One policy to back up the Enterprise Vault Directory, monitoring, FSA Reporting, and auditing databases
- One policy for each Enterprise Vault server to back up open partitions as well as their corresponding Vault Store SQL databases
- One policy to back up index locations
- One policy for each Enterprise Vault server to back up closed and ready partitions

The Database Backup Policy
This policy will only backup the Enterprise Vault Directory, Monitoring, Auditing, and FSA Reporting databases for the Enterprise Vault site.
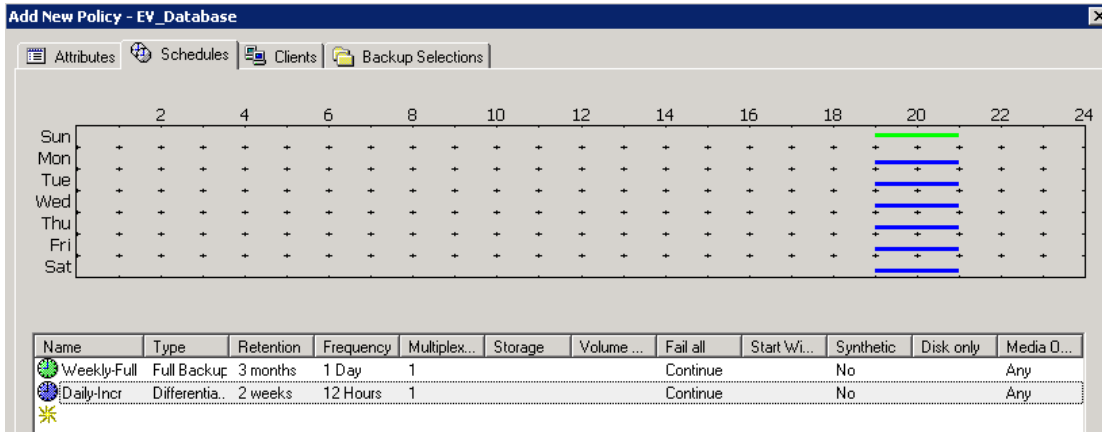
Name: EV_Database
Policy type: Enterprise-Vault
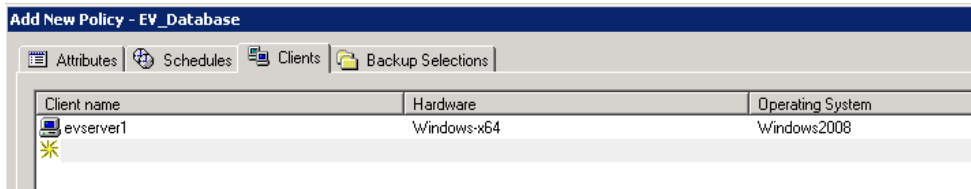
Backing up Enterprise Vault
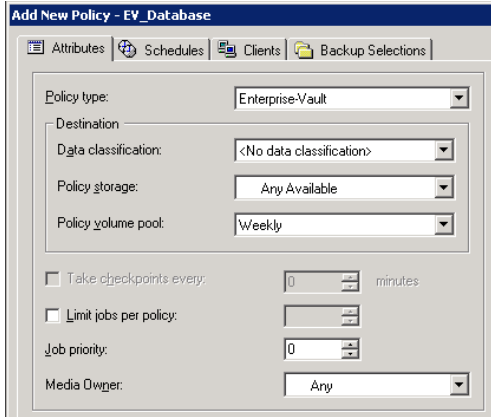
Schedules:

- Weekly Full
- Daily Incremental

Client:

- Only need to specify one EV server in the environment

Backup selections:

