

Technical White Paper - Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

If you have any feedback or questions about this document, please email tfe@veritas.com stating the document title.

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

Contents

Introduction.....	5
Backing up the Enterprise Vault Database Component	5
The Flat File Method	2
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 paused. Enterprise Vault has PowerShell scripts that can control Backup Mode. For more information on Enterprise Vault Backup Mode, see “Backing up Elasticsearch Indexes	2
Differences between Older Indexes and Elasticsearch Indexes.....	2
Rules of Thumb for Elasticsearch Snapshot Locations	2
Creating and Locating Elasticsearch Snapshot Locations.....	3
Creating an Elasticsearch Snapshot.....	5
Using Commercially Available Backup Software	6
Using High Availability and Replication	6
Backing up the Discovery Accelerator and Compliance Accelerator Database Components	6
Discovery Accelerator	6
Compliance Accelerator	7
Backing up Enterprise Vault Index and Vault Store Partition Locations.....	7
Setting and Clearing Backup Mode in the Enterprise Vault Administration Console	7
Setting Backup Mode for an Enterprise Vault Site	7
Setting and Clearing Backup Mode for a Specific Vault Store or Vault Store Group	9
Setting and Clearing Backup Mode for All Indexes/Non-Elasticsearch Indexes on an Enterprise Vault server	11
Setting and Clearing Backup Mode for a Specific Index/Non-Elasticsearch Index Location on an Enterprise Vault Server.....	12
Backing up Elasticsearch Indexes.....	14

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

Differences between Older Indexes and Elasticsearch Indexes.....	14
Rules of Thumb for Elasticsearch Snapshot Locations	15
Creating and Locating Elasticsearch Snapshot Locations.....	15
Creating an Elasticsearch Snapshot.....	17
Setting and Clearing Backup Mode Using the Enterprise Vault Management Shell.....	18
Using Enterprise Vault Management Shell for the First Time	18
Enterprise Vault 8.0SP3 Changes	18
PowerShell Usage for Vault Stores.....	19
PowerShell Usage for Indexes	20
Scripting out PowerShell Commands.....	20
Storage Queues (Enterprise Vault 11 and Later).....	21
Advanced Backup Strategies.....	22
Vault Store Partition Sizes	22
Utilizing Snapshots for Backing up Enterprise Vault.....	22
Back up the Whole Enterprise Vault Server in One Backup Job?.....	23
Virtual Machine Backups.....	23
Backup Frequency for Index and Vault Store Partitions	23
Timing of Backups	23
Backing up Enterprise Vault with Veritas NetBackup	24
The NetBackup Enterprise Vault Backup Agent	24
Note about Using bpstart_notify Scripts	24
Backup Scenario #1: Using file level backups	25
Backup Scenario #2: Using the NetBackup Enterprise Vault Backup Agent.....	28
Sample Environment	28
Proposed Backup Policies	29

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

The Database Backup Policy	29
EVSERVER1 Open Partition Backup.....	31
EVSERVER2 & EVSERVER3 Open Partition Backup	32
Index Backup.....	33
Closed Partition Backup	34
Storage Queue, Enterprise Vault Installation Directory, and VIC Policies Shared Location.....	35
Pros and Cons for Scenario #2.....	35
Backup Scenario #3: Using a Combination of the NetBackup Enterprise Vault Agent and FlashBackup for Windows	36
Sample Environment	36
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	40
Closed Index Backup Policies (EV 10 and later)	41
Storage Queue, Enterprise Vault Installation Directory, and VIC Policies Shared Location.....	41
Pros and Cons for Scenario #3.....	41
Backup Scenario #4: Using NetBackup Accelerator (NetBackup 7.5 and later).....	42
Sample Environment	42
Proposed Backup Policies	43
The Database Backup Policy.....	43
Vault Store and Fingerprint Database Backup Policy.....	45
Open Partition Backup Policy	46

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

Index Backup Policy	47
Closed Partition Backup Policies	47
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 “Backing up Elasticsearch Indexes	
Differences between Older Indexes and Elasticsearch Indexes.....	48
Rules of Thumb for Elasticsearch Snapshot Locations	48
Creating and Locating Elasticsearch Snapshot Locations.....	49
Creating an Elasticsearch Snapshot.....	51
Closed Index Backup Policies (EV 10 and later)	52
Storage Queue, Enterprise Vault Installation Directory, and VIC Policies Shared Location.....	52
Pros and Cons for Scenario #4.....	52
Backup Scenario #5: Backing up Enterprise Vault and Microsoft SQL Servers Running as Virtual Machines	
Sample Environment	53
Pre and Post Backup Scripts	53
Proposed Backup Policies	53
Enterprise Vault.....	53
SQL.....	55
Pros and Cons for Scenario #5.....	57
Other Enterprise Vault Objects to Back Up.....	57
Vault Store Partition Sizing	58
Backing up Discovery Accelerator and Compliance Accelerator	59

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

Introduction

The purpose of this document is to provide best practices for backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator. This document provides examples of using backup scripts and using the Veritas NetBackup and Backup Exec Enterprise Vault agent. The techniques discussed in this whitepaper can also be used with other backup software.

Backing up the Enterprise Vault Database Component

The database component plays a crucial role for Enterprise Vault. All configuration data for an Enterprise Vault installation is stored in the EnterpriseVaultDirectory database. Enterprise Vault uses additional databases such as Vault Store, fingerprinting (Vault Store Group), reporting, and auditing. These databases start with “EV” and must be backed up to ensure proper recovery of Enterprise Vault.

Veritas recommends that all SQL databases are backed up at the same time as other Enterprise Vault data such as Vault Store Partitions and index locations. 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 Veritas NetBackup or Backup Exec, and high availability. Attempting to back up the database components by not using one of the methods that will be discussed in this document 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 an inconsistent 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. Microsoft SQL Server 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 paused. Enterprise Vault has PowerShell scripts that can control Backup Mode. For more information on Enterprise Vault Backup Mode, see “Backing up Elasticsearch Indexes

Starting with Enterprise Vault 14.2, a new indexing engine was implemented that replaces the older 32-bit and 64-bit indexing engines. Elasticsearch requires a different approach for backups compared to the older indexing technologies.

If the Enterprise Vault environment was upgraded to 14.2, it is highly likely that there are non-Elasticsearch 64-bit indexes and potentially older non-Elasticsearch 32-bit indexes. These older indexes will still need to be backed up until the content is either expired, deleted, or upgraded to an Elasticsearch index using the methods described in this document.

If this is a new 14.2 or later installation, there will not be any 64-bit or 32-bit indexes. Therefore, it will be only necessary to configure backups for Elasticsearch indexes.

Differences between Older Indexes and Elasticsearch Indexes

Elasticsearch indexes differ from older index engines in the following ways:

- Elasticsearch does not support direct flat file backups and a direct restore of Elasticsearch index flat files will likely fail or have corrupted data
- Backup Mode is not applicable to an Elasticsearch index location
- Backing up of Elasticsearch indexes requires the use of snapshots
 - The snapshots are essentially dumps of the index and placed in a separate location
 - These file dumps can then be backed up and used to restore the index if needed

Rules of Thumb for Elasticsearch Snapshot Locations

Keep the following in mind when setting up a Elasticsearch snapshot location

- A snapshot location must be defined before Elasticsearch indexes can be properly backed up
- Elasticsearch snapshot locations should be placed on a separate volume from the Elasticsearch index location. The volume can be locally attached to the Enterprise Vault Server or on a network share. It is recommended to use a network share.
- The size of the snapshot volume should be at least the same size of the volume holding the Elasticsearch indexes. If the snapshot volume becomes full, additional snapshot volumes can be created. The old snapshot volume will be placed in read-only mode.
- The first snapshot in a snapshot location will be a full copy of the current Elasticsearch index. Subsequent snapshots will be incremental. The same is true if the version of Elasticsearch is upgraded (such as when upgrading to a future version of Enterprise Vault).
- The Enterprise Vault Service Account (VSA) must have read and write access to the snapshot location
- Elasticsearch snapshot locations can hold up to 500 snapshots. The Enterprise Vault administrator will receive warnings when the snapshot count is over 400. See the **Enterprise Vault PowerShell Cmdlets** guide for more information on managing Elasticsearch snapshots.

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

Creating and Locating Elasticsearch Snapshot Locations

Snapshot locations are managed using the Enterprise Vault Management Shell. A PowerShell cmdlet named **Set-EVIndexSnapshotLocation** is used to create snapshot locations. Once a snapshot location is configured, it will be necessary to restart the Enterprise Vault Indexing service. The options for this cmdlet include:

- **-EVServerName <string>** - The name of the Enterprise Vault index server for which you want to configure an index snapshot location with the specified path. If you omit this parameter, Set-EVIndexSnapshotLocation uses the host name of the Enterprise Vault index server where the command is running. The FQDN must be used for the name of the Enterprise Vault server.
- **-SnapshotLocationPath <string>** - The path of the directory you want to configure for taking snapshots of the indexing data.
- **-WhatIf** - The WhatIf switch instructs the command to simulate the actions that it would take on the object. By using the WhatIf switch, you can preview the changes that would occur without applying any of those changes. You do not need to specify a value with the WhatIf switch.

Examples:

The following defines a snapshot location on the server “evserver” on a locally attached volume:

```
Set-EVIndexSnapshotLocation -EVServerName evserver.local -SnapshotLocationPath  
"J:\SnapShot"
```

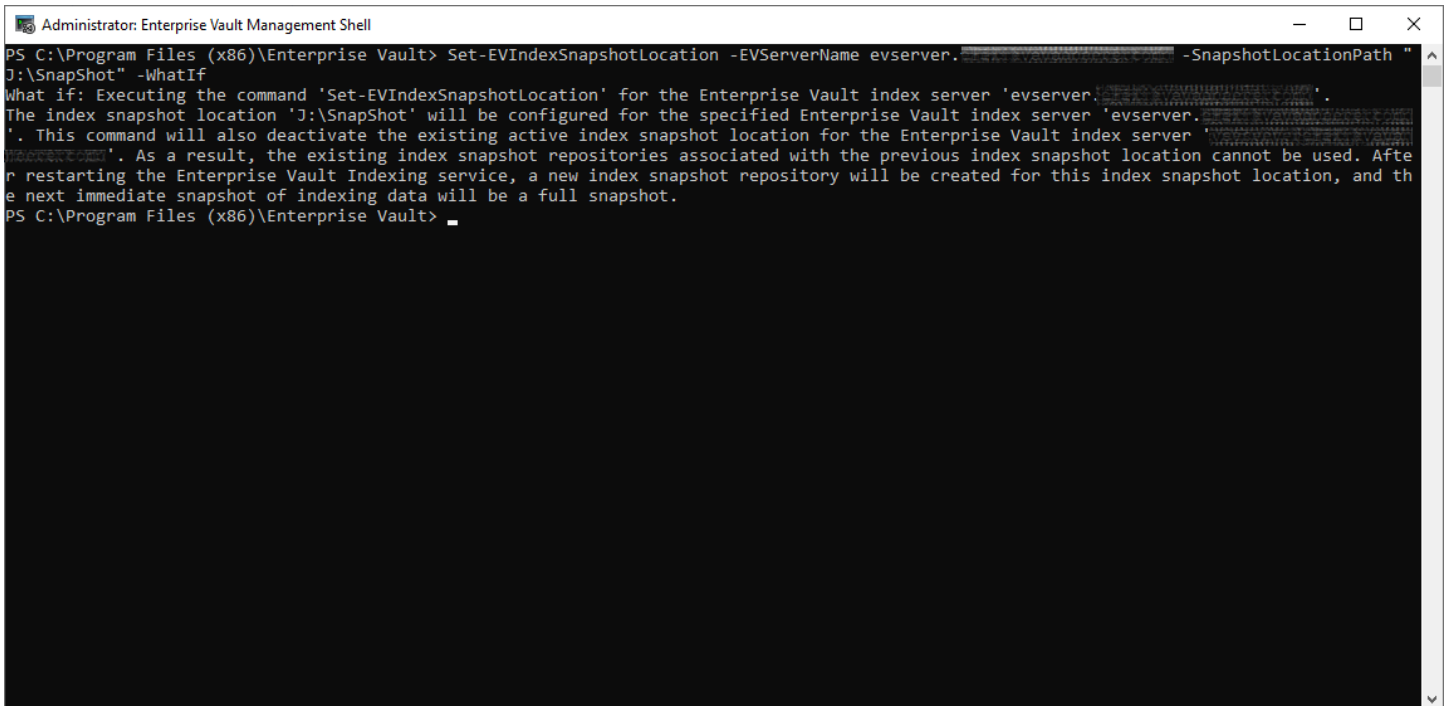
The following defines a snapshot location on the server “evserver” using a network share:

```
Set-EVIndexSnapshotLocation -EVServerName evserver.local -SnapshotLocationPath  
"\\fileserver\snapshots\SnapShot1"
```

The following performs a “What If”

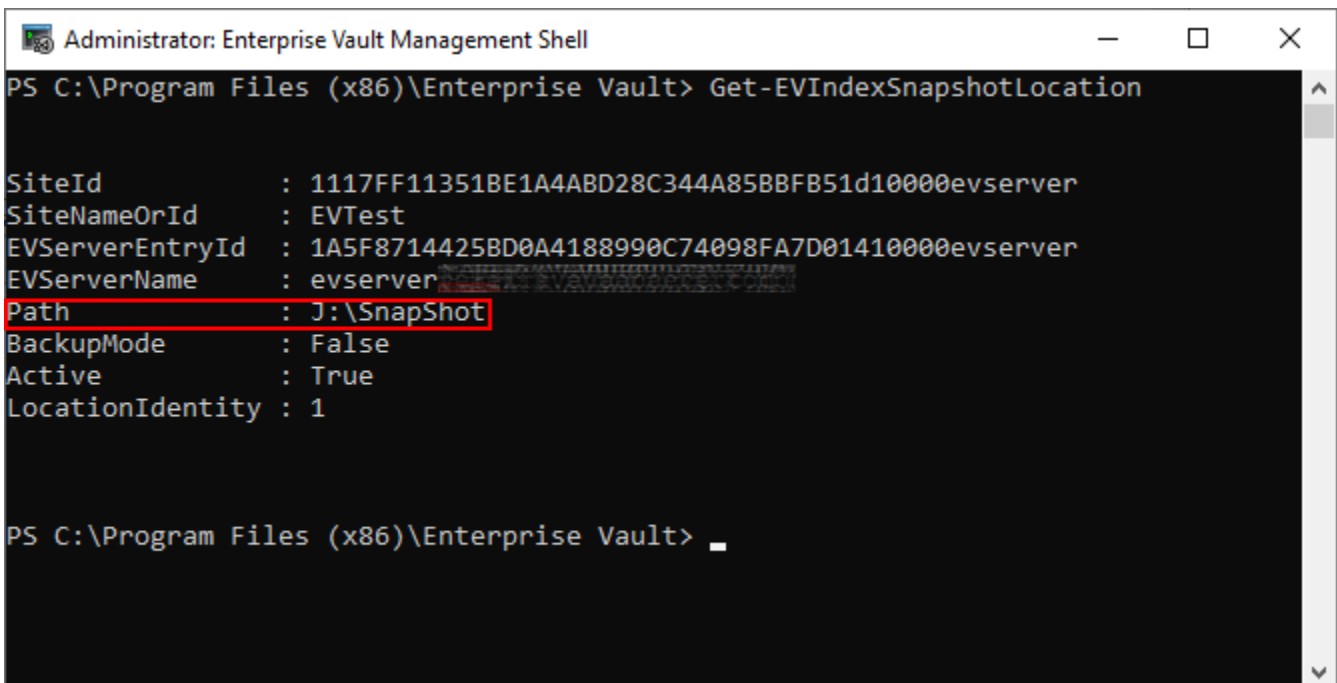
```
Set-EVIndexSnapshotLocation -EVServerName evserver.local -SnapshotLocationPath  
"J:\SnapShot" -WhatIf
```


Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator



```
Administrator: Enterprise Vault Management Shell
PS C:\Program Files (x86)\Enterprise Vault> Set-EVIndexSnapshotLocation -EVServerName evserver. -SnapshotLocationPath "J:\SnapShot" -WhatIf
What if: Executing the command 'Set-EVIndexSnapshotLocation' for the Enterprise Vault index server 'evserver.'.
The index snapshot location 'J:\SnapShot' will be configured for the specified Enterprise Vault index server 'evserver.'. This command will also deactivate the existing active index snapshot location for the Enterprise Vault index server 'evserver.'. As a result, the existing index snapshot repositories associated with the previous index snapshot location cannot be used. After restarting the Enterprise Vault Indexing service, a new index snapshot repository will be created for this index snapshot location, and the next immediate snapshot of indexing data will be a full snapshot.
PS C:\Program Files (x86)\Enterprise Vault>
```

To find existing Elasticsearch snapshot locations, use `Get-EVIndexSnapshotLocation`. Note the Path as this will be needed later in order to back up the location.



```
Administrator: Enterprise Vault Management Shell
PS C:\Program Files (x86)\Enterprise Vault> Get-EVIndexSnapshotLocation

SiteId           : 1117FF11351BE1A4ABD28C344A85BBFB51d10000evserver
SiteNameOrId     : EVTest
EVServerEntryId  : 1A5F8714425BD0A4188990C74098FA7D01410000evserver
EVServerName     : evserver
Path             : J:\SnapShot
BackupMode       : False
Active           : True
LocationIdentity : 1

PS C:\Program Files (x86)\Enterprise Vault>
```

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

Creating an Elasticsearch Snapshot

Before backing up the Elasticsearch snapshot location, it will be necessary to create a snapshot to include the latest changes to the Elasticsearch index location. This is performed by using the **New-EVIndexSnapshot** cmdlet.

