

Enterprise Vault Whitepaper


Backing up Enterprise Vault

This document covers principles for backing up Enterprise Vault and includes advanced backup topics

This document applies to the following version(s) of Enterprise Vault: 6 and later

If you have any feedback or questions about this document please email them to IIG-TFE@symantec.com stating the document title.

This document is provided for informational purposes only. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice. Copyright © 2013 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other

Confidence in a connected world.  **Symantec.**

Document Control

Contributors

Who	Contribution
Evan Barrett	Author
Andreas Bechter	Contributor

Revision History

Version	Date	Changes
1.0	May 2011	Updates for Enterprise Vault 10
2.0	July 2011	Updated backup frequencies for closed partitions
3.0	February 2012	Vault Store partition sizing
4.0	January 2013	NetBackup Accelerator Option
5.0	December 2013	Backing up Enterprise Vault with clustered Microsoft SQL Server using VCS and versions of Enterprise Vault not supported with the NetBackup Enterprise Vault Agent
6.0	April 2014	Updates for Enterprise Vault 11, when using the NetBackup Accelerator option, and other objects that should be backed up

Related Documents

Document Title	Version / Date
Configuring Trigger Files http://www.symantec.com/business/support/index?page=content&id=TECH35610	
Generating PowerShell Backup Commands http://www.symantec.com/business/support/index?page=content&id=TECH75694	

Table of Contents

Overview	1
Backing up the Database Component	1
The Flat File Method	1
Using Commercially Available Backup Software	2
Using High Availability	2
Backing up Enterprise Vault Index and Vault Store Partition Locations	3
Setting and Clearing Backup Mode in the Enterprise Vault Administration Console	3
Setting Backup Mode for an Enterprise Vault Site	3
Setting and Clearing Backup Mode for a Specific Vault Store	4
Setting and Clearing Backup Mode for All Indexes on an Enterprise Vault server	6
Setting and Clearing Backup Mode for a Specific Index on an Enterprise Vault server	7
Setting and Clearing Backup Mode Using the Enterprise Vault Management Shell	9
Using Enterprise Vault Management Shell for the First Time	9
Enterprise Vault 8.0SP3 Changes	10
PowerShell Usage for Vault Stores	11
PowerShell Usage for Indexes	11
Scripting out PowerShell Commands	12
Considerations When Upgrading from Older Versions of Enterprise Vault	13
Storage Queues (Enterprise Vault 11 and later)	13
Advanced Backup Strategies	14
Vault Store Partition Sizes	14
Utilizing Snapshots for Backing up Enterprise Vault	14
Backup the Whole Enterprise Vault server in One Backup Job?	15
Backup Frequency for Index and Vault Store Partitions	16
Timing of Backups	16
Backing up Enterprise Vault with Symantec NetBackup	17
The NetBackup Enterprise Vault Backup Agent	17
Backup Scenario #1: Using file level backups	17
Scenario #2: Using the NetBackup Enterprise Vault Backup Agent	20
Sample Environment	20
Proposed Backup Policies	21
The Database Backup Policy	21
EVSERVER1 Open Partition Backup	23
EVSERVER2 & EVSERVER3 Open Partition Backup	24
Index Backup	25
Closed Partition Backup	26
Pros and Cons for Scenario #2	27
Scenario #3: Using a Combination of the NetBackup Enterprise Vault Agent and FlashBackup for	
Windows	27
Sample Environment	27
Proposed Backup Policies	28
The Database Backup Policy	28
Vault Store and Fingerprint Database Backup Policy	30

Open Partition Backup Policy	31
Index Backup Policy	32
Closed Partition Backup Policies	33
Closed Index Backup Policies (EV 10 and later)	34
Pros and Cons for Scenario #3	34
Scenario #4: Using NetBackup Accelerator (NetBackup 7.5 and later)	35
Proposed Backup Policies	36
The Database Backup Policy	36
Vault Store and Fingerprint Database Backup Policy	38
Open Partition Backup Policy	39
Index Backup Policy	40
Closed Partition Backup Policies	41
Closed Index Backup Policies (EV 10 and later)	42
Pros and Cons for Scenario #4	42
Scenario #5: Using NetBackup where the NetBackup Enterprise Vault Agent Is Not Supported in the Enterprise Vault Environment	43
Sample Environment	44
Proposed Backup Policies	44
Requirements to Implement this Backup Solution	45
The EnterpriseVault_Starter and EnterpriseVault_StarterClosed Backup Policies	48
The EnterpriseVault_ClosedPartitions Backup Policy	50
The EnterpriseVault_Index Backup Policy	50
The EnterpriseVault_OpenPartitions Backup Policy	51
The EnterpriseVault_ClearBackupMode and EnterpriseVault_ClearBackupModeClosed Policies	51
The EnterpriseVault_SQL Backup Policy	52
The EnterpriseVault_SQL_TRX Backup Policy	53
Pros and Cons for Scenario #5	54
Other Enterprise Vault Object to Backup Up	55
Vault Store Partition Sizing	55

Overview

The purpose of this document is to provide best practices for backing up the three main components of Enterprise Vault: The Microsoft SQL Server databases, Enterprise Vault indexes, and Enterprise Vault Vault Stores. This document provides specific examples of backup scripts, registry settings, and additional information for backing up Enterprise Vault with Symantec NetBackup. Covering the standard use of file level backups as well as using the 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. Enterprise Vault also uses databases such as the vault store, fingerprinting, reporting, and auditing. These databases start with “EV” and must be backed up to ensure proper recovery of Enterprise Vault.

Symantec recommends that all SQL databases are backed up at the same time as other Enterprise Vault data such as vault store partitions and indexes. This process ensures the best data integrity if a full restore from backups is required.

This section documents three recommended backup methods: flat files, using 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. Backing up of the database while not in “backup mode” or “read-only mode” leads to a bad data backup resulting in failed restore attempts.

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 places the database(s) associated with Enterprise Vault into “backup mode” allowing for a clean backup of the database. Microsoft SQL Server then dumps 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.

Place Enterprise Vault into Read-Only mode (Enterprise Vault 2007 and earlier) or backup mode (Enterprise Vault 8.0 or later) before initiating the backup routine. This process ensures that all updates to the database are halted.

If copying these flat files to disk, it is highly suggested that the disk be on a different system, preferably at a remote site. While this option may not always be possible, the files should be copied to a physically different disk than the database data and transaction logs.

When using a tape backup ensure that storage is safe preferably at an off-site location. Information is then available in the event of a site failure due to fire, flooding, or other events. Use of a “tape vault” protects tape media from fire and water and other hazardous situations.

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

Other products, such as tape backup or clustering, that work with the SQL backup API to back up databases and transaction logs. As a reminder, the databases should be placed into “backup mode” to ensure data integrity.

When choosing a disk backup as the preferred method, ensure that the backups are migrated to a remote location. If the backup of choice is tape, it is proposed that a tape rotation is used. Tape media should be sent off-site for safe keeping in the event of location disaster.

Symantec Backup Exec and NetBackup contain licensed add-ons accounting for the Microsoft SQL databases and transaction logs that are used with the SQL backup API.

Using High Availability

Using High Availability or clustering allows the Enterprise Vault database components to stay online in the event of a hardware or site failure. Microsoft Cluster Server or Symantec Storage Foundation for Windows with High Availability (SFW-HA) can be configured to host the Enterprise Vault database at the primary location on one or more systems. Configuration can include the host of the database at a remote location for the purposes of failover. This option 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.

As Microsoft SQL has aged the offering of log shipping methods disaster recovery has matured. 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 archived data.

This section documents the requirements for backing up archived content:

The safety copy option within Enterprise Vault indicates all archived items remain present within the target (Exchange, Domino, etc.) until a good backup of the vault store partitions have been completed. These copies provide 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 the item is placed in Backup Mode, it can be safely backed up. 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 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 as shown in Figure 1.

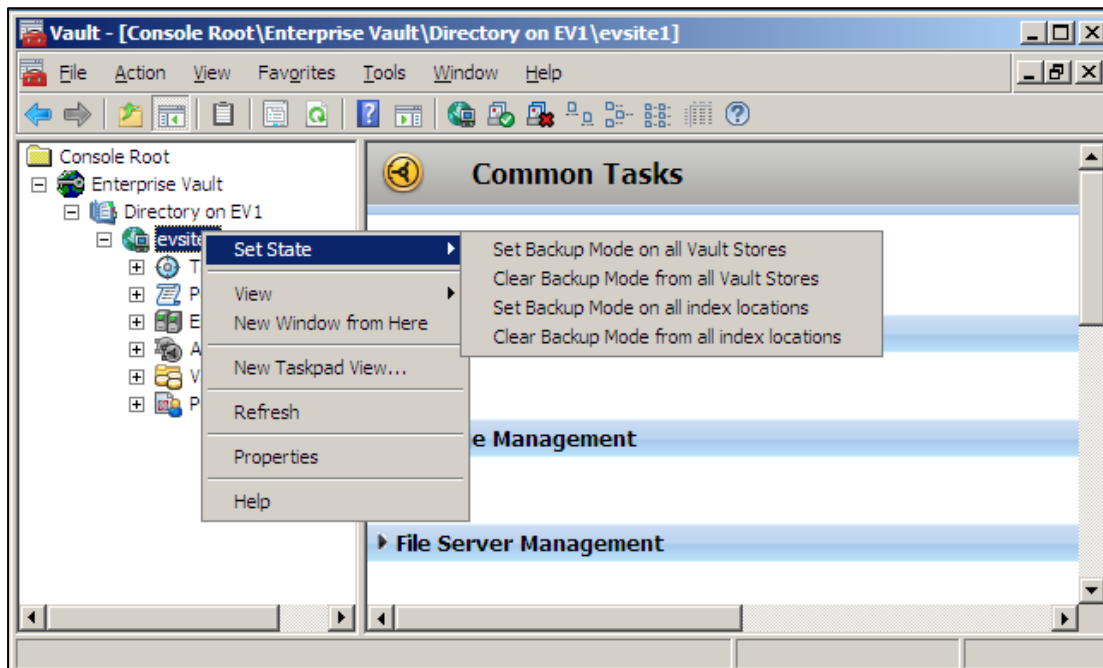


Figure 1 – Setting Backup Mode for an Entire Enterprise Vault Site

Note the four 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.

Selecting “Set Backup Mode” on Vault Stores or index locations at the site level places all contained items in that particular Enterprise Vault site in Backup Mode. A confirmation screen confirms setting. Choosing yes, Enterprise Vault places the selected items in Backup Mode. A second confirmation window appears confirming completion.

Selecting “Clear Backup Mode” on Vault Stores or index locations, Backup Mode restores write functionality. As with the Set Backup Mode option, a confirmation screen confirms the setting change. Once clicking yes, Enterprise Vault changes the Backup Mode.

Setting and Clearing Backup Mode for a Specific Vault Store

Enterprise Vault 8.0 and later also offers the ability to put a particular Vault Store into Backup Mode. This task is easily done by selecting the desired Vault Store, right-clicking on it and selecting Set Backup Mode as illustrated in Figure 2.