- EV_DIR_DB – Backs up the EnterpriseVaultDirectory database
- EV_MONITORING_DB – Backs up the Enterprise Vault Monitoring database
- EV_AUDIT_DB – Backs up the Enterprise Vault Audit database
- EV_FSAREPORTING_DB – Backs up all FSA Reporting databases in the site
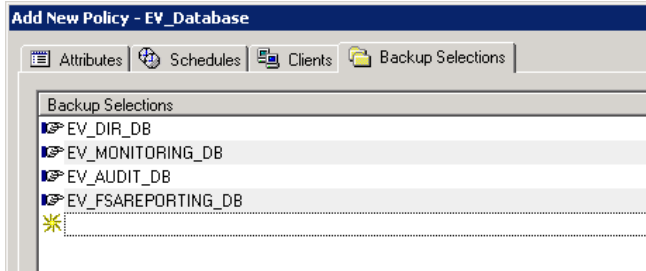
These particular databases cannot be backed up with other Enterprise Vault objects such as indexes or Vault Store partitions and must be in their own policy when using the NetBackup Enterprise Vault agent.

EVSERVER1 Open Partition Backup
This policy will only back up the open Vault Store partitions and Vault Store databases on evserver1.

Name: EV_EVSERVER1
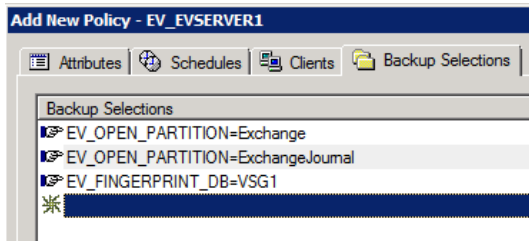Policy type: Enterprise-Vault
Schedules:

- Weekly Full
- Daily Incremental ← Differential backups will also backup and truncate SQL transaction logs

Clients:

- evserver1

Backup Selections:

- EV_OPEN_PARTITION=Exchange ← Backs up the open Vault Store partition for the Vault Store named Exchange as well as the Vault Store Microsoft SQL database
- EV_OPEN_PARTITION=ExchangeJournal ← Backs up the open Vault Store partition for ExchangeJournal
- EV_FINGERPRINT_DB=VSG1 ← Backs up the Microsoft SQL database for the VSG1 Vault Store Group

EVSERVER2 & EVSERVER3 Open Partition Backup
These policies will only back up open Vault Store partitions and Vault Store databases on evserver2 and evserver3

Names: EV_EVSERVER2 & EV_EVSERVER3
Policy type: Enterprise-Vault
Schedules:

19
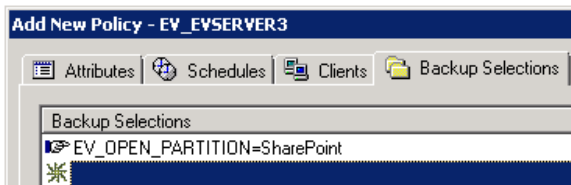
Backing up Enterprise Vault

- Weekly Full
- Daily Incremental

Clients:

- evserver2
- evserver3

Backup selections:

- EV_OPEN_PARTITION=FSA ← Backs up the open Vault Store partition and database for the FSA
  Vault Store
- EV_OPEN_PARTITION=SharePoint ← Backs up the open Vault Store partition and database for
  the SharePoint Vault Store

Index Backup
Name: EV_Indexes
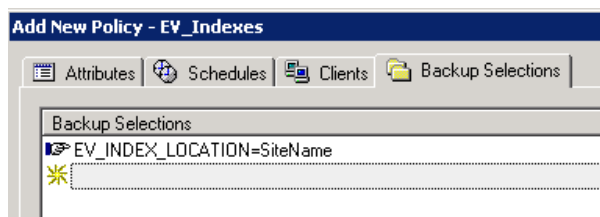Policy type: Enterprise-Vault
Schedules:

- Weekly Full
- Daily Incremental

Clients:

- evserver1 ← Only one of the Enterprise Vault servers needs to be specified. All index locations
  on all Enterprise Vault servers within the site will be backed up with this directive.