This cmdlet creates a snapshot of the Elasticsearch index location. The first snapshot on a newly created snapshot location will be a full copy of the current index. A full snapshot will also be created if the version of Elasticsearch is upgraded (such as when upgrading to a future version of Enterprise Vault). Subsequent snapshots will be incremental. The options for this cmdlet include:

- **-SiteId** - The ID of the Enterprise Vault site for which you want to create the snapshots of index data on all the Enterprise Vault index servers in that site. If you omit this parameter, New-EVIndexSnapshot retrieves the SiteId from the Enterprise Vault index server specified as EVServerName parameter; otherwise, it uses the SiteId of the Enterprise Vault index server where the command is running. You can use the Get-EVSite command to obtain the SiteId.
- **-EVServerName <String>** - The name of the Enterprise Vault index server for which you want to create the snapshot of index data. If you omit this parameter, New-EVIndexSnapshot uses the host name of the Enterprise Vault index server where the command is running. You can use the Get-EVComputers command to obtain the Enterprise Vault server name. The FQDN of the Enterprise Vault server must be used.
- **-IgnoreUnavailable** - (Optional, Boolean) If false, the command returns an error for any data stream or index that is missing or closed. Defaults to false. If true, the command ignores data streams and indices those are missing or closed.
- **-IncludeGlobalState** - (Optional, Boolean) If true, the current global state of Elasticsearch cluster running on Enterprise Vault index server is included in the snapshot. Defaults to false.
- **-Confirm** - (Optional, Boolean) The default value is **\$true**. If true, the user executing the cmdlet will have to confirm whether or not to execute the operation. If using this in a script, specify **-Confirm:\$false**.

Examples:

The following creates an index snapshot on the current server where the command is executed:

```
New-EVIndexSnapshot
```

The following creates an index snapshot on the Enterprise Vault index server named 'ev.domain.local' and will not ask for confirmation. A FQDN for the Enterprise Vault server must be specified:

```
New-EVIndexSnapshot -EVServerName ev.domain.local -Confirm:$false
```

The following creates index snapshots for all Enterprise Vault index server under the site 'site.domain.com'

```
New-EVIndexSnapshot New-EVIndexSnapshot -SiteId site.domain.com
```

The following creates an index snapshot of the Enterprise Vault index server 'ev.domain.local', if IgnoreUnavailable is set to false, the command returns an error for any data stream or index that is missing or closed. If true, the command ignores data streams and indices in indices that are missing or closed.

```
New-EVIndexSnapshot -EVServerName ev.domain.local -IgnoreUnavailable
```

The use of the **New-EVIndexSnapshot** cmdlet can be used in pre-backup scripts. Ensure to specify **-Confirm:\$false** so that confirmation is not required.

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

Setting and Clearing Backup Mode Using the Enterprise Vault Management Shell”.

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 tape for backup medium, ensure that the storage of the tapes is safely located 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, work with the SQL backup API to back up databases and transaction logs. As a reminder, the Enterprise Vault 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 replicated to a remote location in the event of a disaster. If the backup medium 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.

Veritas Backup Exec and NetBackup contain licensed add-ons which can back up the Microsoft SQL databases and transaction logs.

Using High Availability and Replication

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 Veritas InfoScale Availability 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. New versions of Enterprise Vault support SQL “Always On”.

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 the Discovery Accelerator and Compliance Accelerator Database Components

If Discovery Accelerator or Compliance Accelerator is installed in the environment, it is important to back up the database components for each product to protect against hardware or site failures. The methods to protect these databases are similar to Enterprise Vault databases.

Discovery Accelerator

Discovery Accelerator has the following databases:

- Configuration – By default the name of the database is EVConfiguration
- Custodian Manager – This optional database maintains a list of custodians, or users, in an Active Directory or Domino environment. There is one Custodian Manager database per Discovery Accelerator instance

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

- Customer – At least one customer database will be created for a Discovery Accelerator environment. This will contain case and research folder metadata. A Discovery Accelerator environment may have more than one customer database.

Compliance Accelerator

Compliance Accelerator has the following databases:

- Configuration – By default the name of the database is EVConfiguration
- Customer – At least one customer database will be created for a Compliance Accelerator environment. This will contain configuration information for the customer instance. A Compliance Accelerator environment may have more than one customer database.

Backing up Enterprise Vault Index and Vault Store Partition Locations

Developing a reliable backup solution for Enterprise Vault Index and Vault Store Partition locations is crucial for safeguarding valuable archived data. This section outlines the requirements for backing up archived content.

Enterprise Vault can be configured to use Safety Copies. Safety Copies provide a safety net in the event of a hardware failure of the Vault Store Partition(s). There are two methods for Safety Copies:

- Keeping the original item on the archiving target (Exchange, Domino, file servers, etc.)
- Newer versions of Enterprise Vault (11 and later) offer the Storage Queue option. The Storage Queue is located on an Enterprise Vault server and should use fast, redundant storage. During the archive process, archived items are temporarily stored in the Storage Queue and also stored in a Vault Store Partition. When using the Storage Queue, the original item on the target can be deleted immediately such as when archiving Exchange or Domino.

When a Vault Store Partition is successfully backed up, the safety copies will be removed by either deleting the original item on the archiving target (and optionally creating a shortcut or placeholder on the target) or removed from the Storage Queue (and optionally creating a shortcut or placeholder on the target)

Starting with Enterprise Vault 8.0, a new backup mechanism provides the Enterprise Vault administrator an easier way to back up data. Using the Enterprise Vault Administration Console or Enterprise Vault Management Shell (based on Windows PowerShell), the administrator can easily put Enterprise Vault indexes or Vault Stores into Backup Mode. Once the item is placed in Backup Mode, Index and Vault Store Partition locations can be safely backed up. Additional content will not be added or deleted to Enterprise Vault while in Backup Mode. Once a backup has completed, indexes or Vault Stores can be taken out of Backup Mode 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.

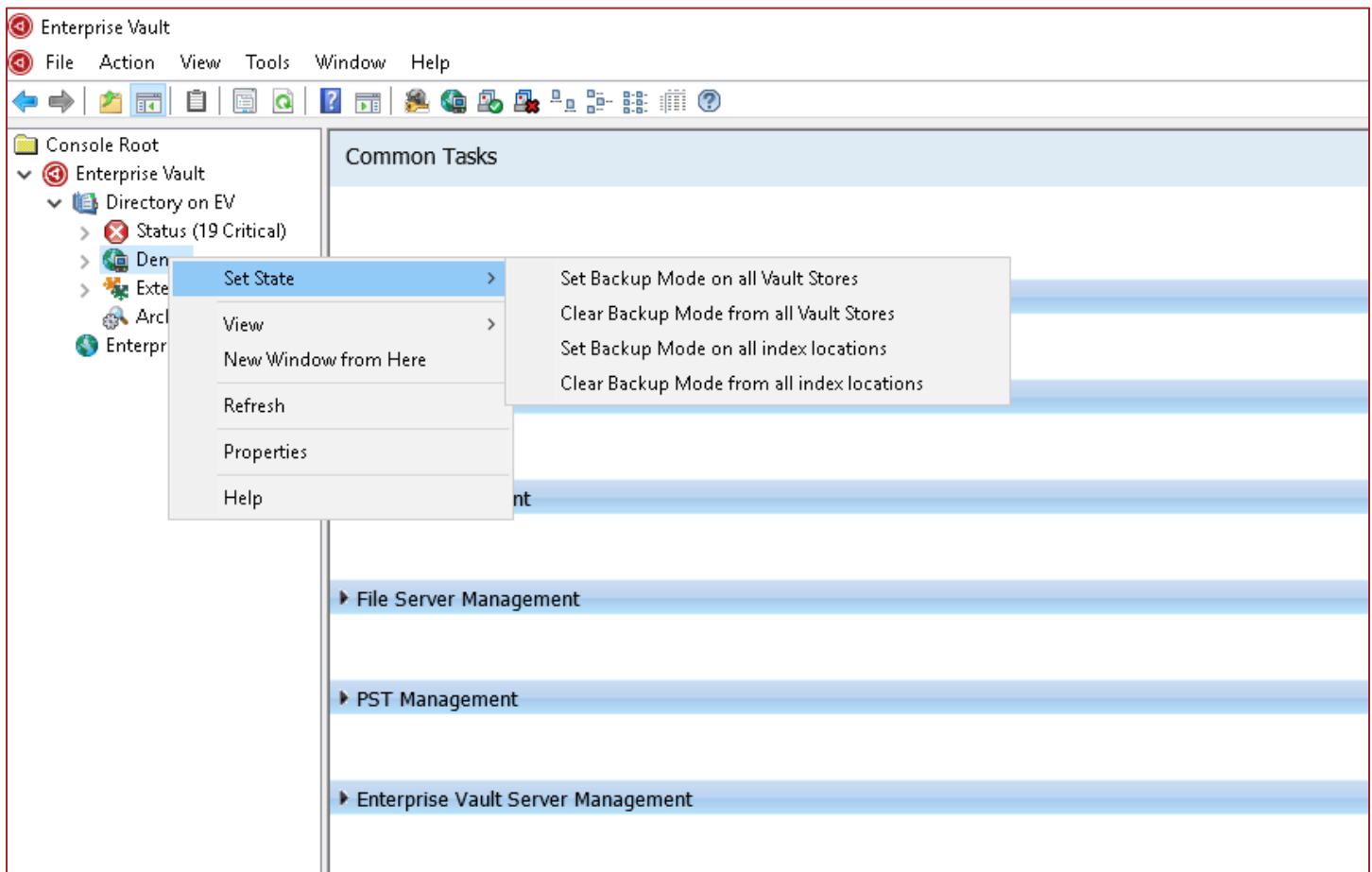
Setting and Clearing Backup Mode in the Enterprise Vault Administration Console

The Enterprise Vault Administration Console, or 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.

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator



Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

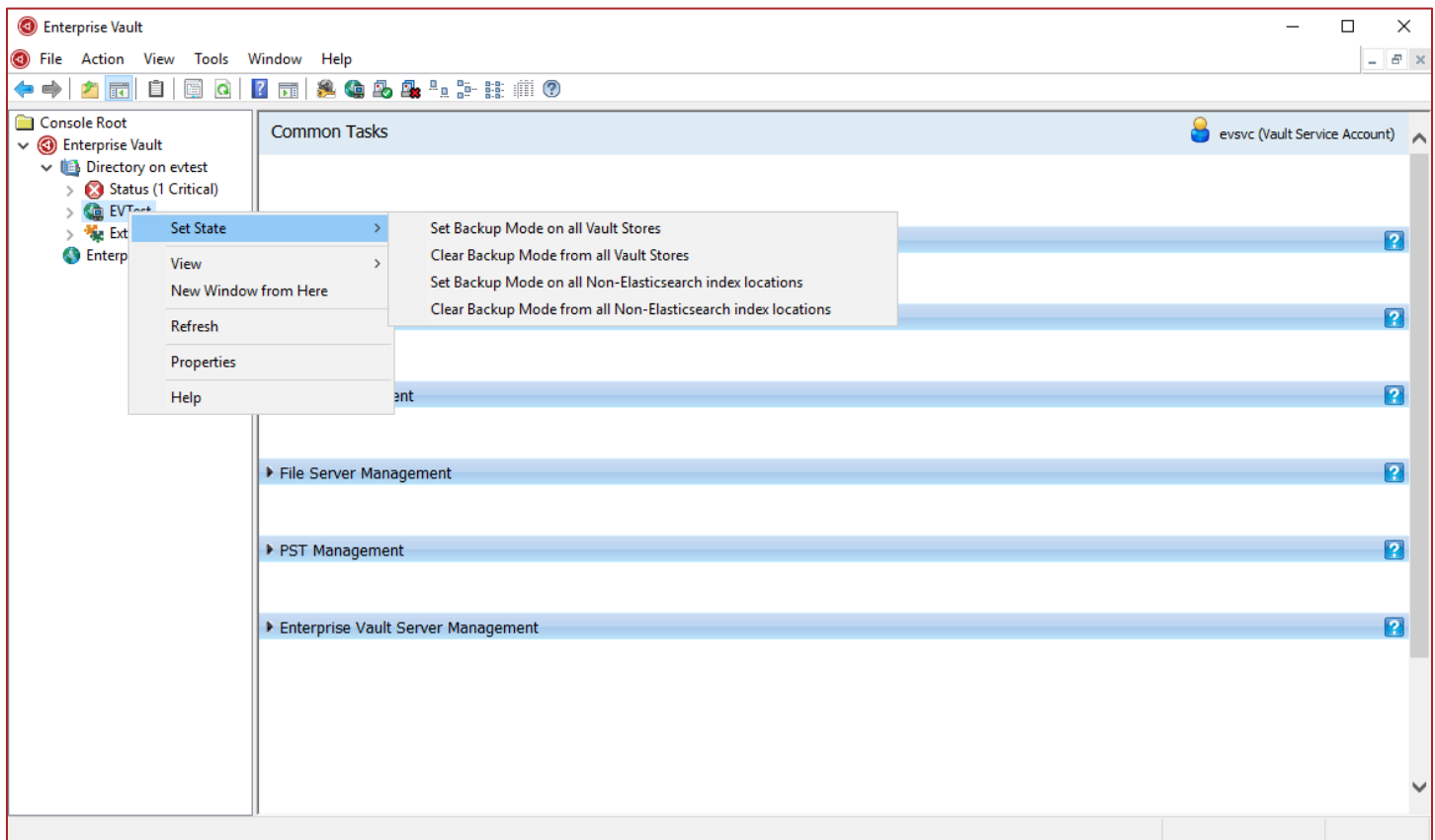


Figure 1 - Setting Backup Mode at the Site Level – Top Image: Prior to EV 14.2, Bottom Image: EV 14.2 and Later

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. For Enterprise Vault 14.2 and later, the index options are now called “Non-Elasticsearch”.

Selecting “Set Backup Mode” on Vault Stores or index locations at the site level places all contained items in that 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.

Note: For Enterprise Vault 14.2 and later, the option to set Backup Mode for Non-Elasticsearch indexes will not be available if there are no Non-Elasticsearch indexes available.

Setting and Clearing Backup Mode for a Specific Vault Store or Vault Store Group

Enterprise Vault 8.0 and later also offers the ability to put a specific Vault Store into Back Mode. This task is easily done by selecting the desired Vault Store or Vault Store Group, right-clicking on it, and selecting Set Backup Mode (Figure 2) or Set State -> Clear Backup Mode from all Vault Stores for a Vault Store Group (Figure 3).

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

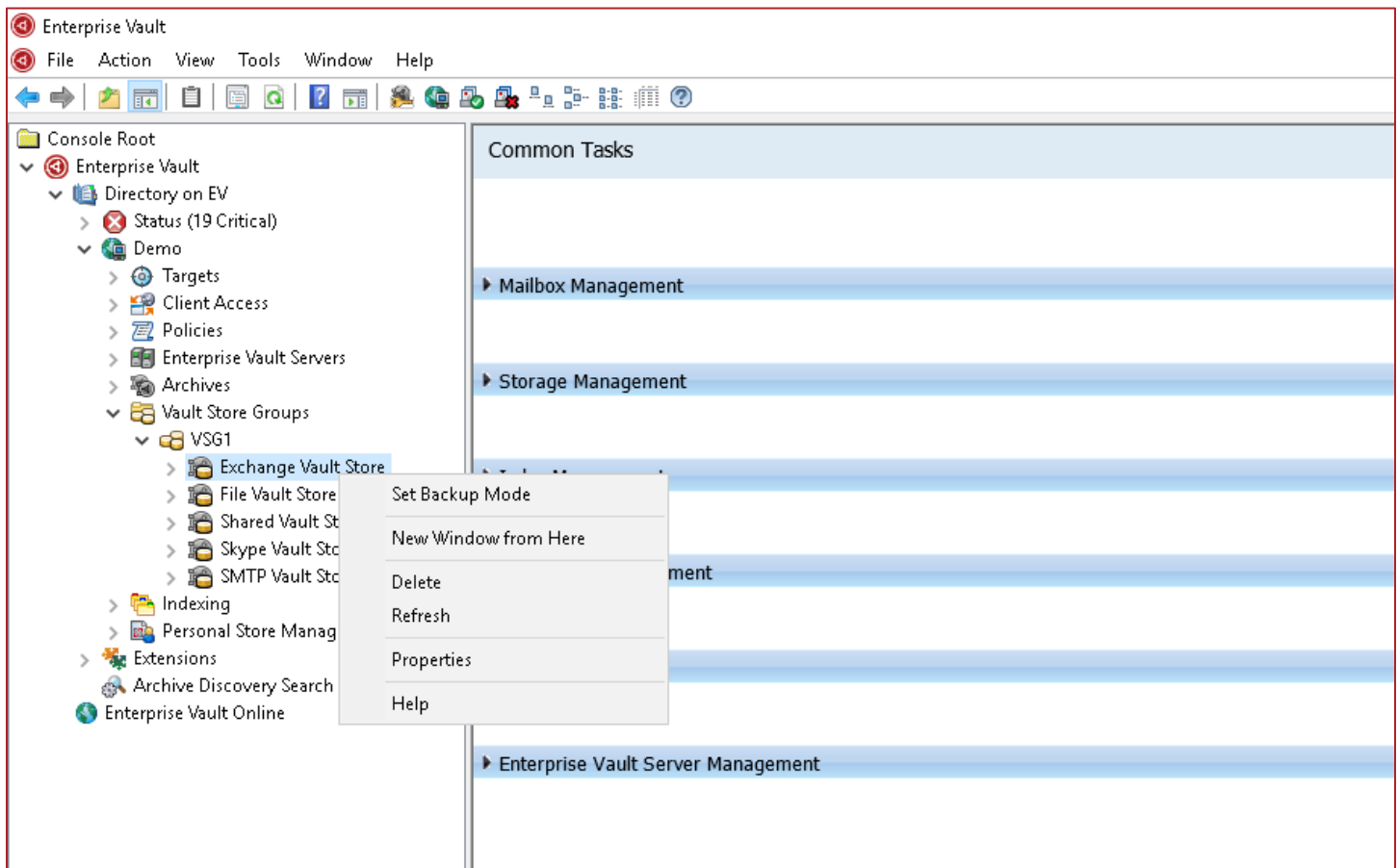


Figure 2 - Setting Backup Mode for a Vault Store

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 are available at a given time. Set Backup Mode noted in Figure 2 or Clear Backup Mode, as illustrated in Figure 3.

