



MIMOSA
SYSTEMS

White Paper

By Martin Tuip

Mimosa Systems, Inc.

April 2008

Messaging, Compliance, and Archiving

*Mimosa™ NearPoint™ for Microsoft®
Exchange Server*

CONTENTS

Introduction4

Business Today5

 Email Archiving Reduces Risk.....6

Current Regulatory and Legal Environment.....7

 The Sarbanes-Oxley Act (SOX).....7

 New Amendments to the FRCP7

 SEC Rules 17a-3 and 17a-4.....8

 Health Insurance Portability and Accountability Act (HIPAA).....8

 Title 21 CFR Part 118

 ISO 15489 (Worldwide)8

 Federal Acquisition Regulations (FAR) Subpart 4.7,
 Contractors Records Retention8

 Title 17 CFR Part 19

 FERC Part 125.....9

 NARA Part 1234.....9

 Freedom of Information Act (FOIA)—for Federal Agencies9

 The Patriot Act.....9

 Federal Employment-Related Regulations 10

 Data Protection Directive (EU)..... 10

 Markets in Financial Instruments Directive (EU) 11

 Freedom of Information Act 2000 (UK) 11

Retaining and Disposing Messaging Data 11

 What Data Needs to Be Preserved 12

 Deciding on Information Retention Categories..... 12

 Disposition of Email from the Email Archive..... 13

The Benefits of Data Consolidation	14
Deployment Features of Exchange 2007	15
Compliance Support.....	16
Legal Discovery.....	17
Retention and Disposition	17
Exchange Migration	18
Exchange Local Recovery of Exchange 2007	19
Remote Recovery of Exchange 2007.....	19
PST File Elimination	22
Unified Messaging Management.....	22
Exchange Version Support.....	23
Log Shipping Versus Journaling/Mailbox Archiving	23
Application Shadowing	24
Application Shadowing Versus Journaling	25
MAPI Does Not Capture All Information.....	26
Performance Advantages.....	26
eDiscovery Advantages	27
Data Protection Advantages	28
Performance Data	28
System Details	28
Tests Performed	29
Test Results	29
Creating the Solution.....	31
Conclusion	32
Related Links.....	31

Introduction

Since the rise of archiving systems in business more than a decade ago, the technology has made great strides forward. Recently, stringent regulations (e.g., SEC-Rule 17a-4) and highly demanding litigation procedures (e.g., the amended Federal Rules of Civil Procedure) have amplified the need for a strong archive system. Messaging systems such as Microsoft® Exchange Server 2007—Microsoft’s latest version of Exchange Server—have also seen their share of changes and improvements in archiving and compliance.

This document is intended as a guide and a blueprint for organizations looking at deploying Microsoft Exchange Server 2007 and Mimosa™ NearPoint™ in their environment. The author has written this whitepaper based on his decade-long experience and knowledge of messaging systems, compliance, and archiving.

About the Author

Martin Tuip is a business development manager for Mimosa Systems, and he lives in the foothills of the Cascade mountain range in Washington state. A published author, he has been awarded the Microsoft Exchange MVP award for nine years in a row. In his IT career he has advised customers about their messaging and archiving system deployments, and he has had a long career working in management and technical roles in the archiving industry.

Business Today

The days of the paper memo as the dominant means of business communications are over. A full 90 percent of business communication today occurs via electronic means—email, instant message (IM), and voicemail.¹

While this change to electronic communication has created huge advances, it also has serious—and costly—repercussions as evidenced by some famous cases from the news. The infamous implosion in 2002 of one of the “Big Five” accounting firms, Arthur Anderson, was largely a result of evidence that came through email in the Enron scandal. Citibank suffered \$400 million in penalties after the attorney general of New York state subpoenaed emails written by stock analyst Jack Grubman and Citigroup chairman Sanford I. Weill. In 2004 the stock price of insurance broker Marsh & McLennan dropped a dramatic 50 percent after emails revealed evidence of kickbacks from insurers. Merrill Lynch was fined \$100 million based on email evidence that they called investments which they publicly hailed, as “dogs” and “disasters” in emails.

The financial company Morgan Stanley has paid millions in fines over the past several years due to its failure to provide requested emails in court and its failure to comply with SEC orders to cease and desist overwriting email backup tapes. Even PriceWaterhouseCoopers had a federal judge recommend a default judgment against them for deleting emails relevant to a \$139 million shareholder suit.

Email discovery is a fact of life, whether it is required by external regulatory investigations, litigation, or internal investigations (such as HR issues). The courts have decided that companies have to keep and be able to recover emails in a reasonable time, as well as show that the email records are complete and not changed. The Amendments to the Federal Rules of Civil Procedure (FRCP), which went into effect on December 1, 2006, require that companies document and enforce policies to retain emails or dispose of them as part of standard operating procedures. According to the FRCP, companies must also discover relevant emails within a reasonable timeframe. Therefore, it is now essential that organizations have in place processes and procedures that can find email and IMs, monitor potential exposure from email and IMs, and understand and mitigate litigation risk.

¹ More than 30 billion emails are sent daily worldwide, more than 90 percent of *all* information is now electronic, and 70 percent of electronic information has never been printed. Source: American Bar Association Digital Evidence Project, February 2005.

Email Archiving Reduces Risk

Today email is held in a variety of locations—on email servers, PCs, file and print servers, DVDs, tapes, and other media. Most organizations lack the ability to reliably find specific emails, and attorneys are now skilled at understanding the weaknesses of email systems and of demonstrating those weaknesses to the court.

Email archiving provides an especially good base platform on which to build systems that identify and mitigate this risk. Companies must ensure that they document the technology, processes, and procedures they use to capture email and IM content, and they must manage the chain of custody of that content to avoid spoliation (in other words, make sure that emails have not been changed). In addition, companies must be able to recover any email in full quickly (SEC Rule 17A requires retrieval within 48 hours). Research shows that the primary driver for implementing email archiving systems is risk reduction—with legal or even corporate boards taking the lead in demanding implementation of an archiving system.²

The degree of risk exposure varies by industry and the degree of regulation. In highly regulated industries (such as financial broker/dealers) compliance is imperative; failure to comply can result not only in multi-million dollar fines, but also in a termination of the business itself—email archiving is necessary and a cost of doing business. At the other end of the spectrum, a local retail shop with small profit margins, for example, might not justify the cost of implementing an email archive system. Organizations such as pharmaceutical companies with a high potential of being sued would be in the middle. For some organizations, the requirement to keep email as proof of contracts (enabled by the Electronic Signatures in Global and National Commerce Act) could be the deciding factor.