Backup selections:

- EV_INDEX_LOCATION=SiteName ← All index locations in the site will be backed up

Closed Partition Backup
These backup policies will only back up closed and ready partitions on evserver1, evserver2, and evserver3.

Names: EV_EVSERVER1_Closed, EV_EVSERVER2_Closed, and EV_EVSERVER3_Closed (three policies)
Policy Type: Enterprise-Vault
Schedules: Monthly_Full ← As closed and ready partitions will not have new data added, the backup frequency can be much less frequent.
Clients:

- evserver1
- evserver2
- evserver3

Backup selections:

- evserver1
    - EV_CLOSED_PARTITIONS=Exchange
    - EV_CLOSED_PARTITIONS=ExchangeJournal
    - EV_READY_PARTITIONS=Exchange
    - EV_READY_PARTITIONS=ExchangeJournal
- evserver2
    - EV_CLOSED_PARTITIONS=FSA
    - EV_READY_PARTITIONS=FSA
- evserver3
    - EV_CLOSED_PARTITIONS=SharePoint
    - EV_READY_PARTITIONS=FSA

Pros and Cons for Scenario #2
Pros:

- Agent automatically discovers open, closed, and ready vault store partitions
- Agent will automatically discover where Enterprise Vault Microsoft SQL databases are located

Cons:

- The NBU EV agent forms file level backups (using VSS snapshots). Large NTFS volumes with numerous savesets may take considerable time to backup.
- Depending on the frequency of backups for closed partitions, partitions that may have recently closed may still have changed data (when collections are enabled) that has not been backed up

Scenario #3: Using a Combination of the NetBackup Enterprise Vault Agent and Flashbackup for Windows

Sample Environment

- One Enterprise Vault server each with indexes and vault stores running Enterprise Vault 9.0
- One Microsoft SQL 2008 R2 server with all Enterprise Vault databases
- One vault store group
- Multiple vault store partitions in open and closed states
    - Partitions are 4TB in size and are NTFS
    - One open vault store partition
    - Four closed vault store partitions

        o   Collections are not enabled
- Storage Foundation 5.1SP1 is installed on the Enterprise Vault 9.0 server

This particular environment has large volumes for Vault Store partitions resulting in millions and millions of saveset files. Regular file-level backups are taking too long. The NetBackup FlashBackup for Windows option will be utilized to reduce backup times.

Proposed Backup Policies
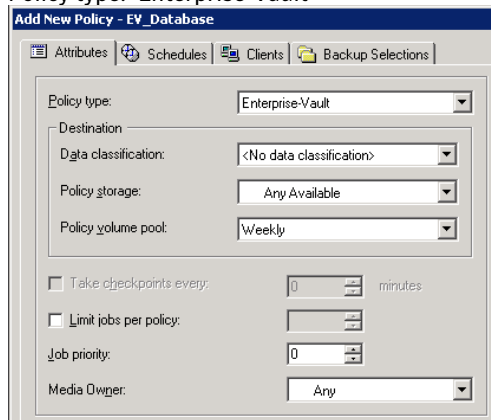This sample environment will have five backup policy configurations:

- One policy to back up the EV directory, monitoring, FSA Reporting, and monitoring databases
- One policy to back up the EV vault store and fingerprint databases
- One policy to back up open vault store partitions
- One policy to back up index locations
- Four policies to back up closed partitions

The Database Backup Policy
This policy will only backup the Enterprise Vault Directory, Monitoring, Auditing, and FSA Reporting databases for the Enterprise Vault site using the Enterprise Vault backup agent.

