WHITE PAPER: TECHNICAL

symantec™

Confidence in a connected world.

PST Migration with Enterprise Vault 8.0: Part 1 - Solution Overview

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 1 – Solution Overview

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 provides a high-level overview of the PST problem, the issues with PST migration, and how the PST migration tools available in Enterprise Vault can solve them. For more detail on the tools themselves, and best practices and tips, please refer to the other whitepapers in this series.

The whitepaper is intended primarily for Symantec and partner System Engineers and aims to:

- prepare you to identify opportunities and present the value proposition for migrating PSTs with Symantec Enterprise Vault
- deliver a brief technical sales presentation regarding PST migration
- understand the technology fundamentals of PST migration

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.

Summary of the PST problem

PST files (also known as Personal Folders or Outlook data files) were not designed to handle the rigorous demands of today's large-scale corporate email requirements. However, many companies allow users to move email from Exchange into PST files for retention. Ultimately, these files create more problems than they solve and are one of the main reasons why organizations eventually seek an enterprise archiving solution. Common PST file problems include:

- Lack of centralized management of which users have created PST files, how many files exist, or what intellectual property they contain
- Propensity for data corruption with limited recovery, resulting in permanent data loss
- Impact on nightly backups, as the archive bit for any opened PST file will be changed and thus require a complete file backup, even if the file has only been viewed
- Increased storage requirements, as single instancing is lost when multiple copies of identical email messages and attachments are stored in disparate PST files
- Lack of content retention enforcement and compliance management
- Difficulty in searching, as a user can only search one PST file at a time, and it is virtually impossible for an organization to locate and search all PST files for compliance and/or discovery purposes, which in itself creates a level of corporate liability.

The Solution: Migrate the contents of PST files into Symantec Enterprise Vault

Symantec Enterprise Vault helps organizations solve the issues outlined in the previous section by migrating PST files into a central archiving repository. Migrating PST files involves more than just importing them into Enterprise Vault. It is a process that entails the following steps:

1. Locate. Enterprise Vault offers "push" and "pull" techniques for locating PST files that are referenced in Outlook profiles and/or that reside on file servers or user client machines.
2. Determine ownership. This critical step addresses the question of who owns the PST files. If an organization cannot automatically determine who owns a PST file, then it cannot automatically assign security to the information it is about to add to the archive. Enterprise Vault offers a number of techniques for establishing the ownership of a PST file and storing that information so that it can be used later to import the data into the appropriate user's archive.

3. Report. A centralized management view of the PST migration process is critical. The Enterprise Vault Administration Console shows a view of all PST file locations, their ownership, and their migration status.
4. Import. The migration of PST files into Enterprise Vault can be triggered manually or automatically within certain time periods. There are a number of different methods to drive PST migration, but all of them assign security and rationalize storage through single instancing and compression within Enterprise Vault.
5. Display. End-user access to imported content must be familiar and easy for a PST migration project to be successful. Enterprise Vault can present imported messages in Outlook, using the same folder names and hierarchy that imported PST files had at the time of migration.
6. Disposal of migrated PST files. Following the successful migration of a PST file, Enterprise Vault can automatically delete or hide it and remove it from the user's Outlook profile.

Overview and comparison of Enterprise Vault PST migration tools

Enterprise Vault provides the following tools for migrating (importing) the contents of PST files to archives:

