WHITE PAPER: TECHNICAL

symantec™

Confidence in a connected world.

PST Migration with Enterprise Vault 8.0:

Part 3 – Planning, Tech Tips & Best Practice

Author: Andy Joyce, EV Technical Product Management
Date: April, 2009

Contents

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

PST Migration with Enterprise Vault 8.0: Part 3 – Planning, Tech Tips & Best Practice

Introduction

This whitepaper is part of a series about the various tools available for PST migration with Symantec Enterprise Vault 8.0. The series comprises the following whitepapers:

- PST Migration with Enterprise Vault 8.0: Part 1 - Solution Overview
- PST Migration with Enterprise Vault 8.0: Part 2 – The Tools in Depth
- PST Migration with Enterprise Vault 8.0: Part 3 – Planning, Tech Tips and Best Practice

This whitepaper looks at some important aspects of a PST migration project; namely, planning and best practice usage of the tools in different migration scenarios.

The whitepaper is intended primarily for Symantec and partner System Engineers and Consultants.

It is assumed that the reader will be familiar with the concepts of PST files, and have some familiarity with general Enterprise Vault concepts and terminology. It is also recommended that this whitepaper is read *after* reading Parts 1 and 2 in this series.

Planning a PST migration strategy

Determining which tools to use

One of the key decisions when planning PST migration is choosing the tool or combination of tools to use. It is unlikely in most environments that a single tool will be an exact fit, although in small, uncomplicated sites this may be the case. Prepare to use more than one PST migration tool as circumstances dictate.

For example, client-driven migration may succeed in migrating most PST files but miss some that are stored on users' home directories on a file server but not mapped in their Outlook profile. In this example, server-driven migration might then be used to locate, collect, and migrate those remaining PST files. Or, if there are only a few PST files to migrate, the PST Migration Wizard may be used once the PST files have been located by the server-driven PST Locator Task.

As another example, server-driven migration may be used if it is known that the majority of PST files are stored on the file server, but client-driven migration is enabled for the "road warriors" that only bring their laptops into the office once or twice a week. In this case, because these users would need to leave their laptops connected to the network and logged into Outlook for some time to complete client-driven migration, it might be more effective to ask the users to copy their PST files to the file server when they come into the office and then let the server-driven migration process them as part of its normal schedule. Or alternatively, the Enterprise Vault administrator could use the PST Migration Wizard to migrate these PST files.

When choosing the PST migration tools to use, consider the following:

- What are the number and total volume of PST files to migrate?
- What is the location of PST files? How many are located on clients? How many on file servers?
- Are there any timing considerations? For example, do all PST files need to be migrated by a certain date? Can PST migration be run only at certain times of the day or days of the week?
- Are many of the PST files password-protected? Is it acceptable to ask users to remove these passwords prior to migration? Does the organization's policy allow use of commercial password resetting software to remove the PST passwords? Are users agreeable to providing the Enterprise Vault administrator with the PST passwords so that the PST Migrator Task can open the PST files? Or, would it be better to use client-driven PST migration so that users are automatically prompted for the PST file password, and it is stored automatically, as the PST file is located by the Enterprise Vault client?
- What is the culture of acceptance of change within the organization? Eliminating PST files from an organization, even into a system such as Enterprise Vault, can result in changes in the way users work. How much difference in the way they work will users tolerate?
- Can users live with short periods when their PST files are unavailable, but the messages are not yet available in the archive? If so, how long is this period? Or, must users have uninterrupted access to their PST files, up to the point that all the migrated messages are available in their archive? Do users need to keep adding messages to their PST files while they are being migrated?