Name: EV_Database
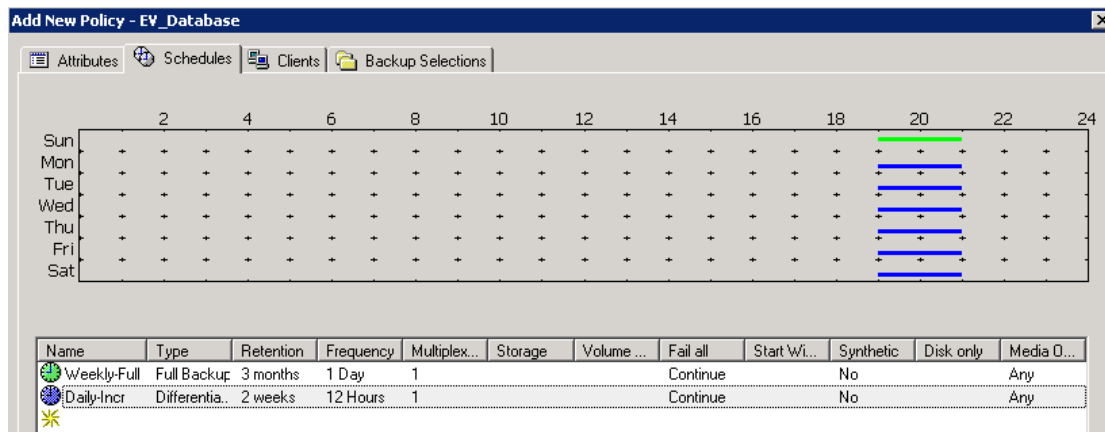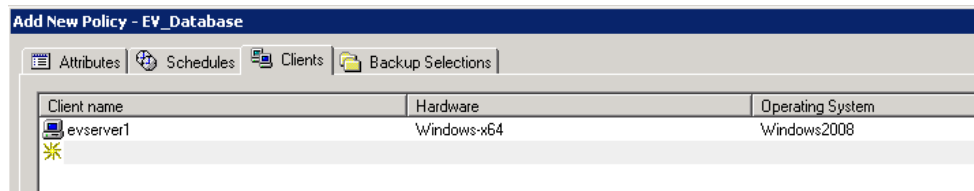Policy type: Enterprise-Vault

Schedules:
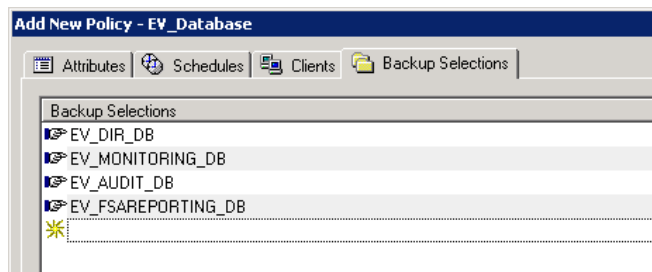
- Weekly Full
- Daily Incremental

Client:

- evserver1

Backup selections:

- EV_DIR_DB – Backs up the EnterpriseVaultDirectory database
- EV_MONITORING_DB – Backs up the Enterprise Vault Monitoring database
- EV_AUDIT_DB – Backs up the Enterprise Vault Audit database
- EV_FSAREPORTING_DB – Backs up all FSA Reporting databases in the site

These particular databases cannot be backed up with other Enterprise Vault objects such as indexes or Vault Store partitions and must be in their own policy when using the NetBackup Enterprise Vault agent.

Vault Store and Fingerprint Database Backup Policy
This policy will use the Enterprise Vault backup agent and only back up the Microsoft SQL databases for the fingerprint and Vault Store database.