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

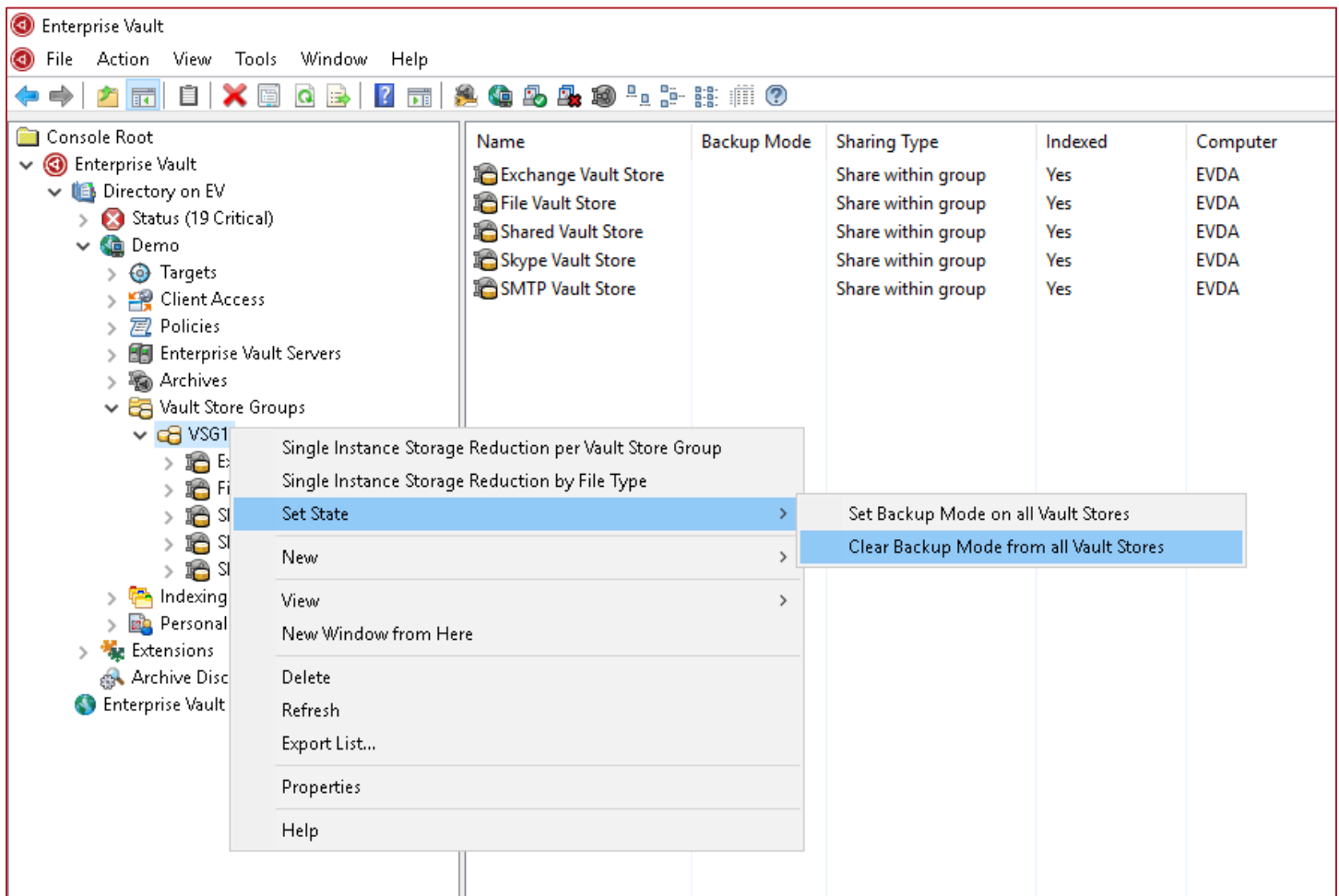


Figure 3 - Clearing Backup Mode on a Vault Store Group

Setting and Clearing Backup Mode for All Indexes/Non-Elasticsearch Indexes on an Enterprise Vault server

Setting and Clearing Backup Mode on all indexes on an 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. Note that for **Enterprise Vault 14.2 and later**, this is labelled as “Set Backup Mode on all Non-Elasticsearch index locations” and “Clear Backup Mode on all Non-Elasticsearch index locations”.

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

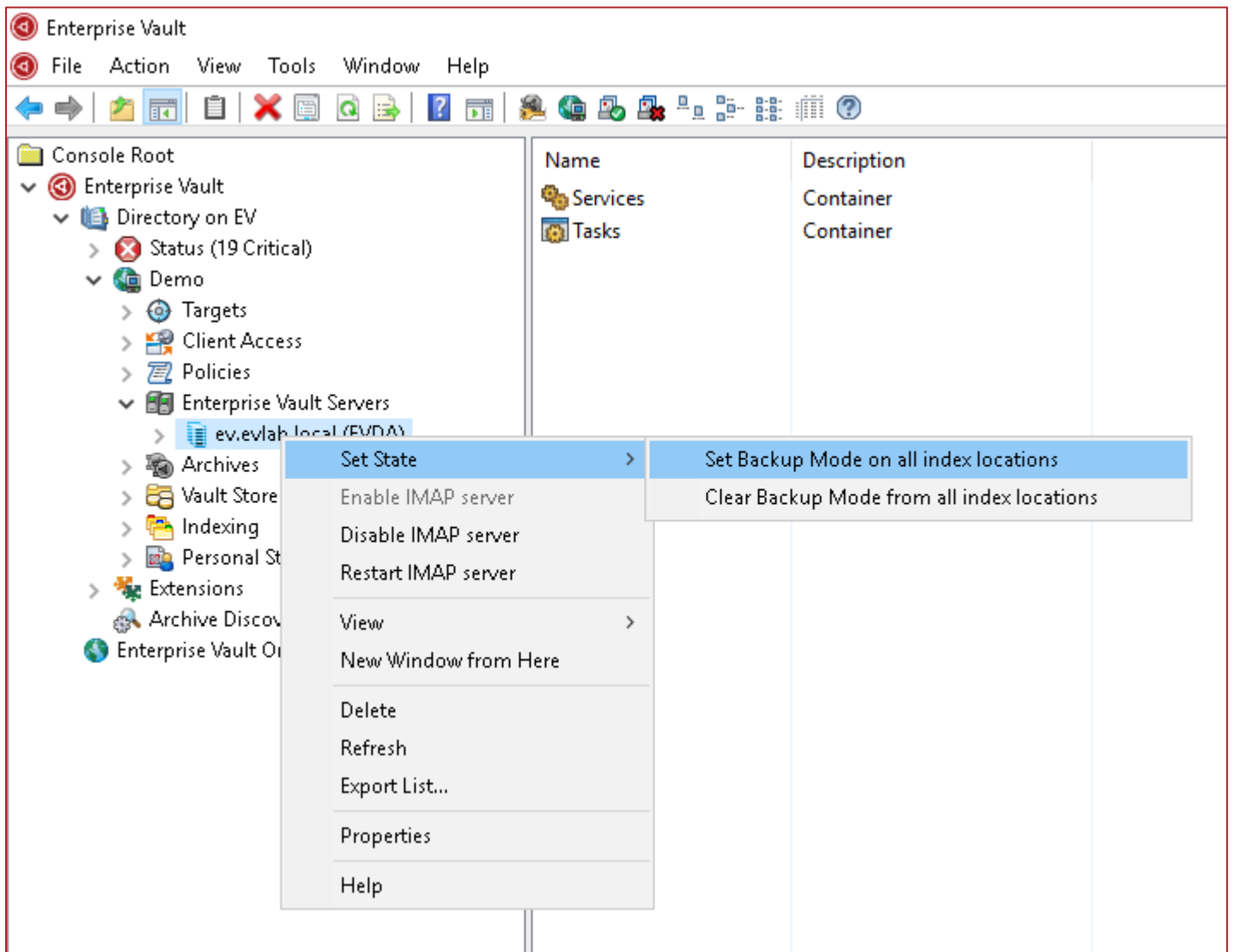


Figure 4 - Setting Backup Mode for All Indexes on an Enterprise Vault Server

Setting and Clearing Backup Mode for a Specific Index/Non-Elasticsearch Index Location on an Enterprise Vault Server

If an 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 later

- 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.

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

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

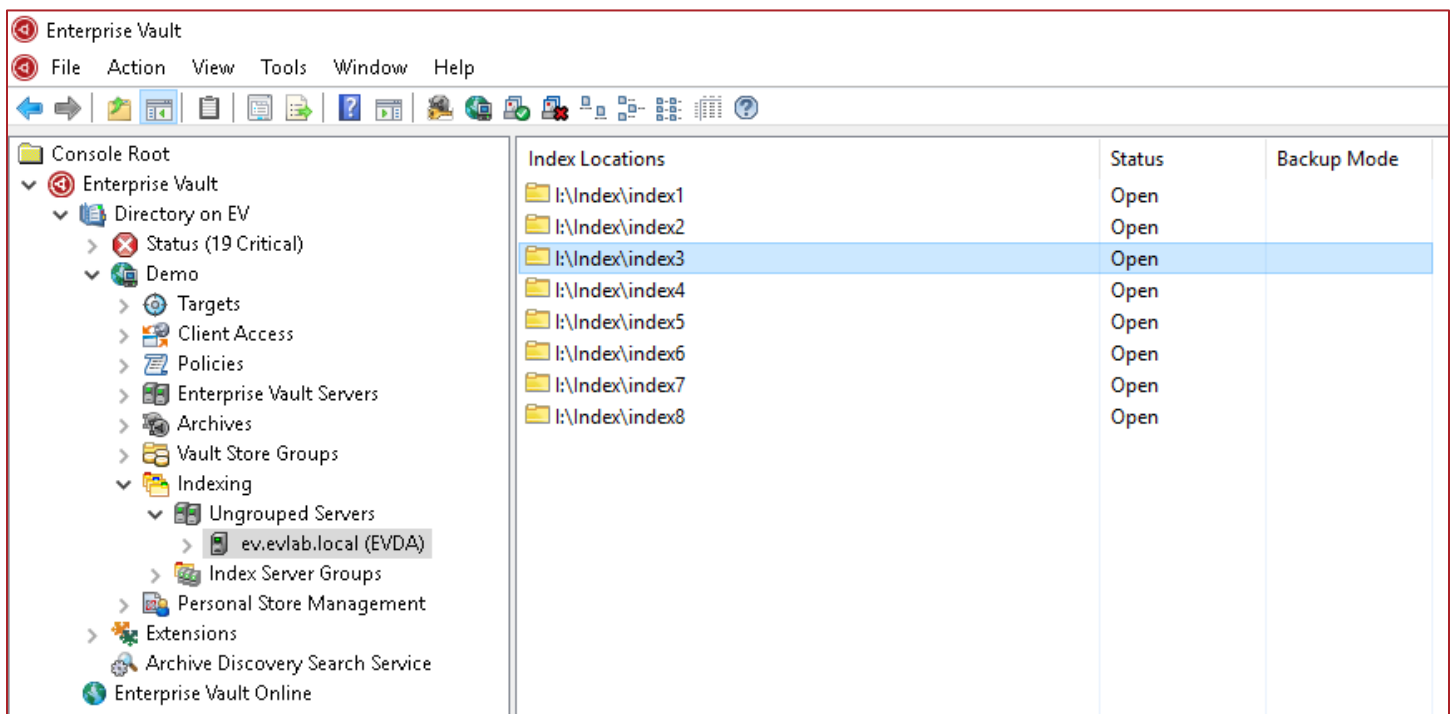


Figure 5 - Setting Backup Mode on an Index Location

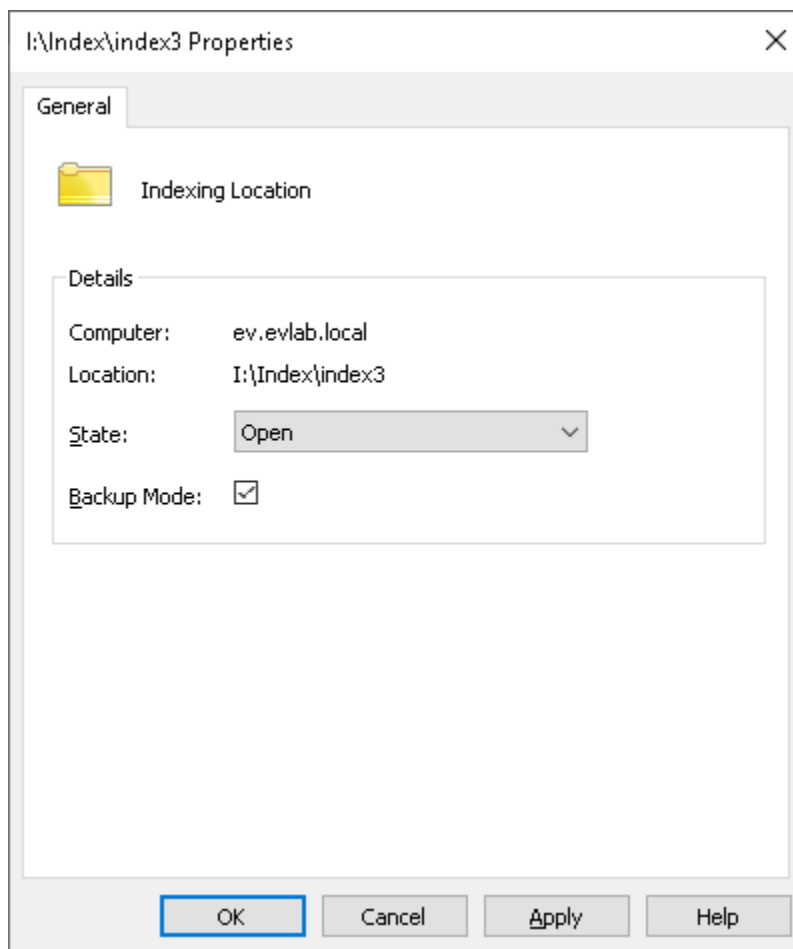


Figure 6 - Setting Backup Mode on an Index Location (EV 10 or Later)

Backing up Elasticsearch Indexes

Starting with Enterprise Vault 14.2, a new indexing engine was implemented that replaces the older 32-bit and 64-bit indexing engines. Elasticsearch requires a different approach for backups compared to the older indexing technologies.

If the Enterprise Vault environment was upgraded to 14.2, it is highly likely that there are non-Elasticsearch 64-bit indexes and potentially older non-Elasticsearch 32-bit indexes. These older indexes will still need to be backed up until the content is either expired, deleted, or upgraded to an Elasticsearch index using the methods described in this document.

If this is a new 14.2 or later installation, there will not be any 64-bit or 32-bit indexes. Therefore, it will be only necessary to configure backups for Elasticsearch indexes.

Differences between Older Indexes and Elasticsearch Indexes

Elasticsearch indexes differ from older index engines in the following ways:

- Elasticsearch does not support direct flat file backups and a direct restore of Elasticsearch index flat files will likely fail or have corrupted data
- Backup Mode is not applicable to an Elasticsearch index location
- Backing up of Elasticsearch indexes requires the use of snapshots
 - The snapshots are essentially dumps of the index and placed in a separate location
 - These file dumps can then be backed up and used to restore the index if needed

Rules of Thumb for Elasticsearch Snapshot Locations

Keep the following in mind when setting up a Elasticsearch snapshot location

- A snapshot location must be defined before Elasticsearch indexes can be properly backed up
- Elasticsearch snapshot locations should be placed on a separate volume from the Elasticsearch index location. The volume can be locally attached to the Enterprise Vault Server or on a network share. It is recommended to use a network share.
- The size of the snapshot volume should be at least the same size of the volume holding the Elasticsearch indexes. If the snapshot volume becomes full, additional snapshot volumes can be created. The old snapshot volume will be placed in read-only mode.
- The first snapshot in a snapshot location will be a full copy of the current Elasticsearch index. Subsequent snapshots will be incremental. The same is true if the version of Elasticsearch is upgraded (such as when upgrading to a future version of Enterprise Vault).
- The Enterprise Vault Service Account (VSA) must have read and write access to the snapshot location
- Elasticsearch snapshot locations can hold up to 500 snapshots. The Enterprise Vault administrator will receive warnings when the snapshot count is over 400. See the **Enterprise Vault PowerShell Cmdlets** guide for more information on managing Elasticsearch snapshots.

Creating and Locating Elasticsearch Snapshot Locations

Snapshot locations are managed using the Enterprise Vault Management Shell. A PowerShell cmdlet named **Set-EVIndexSnapshotLocation** is used to create snapshot locations. Once a snapshot location is configured, it will be necessary to restart the Enterprise Vault Indexing service. The options for this cmdlet include:

- **-EVServerName <string>** - The name of the Enterprise Vault index server for which you want to configure an index snapshot location with the specified path. If you omit this parameter, Set-EVIndexSnapshotLocation uses the host name of the Enterprise Vault index server where the command is running. The FQDN must be used for the name of the Enterprise Vault server.
- **-SnapshotLocationPath <string>** - The path of the directory you want to configure for taking snapshots of the indexing data.
- **-WhatIf** - The WhatIf switch instructs the command to simulate the actions that it would take on the object. By using the WhatIf switch, you can preview the changes that would occur without applying any of those changes. You do not need to specify a value with the WhatIf switch.