Email archiving provides an infrastructure base for organizations to reduce risk. The IT staff plays an important role in putting an archive system in place, but others within the organization—in compliance, legal, and business operations—are usually needed for their help with implementation procedures and other technologies to reduce risk (e.g., compliance training, filtering email for words and phrases, eDiscovery). For specifics on setting up the correct infrastructure to reduce risk, refer to “Creating the Solution” later in this whitepaper.

² The typical Fortune 500 company has 125 ongoing cases, with at least 75 percent requiring electronic discovery; it's estimated that U.S. companies spent \$1.2 billion in outside eDiscovery services in 2005 and \$1.9 billion in 2006, and 62 percent of companies surveyed doubt they can show that their electronic records are accurate and reliable. Source: American Bar Association Digital Evidence Project, February 2005.

Current Regulatory and Legal Environment

Odds are very high that your company or firm is subject to some regulation about how you retain records. Some industries might face stricter rules than others (a health care company is probably subject to more rules than a tool-and-die shop, for example), but regulations are something that just about everybody has to deal with.

This section reviews some of the current laws regarding email retention.

The Sarbanes-Oxley Act (SOX)

Passed mostly in response to the front-page news headlines of corporate corruption and financial scandals in recent years—namely Enron and WorldCom—SOX provides severe criminal penalties, including prison sentences, for corporate executives who knowingly destroy business documents and other information used in running the enterprise. The act also calls out specific types of records that need to be retained and requires a records retention period of seven years.

New Amendments to the FRCP

A number of amendments to the Federal Rules of Civil Procedures (FRCP) took effect on December 1, 2006. These new revisions are having a major effect on how companies retain, store, and produce electronic data for litigation. The rules that most affect organizations now are:

Rules 16 and 26. These rules call for organizations to “...give early attention to issues relating to electronic discovery, including the frequently recurring problems of the preservation of the evidence...” Organizations must be ready to discuss a strategy for dealing with electronically stored evidence at the very first meeting with other parties in litigation.

Rule 37(f). This rule provides a “safe harbor” for data destruction. Organizations face no penalties for deleting electronically stored information in keeping with routine operation of IT systems if the party took “reasonable” steps to preserve it. However, any destruction must result from routine operation and be done in good faith, a systemized framework must be in place, and this systemized framework must have integrated litigation hold procedures.

Rule 34(b). This rule requires organizations to produce electronically stored information in its native format with its metadata intact and to prove chain of custody. While the duty to preserve evidence is narrowed only to relevant data, the potential repercussions are great. For example, if a defensible process is not demonstrated, opponents might be granted access to an organization’s network.

SEC Rules 17a-3 and 17a-4

These rules require brokers and traders to retain and store specific records, such as customer communications and customer account trading activities, for a specific period of time on nonrewritable electronic media (WORM) and make them ready for easy review by the SEC within a reasonable timeframe, typically 24 hours.

Health Insurance Portability and Accountability Act (HIPAA)

Among other things, HIPAA requires that patient records and related data (including related email) must be archived for at least two years after the death of the patient in a secure manner that ensures privacy and content integrity.

Title 21 CFR Part 11

This rule requires that “copies” of all records be kept “in common portable formats” and that the original content and meaning of the records must be preserved. It also requires the protection of records to enable their accurate and ready retrieval throughout the records retention period. Retention periods include:

- Food (manufacturing, processing, packing): Two years after release
- Drugs (manufacturing, processing, packing): Three years after distribution
- Bio products (manufacturing, processing, packing): Five years after end of manufacturing

ISO 15489 (Worldwide)

This standard offers guidelines on the classification, conversion, destruction, disposition, migration, preservation, tracking, and transfer of records.

Federal Acquisition Regulations (FAR) Subpart 4.7, Contractors Records Retention

This regulation provides policies and procedures for retention of records by federal government contractors to meet the records review requirements. All individuals and companies who contract to supply goods or services to the federal government must retain all related records—hard copy or electronic. It also provides for “timely and convenient access” in the case of an audit, and it applies to both conventional and electronic records.

Title 17 CFR Part 1

This regulation allows record keepers for futures trading companies to store information either on electronic media or on micrographic media. This regulation also requires that “record keepers store required records for the full five-year maintenance period” while continuing to provide commission auditors and investigators with timely access to a reliable system of records.

FERC Part 125

This rule sets specific retention periods for the public utilities industry and states that the records must have a life expectancy equal to or greater than the specified retention periods.

NARA Part 1234

The National Archives and Records Administration (NARA) regulations specify what government agency records are kept, for how long, and in what form, and how they are to be accessed.

Freedom of Information Act (FOIA)—for Federal Agencies

FOIA allows for the full or partial disclosure of previously unreleased information and documents controlled by the U.S. Government. The act, which relies on the NARA regulations above, defines federal agency records subject to disclosure, outlines mandatory disclosure procedures, and under certain circumstances, specifies timeframes for response.

The Patriot Act

The Patriot Act requires the Secretary of the Treasury to prescribe regulations “setting forth the minimum standards for financial institutions and their customers regarding the identity of the customer that shall apply in connection with the opening of an account at a financial institution.” Broker/dealers must have a fully implemented customer identification program (CIP) that includes procedures for making and maintaining a record of all information obtained.

Federal Employment-Related Regulations

Many federal employment regulations require some sort of records retention, and they apply to all companies with employees. Some of the better-known regulations are:

- Title VII of the Civil Rights Act of 1964
- Age Discrimination in Employment Act
- Americans with Disabilities Act
- Family and Medical Leave Act
- Equal Pay Act of 1963
- Vocational Rehabilitation Act
- Employee Retirement Income Security Act of 1974
- National Labor Relations Act
- Fair Labor Standards Act

The employment regulations are a good sampling of employer requirements, so any company that employs people should at least consider email archiving as a way to meet the above regulations.

The regulatory requirements outlined in the preceding list are the main federal government drivers for records retention, including email data, but keep in mind that these are not all of them. More than 10,000 records retention regulations are effective in the U.S. Many of these are state mandated, so a review of the regulations in the states where your company operates would be a wise idea.