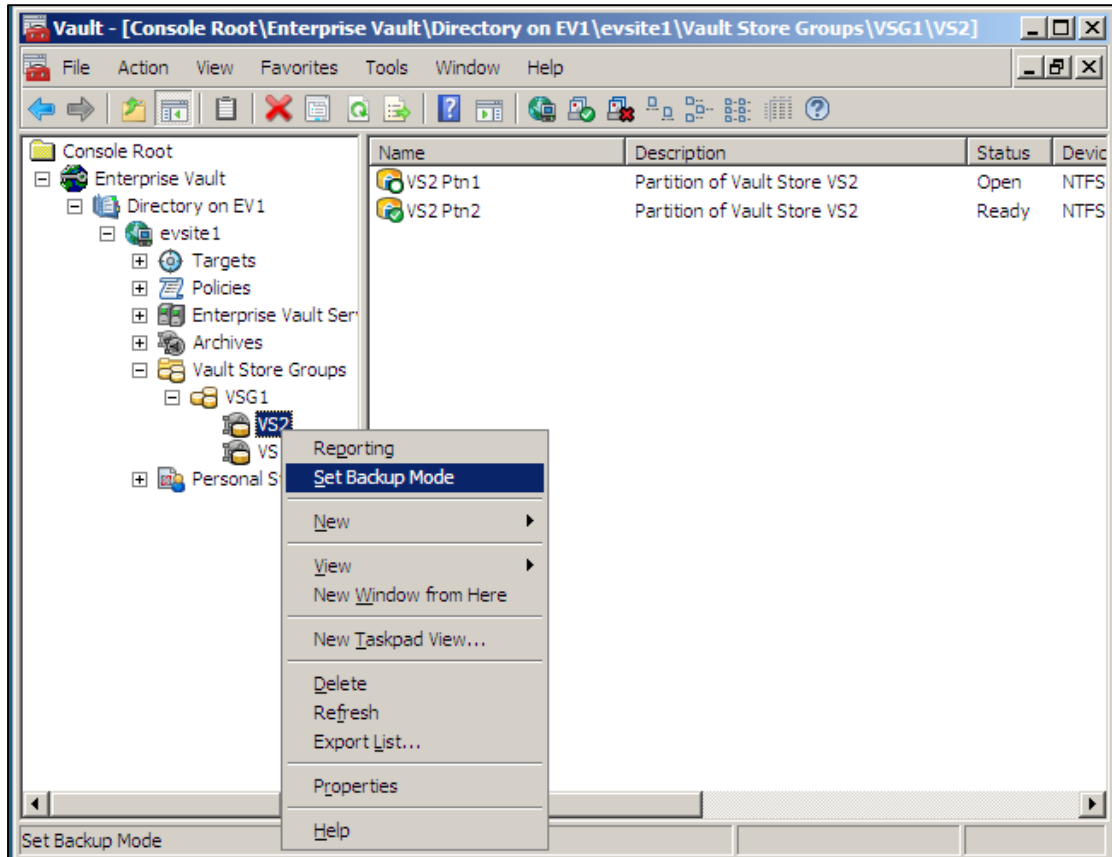


Figure 2 – Setting Backup Mode for a Vault Store

Clearing Backup Mode uses the same process as setting Backup Mode.

Note: The available options vary depending on the backup status of the Vault Store. Only one of the two options is available at a given time. Set Backup Mode noted in Figure 2 or Clear Backup Mode, as illustrated in Figure 3.

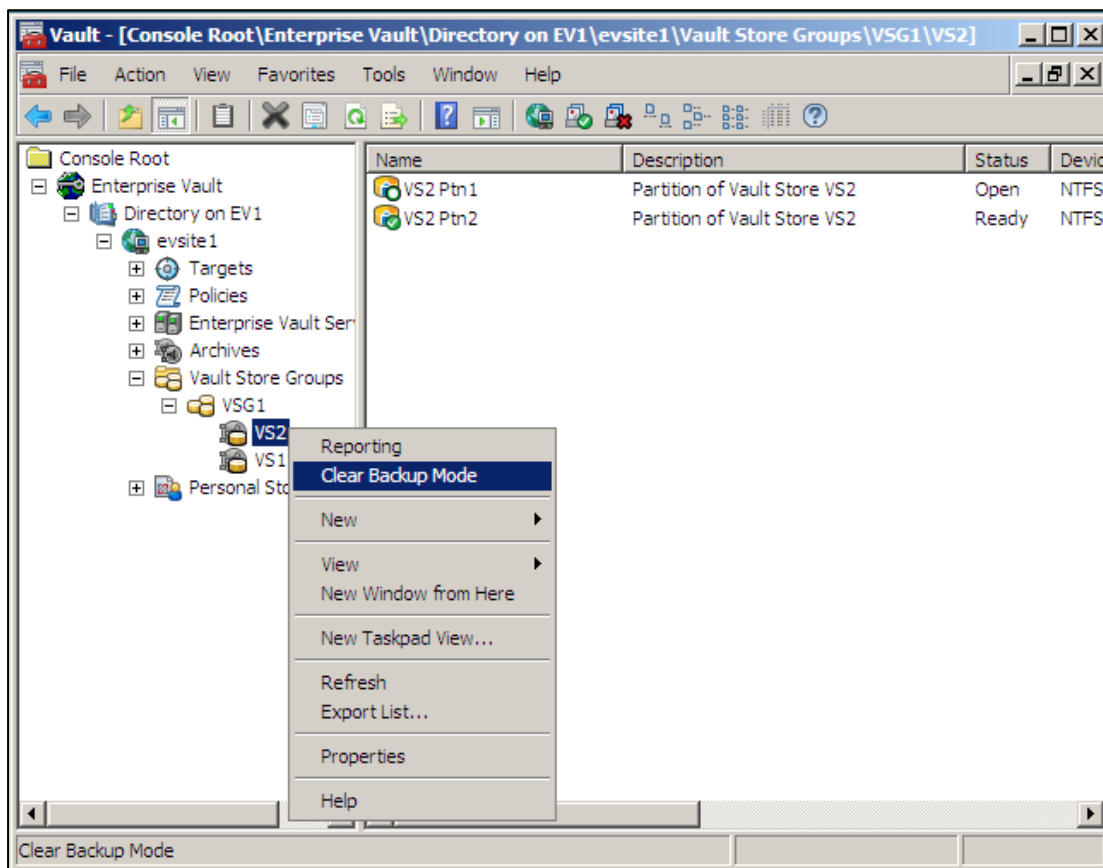


Figure 3 – Clearing Backup Mode for a Vault Store

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 can be completed using the VAC.

- Expand Enterprise Vault servers
- Right-click on the desired Enterprise Vault server
- Click on Set State
- Select either “Set Backup Mode on all index locations” or “Clear Backup Mode from all index locations” as shown in Figure 4.

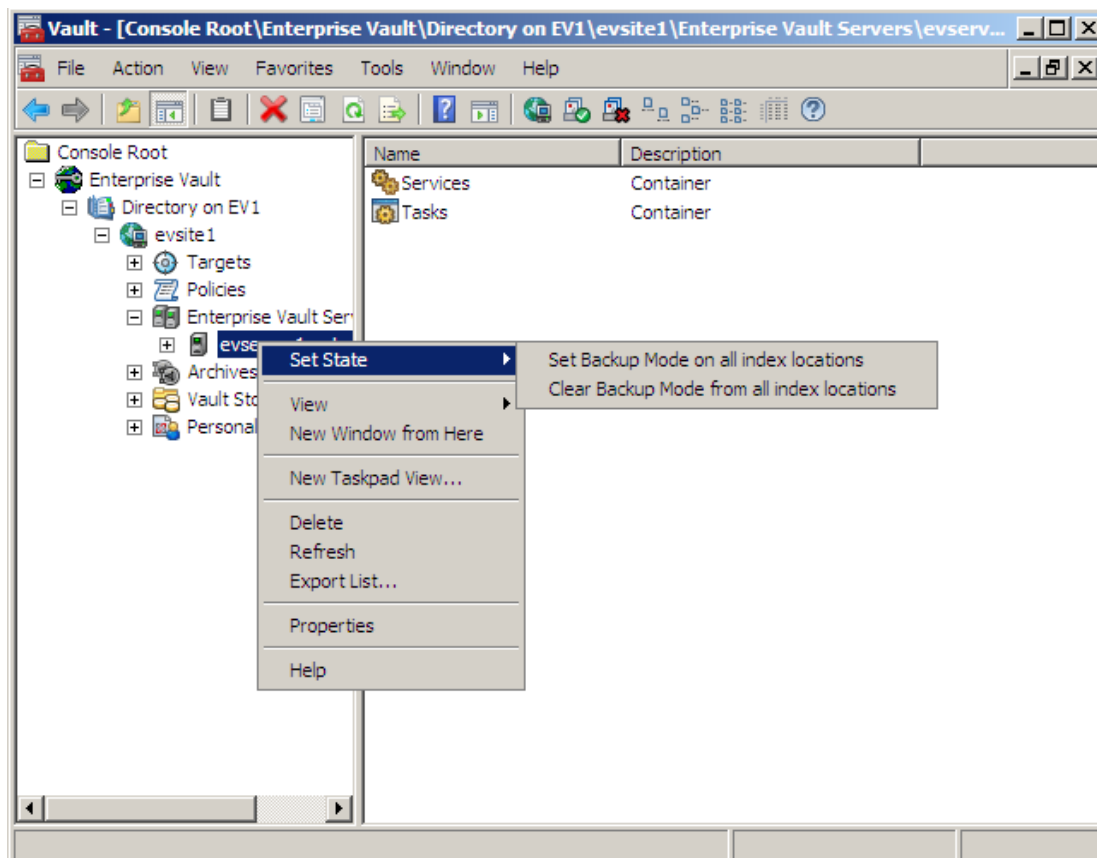


Figure 4 – Setting Backup Mode for All Indexes

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 also use the VAC for Enterprise Vault 8.0 and 9.0.

- Expand out to Enterprise Vault servers
- Expand the desired server
- Click on Services
- Double-click on the Enterprise Vault Index Service (to bring up its properties)
- Select the Index Locations tab.

Placing or clearing the check can change the status of the index location “Backup Mode” as detailed in Figure 5.

Setting Backup Mode on an individual index location in Enterprise Vault 10 and later is slightly different. Follow these steps to set an individual index location to backup mode further illustrated in Figure 6:

- Navigate to the Indexing container

Note: The indexing servers are located in either the Ungrouped Servers or Index Server Groups container.

- Highlight the Enterprise Vault server which houses the index location
- Right-click on the index location
- Select Properties
- Click on the “Backup Mode” Checkbox
- Click on OK

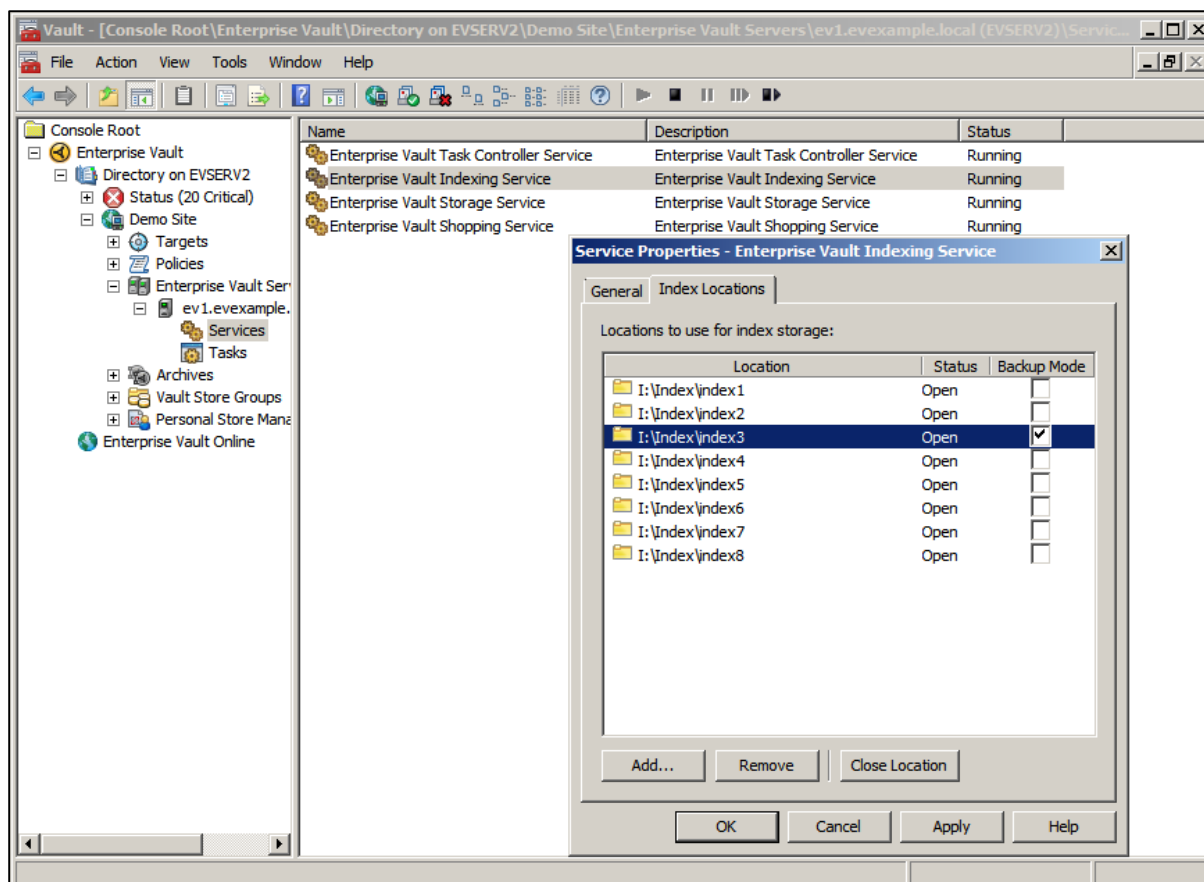


Figure 5 – Setting Backup Mode on an Index Location (Enterprise Vault 8 and 9)