Examples:

The following defines a snapshot location on the server “evserver” on a locally attached volume:

```
Set-EVIndexSnapshotLocation -EVServerName evserver.local -SnapshotLocationPath  
"J:\SnapShot"
```

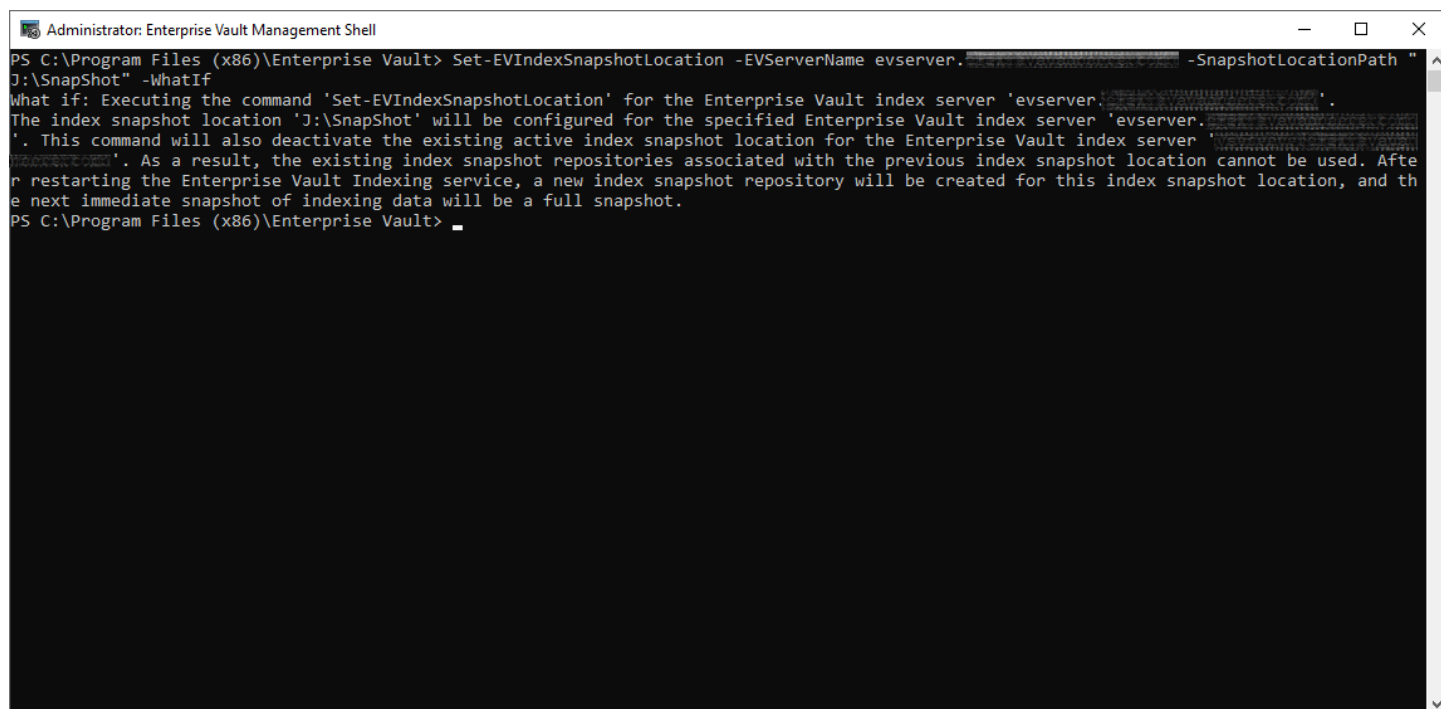
The following defines a snapshot location on the server “evserver” using a network share:

```
Set-EVIndexSnapshotLocation -EVServerName evserver.local -SnapshotLocationPath  
"\\fileserver\snapshots\SnapShot1"
```

The following performs a “What If”

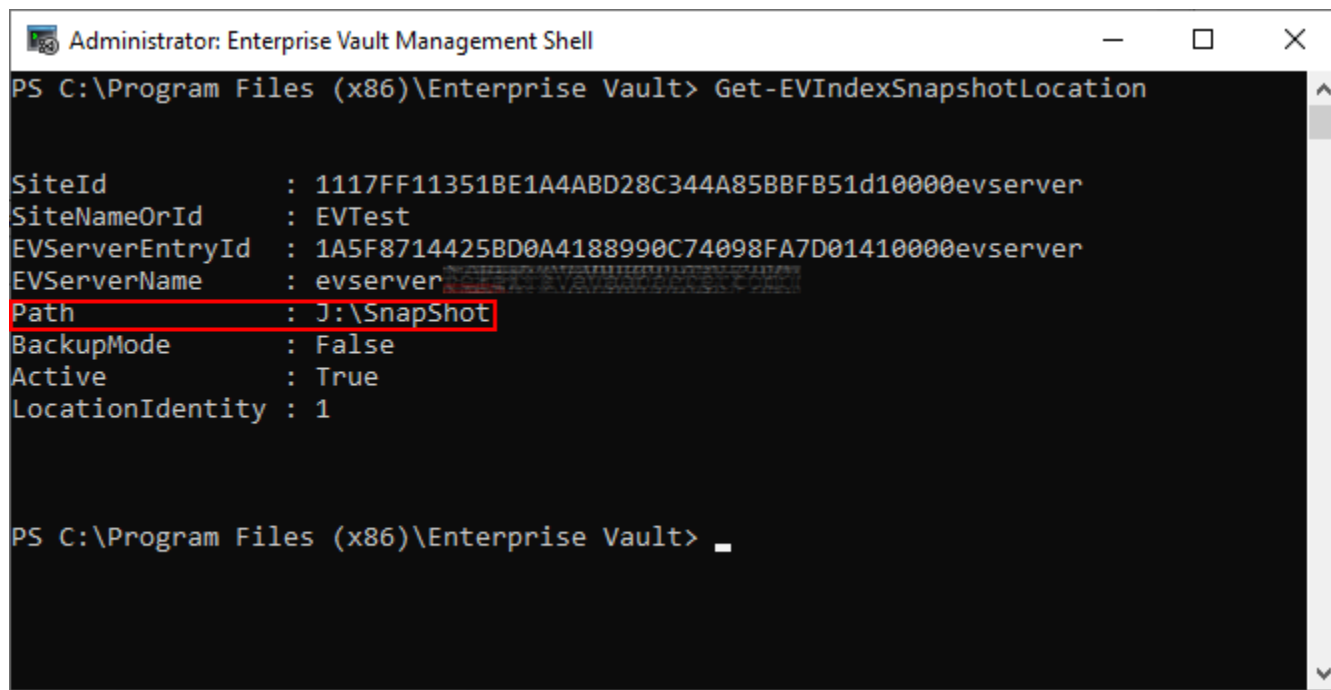
Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

```
Set-EVIndexSnapshotLocation -EVServerName evserver.local -SnapshotLocationPath "J:\SnapShot" -WhatIf
```



The screenshot shows a Windows command prompt window titled "Administrator: Enterprise Vault Management Shell". The command prompt is at the directory "PS C:\Program Files (x86)\Enterprise Vault". The command entered is "Set-EVIndexSnapshotLocation -EVServerName evserver.local -SnapshotLocationPath 'J:\SnapShot' -WhatIf". The output shows a confirmation message: "What if: Executing the command 'Set-EVIndexSnapshotLocation' for the Enterprise Vault index server 'evserver.local'. The index snapshot location 'J:\SnapShot' will be configured for the specified Enterprise Vault index server 'evserver.local'. This command will also deactivate the existing active index snapshot location for the Enterprise Vault index server 'evserver.local'. As a result, the existing index snapshot repositories associated with the previous index snapshot location cannot be used. After restarting the Enterprise Vault Indexing service, a new index snapshot repository will be created for this index snapshot location, and the next immediate snapshot of indexing data will be a full snapshot." The prompt then returns to "PS C:\Program Files (x86)\Enterprise Vault>".

To find existing Elasticsearch snapshot locations, use `Get-EVIndexSnapshotLocation`. Note the Path as this will be needed later in order to back up the location.



The screenshot shows the same "Administrator: Enterprise Vault Management Shell" window. The command entered is "Get-EVIndexSnapshotLocation". The output displays the following properties for the index server:

SiteId	: 1117FF11351BE1A4ABD28C344A858BFB51d10000evserver
SiteNameOrId	: EVTest
EVServerEntryId	: 1A5F8714425BD0A4188990C74098FA7D01410000evserver
EVServerName	: evserver
Path	: J:\SnapShot
BackupMode	: False
Active	: True
LocationIdentity	: 1

The prompt then returns to "PS C:\Program Files (x86)\Enterprise Vault>".

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

Creating an Elasticsearch Snapshot

Before backing up the Elasticsearch snapshot location, it will be necessary to create a snapshot to include the latest changes to the Elasticsearch index location. This is performed by using the **New-EVIndexSnapshot** cmdlet.

This cmdlet creates a snapshot of the Elasticsearch index location. The first snapshot on a newly created snapshot location will be a full copy of the current index. A full snapshot will also be created if the version of Elasticsearch is upgraded (such as when upgrading to a future version of Enterprise Vault). Subsequent snapshots will be incremental. The options for this cmdlet include:

- **-SiteId** - The ID of the Enterprise Vault site for which you want to create the snapshots of index data on all the Enterprise Vault index servers in that site. If you omit this parameter, New-EVIndexSnapshot retrieves the SiteId from the Enterprise Vault index server specified as EVServerName parameter; otherwise, it uses the SiteId of the Enterprise Vault index server where the command is running. You can use the Get-EVSite command to obtain the SiteId.
- **-EVServerName <String>** - The name of the Enterprise Vault index server for which you want to create the snapshot of index data. If you omit this parameter, New-EVIndexSnapshot uses the host name of the Enterprise Vault index server where the command is running. You can use the Get-EVComputers command to obtain the Enterprise Vault server name. The FQDN of the Enterprise Vault server must be used.
- **-IgnoreUnavailable** - (Optional, Boolean) If false, the command returns an error for any data stream or index that is missing or closed. Defaults to false. If true, the command ignores data streams and indices those are missing or closed.
- **-IncludeGlobalState** - (Optional, Boolean) If true, the current global state of Elasticsearch cluster running on Enterprise Vault index server is included in the snapshot. Defaults to false.
- **-Confirm** - (Optional, Boolean) The default value is **\$true**. If true, the user executing the cmdlet will have to confirm whether or not to execute the operation. If using this in a script, specify **-Confirm:\$false**.

Examples:

The following creates an index snapshot on the current server where the command is executed:

```
New-EVIndexSnapshot
```

The following creates an index snapshot on the Enterprise Vault index server named 'ev.domain.local' and will not ask for confirmation. A FQDN for the Enterprise Vault server must be specified:

```
New-EVIndexSnapshot -EVServerName ev.domain.local -Confirm:$false
```

The following creates index snapshots for all Enterprise Vault index server under the site 'site.domain.com'

```
New-EVIndexSnapshot New-EVIndexSnapshot -SiteId site.domain.com
```

The following creates an index snapshot of the Enterprise Vault index server 'ev.domain.local', if IgnoreUnavailable is set to false, the command returns an error for any data stream or index that is missing or closed. If true, the command ignores data streams and indices in indices that are missing or closed.

```
New-EVIndexSnapshot -EVServerName ev.domain.local -IgnoreUnavailable
```

The use of the **New-EVIndexSnapshot** cmdlet can be used in pre-backup scripts. Ensure to specify **-Confirm:\$false** so that confirmation is not required.

Setting and Clearing Backup Mode Using the Enterprise Vault Management Shell

Enterprise Vault 8 and later offers a PowerShell option that allows the administrator to control Backup Mode for Enterprise Vault through the use of scripting. This option 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).

NOTE: Keep in mind that Elasticsearch index locations (Enterprise Vault 14.2 and later) cannot be placed in Backup Mode. Please read the section in this document entitled **Backing up Elasticsearch Indexes**.

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

https://www.veritas.com/content/support/en_US/doc/95957167-136587294-0/v35699192-136587294

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 in the default browser as shown in Figure 7.

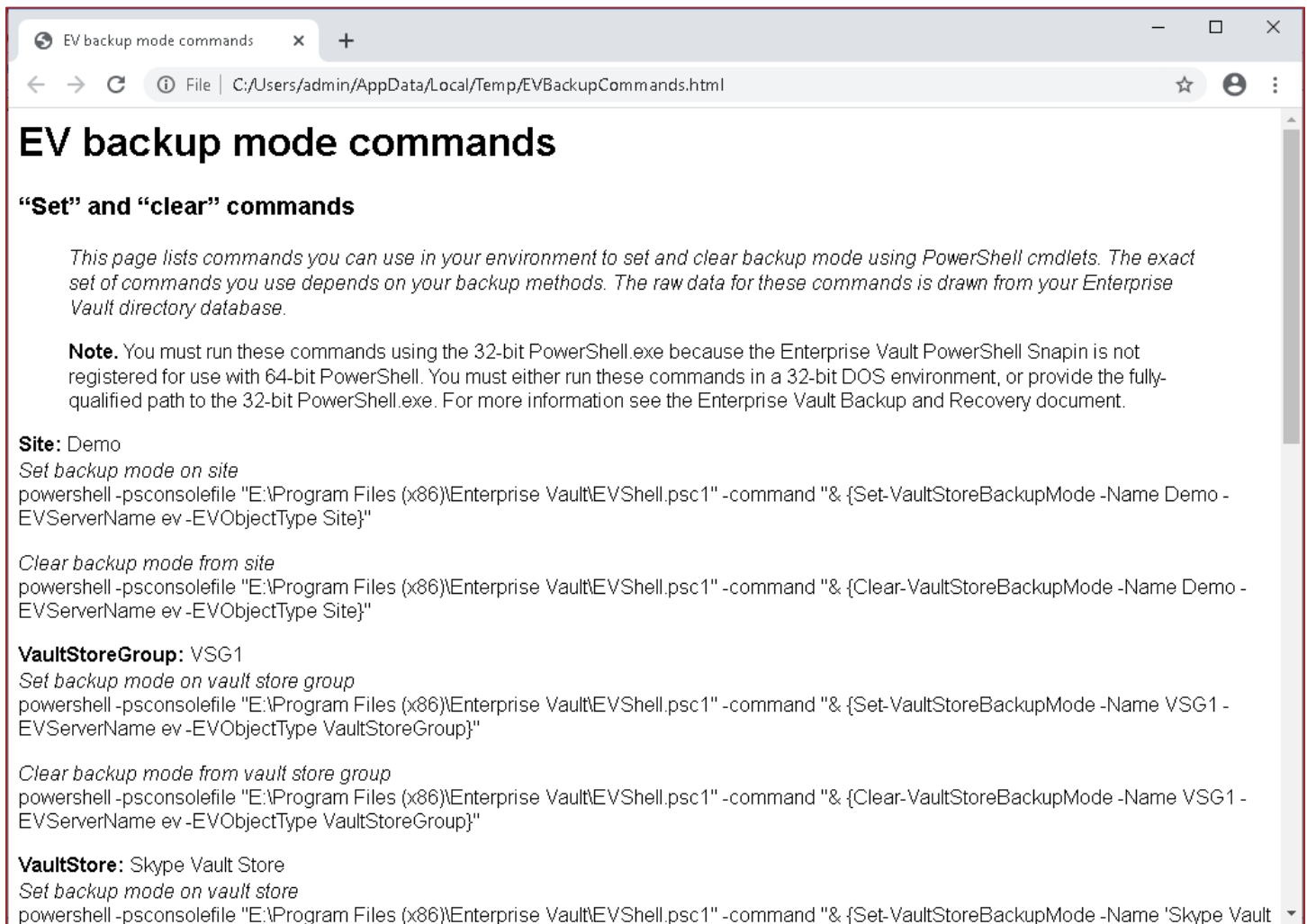


Figure 7 - TransformBackup.ps1 Script Output Example

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:

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

```
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

Commercial backup software usually 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.

NOTE: if your environment does not have any 32-bit or 64-bit indexes (such as when Enterprise Vault was originally installed with version 14.2 or later), it is not necessary to run PowerShell scripts to control Backup Mode for indexes.

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

Pre-Backup.bat:

```
%SystemRoot%\syswow64\WindowsPowerShell\v1.0\powershell.exe -PSConsole "C:\Program Files\Enterprise Vault\evshell.psc1" set-indexlocationbackupmode EVServer1 'life line'

%SystemRoot%\syswow64\WindowsPowerShell\v1.0\powershell.exe -PSConsole "C:\Program Files\Enterprise Vault\evshell.psc1" set-vaultstorebackupmode 'life line' EVServer1 Site
```

If running Enterprise Vault 14.2 or later, include the following to create an Elasticsearch snapshot:

```
%SystemRoot%\syswow64\WindowsPowerShell\v1.0\powershell.exe -PSConsole "C:\Program Files\Enterprise Vault\evshell.psc1" new-evindexsnapshot -EVServerName evserver1.site.domain -confirm:$false
```

Post-Backup.bat:

```
%SystemRoot%\syswow64\WindowsPowerShell\v1.0\powershell.exe -PSConsole "C:\Program Files\Enterprise Vault\evshell.psc1" clear-indexlocationbackupmode EVServer1 'life line'