Data Protection Directive (EU)

Not only North America has regulatory requirements—European data protection and privacy requirements exceed those of the United States'. The EU Data Protection Directive mandates that each EU member nation pass a privacy law and create a Data Protection Authority to protect its citizens' privacy and to also investigate any breaches of it. It is an explicit requirement of the Seventh Principle of the EU Data Protection Directive that "organizations take appropriate technical and organizational measures against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data." Corporate email, since it usually identifies the names of the sender and recipient(s), falls under the definition of "personal data" which therefore needs to be protected. In much of Europe, allowing employers to read employee e-mails would be considered a violation of privacy laws. Individuals also have the right to find out what information is held about them in any organization, at any time and have any incorrect information deleted. This capability to retrieve and correct must be built into any an organization's email management policy.

Markets in Financial Instruments Directive (EU)

The EU's Markets in Financial Instruments Directive (MiFID) provides a harmonized regulatory regime for investment services across the 30 member states of the European Economic Area. It covers reporting information to customers, obtaining information from customers, customer agreements, management of conflicts of interest, compliance arrangements, and internal systems and controls. In each of these areas, email records play a significant role in post-event demonstrations that the firm complied with the requirements of the directive. Financial institutes across Europe must therefore ensure that their MiFID compliance activity extends to email archiving and retrieval.

Freedom of Information Act 2000 (UK)

Like its US equivalent, the UK Public Sector organizations have to comply with the Freedom of Information Act 2000 (FOIA). This act allows for the full or partial disclosure of previously unreleased information and documents controlled by public sector organizations to interested members of the public. UK public sector organizations need to ensure that data is available when it is requested by interested parties. The FOIA also creates a specific criminal offence under its section 77 that does not allow altering, defacing, erasing, destroying any record (including electronic records like email) with the intention of preventing the disclosure of its information. This means that public sector organizations that allow individuals to determine which emails they should destroy may, by default, be in breach of this section and liable for criminal sanction.

Retaining and Disposing Messaging Data

Laws and regulations are not the only determinants of what data organizations need to retain. To achieve a state of litigation readiness (and thus decrease eDiscovery costs), organizations must retain more than just email messages and attachments. Mailboxes, such as those in a Microsoft Exchange system, contain not only email, but also other information that is touched, used, and managed by the end user. This information, for example, can include calendars, tasks, and contact information, all of which can be required to be retained for legal compliance or be requested to be disclosed in litigation. It is a common misperception that only email is targeted in eDiscovery or litigation. An example is the case of *Trigon Insurance v. United States*, 204 F.R.D. 277 (E.D. Va., 2001).

In this corporate taxpayer suit, the United States hired a litigation support company which, in turn, hired third-party experts to consult and testify in the case. As per their company policy, the litigation support company destroyed all email messages and draft reports between themselves and the third-party experts. Based on the facts of this specific case, the court found that the email messages and the drafts would have been discoverable, and the United States was held responsible for the intentional spoliation of these documents. The court imposed sanctions on the United States in the form of adverse inferences regarding the content of the destroyed electronic documents.

What Data Needs to Be Preserved?

In litigation, all of the data in mailboxes is discoverable, including items—such as contacts, meeting invitations, and tasks—that previously flew under the radar. One example is custodian PST files, which are acquired from their local hard drives and are often sought for relevant information. In some cases, PST files will be produced, but certain contents (emails, attachments, calendar events, and so on) are either removed or redacted—both of which result in different options for producing the inclusive set of relevant mailbox items. Attachments are also a common target for relevancy.

Deciding on Information Retention Categories

Traditional “records management” utilizes an administrative system (or archiving system) to direct and control the creation, version control, distribution, filing, retention, storage, and disposal of records, in a way that is administratively and legally sound, while at the same time serving the operational needs of the organization and preserving an adequate historical record. The key term here is “record”—usually seen as transactional in nature. With the FRCP amendments, however, the traditional definition of a record is no longer adequate. Organizations need to extend records management capabilities to all electronic information, a practice referred to as *retention management*.

Good retention management practices allow organizations to:

- Mitigate compliance and litigation risks by proactively managing the retention and disposition of all potentially discoverable information.
- Reduce costs, particularly space costs, by ensuring that only important information is retained.
- Save time and increase productivity by making information easier and faster to find.
- Increase the reliability of information by managing the appropriate versions of information assets and ensuring that they have high value as evidence if they are needed in a court of law.

The benefits of first developing and then automating an email retention policy are threefold:

- **More effective regulatory compliance.** Email retention for regulatory compliance isn't a choice, but rather an absolute requirement. The only choice your company will have is in how you meet the requirements: manually or with an email archiving automation system. Creating and automating your email retention policy lowers your overall risk of noncompliance and ensures that all required email is kept for the required time period.
- **Better legal risk management.** The ability to show a court an updated and regularly enforced email retention policy can demonstrate retention policy intent and negate claims of spoliation by the plaintiff's attorney.
- **More consistent corporate governance.** Businesses rely on the generation, use, and reference of data to make ongoing business decisions. The data that a business generates has a value to the business if that data can be used efficiently. An effective retention policy ensures that information is available for some period of time, and an email archiving system allows for quick search and reference.

Please note that an archiving system should allow you to granularly apply retention policies to items that need different management (such as calendars and contacts). For specific advice, contact your local practitioner.

Disposition of Email from the Email Archive

Most email archiving solutions allow you to set basic retention policies within the system. Most companies start out by defining email retention policies based on their hard-copy retention schedule, which is a huge mistake. Hard-copy retention schedules are based on the content of each record. This strategy assumes that each employee is deciding on a record-by-record basis what specific business use the record reflects and, based on the retention schedule, how long it should be kept. However, most records in business these days are electronic, and an employee can generate hundreds per day.

An email retention policy should set retention policies based on department, accounting code, division, or geographic location (other countries have different retention laws). No email archiving solution has the ability to "decide" what any given email or attachment is about, and then apply a specific retention period to it. Some of the better email archiving solutions will integrate with Microsoft's Active Directory, giving you the ability to set retention policies and keep them current based on the employee's location, department, or accounting code. Email retention policies are usually set centrally by the IT group and applied throughout the email system. Remember that policies can be set for the entire mailbox or for specific folders within the mailbox, such as Calendar, Deleted Items, Drafts, Junk Mail, and so on. In this case, it would be wise to exclude the Junk Mail folder from

the archive. You should also look for the ability to include emails in the retention policy for an indefinite period of time. This feature allows you to set a litigation hold, in response to litigation, by simply clicking a “Hold Disposition Process Indefinitely” box. When setting the actual retention period, you want to be more specific than one-year increments. Archiving solutions should give you the ability to designate days, months, or years.

Also, it is a good idea to be able to include or exclude different message classes. For example, for those companies with digital phone systems with unified messaging, voicemails attached to emails can be excluded to save storage space.