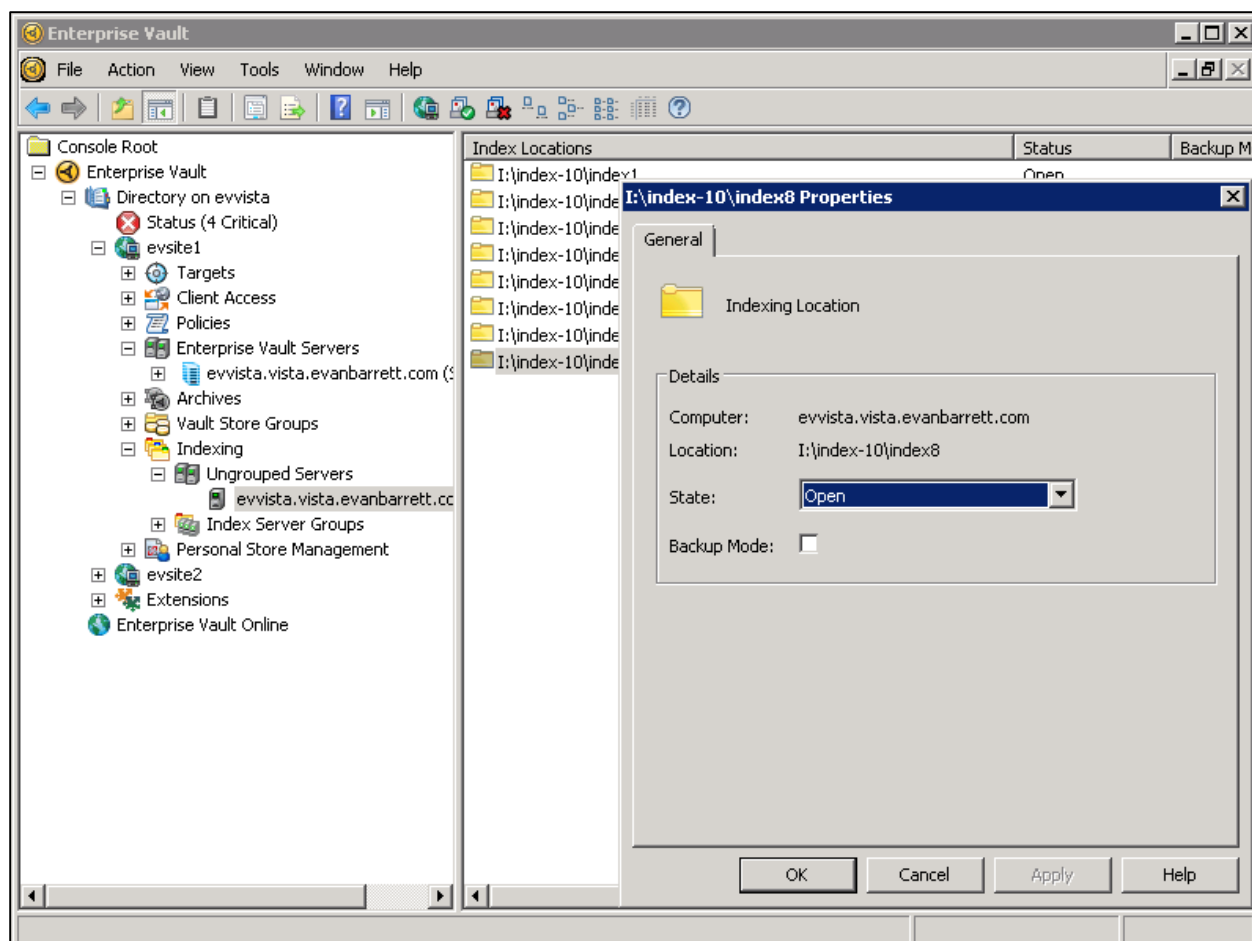


Figure 6 – Setting Backup Mode on an Index Location in Enterprise Vault 10 or Later

Setting and Clearing Backup Mode Using the Enterprise Vault Management Shell

Enterprise Vault 8 and later offers a new PowerShell tool that allows the administrator to control Backup Mode for Enterprise Vault through the use of scripting. This tool 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 (and is a requirement for later versions of Enterprise Vault).

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

appears 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 is available 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 generates an HTML file which opens the default browser as shown in Figure 7.

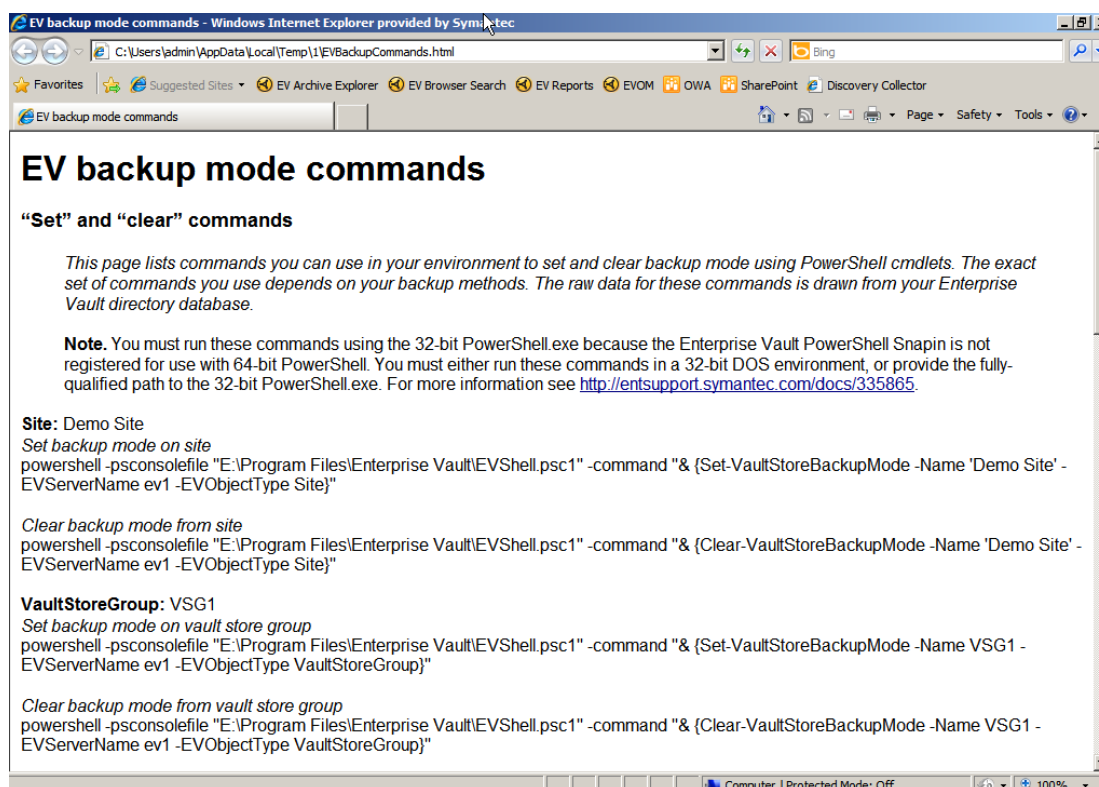


Figure 7 – Transform-Backup.ps1 Script Results**PowerShell Usage for Vault Stores**

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 allows the administrator to run pre and post backup script files from a .bat or .cmd file. The following examples, using a batch file, will place a Vault Store or Index into and out of Backup Mode. The example makes the following assumptions: 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. It is necessary to use the 32-bit version of PowerShell.

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 before version 8.0 rely on Windows Registry modifications and the stopping and starting certain EV services. Upgrades to Enterprise Vault 8.0, the previous backup methods still apply. Warning messages generate 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 the new Backup Mode is then disabled.

To use the new Backup Mode method in Enterprise Vault 8 after an upgrade, the following Windows Registry values are removed from HKEY_LOCAL_MACHINE\Software\KVS\Enterprise Vault\Storage:

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

Storage Queues (Enterprise Vault 11 and later)

Enterprise Vault 11 introduced a new feature that places safety copies on the Enterprise Vault server. If storage queues are used, the original item will be deleted from the source once the item has been successfully written to the Vault Store partition as well as the storage queue.

Since the storage queue contains safety copies of archived items, it is important to perform daily full backups of the storage queue location immediately before the backup of Vault Store partitions. The storage queue location will vary depending on a few factors but will either be placed in the EV Cache location or in the MSMQ folder structure. By default, the folder is named EVStorageQueue.

As of the publication date of this whitepaper, the NetBackup and Backup Exec EV agents do not currently backup this location. It will be necessary to create a separate backup job.

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 and later) automatically opens the next “ready” partition when configured properly.

Utilizing Snapshots for Backing up Enterprise Vault

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 required time in Backup Mode. Here are the recommended steps:

1. Snap back existing snapshot volumes to their original counterparts (if volumes already have a snapshot)
2. Put index or Vault Stores in Backup Mode (or Read-Only Mode with older versions of Enterprise Vault)
3. Perform snapshot operation
4. Clear Backup Mode for indexes or Vault Stores.
5. 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”. More information on trigger files can be found here: <http://www.symantec.com/business/support/index?page=content&id=TECH35610>.

Figure 8 shows how set up a Vault Store partition to use a trigger file with Enterprise Vault 9 and later:

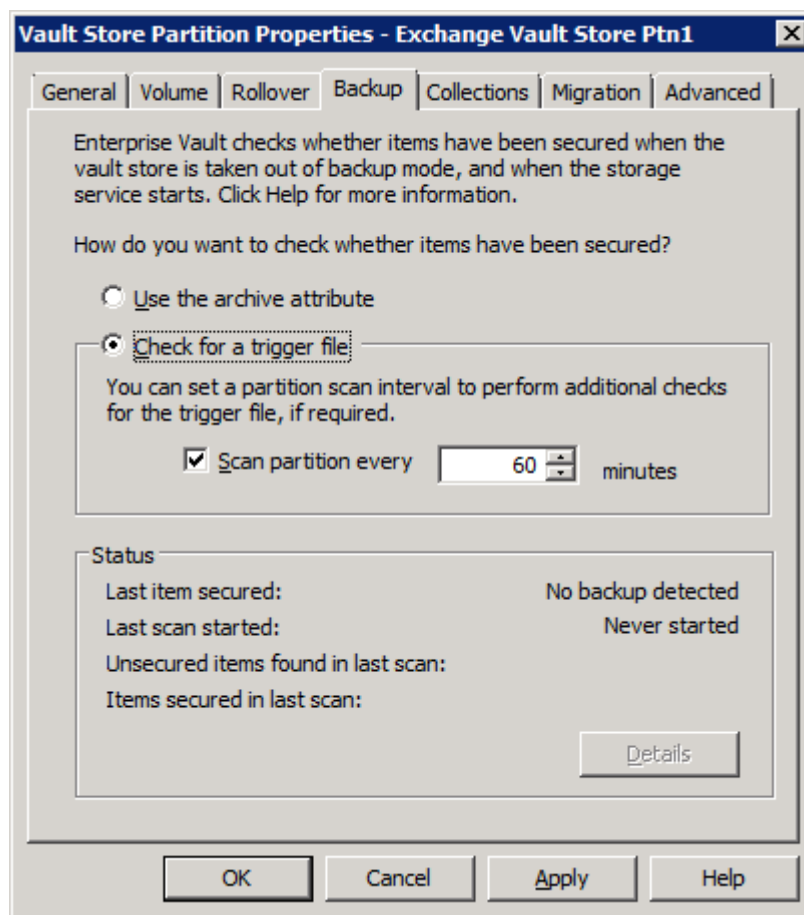


Figure 8 – Configuring a Vault Store Partition to Use Trigger Files

Backup the Whole Enterprise Vault server in One Backup Job?

If a separate backup job cannot be used to back up 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. If a separate job can be created for the purposes of backing up Enterprise Vault data, the following requirements should be followed during 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 I:\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 to backup newly archived data. As a daily full backup may not always be feasible, a weekly full backup and daily incremental backup strategy may be more practical.

To reduce the amount of data being backed up, EV Vault Store partitions that have been closed can be backed up less frequently. Since no additional data is added to a closed vault store partition, a backup can be performed in different intervals. The retention period for a backup image of closed partitions is set so that there are at least two copies of the backup.

With Enterprise Vault 10 and later, a closed index location does not add new index data. However, metadata and deletions can still occur. A closed index location can be backed up less frequently (such as once per week).