- Are the client machines protected by the Windows XP firewall, or any other firewall technology? Is file sharing enabled? Does the Enterprise Vault Service Account have access to the drives on the client machines? If not, is there an alternative account that does?
- Will the Enterprise Vault Service Account, or another account, have access to scan the registry remotely on the client machines?
- Can all or most PST files be migrated using the same PST Migration Policy? Are any exceptions required?
- How many users are located remotely to the Enterprise Vault servers? How many road warriors are there? How often are these people in the office?
- Are many PST files accessed by several users? For example, an executive may have a PST file that is sometimes accessed by an assistant. Special consideration needs to be given to these cases.
- Do you want to send email messages to each user as their PST files are migrated?
- Are there are a large number of PST files to migrate that need to be associated with mailboxes/archives programmatically? For example, this might be the case when PST files are being used to migrate legacy data from another mail system.
- Are there any local or organizational privacy laws, regulations, or guidelines that might prevent a fully automated ingestion of users' PST files into an archive?

A generic PST migration strategy

Organizations should carefully review their environment, culture, and PST migration requirements to develop the best plan for PST migration. Symantec Professional Services can assist with this process. Following is a generic PST migration strategy to use as a basis.

1. Complete implementation and rollout of mailbox archiving, and complete "backlog" mailbox archiving; this ensures that the Enterprise Vault server(s) will have maximum resources available for PST migration. This also allows more time for users to become comfortable with the concept of email archiving and aware of the benefits of such features as the Enterprise Vault search capability. This generally makes the PST migration process run more smoothly.
2. Enable PST "marking"[1] well in advance of the PST migration. This helps ensure that as many PST files as possible are marked, reducing the need for the Enterprise Vault administrator to manually assign the associated mailbox and target archive for each PST file.
3. Communicate to users that PST migration is about to commence. It is essential for a PST migration project to be successful to have regular and clear communication about the process, timing, and changes to the way that users will access their data. Remember that depending on the PST migration method chosen, there may be some time when users do not have access to their PST files and messages are not yet available in their archive. Also, an enterprise wide PST migration can take several months, so users may forget what they were told at the beginning of the project and need reminders as the project progresses. Remember to highlight the benefits of the Enterprise Vault solution, such as the powerful search capabilities and the security of having their messages stored centrally and backed up.
4. If PST files are mainly located on client machines:
    - Enable client-driven migration to get most current PST files (those mapped in the Outlook profiles) and other PST files on users' desktops. Start by enabling only a small pilot group for client-driven PST migration, and then slowly increase this number in batches while monitoring the typical PST ingestion rates (gigabytes per hour) being achieved. Note that enabling a large number of mailboxes at once will result in a flood of PST chunks being sent to the Enterprise Vault server(s) the next morning as the users log in to Outlook.
    - Once client-driven PST migration has located and migrated as many PST files as it can, use server-driven locate, collect, and migrate to locate any other PST files from file servers and, possibly, desktops that remain because they have not been opened in Outlook recently.
    - Based on the number and nature of the PST files that the locate finds, either use server-driven PST migration to collect and migrate them, or use the PST Migration Wizard to

[1] PST marking is the process of automatically writing information about the owner of the PST into the file itself so that this information can be used later by the migration process. This is done by the Enterprise Vault Outlook Add-in, and is described in Part 2 of this series.

manually import the PST files. If server-driven PST migration is used, then the PST Migration Wizard may still be used to handle any exceptions.

5. If PST files are mainly located on file servers:
   - Use server-driven locate, collect, and migrate to locate and migrate PST files from file servers.
   - Enable client-driven migration to locate and migrate any PST files located on the users' desktops.
   - Optionally, use the PST Migration Wizard to handle any exceptions.

Comparison of PST migration tools

Table 1 summarizes the benefits and features of the various PST migration methods available with Enterprise Vault. Wizard-driven and scripted are grouped together as they are similar, but differences are highlighted as appropriate.