Based on the retention time period governed by the email archiving solution, records such as email, attachments, and other objects will be automatically deleted out of the email archive if no litigation hold process is in place. Some archiving solutions automatically hold email that has reached the end of the retention period until someone, usually IT, approves the deletion. As you can imagine, in large systems with millions or billions of emails, this policy isn't effective.

The Benefits of Data Consolidation

One of the primary reasons for consolidating data is potential storage cost savings. Centralizing storage can save larger corporations millions of dollars annually and when you consider that unstructured information takes up a huge chunk of storage in an organization (it is generally accepted that unstructured content makes up at least 80 percent of the data within any given organization). Because so much of this unstructured information is either created in or travels through the messaging system, an email archiving solution is a good start for consolidating data.

Once an email archiving solution is in place, the next step is to inventory potential PST files in the environment. Within larger organizations, PST files (known as Outlook Personal Folders) have grown out of control, creating not only a huge eDiscovery risk, but also a time-consuming and expensive process that's needed to collect them. The problem with PST files is that the storage format isn't efficient, and administrators find that it's impossible to know what information resides in these files.

Importing these files and getting these files off file servers, desktops, and other locations into an archive can result in storage savings of several terabytes while also reducing the legal risk of having this information unmanaged.

Deployment Features of Exchange 2007

Microsoft Exchange Server 2007 is one of the leading enterprise messaging applications. Exchange 2007 was released in early 2007 and it delivers new advances in performance, scalability, security, and mobile messaging support. It is the latest addition in a long line of very successful Exchange Server versions dating from the early 1990s. Further improvements to the Exchange Management Console and added functionality to data protection became available with the recent release of Exchange 2007 Service Pack 1 in the fall of 2007.

Exchange 2007 delivers significant improvements with respect to addressing availability and compliance requirements. Third-party solutions offer customers added value that complements Exchange functionality to fully meet ever-increasing regulatory and data protection requirements. This section introduces Mimosa Systems and its product NearPoint for Microsoft Exchange Server and describes how NearPoint complements and extends Exchange 2007. We'll also look at how NearPoint adds important benefits for compliance, storage management, and disaster recovery simultaneously.

Mimosa NearPoint is a next-generation email archiving solution that delivers archiving, eDiscovery, recovery, disaster recovery, and storage management in a single integrated solution. For managing Exchange Server 2007, NearPoint performs multiple important functions that improve the overall performance of Exchange. NearPoint:

- Adds powerful tools for legal discovery
- Stores email in a compliance archive
- Extends native Exchange recovery capability
- Gives end users easy access to archived mail

Compliance Support

For compliance, Mimosa NearPoint stores not only all Exchange email and attachments, but also other critical information—such as calendar, tasks, and contact data—in an indexed archive that meets all laws for regulatory compliance. NearPoint extends the Exchange 2007 retention capability and provides enterprise-wide policy enforcement that is managed at the server level, thus preventing user intervention. Mimosa NearPoint integrates with the Exchange 2007 folder-level retention feature, called Managed Folders. While Exchange 2007 offers new functionality, it cannot meet certain compliance requirements on its own:

- **Exchange is not an archive.** It can search, filter, retain, and expire content that's already in Exchange, but it doesn't have any tools for importing existing information from PST files or other sources.
- **Exchange leaves retention decisions up to the user.** Users are free to drag messages into managed folders, but they are not required or compelled to do so.
- **Exchange is not tamper-proof.** Because Exchange isn't an archiving solution, it doesn't include tools to provide tamper detection for stored data (apart from the checksum mechanisms used to ensure integrity of the message databases), and it doesn't natively support nonrewritable storage.
- **Exchange can't capture context.** The journaling support in Exchange can capture messages at the time they're sent or received, but it doesn't capture context, and it places an additional load on the mailbox servers that are responsible for the journaling operations.
- **Exchange has limited indexing.** While the Exchange content indexer is greatly improved, it can only index Exchange data that's currently in a mailbox somewhere. It can't index historical data or data from other sources.

Mimosa NearPoint preserves and manages all Exchange information in a secure, indexed archive for compliance. NearPoint manages retention and disposition policies that are administrator applied and managed, guaranteeing that email data is kept for the time period specified by the compliance policy. Data security is provided with embedded tamper detection and activity tracking. For financial companies that must comply with strict SEC rules for nonerasable, nonrewriteable storage, NearPoint supports the EMC® Centera™ compliance storage device.

Legal Discovery

The search capabilities of Exchange 2007 are greatly expanded relative to previous versions. The full-text indexing engine is up to 35 times faster, and fast full-text search is available from within Outlook 2007 and Outlook Web Access 2007. Exchange 2007 also has a command-line utility that allows a search for specific terms across multiple mailboxes, after which any retrieved messages can be moved to a SharePoint site or a mailbox.

Mimosa NearPoint extends the native Exchange 2007 search capability in two key ways. First, NearPoint manages a complete copy of all current and historical email—this capability enables *all* email to be accessed quickly and easily with a single search. Customers who rely solely on Exchange for discovery, on the other hand, have to restore email from backup tapes to search historical email, which is a costly and time-consuming exercise.

Second, NearPoint provides powerful search tools that auditors can use to search across multiple mailboxes. The Exchange search tool is a command-line utility available from the Exchange System console, which has to be run by the Exchange administrator. In contrast, the NearPoint search tool has an intuitive, easy-to-use GUI that supports search using wild cards, Boolean logic, proximity search, and specification of multiple email properties. NearPoint search results can be sorted and results can be exported in PST files for easy transport.

For legal workflow, the NearPoint eDiscovery Option is an add-on product that enables the reconstruction of complex events to understand user behavior for litigation support and investigations. It offers efficient collaboration capabilities, allowing users to search, share, hold, review, and tag results for export (via PST files). The NearPoint eDiscovery Option allows IT to put litigation and investigation work where it belongs—in the hands of the corporate legal or HR team.

Retention and Disposition

A new feature of Exchange 2007 is the ability to manage email retention at the folder level. Administrators can configure retention settings for folders and messaging types in order to automate the disposition of message content. The Exchange 2007 folder-level retention feature is user driven, which means that end users either have to move emails to specific folders if they need to be retained or designate them relevant to a specific policy.

Mimosa NearPoint can be used in combination with Exchange 2007 folder-level retention policies and extend their functionality to enable full compliance for the most stringent regulations. NearPoint will seamlessly adopt the same folder-level retention policies on Exchange Server in the email archive. The benefit is consistent retention and disposition across Exchange and the NearPoint archive.