Timing of Backups

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 are 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 discusses backing up Enterprise Vault with NetBackup using standard file level backups and using the 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 and later (complete protection requires the agent to be used with the MS-SQL agent).

The Enterprise Vault agent for NetBackup 7.0 and later improves upon the original NetBackup 6.5.4 agent by fully supporting Enterprise Vault 8, 9 (with NetBackup 7.0.1), and 10 (with NetBackup 7.1) 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 backup solution for Enterprise Vault 8, 9, and 10 and uses the newer Backup Mode operations automatically without the use of pre and post backup scripts. Starting with NetBackup 7.0.1, the Enterprise Vault agent is free.

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”.

The Enterprise Vault Agent can also take advantage of the NetBackup’s de-duplication features. Please read the NetBackup documentation on how to configure de-duplication.

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:

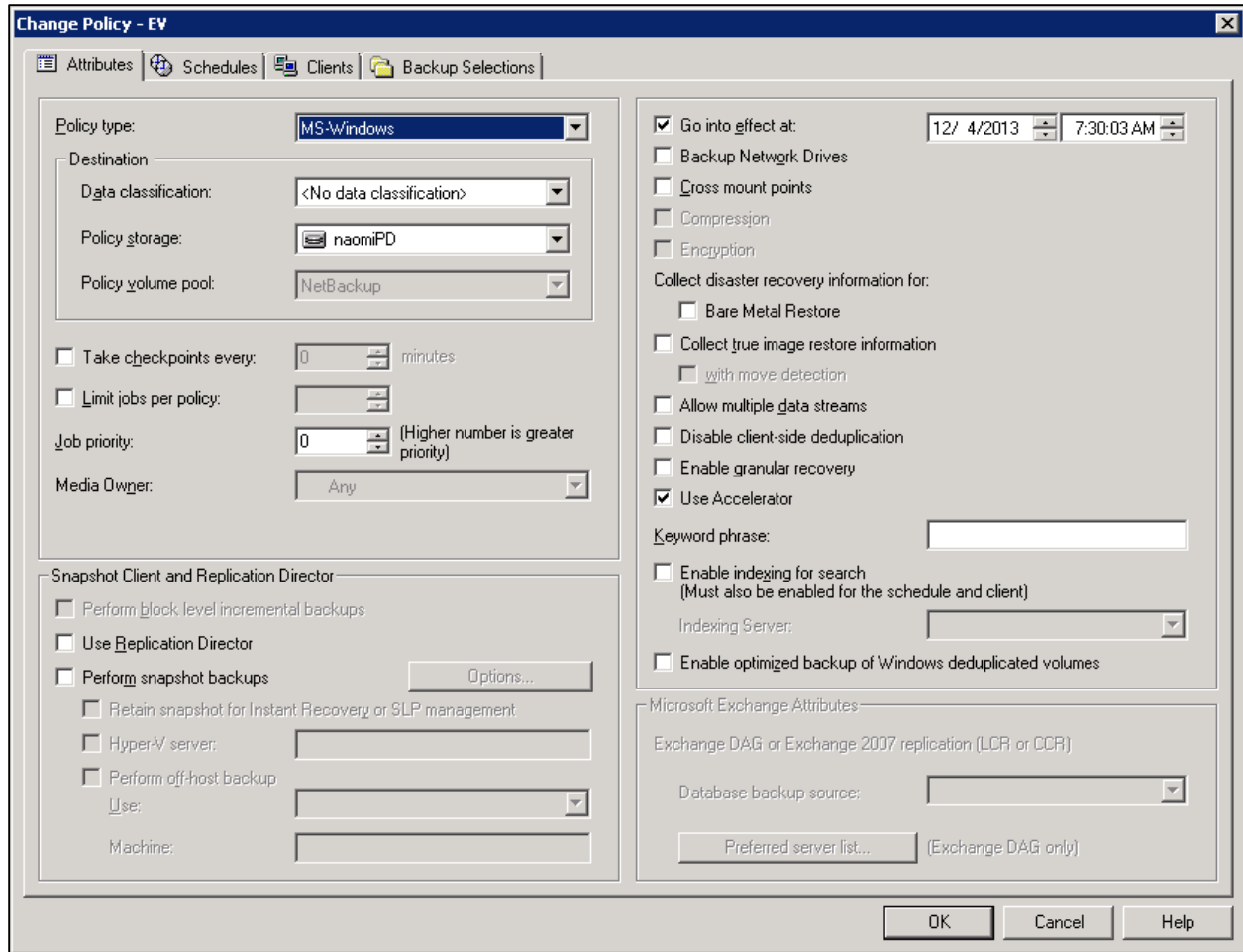


Figure 9 - File-level Backup Attributes

Schedules:

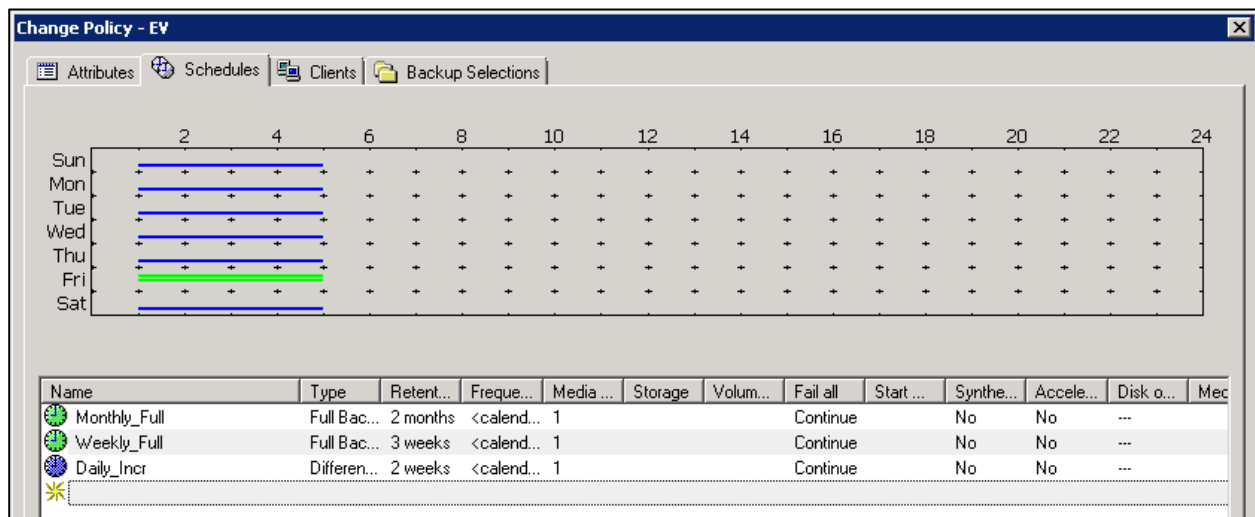
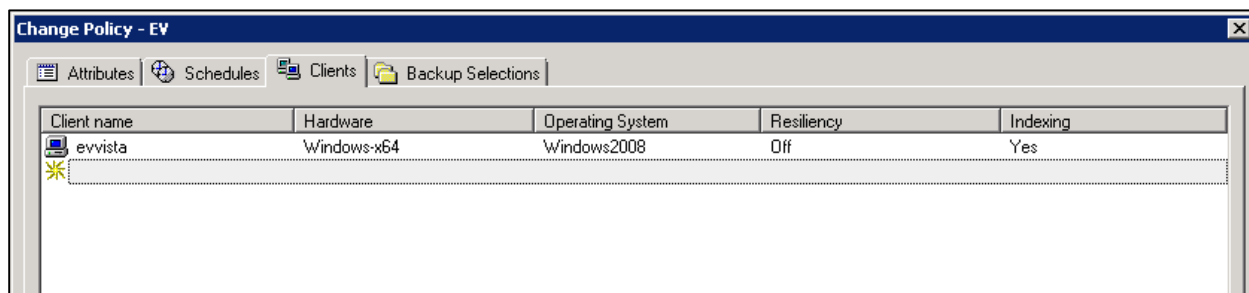
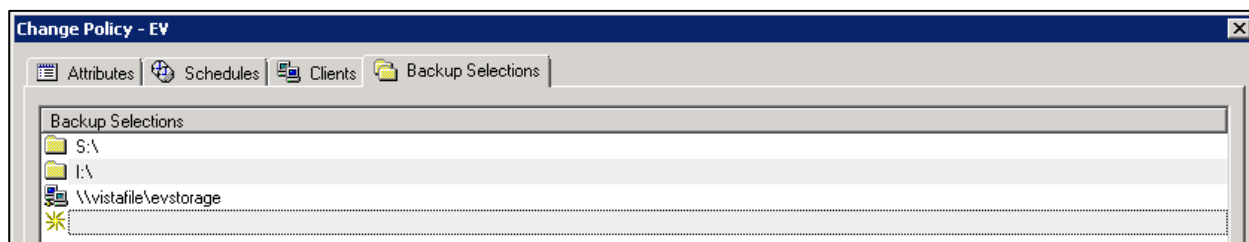


Figure 10 – File-level Backup Schedules

Clients:

**Figure 11 – File-level Backup Clients**

Backup Selections (this example shows local and remote Index and Vault Store partition locations):

**Figure 12 - File-level Backups Backup Selections**

Notes:

The client name(s) should be the DNS alias (CNAME) for the Enterprise Vault Server(s).

It should be noted when backing up network based locations (such as the \\vistafire\evstorage in the example), the NetBackup Client Service should run with a service account that has read or 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 are 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.

Additional considerations:

- 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 also need to be backed up.

Scenario #2: Using the NetBackup Enterprise Vault Backup Agent

Sample Environment

- Three Enterprise Vault 9 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:
 - Exchange
 - ExchangeJournal
 - FSA
 - SharePoint
- One Microsoft SQL 2008 R2 server with the following databases:
 - Directory database
 - Vault Store databases
 - Fingerprint database for VSG1
 - Auditing database
 - FSA Reporting databases
 - Monitoring database

Proposed Backup Policies

This sample environment has 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

Add New Policy - EV_Database

Attributes Schedules Clients Backup Selections

Policy type: Enterprise-Vault

Destination

Data classification: <No data classification>

Policy storage: Any Available

Policy volume pool: Weekly

☐ Take checkpoints every: 0 minutes

☐ Limit jobs per policy:

Job priority: 0

Media Owner: Any

Figure 13 - EV_Database Policy Attributes

Schedules:

- Weekly Full
- Daily Incremental

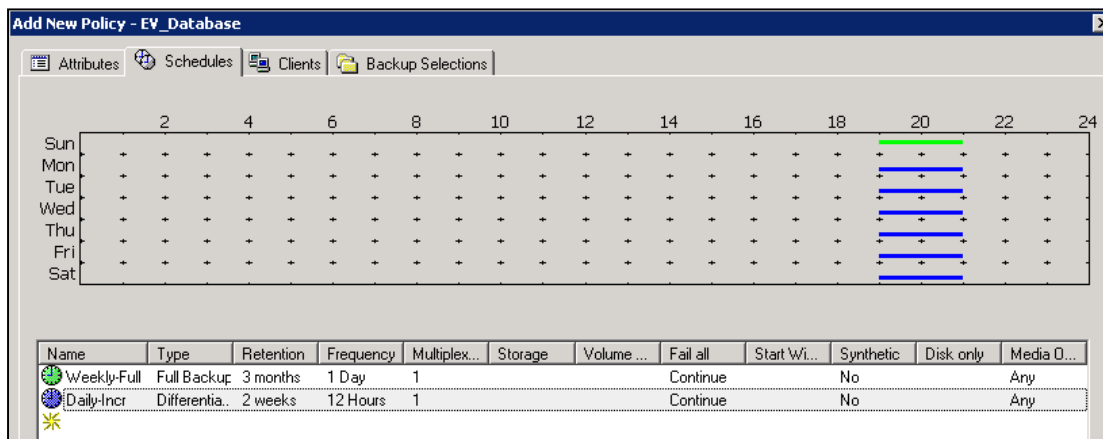


Figure 14 – EV_Database Policy Schedules

Client:

- It is only necessary to specify one Enterprise Vault server in the environment for the core database backups