Name: EV_DB_VS_FP
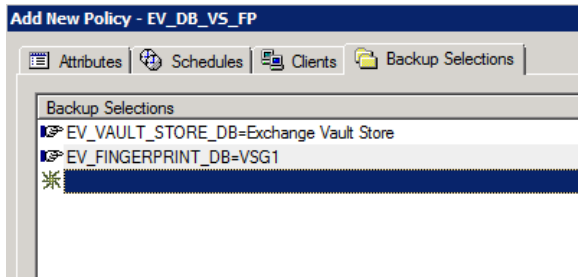Policy type: Enterprise-Vault
Schedules:

- Weekly Full
- Daily Incremental

Client:

- evserver1

Backup selections:

- EV_VAULT_STORE_DB=Exchange Vault Store
- EV_FINGERPRINT_DB=VSG1

Open Partition Backup Policy
This policy will only back up the open Vault Store partition using FlashBackup for Windows. A FlashBackup policy type will not clear the archive attribute. The Vault Store partition must be set up to use a trigger file to remove safety copies. Please read the section entitled "Using Snapshots to Back up Enterprise Vault" for more information.
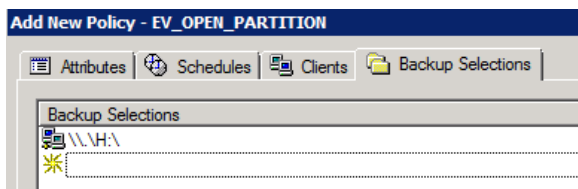
Name: EV_OPEN_PARTITION
Policy type: Flashbackup-Windows
Schedules:

- Weekly_Full
- Daily_Incremental

Backup selections:

- In this scenario, the Vault Store partition is located on the H: drive. When using Flashbackup, the naming convention is slightly different and is specified in this format: **\\.\<drive_letter:>**. In our scenario we would specify: **\\.\H:**.

A bpstart_notify and bpend_notify script must also be used with this policy in order to put Enterprise Vault into Backup Mode. Please read the section entitled "Setting and Clearing Backup Mode Using the Enterprise Vault Management Shell" for more information on how to create these scripts.

Index Backup Policy
This policy will use Flashbackup for Windows to back up the index locations.

Name: EV_Index
Policy type: Flashbackup-Windows
Schedules:

- Weekly Full
- Daily Incremental

Client:

- evserver1

Backup selections:

- In this scenario, the indexes are located on the I: drive. When using Flashbackup, the naming convention is slightly different and is specified in this format: **\\.\\<drive_letter:>**. In our scenario we would specify: **\\.\I:**.

A bpstart_notify and bpend_notify script must also be used with this policy in order to put Enterprise Vault into Backup Mode. Please read the section entitled "Setting and Clearing Backup Mode Using the Enterprise Vault Management Shell" for more information on how to create these scripts.

Closed Partition Backup Policies
These policies will utilize Flashbackup for Windows.

Names: EV_CLOSED_PARTITIONS1, EV_CLOSED_PARTITIONS2, EV_CLOSED_PARTITIONS3, and EV_CLOSED_PARTITIONS4
Policy type: Flashbackup-Windows
Schedules:

- Monthly full ← As closed and ready partitions will not have new data added, the backup frequency can be much less frequent.

Client:

- evserver1

Backup selections:

- In this scenario, the closed Vault Store partitions are located on various volumes (J:, K:, L:, & M:). When using Flashbackup, the naming convention is slightly different and is specified in this format: **\\.\\<drive_letter:>**. In our scenario we would specify: **\\.\J:\\, \\.\K:\\, \\.\L:\\, \\.\M:**.

A bpstart_notify and bpend_notify script must also be used with this policy in order to put Enterprise Vault into Backup Mode. Please read the section entitled "Setting and Clearing Backup Mode Using the Enterprise Vault Management Shell" for more information on how to create these scripts.

Pros and Cons for Scenario #3

Pros:

- Using the EV Agent will automatically discover where Enterprise Vault MS-SQL databases are located
- Using Flashbackup-Windows backup policies will speed up backups where volumes are large and contain potentially hundreds of thousands or millions of saveset files

Cons:

- The open and closed partition backup policies will need to be manually updated when a new open partition is created or when an existing open partition is closed
- The index backup policy will need to be updated when index locations change
- Pre and post backup scripts will need to be maintained properly to ensure Backup Mode is set and cleared

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com