Mimosa NearPoint manages its retention settings based on enterprise-wide, server-based controls that cannot be circumvented by users. Policies are defined at the mailbox level and can be further defined by folder and message class. NearPoint enforces folder retention policies and does not allow user intervention, an important requirement for compliance.

Should litigation arise, NearPoint provides a Retention Hold capability that freezes all retention for a given user until it is released by the administrator. This capability is a mailbox-level retention hold that is managed on the NearPoint Administrator Console. The NearPoint eDiscovery Option allows for message-level retention hold, an additional feature important for legal workflow.

Exchange Migration

Mimosa NearPoint supports Exchange during transition by reducing mailbox size and by protecting mailbox data. To reduce total transition time, mailbox information on the source Exchange Server can be reduced when the mailboxes have been fully archived by NearPoint. Look at a typical Exchange 2003 environment, for example. With NearPoint deployed, all Exchange 2003 mailbox information exists in the NearPoint archive. The administrator can reduce the mailbox size on Exchange Server using native Exchange tools to groom mailboxes to a fixed size (such as 100 megabytes) or a fixed time period (such as 12 months). Transition goes more quickly with reduced mailbox size.

Should any problem occur during transition to the mailbox information, full mailbox restoration can be performed using NearPoint. NearPoint enables administrators to enjoy a faster migration with smaller mailboxes and no risk of losing mailbox information.

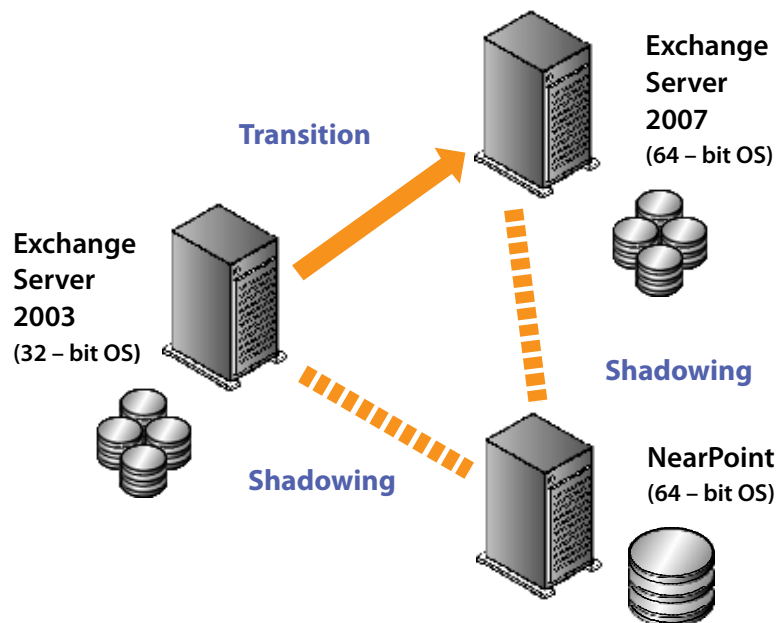


Figure 1. NearPoint Co-existing with Exchange 2003 and 2007 Servers during Transition

Exchange Local Recovery of Exchange 2007

For local Exchange recovery, Exchange 2007 supports two new features: Local Continuous Replication (LCR) and Cluster Continuous Replication (CCR). LCR copies Exchange log files locally and provides on-host data redundancy, reduced backup requirements, and improved database recovery. LCR performs on-host and is restricted to a storage group containing a single database. In addition, LCR consumes local CPU and server resources and should be used with careful planning.

CCR uses the database failure recovery functionality in Exchange 2007 to enable the continuous updating of a second copy of a database with the changes that have been made to the active copy of the database on a passive Exchange Server host. During installation of the passive node in a CCR environment, each storage group and its database is copied from the active node to the passive node. This operation is called seeding, and it provides a baseline of the database for replication. After the initial seeding is performed, log copying and replay are performed continuously. In a CCR environment, the replication capabilities are integrated with the Cluster service to deliver a high-availability solution.

In short, both LCR and CCR are used to restore a full Exchange database or an entire Exchange Server quickly from disk. They cannot perform mailbox-level recovery, or message/folder-level restores, which is where NearPoint complements Exchange 2007. Both LCR and CCR are managed via the new command shell in Exchange 2007.

Remote Recovery of Exchange 2007

Exchange 2007 SP1 delivers a new data protection feature called Standby Continuous Replication (SCR). SCR is designed to provide organizations with redundancy and site resilience and uses log shipping technology to support Exchange Server failover to a standby Exchange. During failover, the SCR target files are mounted on the Standby Exchange Server for access by Outlook clients. SCR uses the Exchange Management Shell and scripts.

Mimosa NearPoint also uses log shipping replication for Exchange data protection, but it delivers additional features for archiving and storage management. The Exchange Mailbox Stores protected on NearPoint can be restored to the primary Exchange Server with simple “one-click” operations. NearPoint does not run Exchange Server software and does not perform as a standby Exchange Server. Rather, NearPoint performs as a combined disk-based recovery application and email archiving application.

Mimosa NearPoint uses Exchange Mailbox Stores to create an email archive. Data extraction, indexing, and de-duplication processes perform on NearPoint and transform the bulk Exchange Mailbox Store files into an Indexed Object Repository. Using powerful search tools provided by NearPoint, users and auditors can search the repository for legal discovery.

Mimosa NearPoint can be used in conjunction with SCR with no interference; but the data protection features of SCR can be performed by NearPoint with fewer restrictions and using a GUI (no scripting).

The following table provides a feature-by-feature comparison of Exchange SCR and Mimosa NearPoint.

