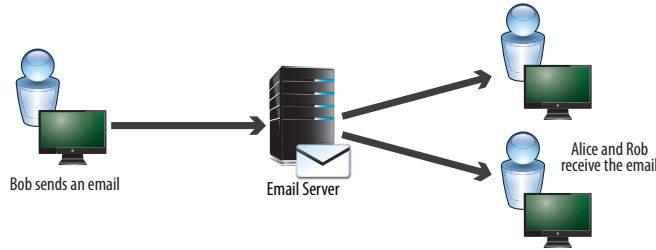


Implementing a PST Management Strategy with the Barracuda Message Archiver

Introduction

PST files have become very common in today's email environment. Typically, when users send and receive email, they are stored on the email server and can be accessed at any time. Growth in usage of email means storage requirements on email servers is growing exponentially. To prevent costs associated with expensive transactional storage, many administrators experiment with offloading emails from the servers into PST files.

RELEASE 1
JULY 2009



Pros:

- Easy access for users
- Single Instance Storage

Cons:

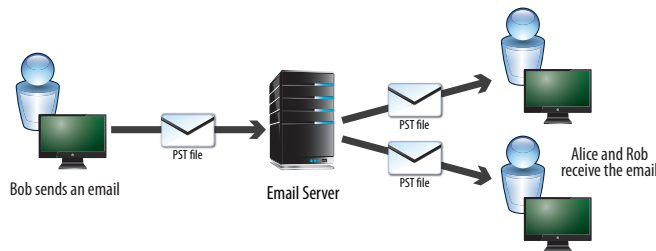
- Soaring costs of storage
- Performance problems
- Licensing issues

PST files have significant downsides. Many organizations are looking for a comprehensive strategy to manage PST files. Eliminating PST files can be done in conjunction with an active archiving. This whitepaper will discuss the problems associated with PST files and lay out a detailed strategy to manage current PST files and ensure that they are not created in the future.

Introduction to PST Files

PST files are used by Microsoft email products, notably Microsoft Outlook, to store local copies of messages, contacts, calendar events, and notes. Since they act as local repositories, PST files are used to offload emails from the email server. Many email users utilize PST files to save emails that can no longer be stored on the server due to mailbox quota restrictions. This process removes emails from the server and moves them to the PST file for local storage. These files can be moved from one system to another and can also be used without an available Microsoft Exchange server.

Problems with PST Files



Pros:

- Reduced load on the server

Cons:

- No Single Instance Storage
- Searching across multiple copies
- Backup storage problems
- Compliance Issues

Moving emails from the server into PST files creates significant challenges. For example, PST files often get corrupted. This happens as users add emails to a PST file indiscriminately. Even minor system hiccups while updating a PST file can cause fatal errors. The probability of errors during updates increases as the size of the PST file grows. Corrupt PST files can cause all emails to become unavailable. When this happens, the user is left without access to their emails and the organization loses valuable information.

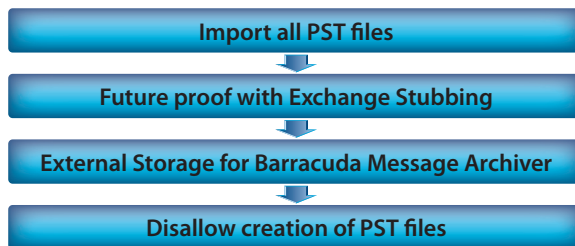
PST files can be used without access to a Microsoft Exchange server. This poses a serious security risk when a user loses their laptop containing PST files. The PST file can be accessed by unauthorized users to retrieve contacts, calendar information, notes, and emails. It is also time consuming to restore emails. A lost laptop is not the only time PST files can be a security issue. A disgruntled employee can delete emails before leaving the company or steal PST files by copying them to a USB storage device.

PST files complicate finding emails. In case of an e-discovery request, an auditor has to ensure that all users' PST files are searched. This is further complicated by the fact that some users might be remote or travelling and their PST files are not available for a period of time.

The distributed nature of PST files causes further complications in terms of compliance and storage management. Since users still have the ultimate control over emails and other items stored in PST files, emails and other items can be deleted from PST files. Furthermore, emails with identical sender and recipient information are stored in multiple locations. Single instance storage is no longer applicable when emails are not stored centrally. If the organization backs up a user's PST files, this lack of single instance storage is often the cause of ballooning storage requirements. The situation is ironic since the original intent of creating PST files was to reduce storage requirements in the first place.

Strategies for eliminating PST files

Removing PST files should not create new problems like increasing storage requirements on the email server or force users to delete emails. Thus, advanced planning is essential for eliminating PST files. The following is presented as a series of steps to plan for eliminating the use of PST files in the organization.