Table 1 - Features and benefits of PST migration methods

	Client-Driven Migration	Server-Driven Migration	Wizard or Scripted Migration
Scenario	Client has a PST file on a laptop in their default profile location and not on the network.	Large amounts of PST files are on user home directories or strewn about network shares.	Location of PST files is known—usually on a file server.
Requirements	Requires Outlook add-in; user must have Outlook open to push data to server; is slower due to chunking process; requires PST Holding folder and Temp folder locations, plus a PST Migrator Task on each mailbox archiving server.	Requires PST Holding folder and Temp folder locations, plus PST Locator, Collector, and Migrator Tasks.	Since importing PST files requires a constant connection to PST, move/copy PST file to a location local to the Enterprise Vault server to increase performance. No PST tasks are required.
PST Location			
Search Outlook profiles	Yes—automatic *All* Outlook profiles for the current user.	Optional—configured via PST Locator Task properties. If set, searches all Outlook profiles on scanned computers (servers or client machines).	No
Search hard disks for PST files	Yes—searches local disks on client computer. Can optionally be restricted to Documents and Settings folders of current user.	Optional—searches all local disks of servers and computers. Configured via PST Locator Task properties.	No
PST Collection/Migration			
Copies PST to centralized location before migration	Yes—copies PST files as smaller chunks to PST Holding folder. One chunk per client is sent and then migrated before the next chunk is sent.	Yes—PST Collector Task copies PST files to centralized PST Holding folder.	No—this is recommended but is a manual task.
Wait until PST files are backed up before commencing migration	No—chunks will be migrated as soon as possible.	Yes—PST Migrator can wait for the PST files in the Holding folder to be backed up, or the administrator can manually set the status to Ready to Migrate. This allows manual intervention such as running an antivirus scan or a third-party password cracker across the PST files prior to migration.	Yes—but this is purely a manual process.

	Client-Driven Migration	Server-Driven Migration	Wizard or Scripted Migration
Use PST marking to determine ownership	No—ownership is assumed to be the primary mailbox of the current Outlook profile.	Yes	Yes—optional. Can be overridden via the wizard or Policy Manager initialization file.
Change/specify Retention Category	No—default Retention Category taken from primary mailbox of current Outlook profile.	Yes—when a PST file is first located, the Retention Category is taken from the PST file, if marked, or the PST Migration Policy, if not marked. This value may then be changed manually via the Administration Console prior to migration.	Yes—if PST file is marked, that Retention Category (the default for the mailbox) will be used. If it is not marked, the default specified in the wizard or Policy Manager initialization file is used and can be overridden on individual PST files.
Leave no shortcuts	Optional—configured via PST Migration Policy.	Optional—configured via PST Migration Policy.	Optional—configured via wizard or Policy Manager initialization file.
Leave shortcuts in PST file	Optional—configured via PST Migration Policy.	Optional—configured via PST Migration Policy.	Optional—configured via wizard or Policy Manager initialization file.
Leave shortcuts in mailbox	Optional—configured via PST Migration Policy.	Optional—configured via PST Migration Policy.	Optional—configured via wizard or Policy Manager initialization file.
Create folders under Root folder or subfolder	Optional—configured via PST Migration Policy.	Optional—configured via PST Migration Policy.	Optional—configured via wizard or Policy Manager initialization file.
Merge folder structures	Optional—configured via PST Migration Policy.	Optional—configured via PST Migration Policy.	Optional—configured via wizard or Policy Manager initialization file.
Disable Outlook AutoArchive	Optional—only works if shortcuts are being left in mailbox; configured via PST Migration Policy.	Optional—only works if shortcuts are being left in mailbox; configured via PST Migration Policy.	Optional—only works if shortcuts are being left in mailbox; configured via wizard or Policy Manager initialization file.
Adjust Exchange quotas	Optional—only works if shortcuts are being left in mailbox; configured via PST Migration Policy.	Optional—only works if shortcuts are being left in mailbox; configured via PST Migration Policy.	No
Restrict shortcuts by age	Optional—configured via PST Migration Policy.	Optional—configured via PST Migration Policy.	No
Populate Vault Cache directly	Yes—automatic if Vault Cache is enabled for mailbox.	No	No
Automatically add space to offline archives	Optional—configured via PST Migration Policy.	No	No
Post-Processing			
Remove PST file from Outlook profile	Yes—automatic when migration of each PST file is completed. Enterprise Vault client will remove the PST file from the profile as soon as it detects that the PST migration is completed.	Optional—configured via mailbox policy, Advanced—Desktop settings. Enterprise Vault client removes the PST file from the Outlook profile on next login if it has been set to read-only/hidden or deleted per PST Migration Policy. The setting in the mailbox policy determines which of these conditions to check to decide whether to	Optional—configured via mailbox policy, Advanced—Desktop settings. Only works if administrator deletes the original PST file or sets it to read-only/hidden.