EXCHANGE 2007 SCR	MIMOSA NEARPOINT
<p>The log shipping technology that SCR uses is a continuous process and uses a pull model. As soon as a new log file has been closed and named with the next-generation sequence log file number, the Exchange Replication Service running on the SCR target pulls the closed log file from the SCR source computer.</p>	<p>Mimosa NearPoint performs in the same fashion and pulls log files from the primary Exchange Sever as soon as a new log file has been closed. NearPoint maintains a pristine copy of the Exchange content.</p> <p>No agent software is installed on Exchange Server.</p>
<p>The target for SCR is either a stand-alone Exchange Mailbox Server or a node in an Exchange failover cluster.</p> <p>Each SCR source can have an unlimited number of SCR targets. No more than four targets are recommended by Microsoft.</p>	<p>Mimosa NearPoint serves as the target and is not running Exchange Server software. Exchange storage groups and all files are stored on the NearPoint disks.</p> <p>NearPoint can support multiple Exchange Servers, and its grid architecture can support hundreds of thousands of mailboxes.</p>
<p>Both the source and the target Exchange computers must be running Exchange 2007 SP1, and they must be running the identical operating system (Windows Server 2003 or 2008).</p>	<p>Mimosa NearPoint runs on Windows Server 2003 and supports Exchange 2007, 2003, and 2000.</p> <p>NearPoint supports different versions of Exchange simultaneously.</p>
<p>SCR in the Standard Edition of Exchange 2007 supports a maximum of five storage groups.</p> <p>SCR in the Enterprise Edition of Exchange 2007 supports a maximum of 50 storage groups.</p>	<p>Mimosa NearPoint supports an unlimited number of storage groups.</p>
<p>SCR supports one mailbox store per storage group.</p>	<p>Mimosa NearPoint supports a maximum of five mailbox stores per storage group.</p>
<p>SCR source and target computers must be in the same Active Directory domain.</p>	<p>Mimosa NearPoint supports Exchange Servers in a single domain and in multiple parent child domains.</p>
<p>SCR target files cannot be backed up. Backups are performed on the SCR source files, which causes the database headers for SCR targets to be updated and log files to be truncated.</p>	<p>Backups are performed nightly on NearPoint independent of Exchange backups. There are no restrictions.</p>

EXCHANGE 2007 SCR	MIMOSA NEARPOINT
SCR log files are replayed with a default delay of 50 log files and 24 hours. The minimum is 50 logs and 0 hours; the maximum is 7 days.	Mimosa NearPoint replays the log files in hourly increments (e.g., 1, 2, 3, 4 hours) that are configurable. The minimum replay time is 30 minutes.
SCR is enabled using the Exchange Management Shell using commands such as: <ul style="list-style-type: none"> • <i>Enable-StorageGroupCopy</i> • <i>ReplayLagTime</i> • <i>TruncationLagTime</i> • <i>SeedingPostponed</i> 	Mimosa NearPoint log shipping is enabled via a GUI and a check box. No scripting is required.
SCR failover is activated using the Exchange Management Shell using commands such as: <ul style="list-style-type: none"> • <i>Dismount-Database</i> • <i>Restore-StorageGroupCopy</i> • <i>Move-StorageGroupPath</i> • <i>Move-DatabasePath</i> • <i>Set-MailboxDatabase</i> • <i>Mount-Database</i> <p>To recover the target SCR files back to the source computer, the target standby computer needs to be configured for SCR in the reverse direction.</p>	Mimosa NearPoint performs a restore and copies the Exchange Store files back to the primary Exchange Server. NearPoint does not perform as a standby Exchange Server. NearPoint supports failover to a standby Exchange Server with the NearPoint Disaster Recovery Option.
Outlook 2007 messaging clients connect to the target Exchange Server after AD replication and the Autodiscover features in Exchange 2007. Outlook 2003 and earlier versions require that the users profile be updated manually.	NearPoint restores the target files back to the primary Exchange Server so the messaging clients do not require redirection. The NearPoint Disaster Recovery Option supports automated Outlook client redirection for Outlook 2003 and 2007.

Mimosa NearPoint performs continuous data protection for Exchange based on the Exchange transaction log files. NearPoint improves Exchange recovery by supporting all versions of Exchange 2000, 2003, and 2007, and it has no restrictions on storage groups or mailbox stores. And it's very important to note that NearPoint performs entirely off-host and does not impede Exchange Server performance. NearPoint can restore a complete Exchange database, mailbox, and individual messages/folders.

In summary, NearPoint extends and improves Exchange recovery as follows:

- No restrictions on storage groups or databases.
- Simple "one-click" recovery procedures; no need to learn a new command shell.
- End users can restore individual messages via Outlook (and Outlook Web Access).

The advantage for organizations is that NearPoint can co-exist with LCR, CCR, and SCR if desired.

PST File Elimination

PST files have become a very popular way for end users to store email locally on desktops and network file servers. These files help reduce the amount of email managed on the Exchange Server and are often necessary to enable users to stay below quota limits. PST files also give users offline access to their data—users enjoy being able to access email when they are not connected to the Exchange Server. Exchange 2007 introduces expanded storage capacity and will support gigabyte-size mailboxes, but users will continue to use PST files for the benefits previously described.

PST files create an extremely difficult challenge for legal discovery, however. Because they exist as independent files, they are not tracked by Exchange and can be easily lost. The email data they contain is critical for compliance and corporate intellectual property, so organizations require a better way to manage them and make sure the data they contain is protected. In addition, because PSTs reside on users' hard drives, there is no centralized view of what data might exist. IT must collect the files from each user's machine—a costly and laborious process.

The Mimosa NearPoint PST Archiving Option archives PST files into the NearPoint archive. With the NearPoint PST Archiving Option, PST files are automatically located across many servers and laptops, mapped to a given user account, and actively imported (or ingested) into the NearPoint archive. This option allows administrators to manage all aspects of PST archiving using a dedicated PST archive management console that provides easy-to-use wizard-driven menus.

Once PST files are loaded into the NearPoint archive, the PST data can be viewed by its original folder hierarchy and searched by auditors for legal discovery. By using the PST Archiving Option, administrators can eliminate the need for PST files altogether, while users can continue to access all their PST information using the self-service search tools provided by NearPoint. The advantage of bringing PST files into the archive directly is that it does not increase the storage footprint of the Exchange database files with stubs or shortcuts.

Unified Messaging Management

Exchange 2007 introduced a new unified messaging server role that integrates voicemail audio files with Exchange as email attachments. Users can access all voice, fax, and email data from one inbox. Administrators need to carefully plan for the impact that unified messaging data will have on Exchange mailbox capacity. Mimosa NearPoint provides multiple features to manage the storage impact of unified messaging data as part of its mailbox management functionality.

- For organizations that wish to exclude voicemail data from the NearPoint archive, NearPoint provides data exclusion policies that manage email data by message class or folder type. Entire mailboxes can also be excluded.

- For organizations that wish to retain voicemail data in the archive and still control its storage utilization, NearPoint Mailbox Extension can be configured to automatically manage storage limits by age and size.
- For organizations that wish to retain instant messages in a unified archive with email, Mimosa Systems has a partnership with FaceTime to capture instant message conversations and store them in the email archive.