%SystemRoot%\syswow64\WindowsPowerShell\v1.0\powershell.exe -PSConsole "C:\Program Files\Enterprise Vault\evshell.psc1" clear-vaultstorebackupmode 'life line' EVServer1 Site
```

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, Veritas recommends that the Storage Queue be configured to use high-speed, highly redundant disk. It is recommended to back up this location using a daily, full backup job. 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 Enterprise Vault 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 and 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 Veritas InfoScale 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 and perform an Elasticsearch snapshot (EV 14.2 and later)
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: https://www.veritas.com/content/support/en_US/article.100016637. Figure 8 shows how set up a Vault Store partition to use a trigger file with Enterprise Vault 9 and later:

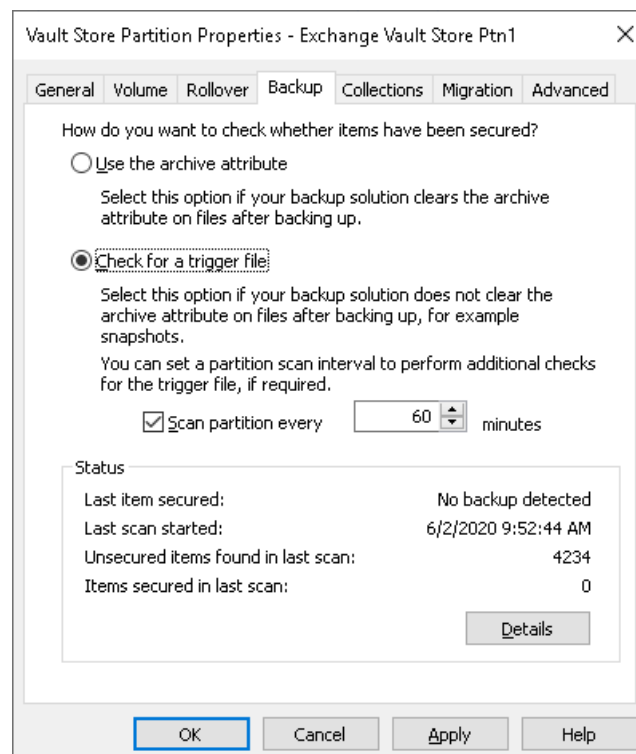


Figure 8 - Configuring a Vault Store Partition to Use Trigger Files

Back up 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)
- Elasticsearch snapshot locations (EV 14.2 and later)

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

Virtual Machine Backups

If the Enterprise Vault or Microsoft SQL Server servers are running in a virtual environment (such as Microsoft Hyper-V or VMware ESXi), the virtual machines can be backed up in whole. Ensure the backup software solution can clear transaction logs on the Microsoft SQL Server virtual machine as part of the backup. Perform the following steps before the virtual machines are backed up:

- Place Enterprise Vault into Backup Mode for Indexes and Vault Stores. This can be performed using PowerShell commands on the Enterprise Vault server instance such as in a script. The script can be scheduled to run minutes before the backup is scheduled to run.
- Ensure to take an Elasticsearch snapshot (EV 14.2 and later). This can be performed using PowerShell commands on the Enterprise Vault server instance such as in a script. The script can be scheduled to run minutes before the backup is scheduled to run.

After backups have completed, take the Enterprise Vault server out of Backup Mode using PowerShell commands on the Enterprise Vault server instance.

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 where possible. 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 lesser intervals. The retention period for a backup image of closed partitions should be 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, storage, and Elasticsearch snapshots (EV 14.2 and later), 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 may be encountered.

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

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.

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 Veritas 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 and later¹ 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 and later 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 “Veritas 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.

Please also ensure that the version of Enterprise Vault being used is supported by the version of NetBackup in use. Please see the NetBackup Application/Database Agent Compatibility list here:

https://www.veritas.com/support/en_US/article.100040093

Note about Using bpstart_notify Scripts

A bpstart_notify script, when present on the client, will run each time a backup starts. The script runs before the backup of any data begins. The script must exit with a status of 0 or the backup will fail.

For more information on bpstart_notify scripts, see:

https://www.veritas.com/content/support/en_US/doc/24437881-126559615-0/v41507490-126559615.

¹ Please see the NetBackup compatibility guide for more information on the versions of Enterprise Vault supported

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

NetBackup will, by default, attempt to use Microsoft VSS (Volume Shadow Copy Service) when backing up Windows clients. Using VSS snapshots provide a point-in-time snapshot of a volume. The VSS snapshot will take place before the execution of any bpstart_notify file.

Many of the backup scenarios when using NetBackup in this whitepaper reference a bpstart_notify script to place Enterprise Vault into Backup Mode. There may be the potential for data loss between the time that a VSS snapshot is performed and when the bpstart_notify script is executed.

For example, the following events occur:

1. A backup starts and a VSS snapshot is created for an EV Vault Store Partition.
2. Enterprise Vault archives an email via SMTP or Exchange journal archiving.
3. The bpstart_notify script executes and places Enterprise Vault into Backup Mode.

The VSS snapshot will not contain the newly archived email as it was archived after the creation of the VSS snapshot. If a restore from this backup is required, that email would not be restored as it would not be contained in the backup set.

To eliminate this potential data loss, it is recommended to use Windows Task Scheduler to control Backup Mode of Vault Stores and Index Volumes. For example, a backup for Enterprise Vault is scheduled at 2:00AM. Windows Task Scheduler is set up to run at 1:58AM to put EV into Backup Mode and at 2:10 AM, Windows Task Scheduler runs to take EV out of Backup Mode. Here is a detailed chain of events:

- 1:58AM – Windows Task Scheduler runs a script to put EV into Backup Mode
- 2:00AM – NetBackup kicks off backup jobs to back up Vault Store Partitions, EV databases, Index Locations, and other recommended Enterprise Vault components
- 2:10AM – Windows Task Scheduler runs a script to take EV out of Backup Mode. NetBackup continues to back up data from the VSS snapshot. Normal Enterprise Vault operations can resume while the backup is ongoing.

The contents of the scripts executed by Windows Task Scheduler can be the same as bpstart_notify and bpend_notify scripts to control Enterprise Vault Backup Mode and manage trigger files as detailed in the scenarios outlined in this whitepaper.

Backup Scenario #1: Using file level backups

This environment contains one Enterprise Vault server with one index location, two Vault Store partitions, Storage Queue, a Veritas Information Classifier (VIC) directory, an Elasticsearch snapshot volume (EV 14.2 and later) and other locations to back up.

Sample Policy: EV

Attributes:

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

The screenshot displays the 'Change Policy - EV' window, which is used for configuring backup policies. The window has a title bar with a close button (X) and a server address bar showing 'Server: nbu2.f...'. Below the title bar are four tabs: 'Attributes' (selected), 'Schedules', 'Clients', and 'Backup Selections'.

The 'Attributes' tab is divided into several sections:

- Policy type:** A dropdown menu set to 'MS-Windows'.
- Destination:** A group box containing:
 - Data classification:** A dropdown menu set to '<No data classification>'.
 - Policy storage:** A dropdown menu set to 'Any_available'.
 - Policy volume pool:** A dropdown menu set to 'NetBackup'.
- Checkpoints and Priority:** A group box containing:
 - Take checkpoints every:** A numeric input field set to '0' with a unit of 'minutes'.
 - Limit jobs per policy:** A numeric input field.
 - Job priority:** A numeric input field set to '0' with a note '(higher number is greater priority)'.
 - Media Owner:** A dropdown menu set to 'Any'.
- Snapshot Client and Replication Director:** A group box containing:
 - ☐ Perform block level incremental backups
 - ☒ Use Replication Director
 - ☐ Enable vendor change tracking for incremental backups
 - ☒ Perform snapshot backups (with an 'Options...' button)
 - ☐ Retain snapshot for Instant Recovery or SLP management
 - ☐ Hyper-V server: (with a text input field)
 - ☐ Perform off-host backup
 - Use:** (with a dropdown menu)
 - Machine:** (with a dropdown menu)
- Go into effect at:** A date and time picker set to 'Sep 15, 2021 10:16:58 AM'.
- Backup options:** A group of checkboxes:
 - ☐ Backup network drives
 - ☐ Cross mount points
 - ☐ Compress
 - ☐ Encrypt
- Collect disaster recovery information for:** A group of checkboxes:
 - ☐ Bare Metal Restore
 - ☐ Collect true image restore information
 - ☐ with move detection

(Required for synthetic backups and Bare Metal Restore)
- ☐ Allow multiple data streams
- ☐ Disable client-side deduplication
- ☐ Enable granular recovery
- ☐ Use Accelerator
- ☐ Enable optimized backup of Windows deduplicated volumes

- Keyword phrase (optional):** A text input field.
- Microsoft Exchange Server Attributes:** A group box containing:
- Exchange DAG or Exchange 2007 replication (LCR/CCR):** A dropdown menu.
- Database backup source:** A dropdown menu.
- Preferred server list...** (with a note '(Exchange DAG only)')
- Dynamic Data Streaming Attributes:** A group box containing:
- ☐ Allow Dynamic Streaming
- Maximum number of streams per volume:** A numeric input field set to '4'.
- Maximum number of files in a batch:** A numeric input field set to '300'.

At the bottom of the window are three buttons: 'OK', 'Cancel', and 'Help'.

Figure 9 - File-level Backup Attributes

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

Schedules:

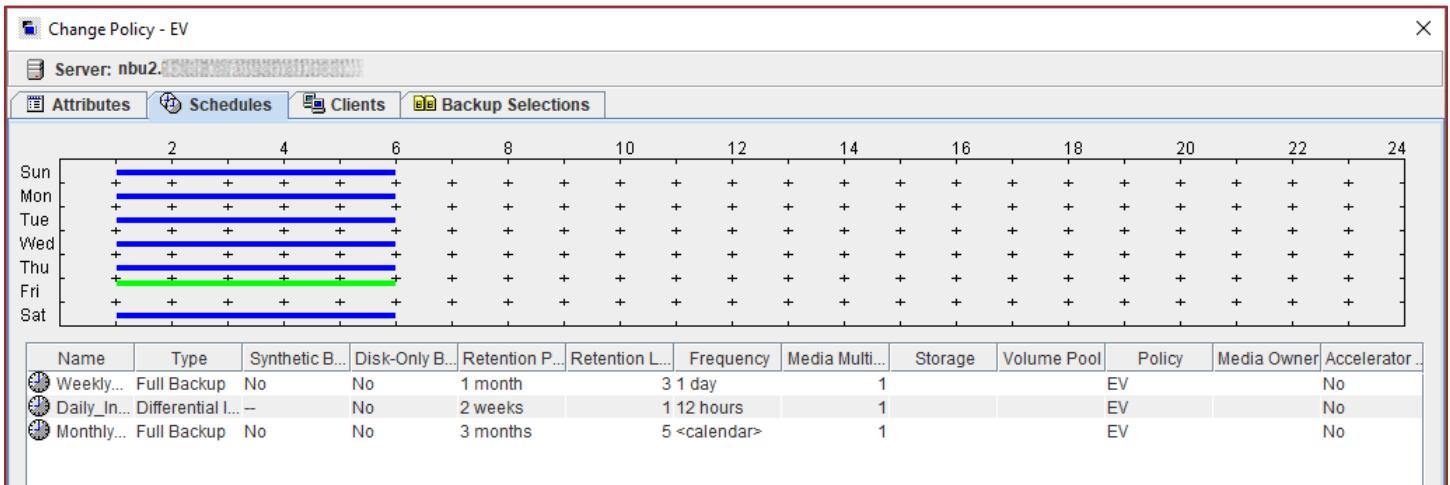


Figure 10 – File-level Backup Schedules

Clients:

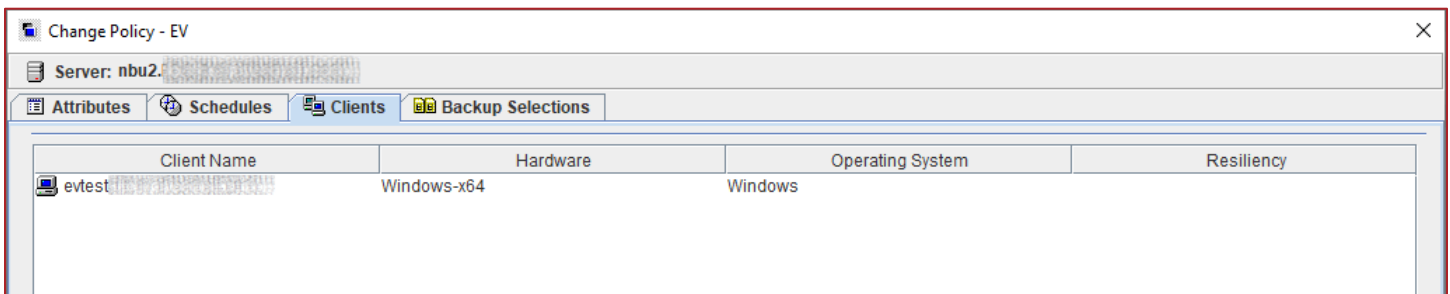


Figure 11 – File-level Backup Clients

Backup Selections (this example shows local and remote Index and Vault Store partition locations as well as other EV components):

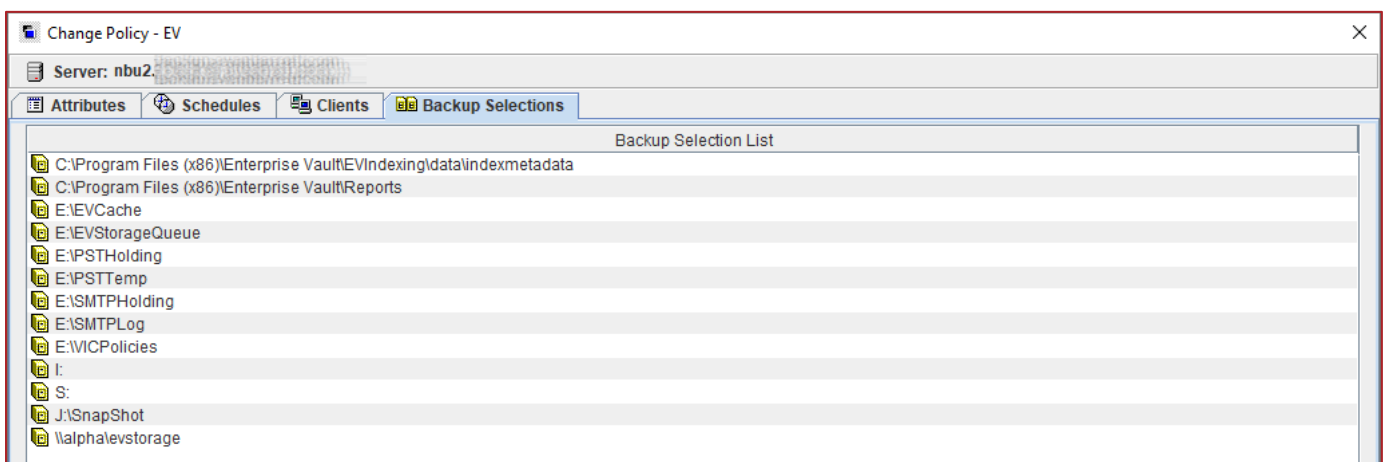


Figure 12 - File-level Backups Backup Selections

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

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 \\alpha\evstorage in the example), the NetBackup Client Service should run with a service account that has read and 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 **“Error! Reference source not found.”**.

See “Note about Using bpstart_notify Scripts” about precautions.

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 a 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.

Backup Scenario #2: Using the NetBackup Enterprise Vault Backup Agent

Sample Environment

- Three Enterprise Vault 12 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 2012 server with the following databases:
 - Directory database
 - Vault Store databases
 - Fingerprint database for VSG1
 - Auditing database
 - FSA Reporting databases
 - Monitoring database

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

Proposed Backup Policies

This sample environment has five backup policy configurations:

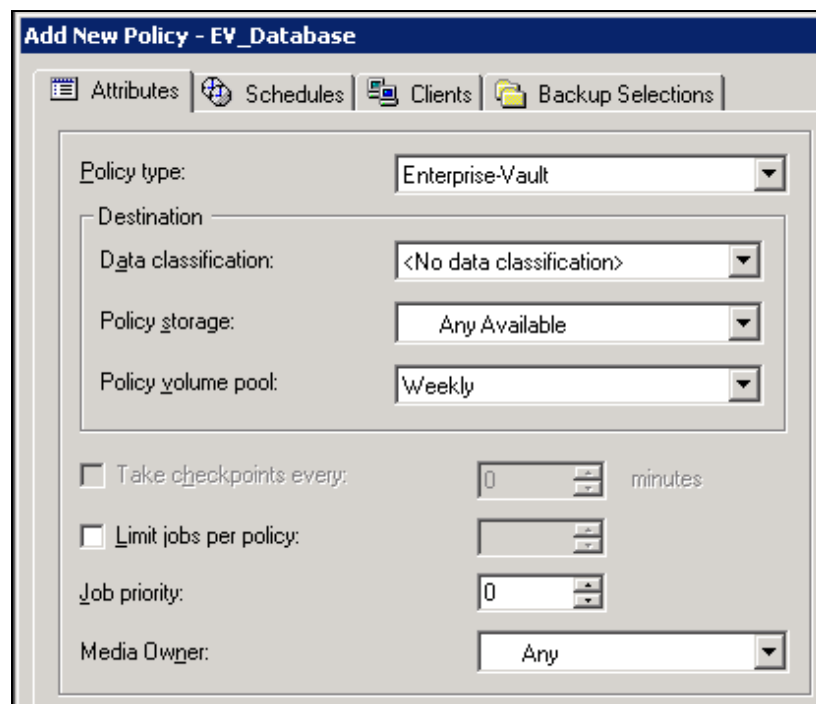
- One policy to back up the Enterprise Vault Directory, Monitoring, FSA Reporting, and Auditing databases
- One policy for each Enterprise Vault server to back up open Vault Store Partitions as well as their corresponding Vault Store SQL databases
- One policy to back up index locations
- One policy for each Enterprise Vault server to back up closed and ready Vault Store Partitions
- One policy for backing up the Storage Queue, the Enterprise Vault installation directory, and the VIC policies share location (EV 12.2 and later)

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



The screenshot shows a dialog box titled "Add New Policy - EV_Database". It has four tabs: "Attributes", "Schedules", "Clients", and "Backup Selections". The "Attributes" tab is selected. The dialog contains the following fields and options:

- Policy type:** A dropdown menu set to "Enterprise-Vault".
- Destination:** A section containing four sub-fields:
 - Data classification:** A dropdown menu set to "<No data classification>".
 - Policy storage:** A dropdown menu set to "Any Available".
 - Policy volume pool:** A dropdown menu set to "Weekly".
- Take checkpoints every:** A checkbox that is unchecked, followed by a numeric input field set to "0" and the text "minutes".
- Limit jobs per policy:** A checkbox that is unchecked, followed by a numeric input field.
- Job priority:** A numeric input field set to "0".
- Media Owner:** A dropdown menu set to "Any".

Figure 13 - EV_Database Policy Attributes

Schedules:

- Weekly Full
- Daily Incremental

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

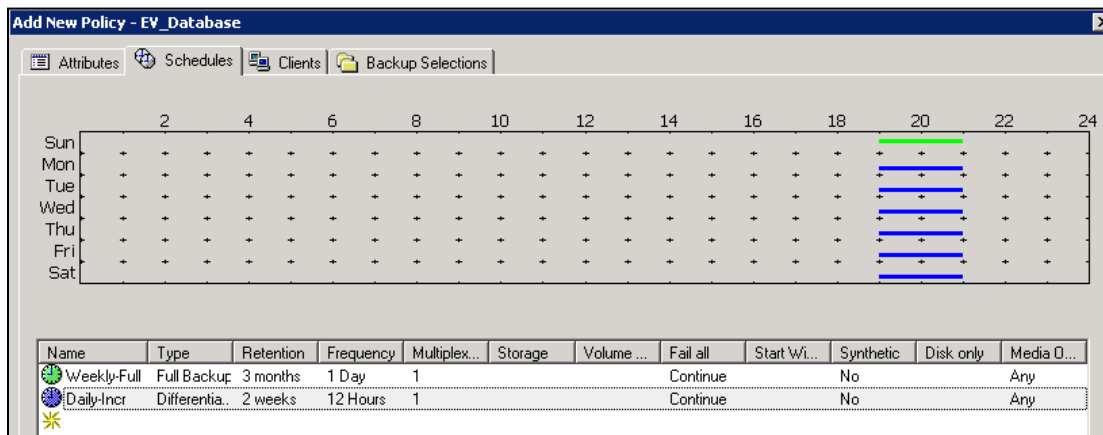


Figure 14 – EV_Database Policy Schedules

Client:

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

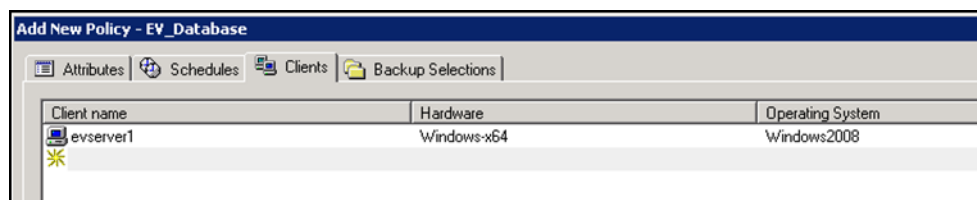


Figure 15 - EV_Database Policy Clients

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

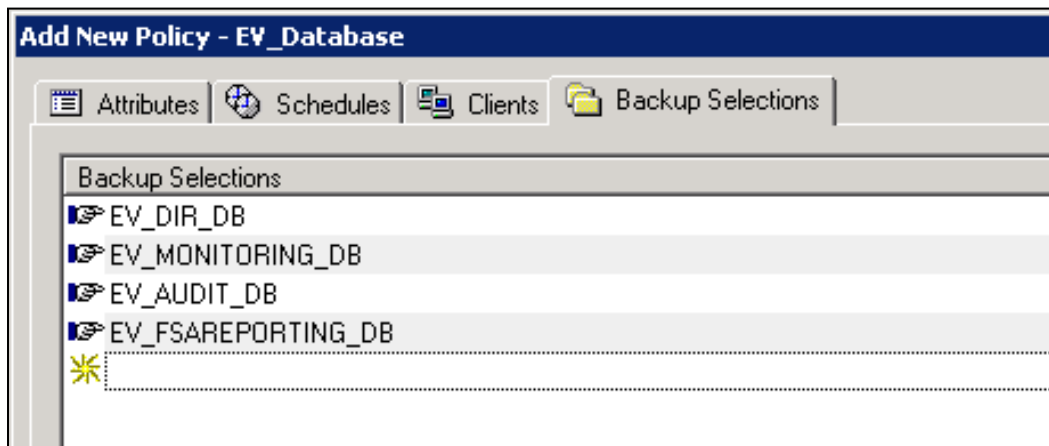


Figure 16 – EV_Database Policy Backup Selections

These 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

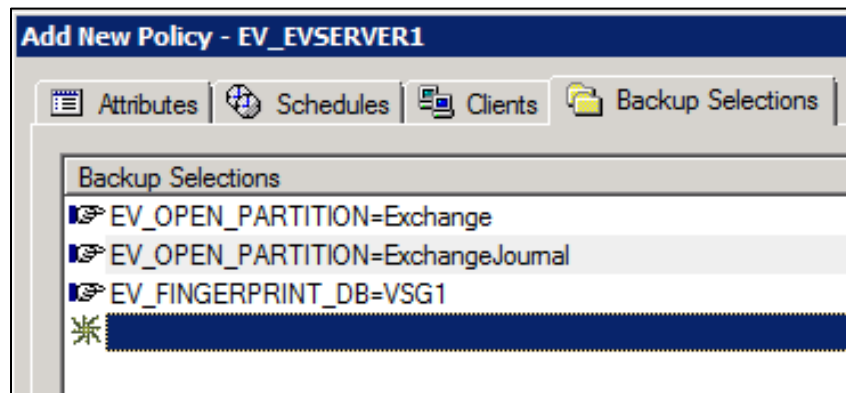


Figure 17 – EV_EVSERVER1 Policy Backup Selections

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

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator



Figure 18 – EV_EVSERVER2 Policy Backup Selections

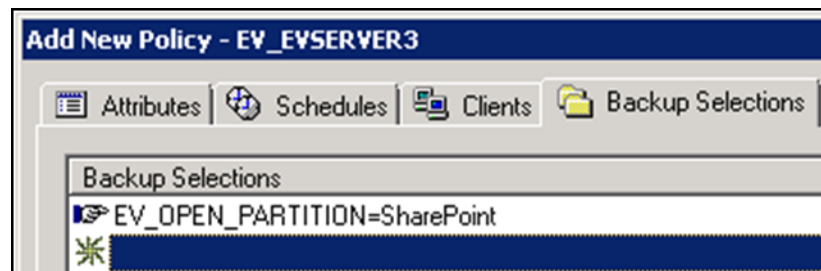


Figure 19 –EV_EVSERVER3 Policy Backup Selections

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 are backed up

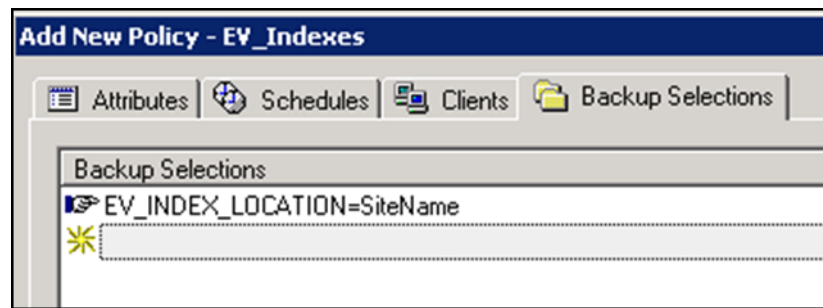


Figure 20 - EV_Indexes Policy Backup Selection

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

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

Storage Queue, Enterprise Vault Installation Directory, and VIC Policies Shared Location

The NetBackup Enterprise Vault Agent does not back up the storage queue, Enterprise Vault installation directory, or the VIC policies shared location. Thus, a separate policy will be needed to be created to back up these components. This example assumes that the VIC Policy shared location is stored on evserver1.

Names: EV_EVSERVER1_Other, EV_EVSERVER2_Other, and EV_EVSERVER3_Other (three policies)

Policy Type: MS-Windows

Schedules:

- Daily full

Clients:

- evserver1
- evserver2
- evserver3

Backup selections:

- evserver1
 - <ev_installation_directory>, e.g.: C:\Program Files (x86)\Enterprise Vault
 - <storage_queue_location>, e.g.: O:\StorageQueue
 - <vic_policy_location>, e.g.: V:\VICPolicies
- evserver2
 - <ev_installation_directory>, e.g.: C:\Program Files (x86)\Enterprise Vault
 - <storage_queue_location>, e.g.: O:\StorageQueue
- evserver3
 - <ev_installation_directory>, e.g.: C:\Program Files (x86)\Enterprise Vault
 - <storage_queue_location>, e.g.: O:\StorageQueue

Pros and Cons for Scenario #2

Pros:

- Agent automatically discovers open, closed, and ready Vault Store Partitions
- Agent automatically discovers which Microsoft SQL servers contain databases for Enterprise Vault

Cons:

- The NBU EV Agent performs file level backups (using VSS snapshots). Large NTFS volumes with numerous Enterprise Vault 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 due to partition collections that has not been backed up or data may be deleted due to expiry of archived content

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

- When using the EV_INDEX_LOCATION directive, *ALL* index locations on *ALL* Enterprise Vault servers in the Enterprise Vault site are backed up. Individual servers cannot be specified.
- Enterprise Vault 10 and later Indexing and 64-Index Volume Locations – Index locations on Enterprise Vault 10 and later 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.

Backup 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 12
- One Microsoft SQL 2012 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
- Veritas InfoScale is installed on the Enterprise Vault 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
- A backup policy to back up other Enterprise Vault components

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

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

The screenshot shows the 'Add New Policy - EV_Database' dialog box with the 'Attributes' tab selected. The 'Policy type' is set to 'Enterprise-Vault'. Under the 'Destination' section, 'Data classification' is '<No data classification>', 'Policy storage' is 'Any Available', and 'Policy volume pool' is 'Weekly'. Below this, there are checkboxes for 'Take checkpoints every:' (set to 0 minutes) and 'Limit jobs per policy:' (empty). 'Job priority' is set to 0, and 'Media Owner' is set to 'Any'.

Figure 21 - EV_Database Policy Attributes

Schedules:

- Weekly Full
- Daily Incremental

The screenshot shows the 'Add New Policy - EV_Database' dialog box with the 'Schedules' tab selected. It displays a calendar grid for the week of Sun to Sat, with a timeline from 2 to 24 hours. Two schedules are listed at the bottom:

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

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

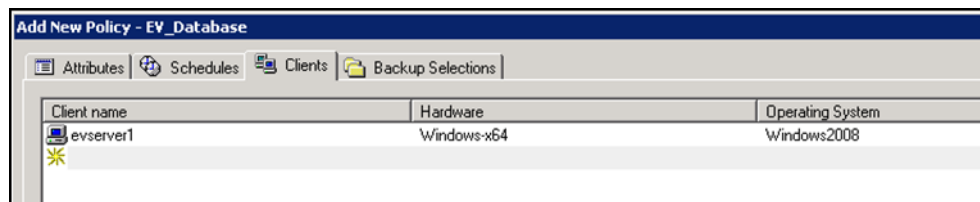


Figure 23 – EV_Database Policy Clients

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

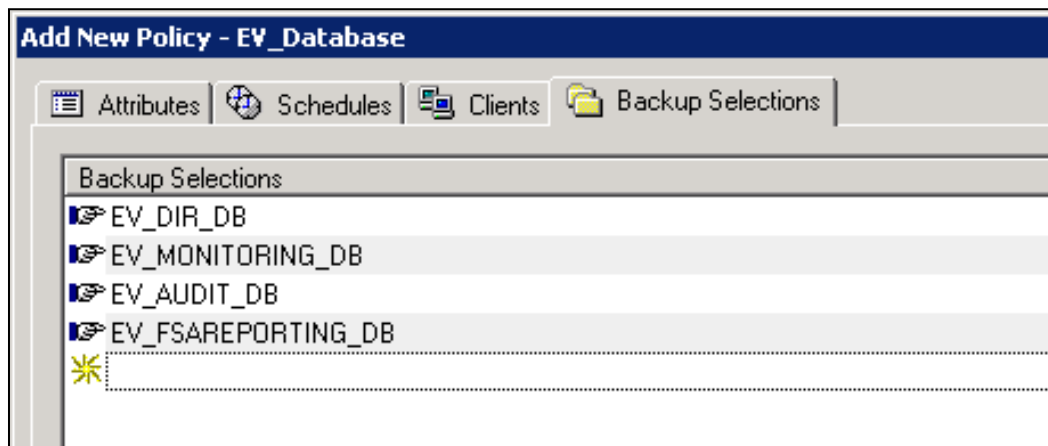


Figure 24 – EV_Database Policy Backup Selections

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:

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

- EV_VAULT_STORE_DB=Exchange Vault Store
- EV_FINGERPRINT_DB=VSG1

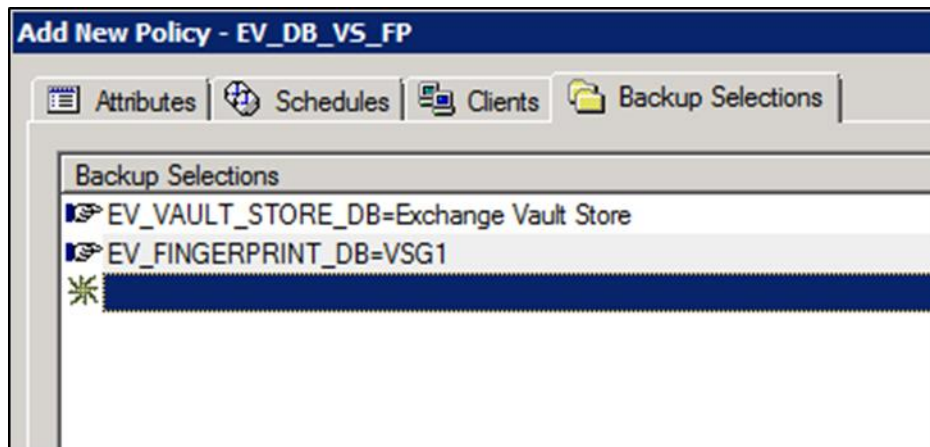


Figure 25 – EV_DB_VS_FP Policy Backup Selections

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:\.

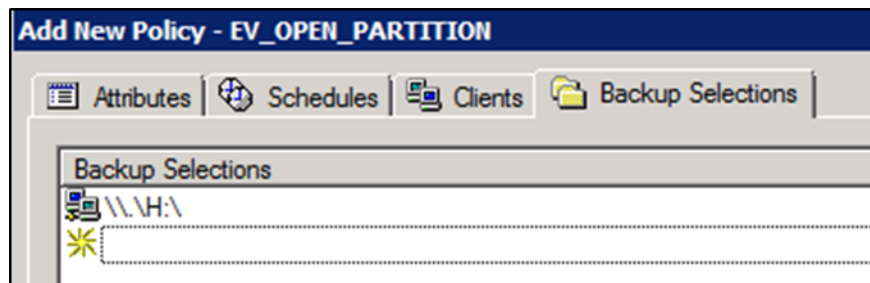


Figure 26 – EV_OPEN_PARTITION Policy Backup Selections

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. Also see “Note about Using bpstart_notify Scripts”.

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

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 do not have any 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. Also see “Note about Using bpstart_notify Scripts”.

Closed Partition Backup Policies

These policies use 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 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:

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

- 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. Also see “Note about Using bpstart_notify 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:>.

Storage Queue, Enterprise Vault Installation Directory, and VIC Policies Shared Location

A separate policy will be needed to be created to back up these components.

Names: EV_Other

Policy Type: MS-Windows

Schedules:

- Daily full

Clients

- evserver1

Backup selections:

- evserver1
 - <ev_installation_directory>, e.g.: C:\Program Files (x86)\Enterprise Vault
 - <storage_queue_location>, e.g.: O:\StorageQueue
 - <vic_policy_location>, e.g.: V:\VICPolicies

Pros and Cons for Scenario #3

Pros:

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

- 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 needs 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

Backup 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.

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 8).

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 script 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.

For sample bpstart_notify.bat and bpend_notify.bat files, see “**Scripting out PowerShell Commands**”.

See “**Note about Using bpstart_notify Scripts**” about precautions.

Sample Environment

- One Enterprise Vault server with indexes and vault stores running Enterprise Vault 12.5
- One Microsoft SQL 2012 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

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

Proposed Backup Policies

This sample environment has five backup policy configurations:

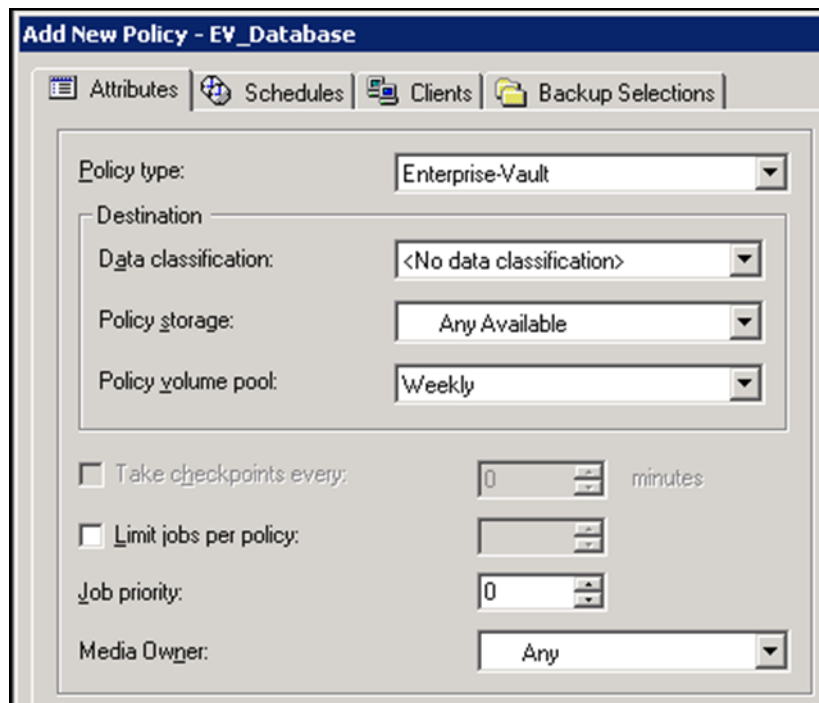
- One policy to back up the EV directory, monitoring, FSA Reporting, and monitoring databases
- One policy to back up the EV vault store and fingerprint databases
- One policy to back up open vault store partitions
- One policy to back up index locations
- Four policies to back up closed partitions
-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

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



The screenshot shows a dialog box titled "Add New Policy - EV_Database". It has four tabs: "Attributes", "Schedules", "Clients", and "Backup Selections". The "Attributes" tab is selected. The dialog contains the following fields and options:

- Policy type:** A dropdown menu set to "Enterprise-Vault".
- Destination:** A section containing four dropdown menus:
 - Data classification:** Set to "<No data classification>".
 - Policy storage:** Set to "Any Available".
 - Policy volume pool:** Set to "Weekly".
- Take checkpoints every:** A checkbox that is unchecked, followed by a spinner box set to "0" and the text "minutes".
- Limit jobs per policy:** A checkbox that is unchecked, followed by a spinner box.
- Job priority:** A spinner box set to "0".
- Media Owner:** A dropdown menu set to "Any".

Figure 27–EV_Database Policy Attributes

Schedules:

- Weekly Full
- Daily Incremental

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

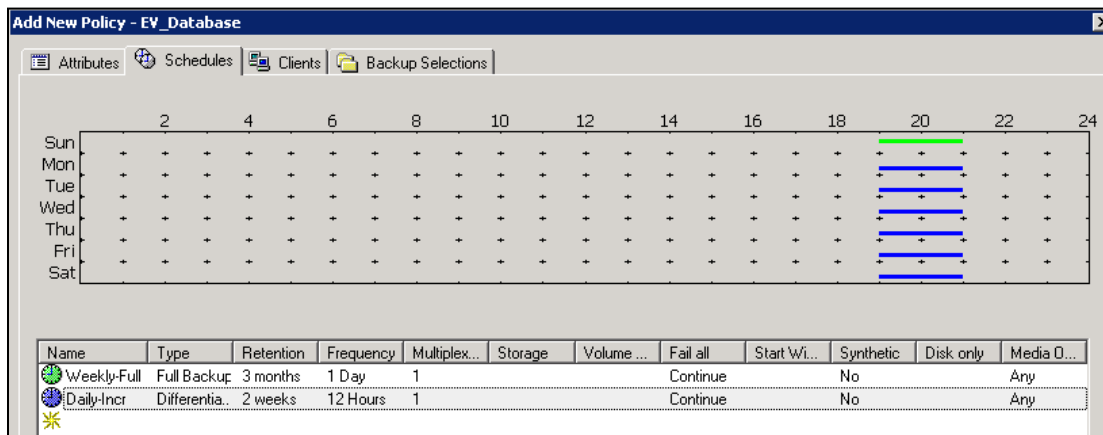


Figure 28 – EV_Database Policy Schedules

Clients:

- evserver1

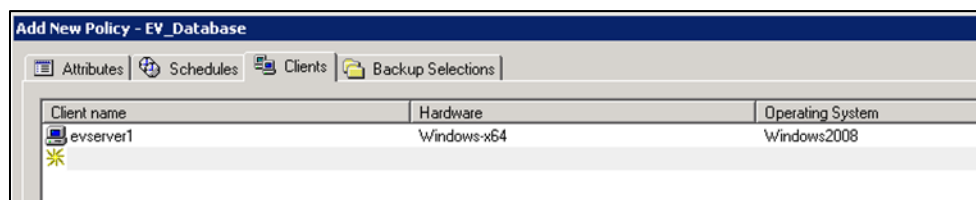


Figure 29 – EV_Database Policy Clients

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

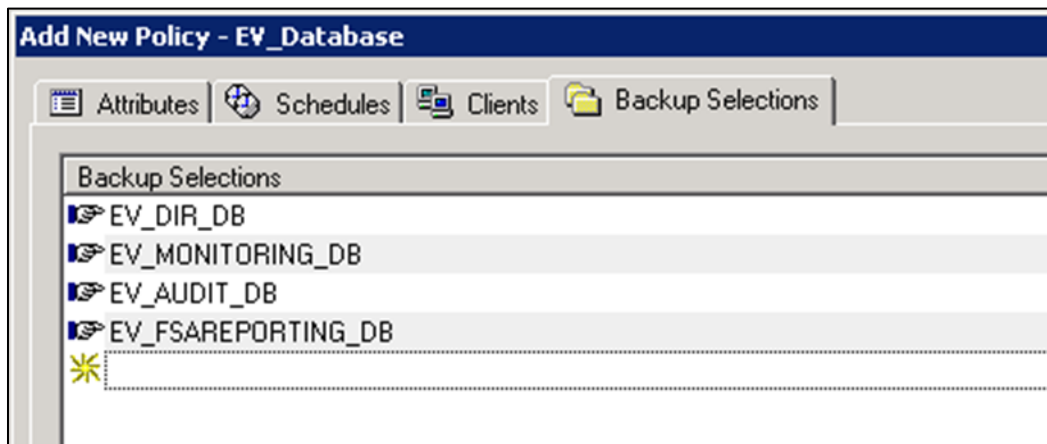


Figure 30 - EV_Database Policy Backup Selections

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

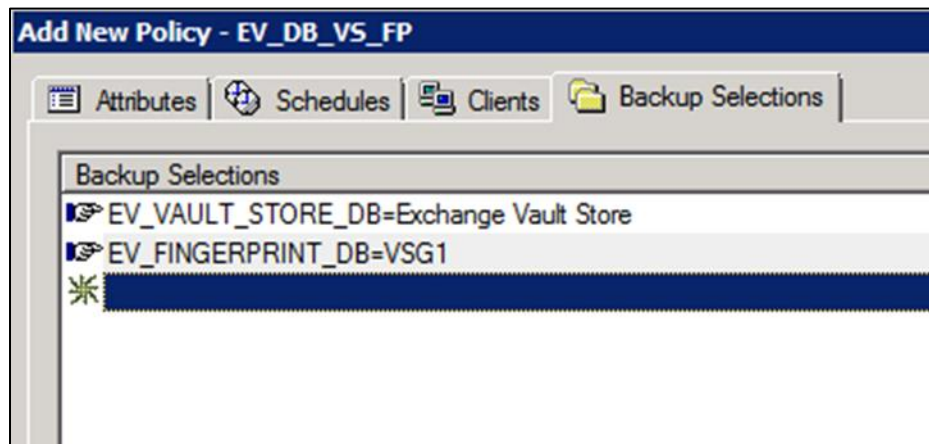


Figure 31 –EV_DB_VS_FP Policy Backup Selections

Open Partition Backup Policy

Name: EV_OPEN_PARTITION

Policy type: MS-Windows with "Use accelerator"

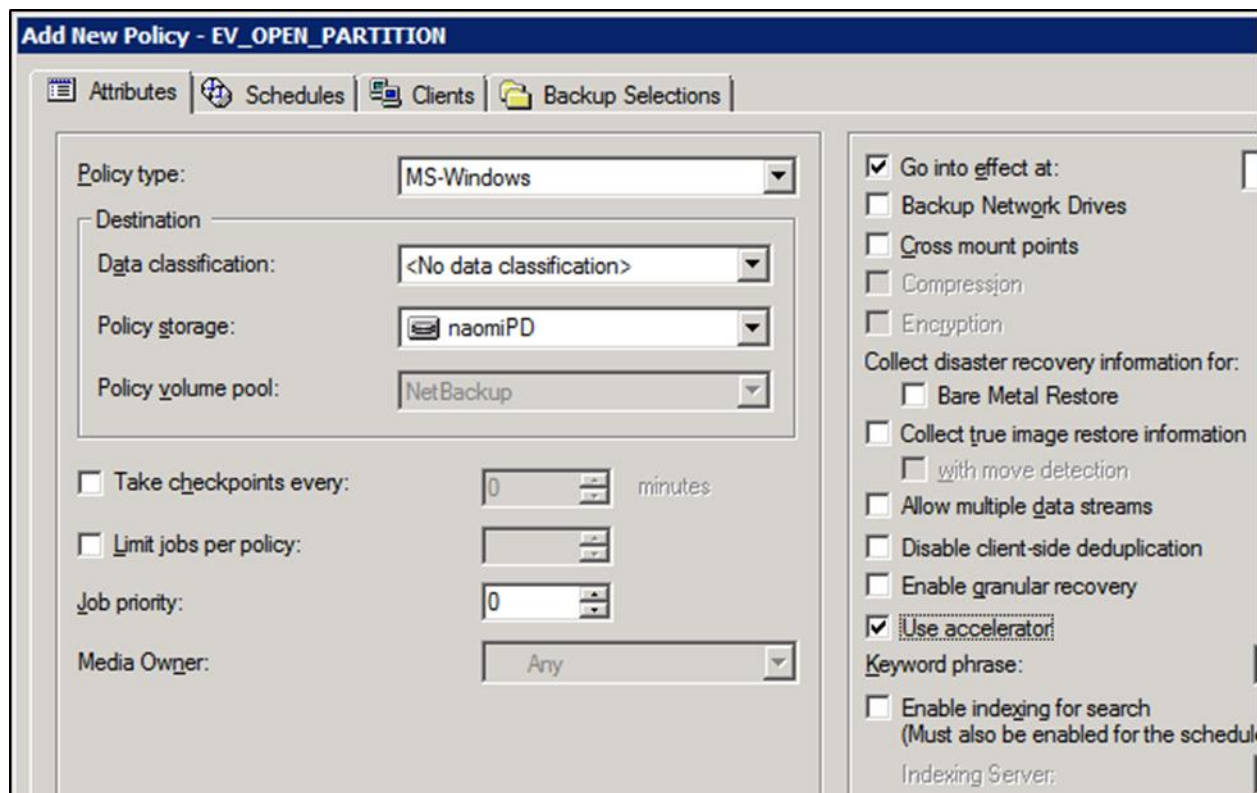


Figure 32 - EV_OPEN_PARTITION Policy Attributes

Schedules:

- Weekly_Full
- Daily_Incremental

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

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 Backup Mode for an Enterprise Vault Site” 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

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

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 bptest_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 “Backing up Elasticsearch Indexes

Starting with Enterprise Vault 14.2, a new indexing engine was implemented that replaces the older 32-bit and 64-bit indexing engines. Elasticsearch requires a different approach for backups compared to the older indexing technologies.

If the Enterprise Vault environment was upgraded to 14.2, it is highly likely that there are non-Elasticsearch 64-bit indexes and potentially older non-Elasticsearch 32-bit indexes. These older indexes will still need to be backed up until the content is either expired, deleted, or upgraded to an Elasticsearch index using the methods described in this document.

If this is a new 14.2 or later installation, there will not be any 64-bit or 32-bit indexes. Therefore, it will be only necessary to configure backups for Elasticsearch indexes.

Differences between Older Indexes and Elasticsearch Indexes

Elasticsearch indexes differ from older index engines in the following ways:

- Elasticsearch does not support direct flat file backups and a direct restore of Elasticsearch index flat files will likely fail or have corrupted data
- Backup Mode is not applicable to an Elasticsearch index location
- Backing up of Elasticsearch indexes requires the use of snapshots
 - The snapshots are essentially dumps of the index and placed in a separate location
 - These file dumps can then be backed up and used to restore the index if needed

Rules of Thumb for Elasticsearch Snapshot Locations

Keep the following in mind when setting up a Elasticsearch snapshot location

- A snapshot location must be defined before Elasticsearch indexes can be properly backed up
- Elasticsearch snapshot locations should be placed on a separate volume from the Elasticsearch index location. The volume can be locally attached to the Enterprise Vault Server or on a network share. It is recommended to use a network share.
- The size of the snapshot volume should be at least the same size of the volume holding the Elasticsearch indexes. If the snapshot volume becomes full, additional snapshot volumes can be created. The old snapshot volume will be placed in read-only mode.
- The first snapshot in a snapshot location will be a full copy of the current Elasticsearch index. Subsequent snapshots will be incremental. The same is true if the version of Elasticsearch is upgraded (such as when upgrading to a future version of Enterprise Vault).
- The Enterprise Vault Service Account (VSA) must have read and write access to the snapshot location

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

- Elasticsearch snapshot locations can hold up to 500 snapshots. The Enterprise Vault administrator will receive warnings when the snapshot count is over 400. See the **Enterprise Vault PowerShell Cmdlets** guide for more information on managing Elasticsearch snapshots.

Creating and Locating Elasticsearch Snapshot Locations

Snapshot locations are managed using the Enterprise Vault Management Shell. A PowerShell cmdlet named **Set-EVIndexSnapshotLocation** is used to create snapshot locations. Once a snapshot location is configured, it will be necessary to restart the Enterprise Vault Indexing service. The options for this cmdlet include:

- **-EVServerName <string>** - The name of the Enterprise Vault index server for which you want to configure an index snapshot location with the specified path. If you omit this parameter, Set-EVIndexSnapshotLocation uses the host name of the Enterprise Vault index server where the command is running. The FQDN must be used for the name of the Enterprise Vault server.
- **-SnapshotLocationPath <string>** - The path of the directory you want to configure for taking snapshots of the indexing data.
- **-WhatIf** - The WhatIf switch instructs the command to simulate the actions that it would take on the object. By using the WhatIf switch, you can preview the changes that would occur without applying any of those changes. You do not need to specify a value with the WhatIf switch.

Examples:

The following defines a snapshot location on the server “evserver” on a locally attached volume:

```
Set-EVIndexSnapshotLocation -EVServerName evserver.local -SnapshotLocationPath  
"J:\SnapShot"
```

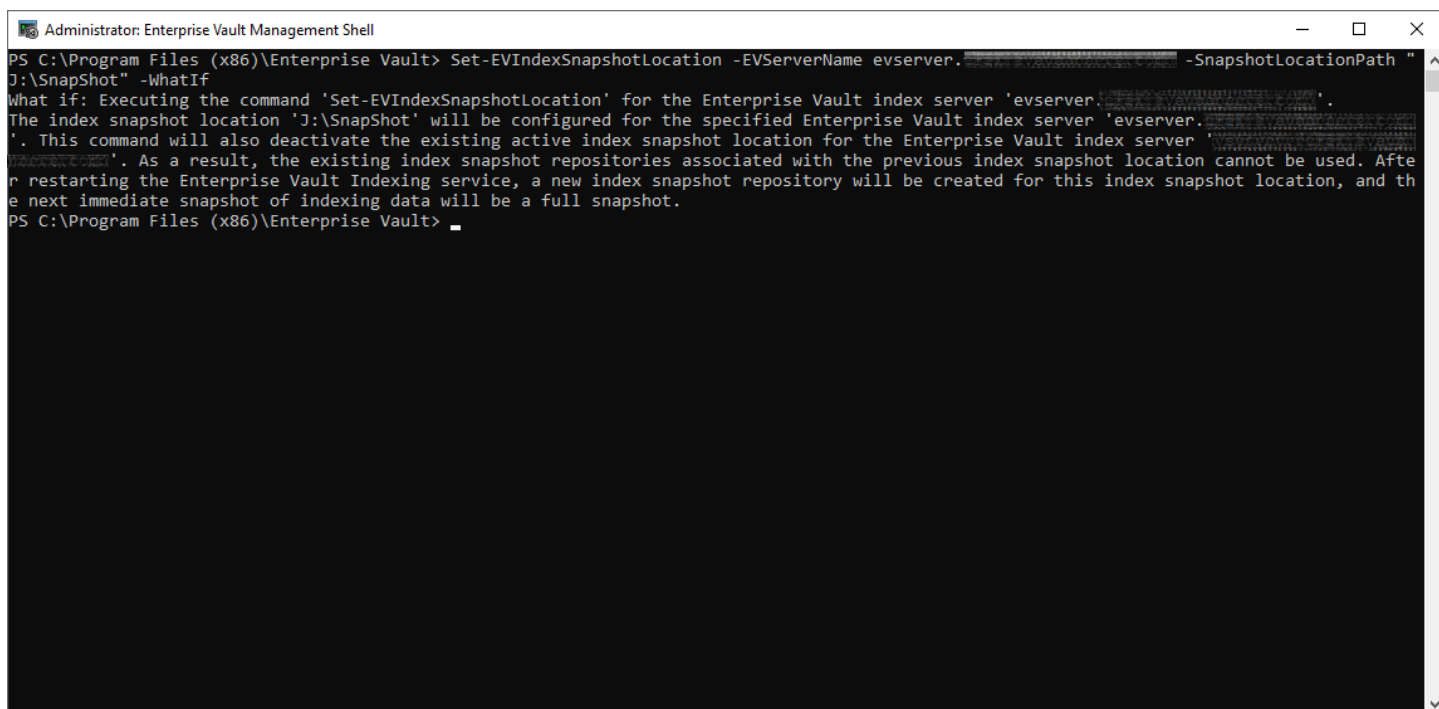
The following defines a snapshot location on the server “evserver” using a network share:

```
Set-EVIndexSnapshotLocation -EVServerName evserver.local -SnapshotLocationPath  
"\\fileserver\snapshots\SnapShot1"
```

The following performs a “What If”

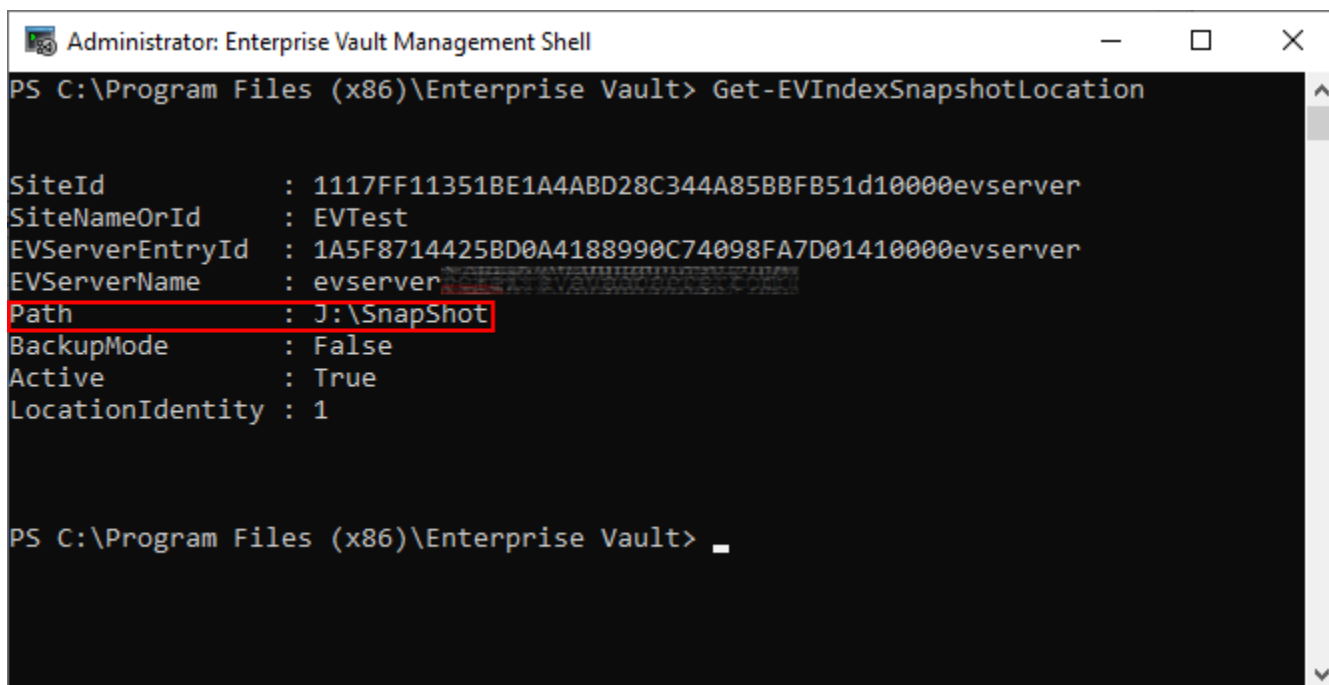
```
Set-EVIndexSnapshotLocation -EVServerName evserver.local -SnapshotLocationPath  
"J:\SnapShot" -WhatIf
```

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator



```
Administrator: Enterprise Vault Management Shell
PS C:\Program Files (x86)\Enterprise Vault> Set-EVIndexSnapshotLocation -EVServerName evserver. -SnapshotLocationPath "J:\SnapShot" -WhatIf
What if: Executing the command 'Set-EVIndexSnapshotLocation' for the Enterprise Vault index server 'evserver.'.
The index snapshot location 'J:\SnapShot' will be configured for the specified Enterprise Vault index server 'evserver.'. This command will also deactivate the existing active index snapshot location for the Enterprise Vault index server 'evserver.'. As a result, the existing index snapshot repositories associated with the previous index snapshot location cannot be used. After restarting the Enterprise Vault Indexing service, a new index snapshot repository will be created for this index snapshot location, and the next immediate snapshot of indexing data will be a full snapshot.
PS C:\Program Files (x86)\Enterprise Vault>
```

To find existing Elasticsearch snapshot locations, use **Get-EVIndexSnapshotLocation**. Note the Path as this will be needed later in order to back up the location.