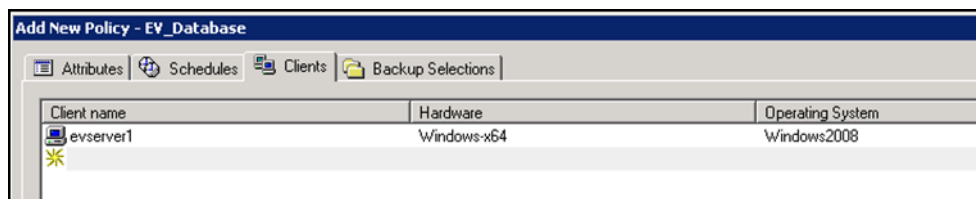


Figure 15 - EV_Database Policy Clients

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

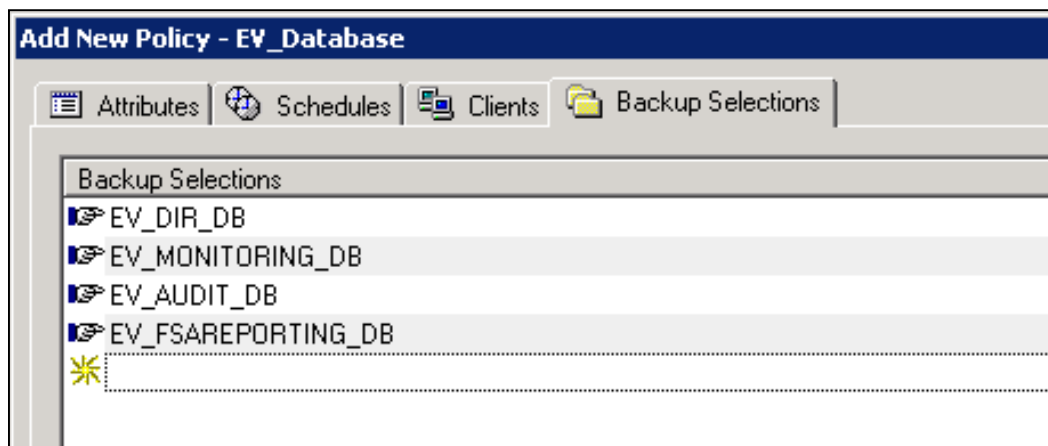


Figure 16 – EV_Database Policy Backup Selections

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 only backs 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 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

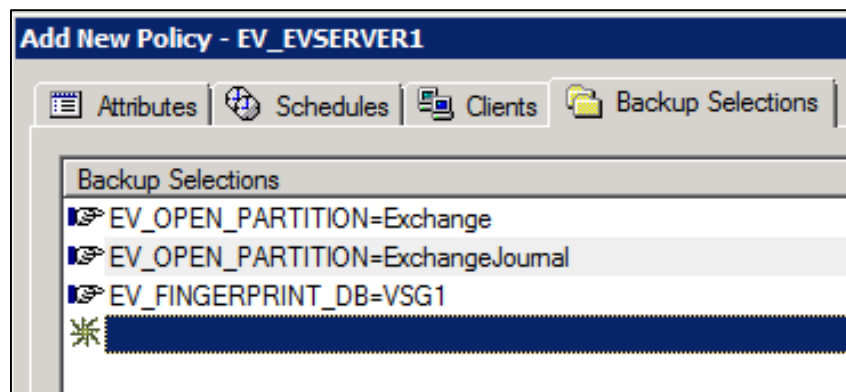


Figure 17 – EV_EVSERVER1 Policy Backup Selections

EVSERVER2 & EVSERVER3 Open Partition Backup

These policies only back up open Vault Store partitions and Vault Store databases on evserver2 and evserver3. It is not necessary to specify the fingerprint database directive as it is backed up with the EVSERVER1 policy.

Names: EV_EVSERVER2 & EV_EVSERVER3

Policy type: Enterprise-Vault

Schedules:

- 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



Figure 18 – EV_EVSERVER2 Policy Backup Selections

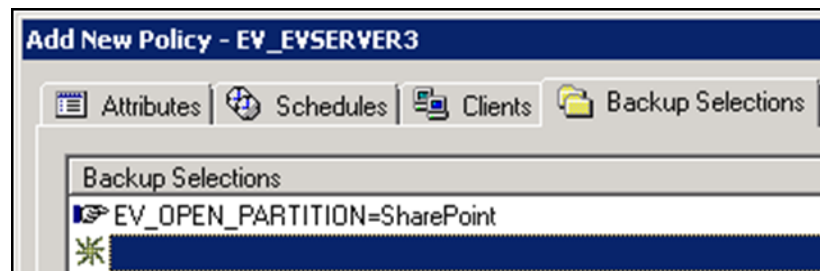


Figure 19 –EV_EVSERVER3 Policy Backup Selections

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 with a site. All index locations on all Enterprise Vault servers within the site is backed up with this directive.

Backup selections:

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

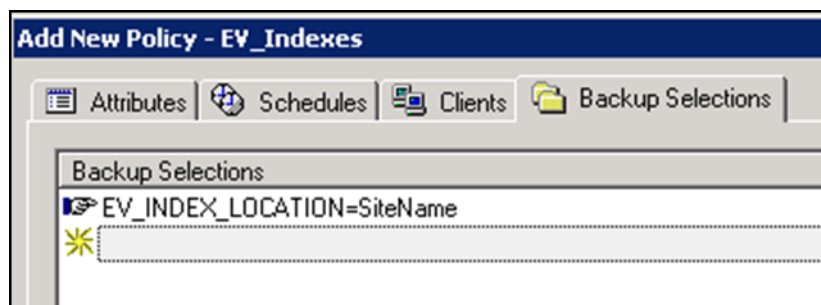


Figure 20 - EV_Indexes Policy Backup Selection

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 do not new data added, the backup frequency can be reduced.
- Weekly incremental – If collections are enabled on partitions, then it is necessary to perform weekly incremental backups. Savesets can still be collected into CAB files after a partition is closed. Failure to back up these changes can cause previously deleted or expired items to reappear during a restore and using the EVSVR utility to validate data in the partitions and the Vault Store database.

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 automatically discovers where Enterprise Vault Microsoft SQL databases are located

Cons:

- The NBU EV Agent performs 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
- Enterprise Vault 10 Indexing and 64-Index Volume Locations – Index locations on Enterprise Vault 10 that are closed behave differently compared to previous versions of Enterprise Vault. A closed index location does not add new index data (but metadata updates and deletions can still occur). As such, these closed index locations do not need to be backed up as frequently as open index locations. The NetBackup Enterprise Vault agent cannot recognize a closed index location at this time.

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

Sample Environment

- One Enterprise Vault server with indexes and vault stores running Enterprise Vault 9

- 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
 - Collections are not enabled
- Storage Foundation 5.1SP1 is installed on the Enterprise Vault 9 server

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

Proposed Backup Policies

This sample environment has 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

Add New Policy - EV_Database

Attributes Schedules Clients Backup Selections

Policy type: Enterprise-Vault

Destination

Data classification: <No data classification>

Policy storage: Any Available

Policy volume pool: Weekly

☐ Take checkpoints every: 0 minutes

☐ Limit jobs per policy:

Job priority: 0

Media Owner: Any

Figure 21 - EV_Database Policy Attributes

Schedules:

- Weekly Full
- Daily Incremental

Add New Policy - EV_Database

Attributes Schedules Clients Backup Selections

Calendar view showing days of the week (Sun-Sat) and hours (2-24). A green bar highlights the 20th hour on Sunday, and blue bars highlight the 20th hour on Monday through Saturday.

Name	Type	Retention	Frequency	Multiplex...	Storage	Volume ...	Fail all	Start Wi...	Synthetic	Disk only	Media O...
Weekly-Full	Full Backup	3 months	1 Day	1			Continue		No		Any
Daily-Incr	Differentia..	2 weeks	12 Hours	1			Continue		No		Any

Figure 22 – EV_Database Policy Schedules

Clients:

- evserver1

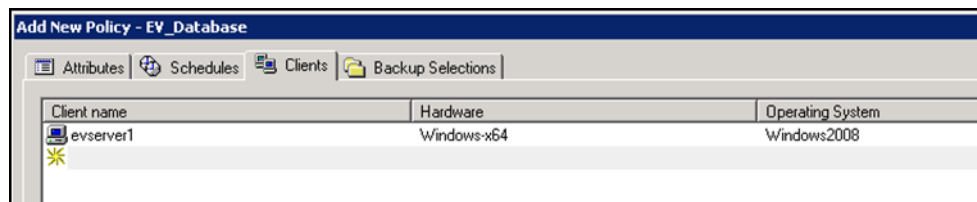


Figure 23 – EV_Database Policy Clients

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

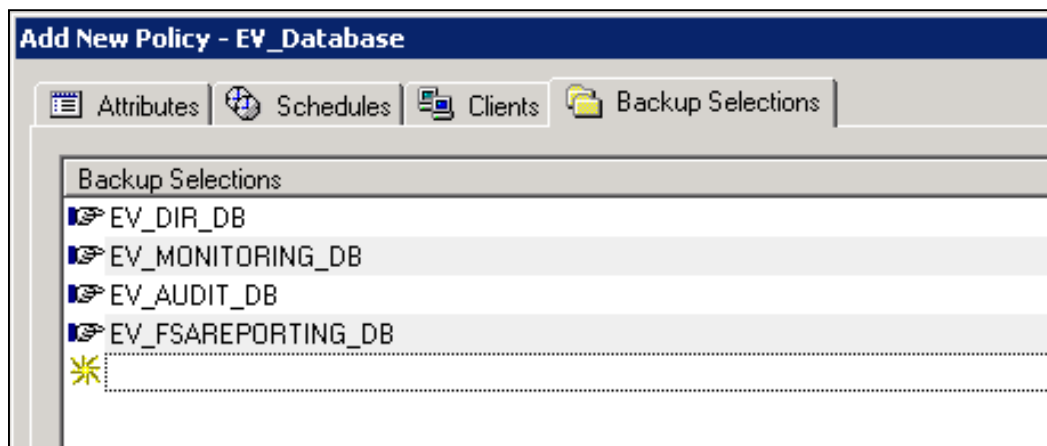


Figure 24 – EV_Database Policy Backup Selections

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 using the NetBackup Enterprise Vault agent.

Vault Store and Fingerprint Database Backup Policy

This policy uses 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

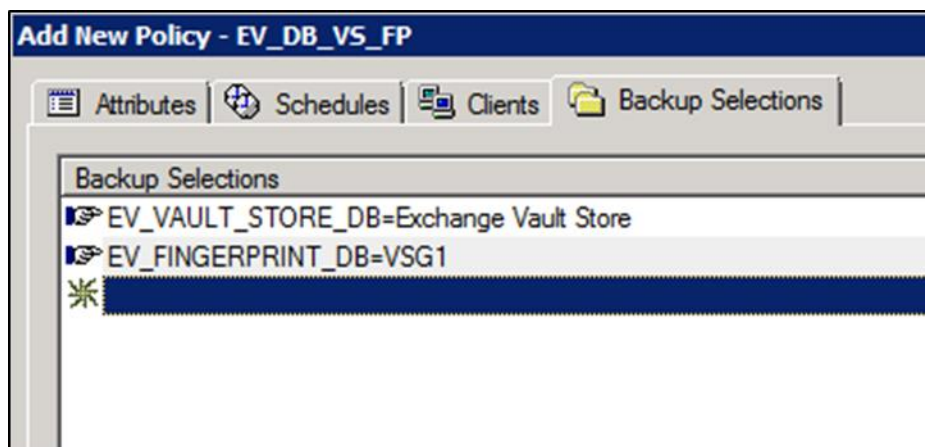


Figure 25 – EV_DB_VS_FP Policy Backup Selections

Open Partition Backup Policy

This policy only backs up the open Vault Store partition using FlashBackup for Windows. A FlashBackup policy type does 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. Using Flashbackup, the naming convention is slightly different and is specified in this format: `\\.\<drive_letter>:\`. In our scenario we would specify: `\\.\H:\`.

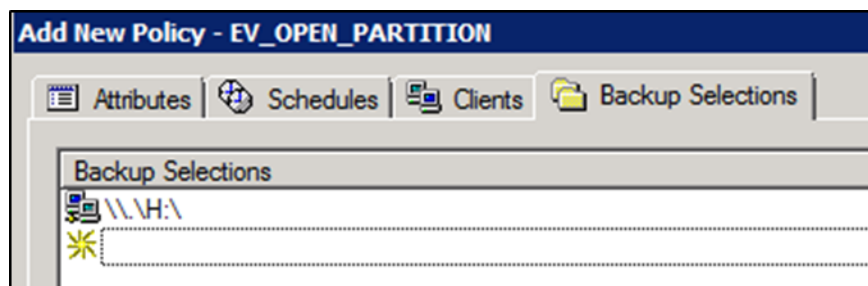


Figure 26 – EV_OPEN_PARTITION Policy Backup Selections

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 uses 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. Using Flashbackup, the naming convention is slightly different and is specified in this format: `\\.\<drive_letter>:\`. In our scenario we would specify: `\\.\I:\`.

