

PST MIGRATION AND ZANTAZ EAS

If you use Microsoft Exchange for your corporate email system you are probably familiar with PST files, otherwise known as “personal storage files.” PST files are a famous annoyance to email system administrators and are a considerable nuisance for users. While they are intended to be a convenient tool to manage and administer corporate email, the reality is that the use of PST files has a detrimental impact on user productivity and causes increased administrative overhead.

PST files often contain private and proprietary information, but their ad-hoc creation results in potentially damaging data residing unmanaged and unmonitored on laptops, hard drives and network servers throughout an organization. The result is increased corporate risk in terms of litigation and regulatory compliance.

Both system administrators and email users struggle to manage the ever-rising tide of corporate email. The quantity and size of email is growing exponentially – frequently beyond the ability of organizations to effectively administer it. In an effort to reign in unwieldy mailboxes, system administrators frequently impose storage limits and users are forced to either delete messages or find other means of saving the information. In order to make room, PST files are used as a “dumping ground” for email and attachments.

While this may seem like a viable solution to email overload, PST files are notoriously unstable; they are easily corrupted, and the larger they become the more likely data will be lost.

THE PLAGUE OF PST FILES

Despite the beneficial aspects of email communication, electronic messaging systems do very little to help organizations manage their vast and dynamic stores of corporate email. While the folder system available in Microsoft Outlook appears to users to be a repository for email messages, the fact is that Outlook is not designed for permanent data storage. Email administrators find that system performance degrades rather quickly as email storage demand grows. When email servers become bogged down with data the more unstable the system becomes.

To avoid system outages and degradation, administrators often impose a limit, or quota, of how much storage users are allowed to consume. Once this threshold is reached users are forced to delete messages. Users get around this limitation by storing email in multiple places (often multiple times). As a result, email takes up residence in a hodge-podge of hard drives, disk drives, tape drives, laser disks, compact disks and network servers of all sizes and types throughout the enterprise. Analysts estimate that 30 percent of stored email records and their attachments can be eliminated because they are redundant copies.

Once stored in PST files, email data is essentially hidden from the organization; unmanaged by administrators and unmonitored by legal counsel and corporate compliance officers. This information, essentially a “corporate memory” of how an organization has conducted itself, is a potent and powerful factor during litigation. Courts in the U.S., as well as many other countries, have ruled that email relating to potential litigation must be preserved as evidence and is subject to disclosure. PST files make complying to a discovery request a difficult (if not impossible) and expensive undertaking. Ensuring compliance with statutory regulations and other compulsory policies is problematic as well. As a result, organizations are exposed to the risk of fines and penalties, shareholder mistrust and diminished customer confidence.

The bottom line is that PST files are a pervasive problem for most organizations that results in several acute managerial difficulties. PST files impact user productivity, drive up administrative costs, and expose organizations to increased litigation risk and compliance complications.

USER PRODUCTIVITY IMPACTS

The convenience of email has an infectious appeal and users are spending more and more time sending, receiving and storing email. Industry analysts estimate that management level workers currently spend an average of four hours a day working with email, and that email related activities are increasing at a rate of about 35 per year. While some of this growth may be due to the progressively pervasive use of email, a good deal of user time is wasted unnecessary filing and searching for email in PST files.

One reason for this is the fact that once email messages are offloaded to PST files, users may, or may not, remember where messages are stored in the ad-hoc archives. Hours are spent combing through the “sent” file or searching offloaded folders for lost messages. While most organizations have backup procedures for email, users cannot access the backup without getting an administrator involved. Many find that the time it takes to actually retrieve a message is often so long that in desperation they simply recreate the message or plead “system failure” in the face of penalties or fines.



Case Study – EDF Energy

When EDF Energy found that 50 percent of its storage capacity was taken up by personal archiving files, the IT department looked to e-mail archiving for a solution.

Rapid e-mail growth has meant trouble for users at EDF Energy, one the largest energy companies in the UK. As with many large enterprises, EDF Energy had instituted storage limits on e-mail to conserve disk space. This required users to constantly manage their inboxes to stay under quota. The choice was either to delete potentially important messages or create PST files.

While the creation of PST files provided temporary relief for users, they created headaches for the IT department. Corrupted PST files were a weekly occurrence that threatened the company’s ability to comply with regulations. Despite the difficulties, PST files kept growing and this created a storage predicament at EDF Energy. About 4 TB of storage space was being consumed by PST files; 50 percent of overall storage capacity.