```
Administrator: Enterprise Vault Management Shell
PS C:\Program Files (x86)\Enterprise Vault> Get-EVIndexSnapshotLocation

SiteId           : 1117FF11351BE1A4ABD28C344A85BBFB51d10000evserver
SiteNameOrId     : EVTest
EVServerEntryId  : 1A5F8714425BD0A4188990C74098FA7D01410000evserver
EVServerName     : evserver
Path             : J:\SnapShot
BackupMode       : False
Active           : True
LocationIdentity : 1

PS C:\Program Files (x86)\Enterprise Vault>
```

Creating an Elasticsearch Snapshot

Before backing up the Elasticsearch snapshot location, it will be necessary to create a snapshot to include the latest changes to the Elasticsearch index location. This is performed by using the **New-EVIndexSnapshot** cmdlet.

This cmdlet creates a snapshot of the Elasticsearch index location. The first snapshot on a newly created snapshot location will be a full copy of the current index. A full snapshot will also be created if the version of Elasticsearch is upgraded (such as when upgrading to a future version of Enterprise Vault). Subsequent snapshots will be incremental. The options for this cmdlet include:

- **-SiteId** - The ID of the Enterprise Vault site for which you want to create the snapshots of index data on all the Enterprise Vault index servers in that site. If you omit this parameter, New-EVIndexSnapshot retrieves the SiteId from the Enterprise Vault index server specified as EVServerName parameter; otherwise, it uses the SiteId of the Enterprise Vault index server where the command is running. You can use the Get-EVSite command to obtain the SiteId.
- **-EVServerName <String>** - The name of the Enterprise Vault index server for which you want to create the snapshot of index data. If you omit this parameter, New-EVIndexSnapshot uses the host name of the Enterprise Vault index server where the command is running. You can use the Get-EVComputers command to obtain the Enterprise Vault server name. The FQDN of the Enterprise Vault server must be used.
- **-IgnoreUnavailable** - (Optional, Boolean) If false, the command returns an error for any data stream or index that is missing or closed. Defaults to false. If true, the command ignores data streams and indices those are missing or closed.
- **-IncludeGlobalState** - (Optional, Boolean) If true, the current global state of Elasticsearch cluster running on Enterprise Vault index server is included in the snapshot. Defaults to false.
- **-Confirm** - (Optional, Boolean) The default value is **\$true**. If true, the user executing the cmdlet will have to confirm whether or not to execute the operation. If using this in a script, specify **-Confirm:\$false**.

Examples:

The following creates an index snapshot on the current server where the command is executed:

```
New-EVIndexSnapshot
```

The following creates an index snapshot on the Enterprise Vault index server named 'ev.domain.local' and will not ask for confirmation. A FQDN for the Enterprise Vault server must be specified:

```
New-EVIndexSnapshot -EVServerName ev.domain.local -Confirm:$false
```

The following creates index snapshots for all Enterprise Vault index server under the site 'site.domain.com'

```
New-EVIndexSnapshot New-EVIndexSnapshot -SiteId site.domain.com
```

The following creates an index snapshot of the Enterprise Vault index server 'ev.domain.local', if IgnoreUnavailable is set to false, the command returns an error for any data stream or index that is missing or closed. If true, the command ignores data streams and indices in indices that are missing or closed.

```
New-EVIndexSnapshot -EVServerName ev.domain.local -IgnoreUnavailable
```

The use of the **New-EVIndexSnapshot** cmdlet can be used in pre-backup scripts. Ensure to specify **-Confirm:\$false** so that confirmation is not required.

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

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 do 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.

Storage Queue, Enterprise Vault Installation Directory, and VIC Policies Shared Location

A separate policy will be needed to be created to back up these components.

Names: EV_Other

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

Schedules:

- Daily full

Clients:

- evserver1

Backup selections:

- evserver1
 - <ev_installation_directory>, e.g.: C:\Program Files (x86)\Enterprise Vault
 - <storage_queue_location>, e.g.: O:\StorageQueue
 - <vic_policy_location>, e.g.: V:\VICPolicies

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:

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

- 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.

Backup Scenario #5: Backing up Enterprise Vault and Microsoft SQL Servers Running as Virtual Machines

Sample Environment

In this scenario, there are both Enterprise Vault and Microsoft SQL Server instances running as virtual machines on VMware ESXi. As both servers are virtual, they will be backed up in whole with all local drives. For more information on the NetBackup VMware policy type, refer to the ***NetBackup Administrator's Guide***.

Pre and Post Backup Scripts

It will be necessary to manage Backup Mode for Enterprise Vault. This can be accomplished by using PowerShell scripts that run before the schedule backup. Windows Task Scheduler can be used to run the scripts a few minutes before the backups are kicked off. A post-backup script will also be required to take Enterprise Vault out of Backup Mode. This can be scheduled to run using Windows Task Scheduler after the backup window.

Pre-Backup Script:

- Place all Vault Stores in Backup Mode
- Place all Index Locations in Backup Mode
- Perform an Elasticsearch snapshot (EV 14.2 and later)

Post-Backup Script:

- Take all Vault Stores out of Backup Mode
- Take all Index Locations out of Backup Mode

Proposed Backup Policies

NetBackup VMware policy types will be used. There will be two separate policies for the backup. These policies should be scheduled to start at the same time in order to preserve the best data consistency in the event a restore is required.

Enterprise Vault

One policy will back up the entire Enterprise Vault virtual server.

Attributes

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

Policy type: VMware

Policy name: VMware-EnterpriseVault

The **Use Accelerator** option can be used

Change Policy - VMware-EnterpriseVault

Server: nbu2

Attributes Schedules Clients Backup Selections VMware Exclude Disks

Policy type: VMware

Destination:

Data classification: <No data classification>

Policy storage: Any_available

Policy volume pool: NetBackup

Take checkpoints every: 0 minutes

Limit jobs per policy:

Job priority: 0 (higher number is greater priority)

Media Owner: Any

Snapshot Client and Replication Director

☒ Perform block level incremental backups

☐ Use Replication Director

☐ Enable vendor change tracking for incremental backups

☒ Perform snapshot backups Options...

☐ Retain snapshot for Instant Recovery or SLP management

☐ Hyper-V server:

☒ Perform off-host backup

Use:

Machine:

☒ Go into effect at: Aug 10, 2020 11:32:27 AM

☐ Follow NFS

☐ Cross mount points

☐ Compress

☐ Encrypt

Collect disaster recovery information for:

☐ Bare Metal Restore

☐ Collect true image restore information

☐ with move detection (Required for synthetic backups and Bare Metal Restore)

☐ Allow multiple data streams

☐ Disable client-side deduplication

☐ Enable granular recovery

☐ Use Accelerator

☐ Enable optimized backup of Windows deduplicated volumes

Keyword phrase (optional):

Microsoft Exchange Server Attributes

Exchange DAG or Exchange 2007 replication (LCR/CCR)

Database backup source:

Preferred server list... (Exchange DAG only)

Dynamic Data Streaming Attributes

☐ Allow Dynamic Streaming

Maximum number of streams per volume: 4

Maximum number of files in a batch: 300

OK Cancel Help

Schedules

It is recommended to do a daily full backup if possible. If not, a weekly full and daily incremental schedule can be used.

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

Name	Type	Synthetic B...	Disk-Only B...	Retention P...	Retention L...	Frequency	Media Multi...	Storage	Volume Pool	Policy	Media Owner	Accelerator ..
Daily_Incr Cumulative ...	--	--	--	2 weeks	1	<calendar>	1			VMware-Ent...		No
Weekly...	Full Backup	--	--	3 months	5	<calendar>	1			VMware-Ent...		No

Clients

Use the name of the virtual machine.

Client Name	Hardware	Operating System	Resiliency
mattie	vmx-13	windows9Server64Guest	

Backup Selections

Use the default ALL_LOCAL_DRIVES directive

VMware

Use the default options unless it necessary to use a different Transport mode type.

SQL

One policy will back up the entire Microsoft SQL Server virtual machine

Attributes

Policy type: VMware

Policy name: VMware-MSSQL

The **Use Accelerator** option can be used

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

Change Policy - VMware-SQL

Server: nbu2

Attributes | Schedules | Clients | Backup Selections | **VMware** | Exclude Disks

Policy type: VMware

Destination:

- Data classification:** <No data classification>
- Policy storage:** Any_available
- Policy volume pool:** NetBackup

☐ Take checkpoints every: 0 minutes

☐ Limit jobs per policy:

Job priority: 0 (higher number is greater priority)

Media Owner: Any

Snapshot Client and Replication Director

- ☒ Perform block level incremental backups
- ☐ Use Replication Director
- ☐ Enable vendor change tracking for incremental backups
- ☐ Perform snapshot backups Options...
 - ☐ Retain snapshot for Instant Recovery or SLP management
 - ☐ Hyper-V server:
 - ☒ Perform off-host backup
 - Use:**
 - Machine:**

Go into effect at: Aug 10, 2020 11:32:27 AM

- ☐ Follow NFS
- ☐ Cross mount points
- ☐ Compress
- ☐ Encrypt

Collect disaster recovery information for:

- ☐ Bare Metal Restore
- ☐ Collect true image restore information
 - ☐ with move detection

(Required for synthetic backups and Bare Metal Restore)

- ☐ Allow multiple data streams
- ☐ Disable client-side deduplication
- ☐ Enable granular recovery
- ☐ Use Accelerator
- ☐ Enable optimized backup of Windows deduplicated volumes

Keyword phrase (optional):

Microsoft Exchange Server Attributes

Exchange DAG or Exchange 2007 replication (LCR/CCR)

Database backup source:

Preferred server list... (Exchange DAG only)

Dynamic Data Streaming Attributes

- ☐ Allow Dynamic Streaming
- Maximum number of streams per volume:** 4
- Maximum number of files in a batch:** 300

OK **Cancel** **Help**

Schedules

A daily full backup schedule is recommended

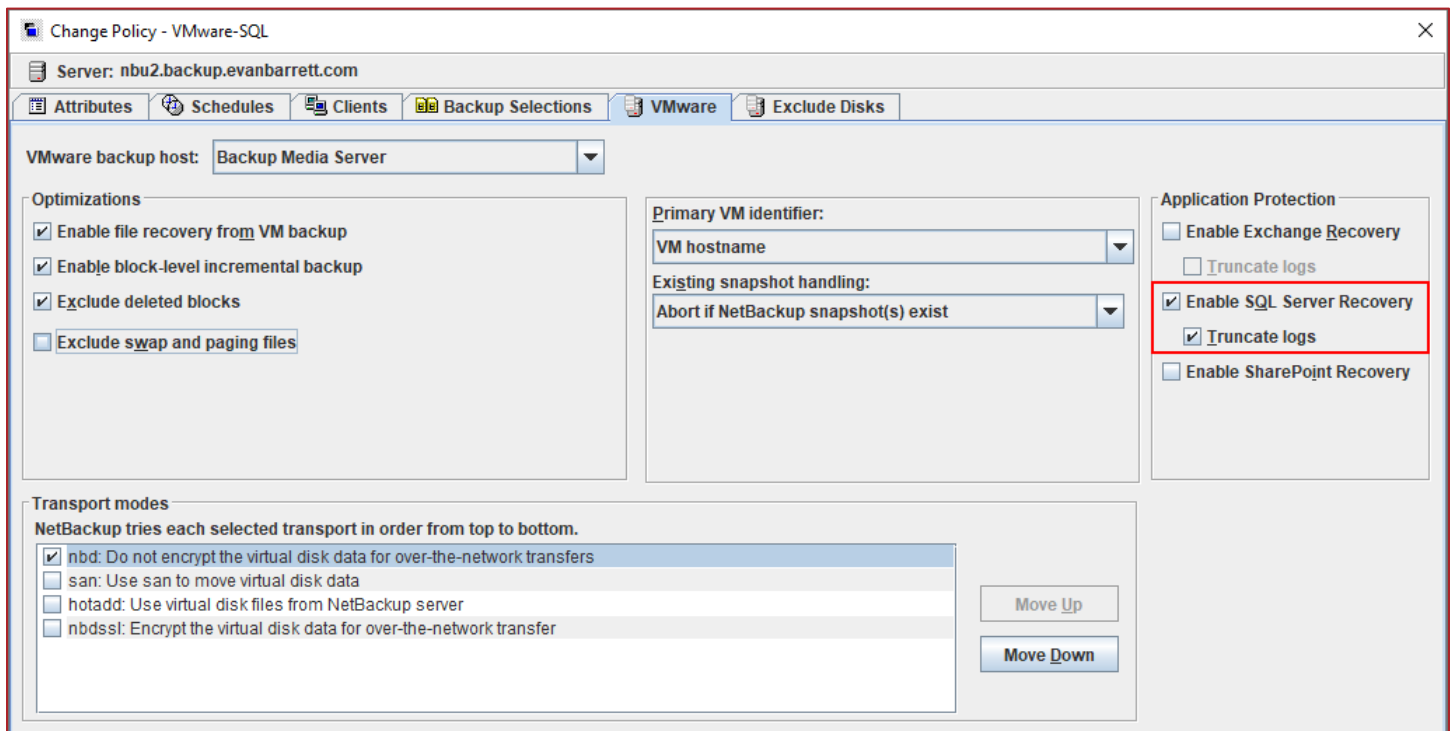
Clients

For VMware Microsoft SQL Server backups to function properly, it will be necessary to use VMware Intelligent query to specify the Microsoft SQL server virtual machine. Please refer to the **NetBackup Administrator's Guide** for more information.

VMware

In the VMware tab, select the preferred transport mode and ensure that Enable SQL Server Recovery and Truncate logs are selected.

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator



Pros and Cons for Scenario #5

Pros:

- A minimal amount of backup policies is required, one for each Enterprise Vault virtual server and one for each Microsoft SQL Server that contains Enterprise Vault databases
- When using the Accelerator option, the length of time for backups of the virtual servers can be greatly reduced depending on the amount of daily change
- Easier restores as the whole virtual machine will be restored with all Enterprise Vault and Microsoft SQL Server data restored

Cons:

- It will be necessary to either manually or schedule pre and post backup scripts to control Enterprise Vault Backup Mode

Other Enterprise Vault Objects to Back 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 at minimum.

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

- **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 when PST migration operations are being performed
- **SSL Certificates** – SSL Certificates for IIS and IMAP (EV 11 and later) should be backed up at least once per week
- **VIC Policies** – Enterprise Vault 12.2 and later introduces a new classification mechanism. It is highly recommended to back up the shared location for VIC policies as the directory will contain any custom-created classification policies, tags, or patterns.
- **Elasticsearch snapshot locations (EV 14.2 and later)** – In order to properly back up Elasticsearch indexes, an Elasticsearch snapshot must be created to a separate Elasticsearch snapshot volume which can be attached to the Enterprise Vault server or a network share (recommended).

Vault Store Partition Sizing

One of the uses cases for 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 occur 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 to optimize backup windows. Let's examine 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 backup point of view.

Another factor with partition sizing is the archiving of the backlog. New implementations of Enterprise Vault generally archive 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

Technical White Paper – Backing up Enterprise Vault, Discovery Accelerator, and Compliance Accelerator

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.

Backing up Discovery Accelerator and Compliance Accelerator

The main components of Discovery Accelerator and Compliance Accelerator are the Microsoft SQL databases. Backing up the database components was discussed earlier in this document in the “**Backing up the Discovery Accelerator and Compliance Accelerator Database Components**” section.

Besides the SQL components, there are other items that should be considered for backup in both Discovery Accelerator and Compliance Accelerator. These include:

- .config files – These are XML files that may contain customized settings for the applications
- Hotword and Hotphrase XML files – These files may contain customized hotwords and hotphrases that are used by Compliance Accelerator
- Export directories – Archived content can be exported by Discovery Accelerator (from Cases and Research Folders) and Compliance Accelerator (from Departments) to a location on the server itself or on a CIFS share

ABOUT VERITAS

Veritas Technologies is a global leader in data protection and availability. Over 50,000 enterprises—including 99 of the Fortune 100—rely on us to abstract IT complexity and simplify data management. Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas supports more than 500 data sources and over 150 storage targets, including 60 clouds. Learn more at www.veritas.com. Follow us on Twitter at [@veritastechllc](https://twitter.com/veritastechllc).

2625 Augustine Drive, Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For specific country offices
and contact numbers,
please visit our website.

VERITAS™