Notes: For Enterprise Vault 10 and later, closed index locations can be backed up separately if they are located on their own volumes. Closed index locations does not have new index data and can be backed up less frequently.

A `bpstart_notify` and `bpend_notify` script must also be used with this policy 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 uses 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 does not have new data added, the backup frequency can be much less frequent.
- Weekly incremental – If collections are enabled on partitions, then it is necessary to perform weekly incremental backups. Savesets can still be collected into CAB files after a partition is closed. Failure to back up these changes can cause previously deleted or expired items to reappear during a restore and using the `EVSVR` utility to validate data in the partitions and the Vault Store database.

Client:

- `evserver1`

Backup selections:

- In this scenario, the closed Vault Store partitions are located on various volumes (J:, K:, L:, & M:). 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 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 Index Backup Policies (EV 10 and later)

These policies use FlashBackup for Windows and is intended to only be used with Enterprise Vault 10 or later. Closed index locations would need to be on their own separate volumes to warrant a separate backup policy.

Names: EV_CLOSED_INDEX1, EV_CLOSED_INDEX2, EV_CLOSED_INDEX3, and EV_CLOSED_INDEX4

Policy type: Flashbackup-Windows

Schedules

- Monthly full ☐ Closed index locations does not need to be backed up as frequently as open index locations
- Weekly incremental

Client:

- evserver1

Backup selections:

- Assuming that the closed index locations are on their own separate volumes, the backup selection would be specified in the following format: \\.\<drive_letter:>\.

Pros and Cons for Scenario #3

Pros:

- Using the EV Agent automatically discovers where Enterprise Vault MS-SQL databases are located
- Using Flashbackup-Windows backup policies speeds 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 need to be manually updated when a new open partition is created or when an existing open partition is closed
- The index backup policy need to be updated when index locations change
- With Enterprise Vault 10 and later, a closed index location does not add new index data (but metadata and deletions can still occur). Closed index locations would need to be on their own separate volumes to warrant a separate closed index location backup policy. These policies would need to be manually updated when an index location is closed.
- Pre and post backup scripts need to be maintained properly to ensure that Backup Mode is set and cleared

Scenario #4: Using NetBackup Accelerator (NetBackup 7.5 and later)

This scenario leverages the Accelerator feature available in NetBackup 7.5 and later. NetBackup Accelerator was introduced in NetBackup 7.5 for file system backups and provided a dramatic reduction in the amount of time required for full backups to disk, such that it is similar to the amount of time required for an incremental backup. For more information visit:

<http://www.symantec.com/connect/blogs/frequently-asked-questions-netbackup-accelerator>

The NetBackup Accelerator option does not clear archive bits after a backup. It will be necessary to configure the Vault Store partitions to use a trigger file (as shown in Figure 33).

Old trigger files will need to be deleted before the backup begins. This can be accomplished by creating bpstart_notify.<policy_name>.bat files for each policy that will back up Vault Store partitions. This file needs to be created in the <installation_directory>\NetBackup\bin directory on each Enterprise Vault server.

The trigger files will need to be created by creating a bpend_notify.<policy_name>.bat for each policy that will back up open and closed partitions. This file needs to be created in the <installation_directory>\NetBackup\bin directory on each Enterprise Vault server.

Sample Environment

- One Enterprise Vault server 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
- Collections are enabled

Proposed Backup Policies

This sample environment has 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

Add New Policy - EV_Database

Attributes Schedules Clients Backup Selections

Policy type: Enterprise-Vault

Destination

Data classification: <No data classification>

Policy storage: Any Available

Policy volume pool: Weekly

☐ Take checkpoints every: 0 minutes

☐ Limit jobs per policy:

Job priority: 0

Media Owner: Any

Figure 27 –EV_Database Policy Attributes

Schedules:

- Weekly Full
- Daily Incremental

Add New Policy - EV_Database

Attributes Schedules Clients Backup Selections

	2	4	6	8	10	12	14	16	18	20	22	24
Sun	+	+	+	+	+	+	+	+	+	+	+	+
Mon	+	+	+	+	+	+	+	+	+	+	+	+
Tue	+	+	+	+	+	+	+	+	+	+	+	+
Wed	+	+	+	+	+	+	+	+	+	+	+	+
Thu	+	+	+	+	+	+	+	+	+	+	+	+
Fri	+	+	+	+	+	+	+	+	+	+	+	+
Sat	+	+	+	+	+	+	+	+	+	+	+	+

Name	Type	Retention	Frequency	Multiplex...	Storage	Volume ...	Fail all	Start Wi...	Synthetic	Disk only	Media O...
Weekly-Full	Full Backup	3 months	1 Day	1			Continue		No		Any
Daily-Incr	Differentia..	2 weeks	12 Hours	1			Continue		No		Any

Figure 28 – EV_Database Policy Schedules

Clients:

- evserver1

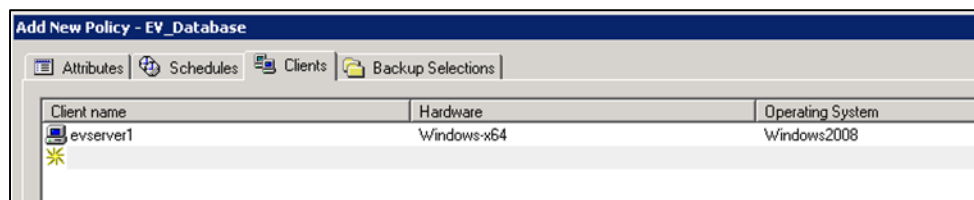


Figure 29 – EV_Database Policy Clients

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

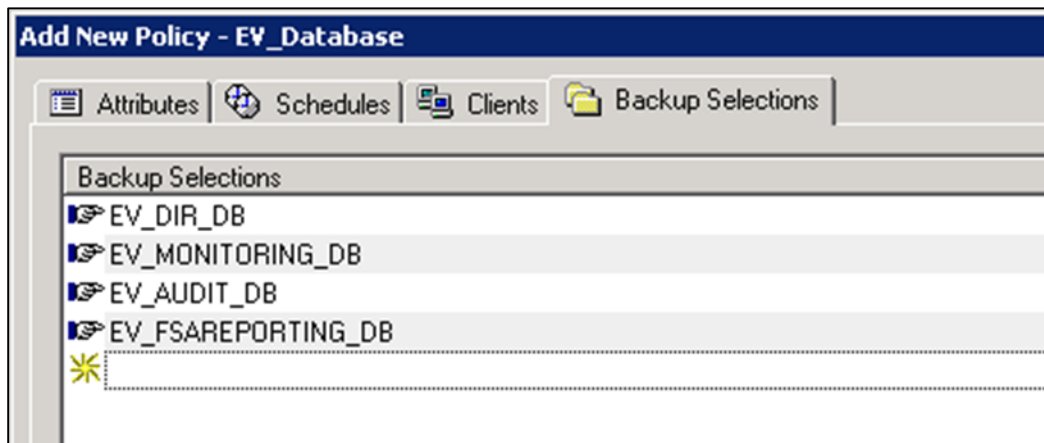


Figure 30 - EV_Database Policy Backup Selections

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 using the NetBackup Enterprise Vault agent.

Vault Store and Fingerprint Database Backup Policy

This policy uses 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

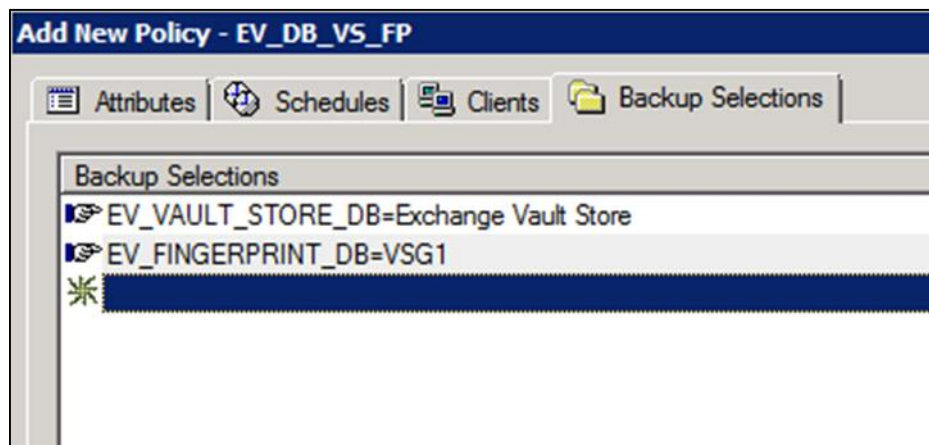


Figure 31 –EV_DB_VS_FP Policy Backup Selections

Open Partition Backup Policy

Name: EV_OPEN_PARTITION

Policy type: MS-Windows with "Use accelerator"

Add New Policy - EV_OPEN_PARTITION

Attributes | Schedules | Clients | Backup Selections

Policy type: MS-Windows

Destination

Data classification: <No data classification>

Policy storage: naomiPD

Policy volume pool: NetBackup

☐ Take checkpoints every: 0 minutes

☐ Limit jobs per policy:

Job priority: 0

Media Owner: Any

☒ Go into effect at:

☐ Backup Network Drives

☐ Cross mount points

☐ Compression

☐ Encryption

Collect disaster recovery information for:

☐ Bare Metal Restore

☐ Collect true image restore information

☐ with move detection

☐ Allow multiple data streams

☐ Disable client-side deduplication

☐ Enable granular recovery

☒ Use accelerator

Keyword phrase:

☐ Enable indexing for search
(Must also be enabled for the schedule)

Indexing Server:

Figure 32 - EV_OPEN_PARTITION Policy Attributes

Schedules:

- Weekly_Full
- Daily_Incremental

Backup selections:

- All open partitions (such as H:\Ptn1, J:\Ptn2, etc.)

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

Name: EV_Index

Policy type: MS-Windows with “Use accelerator”

Schedules:

- Weekly Full
- Daily Incremental

Client:

- evserver1

Backup selections:

- In this scenario, the indexes are located on the I: drive. Specify I:\ in backup selections.

Notes: For **Enterprise Vault 10** and later, closed index locations do not have new index data and can be backed up less frequently.

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

Names: EV_CLOSED_PARTITIONS1, EV_CLOSED_PARTITIONS2, EV_CLOSED_PARTITIONS3, and EV_CLOSED_PARTITIONS4

Policy type: MS-Windows with “Use accelerator” checked

Schedules:

- Monthly full – As closed and ready partitions do not have new data added, the backup frequency can be much less frequent.
- Weekly incremental – If collections are enabled on partitions, then it is necessary to perform weekly incremental backups. Savesets can still be collected into CAB files after a partition is closed. Failure to back up these changes can cause previously deleted or expired items to reappear during a restore and using the EVSVR utility to validate data in the partitions and the Vault Store database.

Client:

- evserver1

Backup selections:

- In this scenario, the closed Vault Store partitions are located on various volumes (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.

Closed Index Backup Policies (EV 10 and later)

The NetBackup accelerator option can also be used when backing up closed Index Locations in Enterprise Vault.

Names: EV_CLOSED_INDEX1, EV_CLOSED_INDEX2, EV_CLOSED_INDEX3, and EV_CLOSED_INDEX4

Policy type: MS-Windows with “Use accelerator” checked

Schedules

- Monthly full ← Closed index locations does not need to be backed up as frequently as open index locations
- Weekly incremental

Client:

- evserver1

Backup selections:

- Assuming that the closed index locations are on their own separate volumes, the backup selection would be specified in the following format: `<drive_letter>:\<path>` such as `I:\index\index01`.

Pros and Cons for Scenario #4

Pros:

- Using the EV Agent automatically discovers where Enterprise Vault MS-SQL databases are located
- Using MS-Windows with “Use accelerator” checked can dramatically speed up backups

Cons:

- The open and closed partition backup policies need to be manually updated when a new open partition is created or when an existing open partition is closed
- The index backup policy needs to be updated when index locations change (EV 10 and later)
- With Enterprise Vault 10 and later, a closed index location does not add new index data (but metadata and deletions can still occur). These policies would need to be manually updated when an index location is closed.
- The backup time for the first full backup will take as long as not using the accelerator option, but subsequent full and incremental backups will be much faster.

Scenario #5: Using NetBackup where the NetBackup Enterprise Vault Agent Is Not Supported in the Enterprise Vault Environment

There are situations where the NetBackup Enterprise Vault Agent may not be supported in particular environments. These environments may include situations where Microsoft SQL Server is clustered with Veritas Cluster Server or other clustered environments or a non-certified or unsupported version of Enterprise Vault. In situations like the one mentioned above, it is necessary to backup Enterprise Vault using standard file-level and MS-SQL agent backups.