Importing Existing PST files

An email archival solution, like the Barracuda Message Archiver, should be used import emails in the PST files. By importing PST files, all emails can be searched from a single place. Additionally, since all emails now reside in a single repository, the Barracuda Message Archiver can perform deduplication of data to eliminate duplicate copies of emails and attachments.

Dealing with mailbox quotas

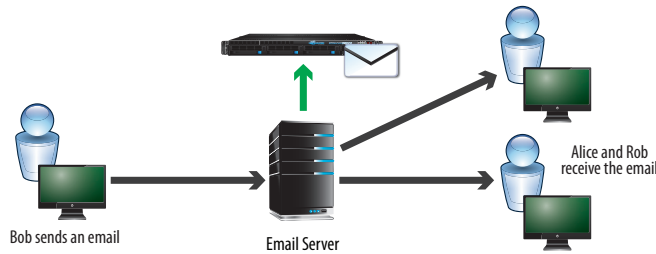
Once PST files have been eliminated from the organization, users will face the problem of storing email. Allowing users to continue storing emails on the server is the wrong solution. With the Exchange Stubbing feature of the Barracuda Message Archiver, email attachments can be removed from the email server and replaced with a small sized pointer or stub. This process eliminates older emails from the email server while still preserving seamless access for users. Users will be able to access stubbed emails from within Microsoft Outlook or Microsoft Outlook Web Access (OWA). Mailbox quota will be a non-issue since emails will not clutter the email server.

Plan for Storage

Any solution that replaces storage of emails in PST files needs to provide robust and scalable storage architecture. The Barracuda Message Archiver features integrated internal storage and has the ability to integrate with external network attached storage. This allows robust storage scalability.

Preventing PST files in the future

Once existing PST files have been eliminated (after importing them in Barracuda Message Archiver) and mailbox space issues have been managed, the last challenge is to make sure new PST files do not get created. There are registry settings available to prevent PST files from being produced in the future.

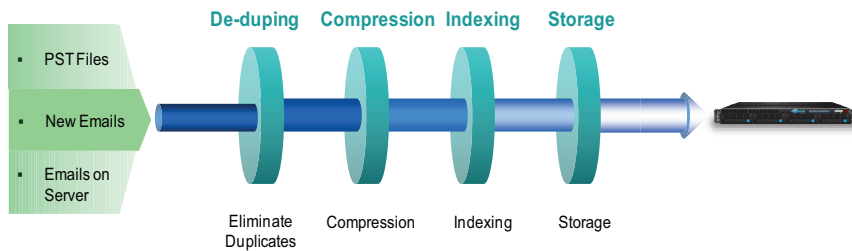


Benefits:

- Single Instance Storage
- Compliant
- Easy to search and satisfy discovery requests
- Easy access to archived emails
- Improved performance of email server
- Reduce cost of storage on email server

About Barracuda Message Archiver

The Barracuda Message Archiver is instrumental in the strategy to eliminate PST files.



The Barracuda Message Archiver is a complete and affordable email archiving solution, enabling users to effectively index and preserve all emails, enhance operational efficiencies, and achieve regulatory compliance needs. All content is deduplicated to ensure only one copy of information is stored and that duplicates do not clog up storage or search results. By leveraging standard policies and seamless access to messages, email content is fully indexed and backed up to enable administrators, auditors, and end users quick retrieval of any email message stored in an organization's email archive.

Conclusion

The right email archiving solution can benefit your email environment in many ways. PST files are increasingly seen as a security threat and an operational nightmare. Eliminating PST files is a priority, but to effectively manage and eliminate them advanced planning is required.

For questions about the Barracuda Message Archiver, please visit <http://www.barracuda.com/archiver> or call Barracuda Networks for a free 30-day evaluation at 1-888-ANTI-SPAM or +1 408-342-5400. For more information on our other security and productivity solutions, please visit <http://www.barracuda.com/products>.

About Barracuda Networks Inc.

Barracuda Networks Inc. combines premise-based gateways and software, cloud services, and sophisticated remote support to deliver comprehensive security, networking and storage solutions. The company's expansive product portfolio includes offerings for protection against email, Web and IM threats as well as products that improve application delivery and network access, message archiving, backup and data protection.

Coca-Cola, FedEx, Harvard University, IBM, L'Oreal, and Europcar are among the more than 100,000 organizations protecting their IT infrastructures with Barracuda Networks' range of affordable, easy-to-deploy and manage solutions. Barracuda Networks is privately held with its International headquarters in Campbell, Calif. For more information, please visit www.barracudanetworks.com.



Barracuda Networks
3175 S. Winchester Boulevard
Campbell, CA 95008
United States
+1 408.342.5400
www.barracuda.com
info@barracuda.com