



MIMOSA
SYSTEMS

White Paper

By Martin Tuip

September 2008

Strategies for PST File Elimination

*Information Immediacy, Discovery
and Continuity*

CONTENTS

Introduction 3

PST File History 3

 Why Did PSTs Become So Popular? 3

PST Legal and Compliance Problems 4

PST File Elimination Strategy 5

The Mimosa NearPoint PST Archiving Option 5

Conclusion 7

Introduction

Email growth is exploding, and the common practice of saving old email and attachments is overburdening email servers. Email usage is expected to grow by 25 to 40 percent annually for the next few years, according to the Radicati Group, impacting performance, recoverability, and total cost of ownership. Email quotas can put a fixed limit on server growth and capacity, but quotas reduce employee productivity and force employees to find off-host methods to store email (PST files)—a practice that increases security risk. The optimal solution to manage email storage is to reduce total storage through selective archiving of old email and attachments to nearline storage that is designed to store and manage large amounts of data. Email servers run more efficiently when overall storage is reduced, and users' productivity improves with easy access to archived messages. This paper will review the Mimosa NearPoint™ for Microsoft® Exchange disk-based data management solution, which optimizes the storage capabilities of Microsoft Exchange Server.

PST File History

In the early days of Exchange, end users had very limited mailbox sizes—around 5MB to 10MB. To store data outside of Exchange, and also to store data when users weren't connected to an Exchange Server, users had the option to create a Microsoft Outlook Personal Store (PST) file. These files were managed through Outlook and allowed end users to drag and drop data to them. The first PST version had a 2GB storage limit, which increased in the unencoded version that became available with Outlook 2003.

Why Did PSTs Become So Popular?

PST files became very popular very quickly because they are easy to use, and Outlook automatically creates PST files for the end user. Though Exchange administrators set low mailbox limits to encourage users to get rid of old email, end users instead created PST files and started to move their data to these files. In addition, PST files gave end users access to their data when they were not connected to the network, so many laptop users moved their data to PST files from their mailbox.

The problem created by this movement to PST files, however, is that there is no centralized management or control of PST files. End users control the creation and location of PST files, which means that the growth of PST files has taken place undetected for more than a decade and is now problematic in several areas:

Size Limitations and Data Loss. When the PST file size is pushed to its limit, chances are that corruption will occur, ultimately resulting in a loss of data since few options are available to recover data successfully from such a state. And for PST files located on local or remote machines that are not part of a general backup process, no backup is available in case of file corruption.

Infrastructure Cost. PST files have a significant impact on IT helpdesks, since end users typically contact the IT helpdesk in an attempt to save corrupted PST files, resulting in higher IT management costs. Also, users of personal folders usually have multiple copies of documents within their PST files. When thousands of users are involved, the increased storage requirements and costs for an enterprise become significant.

Enterprise Risk. PST files are a very portable format and can be used by end users to take their mailbox with them when they leave a company. In addition, PST files can contain critical or confidential information that might be exposed when a laptop is lost or stolen.

PST Legal and Compliance Problems

Just as is the case with regular email, PST files contain data that is considered a business record and so is subject to eDiscovery requests. As mentioned earlier, the nature of PST files and their dispersed storage locations make it nearly impossible for organizations to perform records retention on the data residing in these files, or to dispose of records and emails that no longer need to be retained for compliance or business reasons. Litigation causes another major problem area, as the information in PST files is stored locally and is difficult to search and collect. In most litigation situations involving PST files, manual intervention is needed to get the data required for eDiscovery.

In the end, organizations that do not resolve the enormous risk that PST files pose risk losing or failing to preserve critical business records. To properly control and manage corporate information, organizations need to review the usage and risks of PST files, create a policy regarding their existing and future use, and implement and enforce that policy.

PST File Elimination Strategy

The strategy to eliminate PST files in an organization is fairly simple, consisting of the following steps:

1. Create a policy that prohibits the use of PST files.
2. Search and discover all existing PST files.
3. Store PST data in a central archive.
4. Provide self-service access for end users.
5. Optionally, disable PST files.