The proposed solution offers a unique method of backing up Enterprise Vault components. The solution also provides methods to ensure that Enterprise Vault is in Backup Mode.

NetBackup Accelerator was introduced in NetBackup 7.5 for file system backups and provided a dramatic reduction in the amount of time required for full backups to disk, such that it is similar to the amount of time required for an incremental backup. For more information visit:

<http://www.symantec.com/connect/blogs/frequently-asked-questions-netbackup-accelerator>

The NetBackup Accelerator option does not clear the archive bit. When using Accelerator with Enterprise Vault, Vault Store partitions must be set to use a trigger file (as shown in Figure 33). The backup scripts must be configured to create the trigger file after a backup has been completed. See the Enterprise Vault documentation for more information on using trigger files.

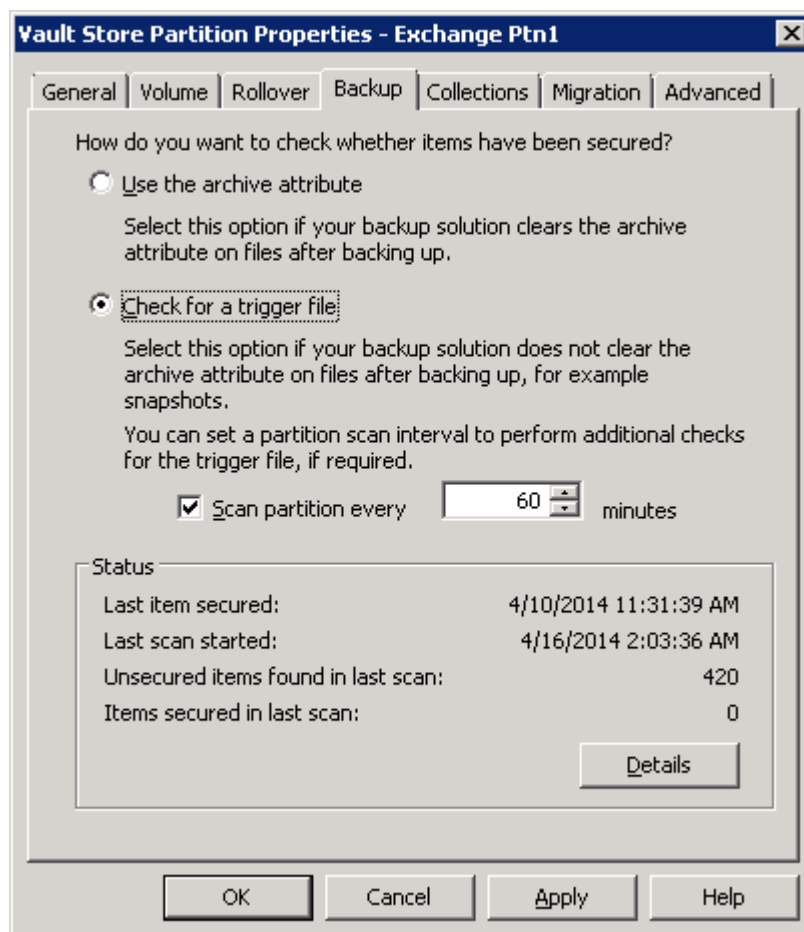


Figure 33 – Using the Trigger File Method for Vault Store Partition Backups

Sample Environment

- One Enterprise Vault 10.0.4 server
- A clustered Active-Passive Microsoft SQL 2008 R2 Server using Veritas Cluster Server
- One Vault Store Group (VSG1)
- Multiple Vault Stores with multiple Vault Store partitions in various states (opened, closed, and ready)
- Indexes are stored on one volume (I:\)

Proposed Backup Policies

In this scenario, there are up to nine backup policies:

- EnterpriseVault_Starter

- EnterpriseVault_StarterClosed
- EnterpriseVault_ClosedPartitions
- EnterpriseVault_Index
- EnterpriseVault_OpenPartitions
- EnterpriseVault_ClearBackupMode
- EnterpriseVault_SQL
- EnterpriseVault_SQL_TRX

Requirements to Implement this Backup Solution

On the Enterprise Vault server, it is necessary to create a new directory (such as C:\backup) with a single text file (such as backup.txt). This directory is necessary for the EnterpriseVault_Starter and EnterpriseVault_StarterClosed backup policies.

On the NetBackup master server, it is necessary to modify the backup_exit_notify file. This file resides in the <installation_directory>\NetBackup\bin directory (Windows) or in the /user/opensv/netbackup/bin directory (UNIX/Linux). The modifications kick off all appropriate backup policies for Enterprise Vault depending on the schedule type (the example here use monthly, weekly, and daily schedules). Services or daemons on the NetBackup Master server will need to be restarted after modifying the backup_exit_notify file.

Here is a sample of a modified backup_exit_notify.cmd file on a Windows NetBackup Master Server:

---- TRUNCATED ----

```
@REM - might want to mail this info to someone
@REM -
@REM - @call %NB_MAIL_SCRIPT% someone_who_cares "NetBackup backup exit"
@REM - %OUTF%
@REM -----

@if %5 lss 2 if %2==EnterpriseVault_Starter goto :EV
@if %5 lss 2 if %2==EnterpriseVault_StarterClosed goto :EVClosed
goto :EndMain
```

```
:EV
echo %3 > c:\startev.txt
if %3==Monthly_Full goto :EVMonthly
if %3==Weekly_Full goto :EVWeekly
if %3==Daily_Incr goto :EVDaily
goto :EndMain

:EVClosed
echo %3 > c:\startev_closed.txt
if %3==Monthly_Full goto :EVMonthlyClosed
if %3==Weekly_Incr goto :EVWeeklyClosed
goto :EndMain

:EVMonthlyClosed
echo monthly_full_closed > c:\monthly_full_closed.txt
@"F:\VERITAS\NetBackup\bin\bpbackup" -i -p EnterpriseVault_ClosedPartitions -
s Monthly_Full -t 13 -w
@"F:\VERITAS\NetBackup\bin\bpbackup" -i -p EnterpriseVault_ClearBackupMode -s
Daily_Full -t 13 -w

goto :EndMain

:EVWeeklyClosed
echo weekly_incr_closed > c:\weekly_incr_closed.txt
@"F:\VERITAS\NetBackup\bin\bpbackup" -i -p EnterpriseVault_ClosedPartitions -
s Weekly_Incr -t 13 -w
@"F:\VERITAS\NetBackup\bin\bpbackup" -i -p EnterpriseVault_ClearBackupMode -s
Daily_Full -t 13 -w

goto :EndMain

:EVMonthly
echo monthly_full > c:\monthly_full.txt
@"F:\VERITAS\NetBackup\bin\bpbackup" -i -p EnterpriseVault_SQL -s Daily_Full
-t 15 -w
```

```

@F:\VERITAS\NetBackup\bin\bpbackup" -i -p EnterpriseVault_Index -s
Monthly_Full -t 13 -w

@F:\VERITAS\NetBackup\bin\bpbackup" -i -p EnterpriseVault_OpenPartitions -s
Monthly_Full -t 13 -w

@F:\VERITAS\NetBackup\bin\bpbackup" -i -p EnterpriseVault_ClearBackupMode -s
Daily_Full -t 13 -w

goto :EndMain

:EVWeekly
echo weekly > c:\weekly.txt

@F:\VERITAS\NetBackup\bin\bpbackup" -i -p EnterpriseVault_SQL -s Daily_Full
-t 15 -w

@F:\VERITAS\NetBackup\bin\bpbackup" -i -p EnterpriseVault_Index -s
Weekly_Full -t 13 -w

@F:\VERITAS\NetBackup\bin\bpbackup" -i -p EnterpriseVault_OpenPartitions -s
Weekly_Full -t 13 -w

@F:\VERITAS\NetBackup\bin\bpbackup" -i -p EnterpriseVault_ClearBackupMode -s
Daily_Full -t 13 -w

goto :EndMain

:EVDaily
echo daily > c:\daily.txt

@F:\VERITAS\NetBackup\bin\bpbackup" -i -p EnterpriseVault_SQL -s Daily_Full
-t 15 -w

@F:\VERITAS\NetBackup\bin\bpbackup" -i -p EnterpriseVault_Index -s
Daily_Incr -t 13 -w

@F:\VERITAS\NetBackup\bin\bpbackup" -i -p EnterpriseVault_OpenPartitions -s
Daily_Incr -t 13 -w

@F:\VERITAS\NetBackup\bin\bpbackup" -i -p EnterpriseVault_ClearBackupMode -s
Daily_Full -t 13 -w

goto :EndMain

:EndMain
@endlocal
@REM - End of Main Program -----

```

The basic flow of the script is the following:

1. If the backup job (EnterpriseVault_Starter or EnterpriseVault_StarterClosed) exits with status 0 or 1 the backup continues.
2. If EnterpriseVault_Starter is the policy, the following occurs:
 - a. If the schedule name is “Monthly_Full”, the following backup policies are launched:
 - i. EnterpriseVault_SQL, schedule: Daily_Full
 - ii. EnterpriseVault_Index, schedule: Monthly_Full
 - iii. EnterpriseVault_OpenPartitions, schedule: Monthly_Full
 - b. If the schedule is “Weekly_Full”, the following backup policies are launched:
 - i. EnterpriseVault_SQL, schedule: Daily_Full
 - ii. EnterpriseVault_Index, schedule: Weekly_Full
 - iii. EnterpriseVault_OpenPartitions, schedule: Weekly_Full
 - c. If the schedule is “Daily_Incr”, the following backup policies are launched:
 - i. EnterpriseVault_SQL, schedule: Daily_Full
 - ii. EnterpriseVault_Index, schedule: Daily_Incr
 - iii. EnterpriseVault_OpenPartitions, schedule: Daily_Incr
3. If EnterpriseVault_StarterClosed is the policy, the following happen:
 - a. If the schedule name is “Monthly_Full”, the following backup policy are launched:
 - i. EnterpriseVault_ClosedPartitions, schedule: Monthly_Full
 - b. If the schedule name is “Weekly_Incr”, the following backup policy are launched:
 - i. EnterpriseVault_ClosedPartitions, schedule: Weekly_Incr

The EnterpriseVault_Starter and EnterpriseVault_StarterClosed Backup Policies

These policies kick off the backup of all Enterprise Vault components. The “StarterClosed” policy kicks off policies related to closed and ready partition backups. In order to control Backup Mode (EV 8 or later), it is necessary to create a bpstart_notify.EnterpriseVault_Starter.bat and bpstart_notify.EnterpriseVault_StarterClosed.bat files in the <installation_directory>\NetBackup\bin directory on the Enterprise Vault server. As the NBU Accelerator does not clear the archive bit, the trigger file method must be used for each Vault Store partition that is backed up. It will be necessary to delete the old trigger file before the backup. The contents of the file should look something like this:

```
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell -psconsolefile
"C:\Program Files (x86)\Enterprise Vault\EVShell.psc1" -command "& {Set-
```

```
VaultStoreBackupMode -Name <site_name> -EVServerName <ev_server_name> -
EVOBJECTType Site}"
```

```
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell -psconsolefile
"C:\Program Files (x86)\Enterprise Vault\EVShell.psc1" -command "& {Set-
IndexLocationBackupMode -EVServerName <ev_server_name> -EVSiteName
<site_name>}"
```

```
@REM - Delete old trigger files for each partition that will be backed up
del "s:\Exchange Vault Store\ptn1\ignorearchivebittrigger.old"
del "q:\FSA Vault Store\ptn2\ignorearchivebittrigger.old"
```

The two PowerShell commands listed above place all Vault Stores and Index Locations into Backup Mode. Replace <site_name> with the name of the Enterprise Vault site. Replace <ev_server_name> with the name of the Enterprise Vault server.