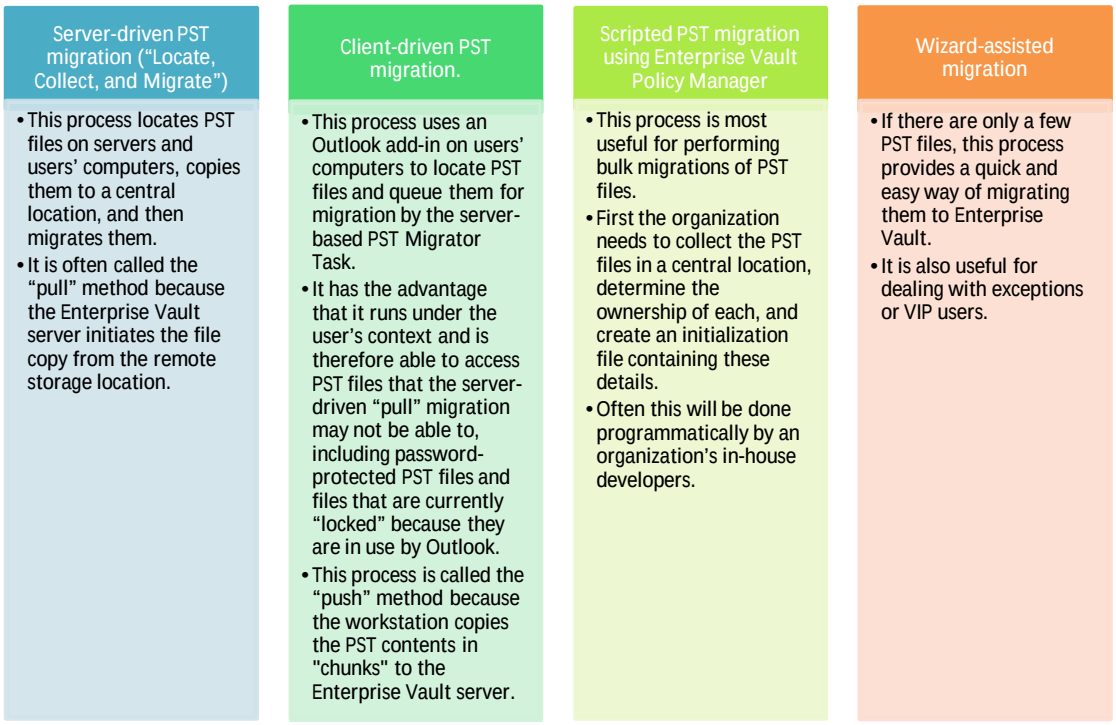


Table 1 provides a high-level functional comparison of the Enterprise Vault PST migration tools. A more detailed comparison of the specific features of each migration tool is provided in *PST Migration with Enterprise Vault 8.0: Part 2 – The Tools in Depth*

Table 1 - Enterprise Vault migration tools comparison

Feature	Server-Driven Migration	Client-Driven Migration	Wizard-Assisted Migration	Scripted Migration Using Enterprise Vault Policy Manager
Simple to use for a few PST files			ü	
Useful for dealing with exceptions or VIP users			ü	
Locates PST files on users' client machines	ü [1]	ü		
Locates PST files on file servers	ü	ü [2]		
Copies PST files to a central location prior to migration	ü	ü [3]		
Suitable for migrating large numbers of PST files	ü	ü		ü [4]
Can use supplied password to open PST file	ü	ü		
Can adjust Exchange Server quotas to allow creation of shortcuts	ü	ü		
Uses hidden mark in PST file to identify the last person accessing it to determine ownership	ü	ü	ü	ü
Uses Outlook profile to determine ownership	ü	ü		
Uses name of host computer to manually determine ownership	ü	ü		
Populates the user's local Vault Cache directly		ü		

A typical PST migration project will utilize two or more of these tools as appropriate; for example, server-driven migration might be the main tool used to locate, collect and migrate the majority of PST files, but the PST Migration Wizard might be used to first migrate the CEO's PST files under the watchful eye of their Executive Assistant.