The Mimosa NearPoint PST Archiving Option

The Mimosa NearPoint PST Archiving Option archives PST files into the NearPoint archive. With this Option, PST files are automatically located across many servers and laptops, characterized to a given user account, and actively imported (or ingested) into the NearPoint archive. With the easy-to-use NearPoint wizard-driven menus, administrators manage all aspects of PST archiving using a dedicated PST Archive management console (Figure 1). And for end users who want to retain personal control over their PST files, a manual PST archiving method is available that operates within Outlook. Once PST files are loaded into the NearPoint archive, the PST data can be viewed by its original folder hierarchy and searched by auditors to support legal discovery. (Figure 2) By using the PST Archiving Option, administrators can eliminate the need for PST files altogether. The NearPoint PST Archiving Option offers these benefits:

- Allows central management of all PST data in an indexed email archive.
- Enables full-text search of all PST data, including attachments, for legal discovery.
- Offers Self-Service Access™ for legal discovery and individual search and retrieval.
- Applies company email retention and disposition policies consistently for compliance.
- Eliminates the need for PST files and reduces storage demand on desktops and file servers.

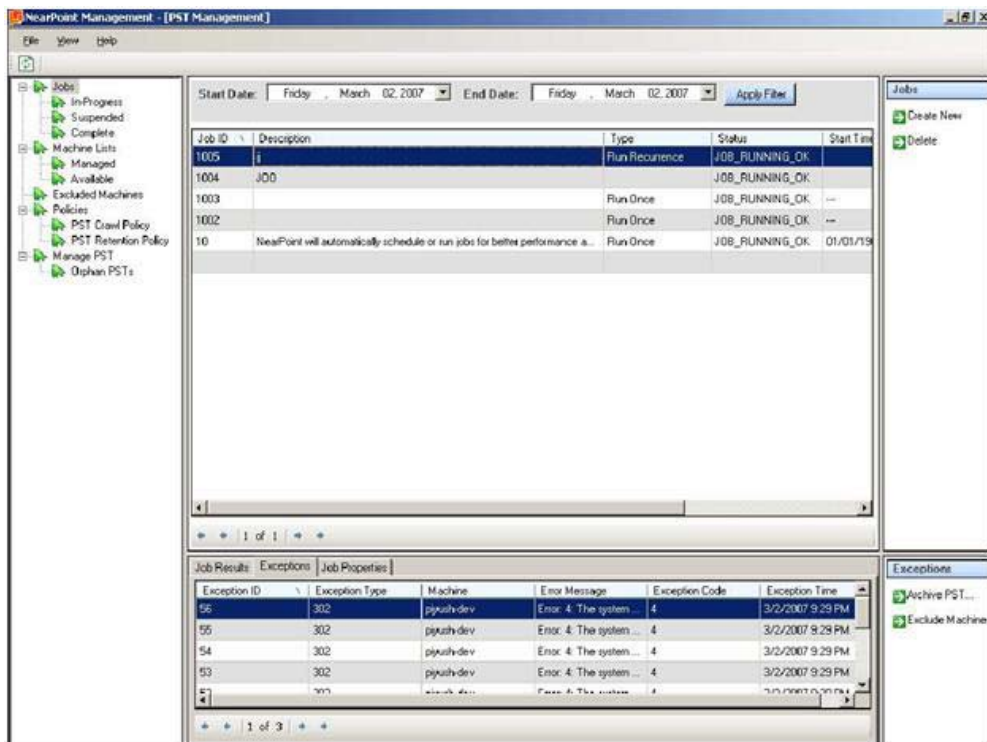


Figure 1. Mimosa NearPoint PST Archive Management Console

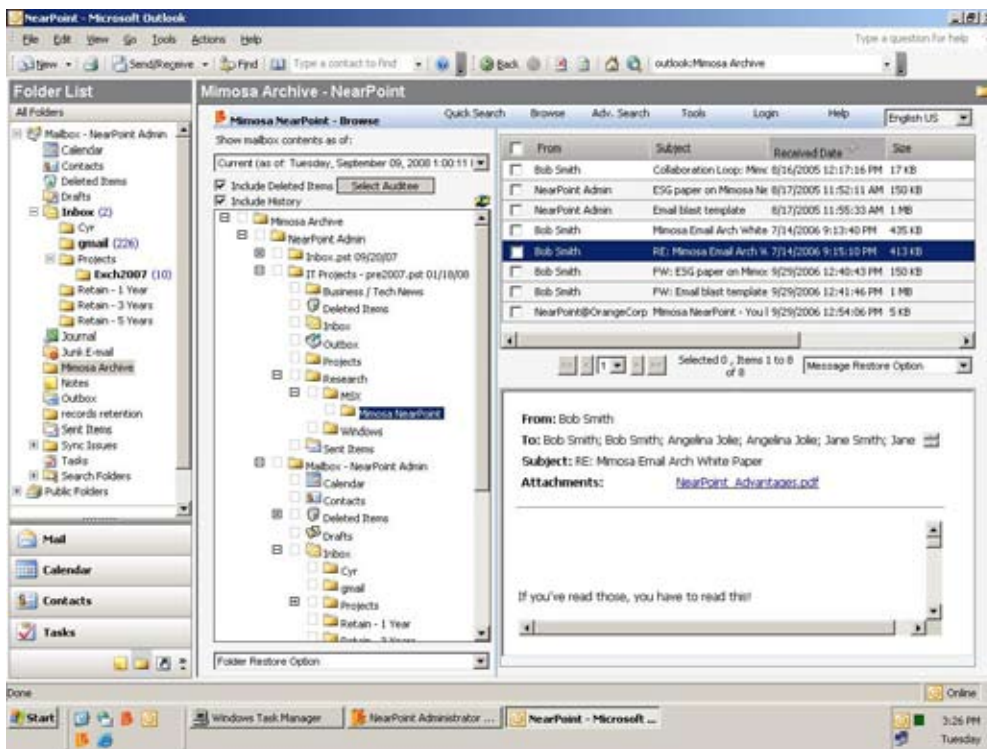


Figure 2. Mimosa NearPoint Self Service Access with PST View

Conclusion

Managing Exchange storage is a balancing act between users who want to store more data and administrators who want a smaller Exchange database. Mimosa NearPoint complements Microsoft Exchange by off-loading the burden of managing cumbersome attachment files. This action dramatically reduces total Exchange