EnterpriseVault_Starter Policy

Policy type: MS-Windows

Schedules:

- Monthly_Full
- Weekly_Full
- Daily_Incr

Client:

- Evserver

Backup Selections:

- C:\backup

EnterpriseVault_StarterClosed Policy

Policy type: MS-Windows

Schedules:

- Monthly_Full – Should not be schedule to run at the same time as the EnterpriseVault_Starter policy

- Weekly_Incr - Should not be schedule to run at the same time as the EnterpriseVault_Starter policy

Client:

- evserver

Backup Selections:

- C:\backup

The EnterpriseVault_ClosedPartitions Backup Policy

Policy type: MS-Windows – Enable Accelerator if possible

Schedules:

- Monthly_Full – Ensure no backup windows are defined
- Weekly_Incr – Ensure no backup windows are defined

Clients:

- evserver

Backup Selections:

- Include all paths to closed and ready partitions

The EnterpriseVault_Index Backup Policy

Policy type: MS-Windows – Enable Accelerator if possible

Schedules:

- Monthly_Full – Ensure no backup windows are defined
- Weekly_Full – Ensure no backup windows are defined
- Daily_Incr – Ensure no backup windows are defined

Clients:

- Evserver

Backup Selections:

- Include all paths to Index Locations

The EnterpriseVault_OpenPartitions Backup Policy

Policy type: MS-Windows – Enable Accelerator if possible

Schedules:

- Monthly_Full – Ensure no backup windows are defined
- Weekly_Full – Ensure no backup windows are defined
- Daily_Incr – Ensure no backup windows are defined

Clients:

- evserver

Backup Selections:

- Include all paths to open Vault Store partitions

The EnterpriseVault_ClearBackupMode and EnterpriseVault_ClearBackupModeClosed Policies

The purpose of these policies is to clear Backup Mode and create trigger files for the partitions that will be backed up.

Policy type: MS-Windows

Schedules:

- Daily_Full – Ensure no backup windows are defined

Client:

- evserver

Backup Selections:

- C:\backup

In order to clear Backup Mode (EV 8 or later), it is necessary to create a
bpend_notify.EnterpriseVault_ClearBackupMode.bat and
bpend_notify.EnterpriseVault_ClearBackupModeClosed.bat files in the

<installation_directory>\NetBackup\bin directory on the Enterprise Vault server. It will also be necessary to create trigger files for each Vault Store partition that was backed up by the policy (these should be created before clearing Backup Mode). The contents of the file should look something like this:

```
@REM - Create trigger files for each partition that was backed up

ECHO > "s:\Exchange Vault Store\ptn1\ignorearchivebittrigger.txt"

ECHO > "q:\FSA Vault Store\ptn2\ignorearchivebittrigger.txt"

C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell -psconsolefile
"C:\Program Files (x86)\Enterprise Vault\EVShell.psc1" -command "& {Clear-
VaultStoreBackupMode -Name <site_name> -EVServerName <ev_server_name> -
EVOBJECTType Site}"

C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell -psconsolefile
"C:\Program Files (x86)\Enterprise Vault\EVShell.psc1" -command "& {Clear-
IndexLocationBackupMode -EVServerName <ev_server_name> -EVSiteName
<site_name>}"
```

The two PowerShell command listed above clears all Vault Stores and Index Locations from Backup Mode. Replace <site_name> with the name of the Enterprise Vault site. Replace <ev_server_name> with the name of the Enterprise Vault server.

The EnterpriseVault_SQL Backup Policy

Policy type: MS-SQL-Server

Schedules:

- Daily_Full – Ensure that no backup windows are defined
- Default-Application-Backup – Automatically set to run 24/7

Clients:

- MS SQL Server containing Enterprise Vault databases

Backup Selections:

- Include the path to the name of the SQL backup script as created with the NetBackup MS SQL Client (example: C:\Program Files\Veritas\NetBackup\DbExt\MsSql\EV-Full.bch). The batch file should include all Enterprise Vault databases such as EnterpriseVaultDirectory, EnterpriseVaultMonitoring, Vault Store Group databases, and Vault Store databases.

The EnterpriseVault_SQL_TRX Backup Policy

This SQL backup policy is intended to backup and truncate all transaction logs for Enterprise vault Microsoft SQL databases.

Policy type: MS-SQL-Server

Schedules:

- Daily_Full – This should be scheduled to run shortly after the EnterpriseVault_OpenPartitions policy is expected to finish
- Default-Application-Backup – Automatically set to run 24/7

Clients:

- MS SQL Server containing the Enterprise Vault databases

Backup Selections:

- Include the path to the name of the SQL backup script as created with the NetBackup MS SQL Client (example: C:\Program Files\Veritas\NetBackup\DbExt\MsSql\EV-TRX.bch). The batch file should include all Enterprise Vault databases such as EnterpriseVaultDirectory, EnterpriseVaultMonitoring, Vault Store Group databases, and Vault Store databases. The “Type of Backup” MUST be set to “transaction log” as shown in Figure 34.

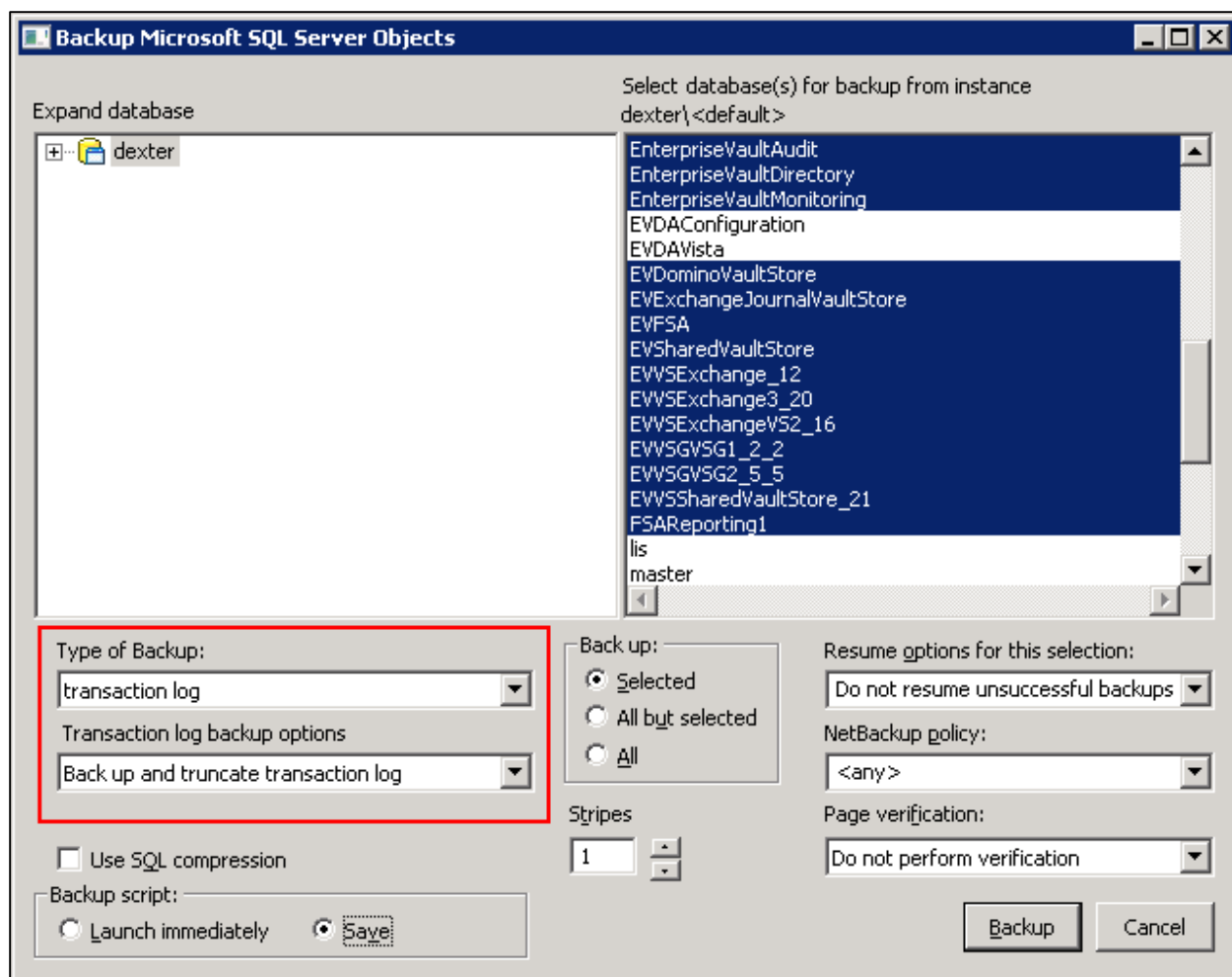


Figure 34 – Configuring a Transactional SQL Backup Script

Pros and Cons for Scenario #5

Pros:

- The backup of all Enterprise Vault components can be scheduled through two tasks
- The NetBackup Accelerator (NBU 7.5 and later) feature can be used with the backup of Vault Store partitions and Index Locations
- bpend_notify scripts control the EV Backup Mode

Cons:

- Backup selections for policies needs to be updated manually when the status of a Vault Store partition changes (such as from opened to closed and ready to open)

Other Enterprise Vault Object to Backup Up

Besides the index, database, and Vault Store partitions, there are other objects in Enterprise Vault that should be backed up. These objects include:

- The Registry – Enterprise Vault does store settings in the Windows Registry and should be backed up weekly
- Application Installation Path – There can be files created by administrators that should be backed up. These files include any custom EVPM scripts, customized settings for EV processes (.config files), and custom message files (such as messages when a user is enabled for mailbox archiving)
- EV Storage Queue (EV 11 and later) – The storage queue contains safety copies of archived items. In the event of a full restore, storage queue locations should be backed up before Vault Store partitions and done so with a daily full backup.
- Index Metadata locations (EV 10 and later) – The index metadata locations should be backed up daily.
- PST Temp and PST Holding areas – In the event of a full restore, these locations should be backed up daily.
- SSL Certificates – SSL Certificates for IIS and IMAP (EV 11 and later) should be backed up at least once per week

Vault Store Partition Sizing

One of the main reasons to implement Enterprise Vault is to reduce the amount of storage required on target systems such as Exchange or file systems. This reduction on the target systems reduces the amount of data and time needed to backup these applications. Enterprise Vault can greatly reduce the size of the original content through compression and Optimized Single Instance Storage (OSIS). Even with the size of the original content reduced, back up of this archived content is still a necessity.

With Enterprise Vault 8.0 and later, a feature named Partition Rollover is available to automatically close a partition based either size, date, or both. Once a rollover threshold is met, the partition is closed and the next available ready Vault Store partition is set to an open state. A closed partition does not have any new data added to it. The only changes to the partition occurs if collections are enabled (by default,

collections are active for up to 10 days) and when archived content expires. Thus, back up of closed partitions does not need to happen as frequently as open partitions.

It is given that the larger a Vault Store partition is, the longer it takes to back up. Sizing of a partition is very important in order to optimize backup windows. Let's take a look at two different methodologies for sizing Vault Store partitions. As an example, an Enterprise Vault environment adds an average of 10GB per day of new content. If a Vault Store partition is sized at 5TB and rollover is based on volume size, it takes around 500 days to fill up that partition. During those 500 days, the amount of time it takes to fully back up that 5TB volume continually grows. If the partition size is 200GB, it fills up and closes much faster (within 20 days). However, it is necessary to create and manage numerous partitions to accommodate growth from an Enterprise Vault and backup point of view.

Another factor with partition sizing is the archiving of the backlog. New implementations of Enterprise Vault generally archives more data initially as older content is archived first. The daily archiving rate is much higher initially. Once this backlog has been archived, only newer items are archived (based on archiving policy configuration) and the daily archiving rate should be much lower.

One last factor in partition sizing to consider is the backup window and environment. How long is the backup window for a full backup of a partition? Other factors can affect the backup window include the performance of the storage for the partition, network bandwidth and utilization, backup load of the backup server during the backup window, and the type of backup medium being used (such as tape or disk). Take the following example:

- Full backup window is four hours
- Gigabit Ethernet network (~100MB/sec)
- LTO3 tape drives (~60MB/sec)
- Vault Store partition size is 5TB

Based on the example, a four hour backup window would only back up around 850GB (60MB/second * 3600 seconds an hour * four hours) of data within an optimal environment. This assumes that storage used for the partition can push at least 60MB/sec. Due to the nature of how archived data is stored in the partition, it is likely that the throughput from disk can be considerably less. The size of this partition is too large for the backup window. In this situation the partition should be sized at 800GB or less (400-500GB).

In conclusion, sizing of a Vault Store partition requires the knowledge of all the components in the archiving environment. Estimating or knowing the daily archiving rate will provide a basis around storage requirements and account for future growth. Know the amount of backlog to be archived for new Enterprise Vault installations as the daily archiving rate is generally much higher initially. Monitor the backup environment as well so that partitions are backed up in the time allotted.

About Symantec:

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

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: **www.symantec.com**

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

Copyright © 2013 Symantec Corporation. All rights reserved. Symantec and the Symantec logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.