[1] May be restricted by client security settings
[2] If PST is mapped in user's Outlook profile
[3] The PST contents are packaged in to 10MB chunks and copied to the EV server and ingested one-per client at a time
[4] PST files need to be listed in initialization file

Overview of common Enterprise Vault PST migration functionality

Regardless of which methods are used, PST migration with Enterprise Vault provides some features and functions common to two or more tools:

- Each archivable item found in the PST file is migrated into a mailbox archive—selected either manually or automatically depending on the migration method.
- Duplicate messages and attachments are single-instanced within Enterprise Vault; that is, if deemed identical via a fingerprinting process, only the first instance is stored and subsequent duplicate instances simply use pointers to the stored first instance.
- As a message or attachment is stored in Enterprise Vault, it is usually compressed (typically about 50% for Office 2003 documents). With the combination of compression and single-instancing, the amount of data to archive PST file contents can typically be less than 40% of the original data size, as illustrated in Figure 1.

Figure 1 - Comparison of original vs. archive storage for 100 GB of typical PST files

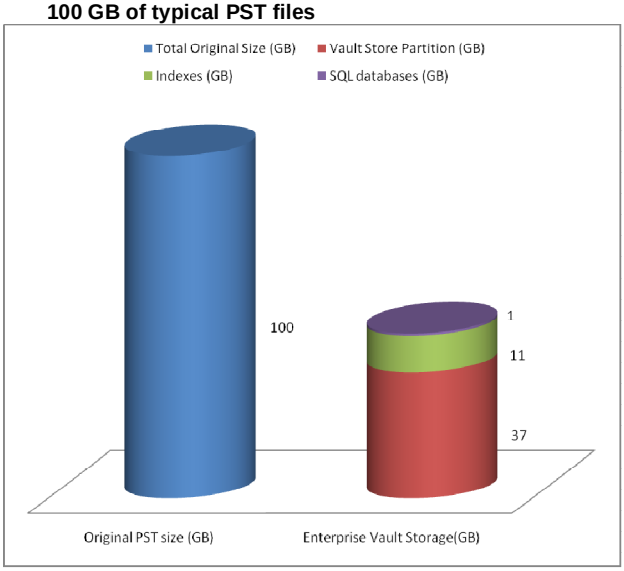
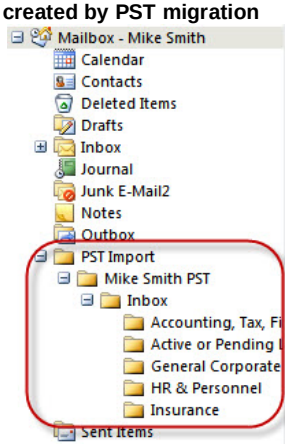


Figure 2 - Example of mailbox folders created by PST migration



- An HTML copy is created for web browser access and "future-proofing."
- The item's meta-data and, optionally, content[5] are indexed for searching.
- Optionally, shortcuts may be created in either the associated mailbox or the original PST file, or not at all. If shortcuts are created in mailboxes, then they are created in folder structures closely resembling the original folder structures in the PST files, although these may be merged if multiple PST files are being migrated for each user. Figure 2 gives an example.
- The number of shortcuts created in each mailbox can be limited by specifying a maximum age of messages for which shortcuts should be created.
- Non-archivable items are moved into the associated mailbox into the appropriate folders. Typical items would be contacts, tasks, and sticky notes that an organization has chosen not to archive. This ensures that the PST file is empty before deletion.
- Items migrated from each PST file are tagged with the same Retention Category, which identifies how long that item is to be retained in the archive. This may be taken from the PST Migration Policy in effect for that mailbox or specified manually, depending on which method has been used.

[5] depending on indexing level configured for the mailbox archive

- Once the PST file has been successfully migrated, it can be compressed, hidden, set as read-only or deleted. The Enterprise Vault Outlook add-in can be configured to automatically remove references to migrated PST files from the user's Outlook profile.
- If the migration has been configured to leave shortcuts in the mailbox, then an optional email message can be sent to the mailbox when each PST file is successfully migrated. The content of the message can be customized; typically this is done to explain to the user what has happened to their PST file, and how they can now access the data.

How Enterprise Vault meets PST migration challenges

As described previously, the process of migrating PST files into an archive solution presents challenges. Enterprise Vault meets those challenges as detailed in Table 2.