storage and results in faster backups (and recoveries) and improved overall Exchange efficiency. Excess Exchange storage capacity can be used to support additional mailboxes per server, or it can be saved for future growth needs. Using the NearPoint PST Archiving Option, existing PST files are archived directly into the NearPoint archive, where the data they contain is protected and searchable. Mimosa NearPoint stores and manages an indexed repository of all Exchange items and supports fast, self-service access of all historical email by users and auditors. You can rely on NearPoint for its superior search and restore ability, and let NearPoint manage Exchange data over its entire life cycle. Exchange Server runs faster and more efficiently when its storage is optimized using Mimosa NearPoint for Microsoft Exchange.

For more information about Mimosa NearPoint for Microsoft Exchange Server, contact your Mimosa Sales Representative at (408) 970-9070 or visit our web site at www.mimosasystems.com.



MIMOSA SYSTEMS HEADQUARTERS

United States
 3200 Coronado Drive
 Santa Clara, CA 95054
 T 408-970-9070
 F 408-970-9041

Email: info@mimosasystems.com
 Sales: sales@mimosasystems.com
 Technical Support: support@mimosasystems.com
 Public Relations: pr@mimosasystems.com

WORLDWIDE OFFICES

United Kingdom
 400 Thames Valley Park Drive
 Thames Valley Park
 Reading RG6 1PT
 T +44 (0) 118 963 7860

Germany
 Max-Plank-Strasse 8
 85609 Aschheim-Dornach
 T +49 89 904 7551-0

India
 8th Floor, Amar Genesis
 ITI Road, Aundh
 Pune 411 007 India
 T +91 20 4048596



Partner

© 2008 Mimosa Systems, Inc. All rights reserved worldwide. Mimosa, Mimosa Systems, the Mimosa logo, Mimosa NearPoint, and Self-Service Access are trademarks of Mimosa Systems, Inc. in the United States and other countries. Other product names mentioned herein may be trademarks or registered trademarks of their respective owners. PTWP_0908_NA