“Given our large volume of data, I was particularly interested in how quickly data could be archived and retrieved,” said Mike Howard, an EDF Energy technology strategist. His team examined several e-mail archiving products and chose ZANTAZ Enterprise Archive Solution. ZANTAZ EAS enables organizations to create an archive of their corporate information including e-mail messages and files.

The archive provides two fundamental benefits. First, it improves e-mail system performance and stability by offloading large volumes of information in a central e-mail archive. This automated process optimizes storage through a “single instance storage” algorithm applied across the entire archive as well as optimal data compression of all archived objects. “ZANTAZ EAS’ single instance storage and compression dramatically improved performance

and were key factors in our decision to purchase EAS,” said Howard. Second, EAS preserves and protects corporate information assets for compliance with industry regulations and for supporting litigation events. With EAS, organizations can retain their e-mail and attached records for as long as regulations stipulate and can rapidly and reliably search for information required for litigation discovery.

EDF Energy is now archiving more than 1.5 million messages each week with EAS. The company has already drastically reduced storage demand and eliminated the need for PST files across the enterprise. With EAS, data that previously took two to three days to recover is retrieved in under a second, and PST file corruption has been eliminated. They have been able to eliminate the need for disk expansion for the data servers, which amounts to £100,000 in hard dollar savings, and when factoring the support savings on restoration of corrupt PST files the savings to the organization is far greater than expected. “The benefits of archiving digital information are seen at the operational level through efficiencies, and business level through easy access to information required for compliance,” said Howard.

For compliance, EDF Energy is now confident that when all PST files have migrated to EAS, all data will be easily and quickly retrieved. “With ZANTAZ EAS we have ensured compliance for e-mail as required,” said Howard. “EAS was a win-win installation for EDF Energy.”



While limiting the size of emailboxes may curb the demand for email storage in the short-term and temporarily alleviate sluggish system performance, the practice ultimately forces users to spend time managing their mailbox that would otherwise be more productively used.

ADMINISTRATIVE IMPACTS

When PST files grow in size they become unstable. As a result, administrations often find themselves with a substantial number of help desk calls from users needing assistance to recover information from corrupted PST files. Research indicates that it takes email administrators nearly two hours to recover a message if it is recent (within a month). The time stretches to over 11 hours if the message is over a year old. As a result, restoring email is a significant drain on administrative resources as well as user resources. One might think that it would be easier to restore a lost mailbox using PSTs but constant file corruption, along with difficulty getting access and completing backups, makes the job of restoring lost or damaged email messages a nightmare.

The inability of administrators to access and restore PST files can foil attempts to recover critical information contained in corrupted email boxes. The reason is that a PST can be opened by only one machine at a time. This prevents administrators and users from working from the same PST at the same time. Users often delete their PST files by mistake and forget their passwords, making recovery nearly impossible. Even though there are unsupported tools to crack lost passwords, it can take a significant amount of time to do so. The result is that valuable information is lost and time is wasted looking for or recreating messages.

LITIGATION AND COMPLIANCE IMPACTS

Negotiations, bids, proposals, contracts, legal agreements, regulatory forms, and a host of other vital correspondence now find form in email. For trial lawyers email often represents the “smoking gun” that will win their case or force a settlement and attorneys aggressively lobby courts for access to their opponents email stores. A variety of new regulatory and legislative acts have been implemented that require organizations to archive their email; some legal retention periods stretch from seven to 15, and even up to 26 years.