Table 2 – PST migration challenges and Enterprise Vault solutions

Challenge	Enterprise Vault Solutions
Locating the PST files - especially on PCs and laptops	The server-driven PST Locator Task uses NETBIOS or Active Directory to search specified domains, and then computers, for PST files by doing a hard-disk and/or registry search. Client-driven PST migration runs under the context of the logged-on user to search for their PST files using a hard-disk and/or registry search, and also targets the PST files open in the user's Outlook profile.
Accessing the PST files to migrate them (due to file permissions, passwords, users locking them, the PC being offline, etc.)	Server-driven migration can be scheduled to move the PST files to a central holding area overnight when users are not accessing them. Password-protected PST files are identified and, when the password is provided, can be input to the PST Migrator Task so it can open the PST file for migration. Client-driven migration runs under the context of the user and will prompt for the password to open the PST file, if necessary. Users may also have the PST files open and continue to use them, including adding items to the file, as it is migrated by client-driven migration. Client-driven migration also pushes chunks of the PST files to the Enterprise Vault server when the PC is online (solving the issue of PCs/laptops being switched off or not online), and these chunks are then migrated by the server-side PST Migrator Task. When the last chunk has been migrated, the PST file is removed from the user's profile automatically.
Network bandwidth consumed by PST migration	Server-driven migration can be configured to run on a schedule and the number and volume of PST files being migrated at any one time can be controlled. The server-side migration copies the PST file to a centralized holding area and then migrates it from there—minimizing network traffic. Client-driven migration sends each PST file it discovers in 10-megabyte chunks to the server for migration, one at a time, with the next chunk sent only when the previous one has been migrated.
Time consumption of migrating many gigabytes or terabytes of PST files	Migrating a large volume of PST files can take a long time; however, once Enterprise Vault PST migration is set up and scheduled, it can be left with minimal supervision to continue migrating PST files in the background. Client-driven migration in particular makes this process virtually transparent to end users. That said, Enterprise Vault PST migration is multi-threaded and each server may process up to 6 gigabytes of PST files per hour, with appropriately configured hardware.

Overcoming users' resistance to change in terms of the way they access their email	All Enterprise Vault PST migration methods make it possible to preserve the original folder structures from the PST files within the archives, and optionally within users' mailboxes. This means the impact on users, and amount of training required post-migration, is minimal. An email can be automatically sent to users after a PST file is migrated, informing them of the migration and giving them any additional information, such as usage tips, that the organization wants to communicate.
Removing migrated PST files from users' Outlook profiles seamlessly	If a PST file is moved from its original location for migration, or deleted after migration, then it should also be removed from the user's Outlook profile to prevent errors and confusion. The Enterprise Vault solution does this automatically.
Determining ownership of each PST file so that the contents can be migrated into the appropriate place in the archive and the appropriate access and security can be applied.	Enterprise Vault has several methods to determine the ownership of a PST file, including looking at the Windows permissions assigned to the folder where the PST file is located, or having the Enterprise Vault client "mark" a PST file with details of the last user that accessed it. Ownership can also be set manually to handle any exceptions, such as PST files being shared by multiple users or those not accessed recently. The Enterprise Vault administrator may also designate that any PST files found on a specific PC belong to a certain user.

More information

The remaining whitepapers in this series contain more information about the PST Migration tools available in Symantec Enterprise Vault 8.0, and are written to deeper technical level than this one, which is intended as an overview.

In addition, the standard Enterprise Vault documentation includes a detailed section on PST migration. For more information, refer to the following document:

> *Symantec Enterprise Vault™ Administrator's Guide*
> *Administrators_Guide.pdf* or *Administrators_Guide.chm* (compiled HTML help file)

These documents can be found in the Documentation folder on the Enterprise Vault distribution CD, or in the Enterprise Vault installation folder (usually C:\Program Files\Enterprise Vault) once the software has been installed.

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