	Client-Driven Migration	Server-Driven Migration	Wizard or Scripted Migration
		remove the PST file from the profile.	
Delete PST file	Optional—configured via PST Migration Policy. Note: If the Vault Store is set to remove safety copies after backup, the PST file will not be deleted until after the backup has been completed.	Optional—configured via PST Migration Policy. Note: If the Vault Store is set to remove safety copies after backup, the PST file will not be deleted until after the backup has been completed.	Optional—configured via wizard or Policy Manager initialization file; deletion does not check for backup completion.
Compact/read-only/hide PST file	No	Optional—configured via PST Migration Policy.	Optional—configured via wizard or Policy Manager initialization file.
Send email notification to mailbox	Optional—configured by editing/moving message template files to Enterprise Vault installation folder. Email notification message is sent to mailbox when client-driven migration is enabled and/or after each PST file is migrated.	Optional—configured by editing/moving message template files to Enterprise Vault installation folder. Email notification message is sent after each PST file is migrated. Note: Email is *only* sent if migration is configured to leave shortcuts in the mailbox.	Optional—configured by editing/moving message template files to Enterprise Vault installation folder. Email notification message is sent after each PST file is migrated. Note: Email is *only* sent if migration is configured to leave shortcuts in the mailbox.

Tips for Enterprise Vault specialists

Following is a list of tips and tricks for installing, configuring, and running the PST migration tools.

- A PST migration project takes time. It has taken an organization significant time to generate the data stored in the PST files, so it will take time to ingest all this data into Enterprise Vault. The officially benchmarked ingestion rate is around 4-5 gigabytes per hour[2], but throughput has been observed to vary greatly, both higher and lower. Many factors affect this rate, such as type of attachments, network usage, and frequency that users log in to Outlook (when using client-driven migration). In any PST migration project, the key is to first benchmark the PST migration in your own environment to determine the expected migration throughput rate.
- It's important to understand that some of the PST migration processes take time and can appear to be "stuck" when really they are just waiting for the next cycle to begin. For example, client-driven migration will only perform its scan for PST files once per day (about one minute after the user first logs in to Outlook). If a PST file is subsequently created or added to the Outlook profile, it will not be picked up by the client-driven scan until the user's first logon the next day. In the normal course of events, this should not be a problem, but it could be frustrating or confusing, especially when conducting testing. Fortunately, it is possible to "reset" the scan by deleting the following registry key:

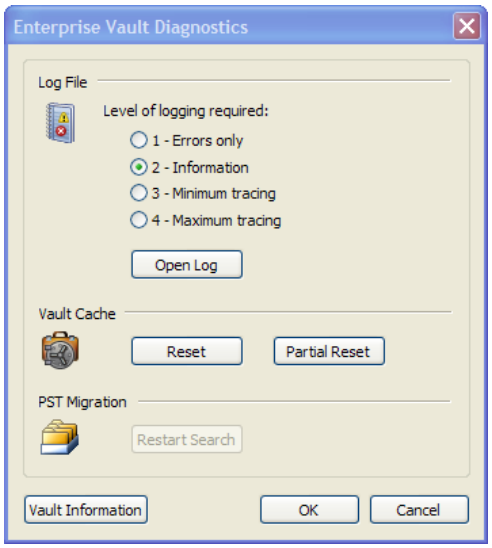
  HKEY_CURRENT_USER\Software\KVS\Enterprise Vault\Client\LastPSTSearch