Using a combination of these policy-driven features, administrators can control and manage archive storage levels and experience no impact from the introduction of new data types such as unified messaging.

Exchange Version Support

A major change of note to Exchange 2007 is the move to a 64-bit operating system platform. This important change ushers in a new level of performance and scalability for Exchange Server. Mimosa NearPoint fully supports and runs on a 64-bit environment.

Mimosa NearPoint runs on both 32-bit and 64-bit OS versions. In 32-bit mode, NearPoint supports Exchange 5.5, 2000, and 2003. In 64-bit mode, NearPoint supports Exchange 5.5, 2000, 2003, and 2007.

To take advantage of the Mimosa NearPoint Self-Service Access™ capability, NearPoint supports Outlook versions 2000, 2002 (XP), 2003, and 2007, as well as Outlook Web Access (OWA).

Log Shipping Versus Journaling/Mailbox Archiving

Mimosa NearPoint for Microsoft Exchange Server offers a proprietary data capture method based on the Exchange transaction log files. Mimosa calls its unique data capture method Application Shadowing—a method of database replication for Exchange that is also referred to as log shipping. Mimosa Systems was the first company to develop log shipping for Microsoft Exchange. Exchange is a database at its core, and it is natural for Exchange to support log shipping.

Naturally, organizations should choose the email archival solution that best fits their needs. Mimosa believes and customers confirm that Exchange log shipping provided by NearPoint is ground-breaking new technology for Exchange Server, since it delivers major advantages over journaling for Exchange compliance archiving. Our customers agree, citing the “shadow database” as one of the major benefits provided by NearPoint.

Some people claim that journaling is the recommended method for Exchange compliance archiving, but they are ignoring the major negative performance impact that journaling has, as well as its shortcomings for eDiscovery.

Mimosa NearPoint is a complete Exchange data management solution that supports compliance archiving, eDiscovery, recovery, and storage optimization in a single integrated solution. Log shipping is the only data capture method that can ingest the complete set of Exchange email and metadata that is relevant to eDiscovery, archiving, and recovery. NearPoint is a result of Mimosa Systems' deeper understanding of the archiving problem space and learning from the shortcomings of journaling-based products.

Application Shadowing

Application Shadowing uses the Exchange log files to capture Exchange information. It closely resembles other log shipping methods available for Microsoft SQL Database and Oracle® Database. Application Shadowing begins with a full Exchange backup using the ESE backup API that is provided by Microsoft for online Exchange backup. Next, it captures the log files, in real time, as they are committed to disk on Exchange. The log files are small in size (5MB, or 1MB in Exchange 2007) and are easily copied to the NearPoint server the instant they are committed to disk. The log files are "replayed" on the off-host Exchange database files (EDBs) at a frequency that is configurable (e.g., one hour). Each log contains a complete set of all Exchange database transactions that occurred until the log files closed.

Log shipping is application intelligent and prevents data corruption from infecting the backup copy. Traditional replication methods copy blocks of Exchange data and are not application intelligent. If corruption exists, traditional methods will copy the corruption to the backup copy. Log files contain checksum bits embedded in each page of data. Using the ESE API, NearPoint has access to the parity information and is able to detect immediately if any corruption exists. In this manner, single-bit errors and other forms of corruption are prevented from reaching the backup copy.

Application Shadowing manages a "warm" standby copy of the Exchange database(s) off-host on the NearPoint server. The off-host EDBs are available for recovery, and NearPoint uses the content to build an indexed repository through a process called Smart Message Extraction. All processing that Smart Message Extraction performs for extracting email, indexing, and checking for duplication is performed off-host and avoids impacting Exchange. NearPoint manages a complete copy of Exchange information and supports Exchange recovery, archiving, eDiscovery, and storage optimization.

Application Shadowing Versus Journaling

Mimosa designed NearPoint Application Shadowing to overcome the limitations of Exchange journaling for compliance archiving and to support the wide range of Exchange email data management functions that NearPoint delivers. Application Shadowing provides several key advantages over journaling. First, it performs with no agent software on the Exchange Server; NearPoint performs off-host with no impact on the Exchange Server. In addition, Application Shadowing captures complete Exchange Mailbox information, including all email, folders, deletions, calendars, contacts, notes, and tasks—providing many advantages for eDiscovery and recovery. The following table lists specific advantages of Application Shadowing and makes comparisons with journaling in the areas of performance, eDiscovery, and data protection (see Table 1).

	MIMOSA NEARPOINT APPLICATION SHADOWING	MICROSOFT EXCHANGE JOURNALING*
PERFORMANCE ADVANTAGES	<ul style="list-style-type: none"> Transaction log shipping has no impact on Exchange. Zero footprint on Exchange. 	<ul style="list-style-type: none"> Every message sent/received is copied to a separate Journal Mailbox for all members of Information Store. 15%-30% performance decrease (Microsoft recommends separate dedicated Journal server). Requires expensive restructuring of Exchange environment. Requires dedicated journaling servers for enterprise wide deployments.
EDISCOVERY ADVANTAGES	<ul style="list-style-type: none"> Transaction logs capture every change made to a message, not just sent/received items. Captures complete mailbox information (email, folders, calendars, contacts, notes, tasks, etc.). Captures all mailbox folder information. Capture all Meta information and special properties of email. 	<ul style="list-style-type: none"> Does NOT capture what happens to a message/item as it resides on the Exchange server. Does NOT capture when a message is deleted. Does NOT capture personal calendars, notes, tasks, and journals.
DATA PROTECTION ADVANTAGES	<ul style="list-style-type: none"> Log shipping creates a “warm” standby copy of Exchange database(s) off-host; available for database restore locally and remotely for data recovery. Fast disk-based recovery reduces RTO to minutes vs. hours for traditional tape-based recovery methods. Continuous data protection based on log files reduces RPO to mere seconds. 	<ul style="list-style-type: none"> Journaling-based archival solutions provide no data protection for Exchange.

Table 1. Application Shadowing (Log Shipping) Advantages Comparison with Journaling

*Exchange 2003 version.

MAPI Does Not Capture All Information

The biggest difference between Application Shadowing and journaling is the way in which information is captured and guaranteed. Legacy MAPI-based archiving products have to rely on two separate processes to capture all mailbox content. First, the journaling pass captures all email messages and meeting requests that are actively sent. Second, an archiving run is performed—a process that generally is configured to run during off-hours and can't overlap the backup process. This process crawls every single item in the mailbox in the same way as brick-level backups performed in the late 1990s. The performance impact of these archiving runs on the Exchange Servers is huge and can impact the end user. The archiving product will then attempt to capture a copy of those items that journaling didn't capture (such as voicemail messages, tasks, and, more important, manual calendar items from a user's mailbox). In general, two archiving runs occur 24 hours apart, which leaves a very big gap to capture all of the content. This gap leaves plenty of time for end users to modify and delete important unaudited information.