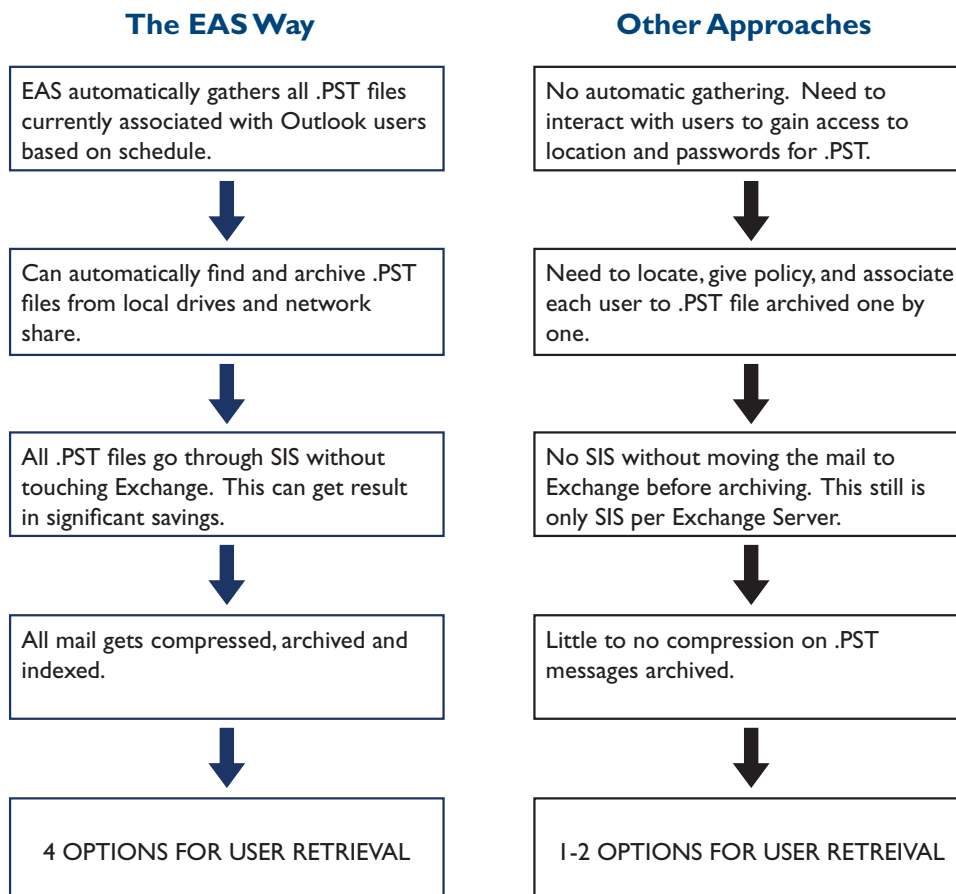
PST files make it nearly impossible to effectively store, find and examine all the information connected with a pressing legal or regulatory issue. Complying with an email discovery request, either from opposing counsel or a regulatory agency, can be extraordinarily difficult and costly. Companies will find themselves between a rock and a hard place when asked to produce all the email pertaining to a matter; often going back months or years. Scouring tape backups, network drives, workstations and laptops for relevant email takes tremendous effort. As a result, finding, filtering and reproducing the discovery information demanded can cost millions.

To mitigate the potential risks associated with discovery, some companies have a policy to intentionally delete email messages (after 90 days, for example). This type of approach can backfire, however, as was the case in the infamous “fen-phen” diet drug suit. One of the manufacturers was severely sanctioned for overwriting tape backups. The court instructed the jury to infer that the deleted messages contained evidence that was potentially damaging, and that the company had either negligently or intentionally destroyed the evidence

The bottom line is that companies really have no idea what is stored out in PST files. There is no administrative or management visibility to what has been created, what it says, or where it is located. PST files can result in critical or damaging information becoming “lost” in the system and, as a result, compliance and spoliation is a mounting corporate risk. Courts and regulatory agencies have very little patience for companies who claim that they don’t have adequate systems in place to manage, secure and control corporate email data.

SINGLE INSTANCE STORAGE

Administrators often point to the notion of “single instance storage” as the holy grail of effective email management. For example, if Mr. Smith, Mr. Jones and Ms. Brown all receive the same email, then later save that information in their own PST file, three copies of that message now exist. As a result, storage demand grows exponentially, administration requirements compound, and searching for and finding corresponding messages become increasingly complex. In this way, PST files apply a multiplicative factor on the volume of email that is stored enterprise wide and the associated implications. To make matters worse, if a user



sends an email with an attachment (a PDF file for example), to six different recipients, the result is six different instances of that PDF file in that individual's "sent" box. If that user then offloads his "sent" messages to a PST file the result will be six different copies of the PDF attachment in storage. Consequently, any hopes of storage optimization are completely compromised by the use of PST files.

Analysts estimate that an average of three extra copies of every email message (and associated attachments) are duplicated on corporate email systems. As a result, administrators are casting about for relief by ensuring true single instance storage. While marketing pundits often purport that Exchange facilitates single instance storage, the truth is that PST files encourage duplication and message redundancy is often rampant. The numbers can be staggering. Organizations can often suffer a doubling, or even tripling, of this redundancy across multiple mail stores.

Therefore, it stands to reason that by implementing single instance storage administrators can recover two-thirds of the space currently gobbled up by email and ensure that messages can be found and retrieved when needed. But again, PST files present a problem; preventing the potential savings in hardware and administrative costs and inhibiting the ability to effectively manage the risk associated with the information they contain.

CENTRALLY MANAGED EMAIL ARCHIVE

Instead of forcing users to create ad-hoc email archives by dumping messages into unmanaged PST files, a better administrative approach is to create centrally managed archive designed to store large volumes of email data and allow those messages to be retained and accessible at all times. This approach enables IT administrators to offload the burden on email servers and improve the stability and performance of their systems. It also eliminates user hassle and concern over email messages and allows workers to concentrate more productively on their core tasks and responsibilities. A centralized email archive provides corporate counsel and compliance officers immediate access to corporate email and bolsters the legal team's ability to quickly and completely respond to litigation or regulatory demands.