  Then, logging back in to Outlook will initiate another scan for PST files. With Enterprise Vault 8.0 this can also be done from the Enterprise Vault Diagnostics dialog; in Outlook CTRL-Shift-Click one of the Enterprise Vault toolbar buttons to open the dialog. This is shown in Figure 1. Note in this figure the "Restart Search" button is greyed out because client-driven migration is not enabled.

[2] Migrating a standard mix of messages, averaging 100KB in size, with approx 20% having Office attachments. On a dual-CPU 2.8Ghz server (with appropriate storage and SQL server), the ingest rates is 25,000 items per hour (approximately 2.5GB/hr). On a Quad-CPU server, the ingestion rates rises to 40,000 items per hour (approximately 4GB/hr). Use of a dual Quad-Core server will increase this further to around 60,000 items per hour.

- Client-driven PST migration can be monitored/troubleshooted using the Enterprise Vault client tracing; this is initiated and the log file can be opened from the Enterprise Vault Diagnostics. The level of tracing can also be controlled (see Figure 1); generally level 3 "Minimal tracing" is sufficient.

Figure 1 - Enterprise Vault Diagnostics



- Neither client- nor server-driven migration will locate PST files that are located on DFS shares. This is because, in both cases, the server must resolve the PST file path to an actual location so it can be sure the PST file is not being migrated by both server- and client-driven migration.
- If Vault Stores are configured to remove safety copies after backup, then most client- and server-driven migration will stay in Completing status until after the backup of the stores has been completed. As with the removal of safety copies from mailboxes after backup completion, the StorageFileWatch process must check the backup status of each archive saveset and any shared SISparts; it does this once when the Storage Service is started and, by default, every 12 hours thereafter. During testing, a manual restart of the Storage Service is generally acceptable to trigger the StorageFileWatch process rather than waiting for up to 12 hours. Alternatively, the StorageFileWatch frequency can be changed with the following registry key:

  HKEY_LOCAL_MACHINE\Software\KVS

  \Enterprise Vault\Storage\FileWatchScanInterval

  This is a DWORD value, equal to the number of minutes between scans. Note that once in production, the Storage Service will usually be restarted each day following the backup, and the StorageFileWatch scan will occur naturally after the backup, so there should be no need to change the scan frequency.
- Any Outlook rules that a user has configured to deliver or copy messages into a PST file will no longer work after PST migration and removal of the PST file from the Outlook profile. This should be expected and communicated to users as part of PST migration awareness.
- The Enterprise Vault server that runs the PST Migrator Task must have a version of Outlook that matches, or is later than, the latest version of the clients. For example, if there are clients with Outlook 2003, then the server must have Outlook 2003 to ensure that the PST Migrator can understand the unicode format of PST files created in Outlook 2003. Beginning with Enterprise Vault 2007, only Outlook 2003 is supported on the Enterprise Vault server.
- As with client-driven PST migration, each computer scanned by the server-driven Locator will only be scanned once per day. To make the PST Locator Task search a computer again within the same day:
  1. Open SQL Enterprise Manager.
  2. Open the EnterpriseVaultDirectory database.
  3. Select the PSTComputers table and right-click. Choose "Return all rows."
  4. Find the row for the computer you want to search again.
  5. Change the LastHardDiskScan and LastRegistryScan fields to a date in the past.