ZANTAZ EAS AND PST MIGRATION

Enterprise Archive Solution (EAS) from ZANTAZ is a highly scalable, Windows-based application that manages the archival and retrieval, and long-term retention of email and associated attachments for Microsoft Exchange. EAS offers options for automatic, policy-driven archival of email messages. With EAS, an organization will:

- Reduce the burden on servers without limiting the use of email
- Improve the reliability and performance of Microsoft Exchange
- Apply storage optimization with single instance storage and data compression
- Empower end-users to access, retrieve and restore mail that has been archived
- Decrease administrative overhead and lessen demand for help desk assistance
- Bolster the ability of corporate legal team's to quickly assess merits of a case
- Ensure quick and complete response to litigation discovery requests
- Improve the ability to demonstrate regulatory compliance

PST FILE GATHERING

EAS is able to locate all PST files created by any user and gather the messages and attachments for archiving. The files can be located anywhere on the network including user workstations and laptops. EAS accomplishes this with a fully automated scheduling process. This means that email administrators no longer have to set arbitrary storage limits and users are relieved of the burden and hassle of actively managing their mailbox. EAS automatically locates and flags all PST files, and this in turn increases the productivity of both administrators and users. With automated PST file gathering, EAS is able to archive user PST files without the need for intervention.

PST FILE ARCHIVING

EAS can archive PST files from local drives, network servers and individual laptops. During the archiving process, EAS applies single instance storage thus ensuring that duplicate copies do not clutter the archive and consume unnecessary storage. The application also applies sophisticated data compression for optimal storage efficiency. As a result, EAS will save an average of 50% of the required storage space typically required. An organization using EAS can be assured that all PST files will be securely archived, stored and accessible for future use.

PST FILE ACCESS

EAS provides immediate and complete access to PST files by creating indexes of archived files and messages to enable efficient search and retrieval. Users are empowered to find and restore lost email messages and attachments without help desk assistance. Administrators are given the ability to access files without delay and determine when they were created, where they reside and how much storage they consume. Legal teams and corporate compliance groups can quickly and completely search for, index and reproduce information to satisfy litigation discovery demands and regulatory compliance concerns. Access via EAS reduces administrative burden, frees users to be more productive, and allows legal teams the ability to quickly assess the merits of a legal case or compliance issue.

PST FILE SEARCHING

EAS gives corporate legal counsel and compliance officers the ability to construct and apply search lexicons – a group of words and terms that are designed to flag potential policy violations or identify relevant discovery data. For example, a broker-trader lexicon will search for words that might indicate insider trading. Other lexicons are constructed for specific industry compliance efforts – Sarbanes-Oxley or HIPAA, for example. Search lexicons can also monitor specific corporate policies around sexual harassment or race discrimination, for example; identifying possible violations for compliance officers who can then review the relevant email messages before litigation issues arise.

PST FILE COMPRESSION AND STORAGE

EAS offers industry-leading file compression resulting in 50% - 80% reduction in storage demand. As a result, organizations benefit from significant savings in space. The quantity and size of email is growing rapidly and with email space requirements reduced, organizations will in turn reduce the cost of enterprise storage overall. In addition to data compression, EAS offers true single instance storage, eliminating redundant email messages and duplicate file attachments. This minimizes the storage demands while increasing the operational performance of Microsoft Exchange servers.

CONCLUSION

PST files may appear to be a convenient tool to manage and administer corporate email, but the implications of their use drive negative impact to user productivity, cause costly administrative overhead, and increase corporate risk in terms of litigation and regulatory compliance. PST files inhibit the ability of organizations to locate, monitor and store critical email and attachments in an organized method. Additionally, PST files tend to be overlooked in the scope of records disposition because organizations lack the necessary tools to locate every PST file that may reside throughout the infrastructure when needed.

EAS is the only solution to employ automatic PST file gathering, data compression and single instance storage. EAS significantly reduces email server overload while securing potentially damaging information and protecting intellectual property. End users are empowered to access, retrieve and restore email regardless of their geographic location and without administrative assistance. Users and administrators, as well as compliance officers and legal counsel have the ability to find information much more readily with completeness and security.

For many organizations, EAS solves the problems and high risks associated with PST files by allowing organizations to gain control over their electronic messaging environment and providing a reliable, flexible and secure archive of all corporate email.