6. Close the table.
7. Restart the PST Locator Task.

- Each PST file will only be marked once per user accessing it, and the marker will only persist for the last user accessing it. Therefore, make sure that you have finalized which Retention Category will be used (set in the PST Migration Policy) before enabling PST marking. Once a PST file has been marked, the Retention Category associated with that PST file *may* be changed via the Administration Console in the time between when the PST file is located (via either client- or server-driven migration) and when its migration starts. However, in practice, this is difficult, particularly with client-driven migration, in which timing is more difficult to control. Therefore, it is better to ensure the Retention Category is set correctly at the beginning. It is a common practice to use a specific Retention Category (or Categories) for PST migration so that those items can be expired or exported from the archive separately.

Removing migrated PST files from Microsoft Outlook profiles

Once a PST file has been migrated, usually it needs to be removed from the user's Outlook profile. As the goal is usually eradication of PST files, the administrator does not want to give users the opportunity to keep using and adding to a PST file once it has been migrated. Obviously, there will be exceptions to this rule, such as when the PST file contains shortcuts or non-archivable items, but generally, once a PST file has been migrated successfully, it is either deleted or set to read-only (which prevents it from being opened, as a PST file must be opened in read/write mode). PST files set to read-only would probably be cleared up later by another process, once the user and administrator were satisfied the migration was 100 percent successful.

Client-driven migration automatically removes a fully migrated PST file from the Outlook profile during it's post-processing phase. For all other methods, the Enterprise Vault End User Extensions may be configured to remove PST files from the Outlook profile on login; this is done by configuring the Remove PST Entries setting in the Advanced—Desktop settings of the mailbox policy as shown in Table 2.

Table 2 - Removing PST Entries

Remove PST Entries Value	Description
0	Do not remove the profile entry after migrating a PST file.
1	Remove the profile entry if the PST file has been deleted from the user's computer.
2	Remove the PST entry if the PST file is read-only.
4	Remove the PST entry if the PST file has the Hidden file attribute set.

Note that the values may be combined as required. For example, to remove PST entries for PST files that are hidden (4) or read-only (2), Remove PST Entries would be set to 6. Note that combining values results in an OR operation, so a value of 7 would result in PST entries being removed for PST files that are deleted (1) OR hidden (4), or read-only (2).

Preventing users from creating or opening PST files after migration

As eradication of PST files, and prevention of future usage, is normally the goal of PST migration, it is important to prevent users from creating additional PST files once the migration is completed (or even before the migration is completed to cap the number of PST files to be migrated). This is not currently a feature of Enterprise Vault but may be achieved in a number of ways, including setting a registry key on each computer (for Outlook 2003) as follows:

1. Start Registry Editor (Regedt32.exe).
2. Locate and then, for Outlook 2003, click the following key in the registry:

   HKEY_LOCAL_MACHINE\Software\Microsoft\Office\11.0\Outlook

   Or, for Outlook 2007

   HKEY_LOCAL_MACHINE\Software\Microsoft\Office\12.0\Outlook
3. For either version, on the Edit menu, click Add Value, and then add the following registry value:

   Value name: DisablePst

   Data type: REG_DWORD

   Value data: 1
4. Quit Registry Editor.

Care should be taken when stopping users from accessing PST files, as the Enterprise Vault User Extensions use PST files as temporary storage for some operations such as opening an item from a shortcut. The archived item is sent as the DVS file from the Enterprise Vault server to the client, and the message is extracted and loaded into the temporary PST file so that it can be opened in Outlook[3]. If support for PST files is completely removed from the user's desktop, then this operation will not work. In these circumstances, it is possible to have the Enterprise Vault server send the item as an MSG file, and then PST support is no longer needed for that operation to function. However, there is another Enterprise Vault client function, Vault Cache, for which PST files are used, and there is no alternative. Vault Cache utilizes PST files, renamed to have a .db file extension, for its cache. As each PST file is kept small—and is a *secondary* copy of the data, not the primary copy—this is a legitimate and effective use of PST files

[3] Note that from Enterprise Vault 8.0, the messages are sent from the EV server to the client in MSG format not in DVS format, and so this is no longer an issue.

About Symantec

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

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

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com