Performance Advantages

Journaling has a negative performance impact on Exchange Server, without question. It is enabled per mailbox store and doubles the number of emails processed. It consumes Exchange Server CPU, memory, and storage resources. If journaling is deployed for multiple mailbox stores, or for the entire Exchange Server, its impact is enormous. In these situations, Microsoft recommends that a dedicated Exchange Server be provisioned for journaling. The following passage from the Microsoft journaling deployment guide describes why journaling adds overhead to the Exchange server.

“When journaling is enabled in a mailbox database and a user who has a mailbox on that mailbox database sends a message, the server generates two messages: one for the recipients and one for the journal recipient. When a message is submitted to a journalized mailbox database, the mailbox database processes the message as it typically would to deliver it, but it also creates a message for the journaling recipient. When a journalized mailbox database receives a message, most of the time, the message has been journalized already. In the receive case, extra processing (beyond reading the journaling property) is required only when the receiving server is the expansion server for the distribution list or when the distribution list is hidden or query-based.

Therefore, you can estimate the effect of journaling on a mailbox database by assuming that the enabled mailbox database can process approximately half of the messages being sent, as long as all other conditions, such as CPU power, bandwidth, storage space, and disk speed, remain constant.”³

³ See <http://technet.microsoft.com/en-us/library/aa997525.aspx>.

It is clear that when the total amount of email traffic for a mailbox store is doubled, there is a price to pay. Estimates for the overhead range from 15 to 30 percent performance degradation. And when all the mailbox stores are enabled for journaling, you must provision a new server to handle the increased workload.

In Exchange 2007, journaling is enhanced in a couple of important ways: the journaling functions are now part of the new Transport Role, and journaling may also be enabled per mailbox. For more information on Exchange 2007 and journaling, refer to <http://www.microsoft.com/exchange/evaluation/features/default.mspx>.

eDiscovery Advantages

The key advantages of NearPoint Application Shadowing for eDiscovery are preservation of the mailbox context and completeness of data capture. Application Shadowing captures the complete mailbox and preserves the mailbox context as well as content. Journaling, on the other hand, collects email for a mailbox store in a single mailbox and does not keep the original sender's (or recipient's) mailbox intact. Being able to preserve the context of a mailbox is very important for legal discovery. Auditors can easily identify custodians for legal discovery by selecting their mailbox, and do not need to identify all email aliases for the custodian(s) being investigated. Auditors benefit from being able to view the archive mailbox in a form that closely resembles its original Exchange rendition. Mimosa NearPoint Self-Service Access provides auditors with a Browse Search tool that displays the archive mailbox in a folder view (see Figure 2). Folder contents can be viewed at any point in time using a drop-down menu.

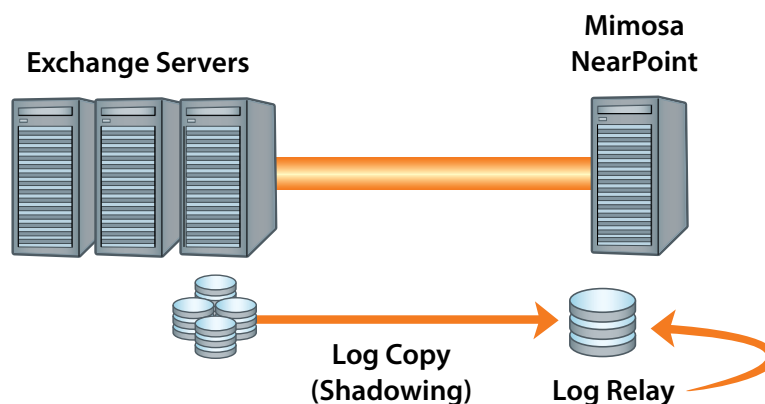


Figure 2. NearPoint Application Shadowing

In addition to preserving the mailbox context, Application Shadowing also preserves the entire content of the mailbox, including all email history (including deletions) and all mailbox items (such as calendars, contacts, notes, tasks, and so on). User behavior can be understood by viewing the complete history of an email item, or by tracing the conversation history of a given email. Information from calendars can be matched with email content.

The record of email deletions is kept and reveals additional user behavior information. Having complete mailbox information available provides more accurate and complete legal discovery results.

Data Protection Advantages

Application Shadowing serves as a continuous data protection method for Exchange. Using Exchange transaction log files, Application Shadowing copies logs to the NearPoint server the instant they are committed to disk. As discussed previously, the log files are replayed into the off-host EDBs. In effect, Application Shadowing creates a “warm” standby copy of the Exchange database(s) off-host, where they are available at any time for recovery. Email archiving solutions that rely on journaling cannot perform Exchange recovery because the email information they capture from the journal mailbox is not complete. Individual messages can be restored, but entire mailbox, database, or storage group restores are not possible.

Using the NearPoint Administrator Console, full Exchange database recovery can be performed with a simple “one-click” operation. Exchange recovery is performed quickly and the data restored is within one log file of being current. Both recovery speed (RTO) and recovery point (RPO) are improved using NearPoint, compared with traditional tape-based recovery methods. Email archival solutions that use journaling do not capture complete Exchange information; hence, they cannot perform Exchange recovery. NearPoint can also restore Exchange EDBs remotely to a standby Exchange Server for disaster protection.

Performance Data

Recent tests prove that log shipping offers major performance benefits in Exchange messaging environments. The Exchange Server 2003 MAPI Messaging Benchmark (MMB3) (<http://technet.microsoft.com/en-us/library/cc164328.aspx>) was used with LoadSim to gather the performance data. Performance results for the 1,000-user testing comparison are shown in the Test Results section that follows.

System Details

Paths

- Gig Ethernet Network between Loadsim Client, Exchange Host, MAPI Archiving Server, and Mimosa Dynamic Log Shipping Destination Server
- Discrete FC storage paths and arrays for Exchange and Archive Servers

Server

Exchange Server Specifications

- Software: Exchange Server on Windows 2003 Enterprise SP2
- CPU: 4 Cores 2 GHz
- RAM: 4GB
- DISK: Qlogic FC HBA to 12 10K-RPM FC Disks RAID 10 (1056 IOPS for Exchange EDB and Logs)

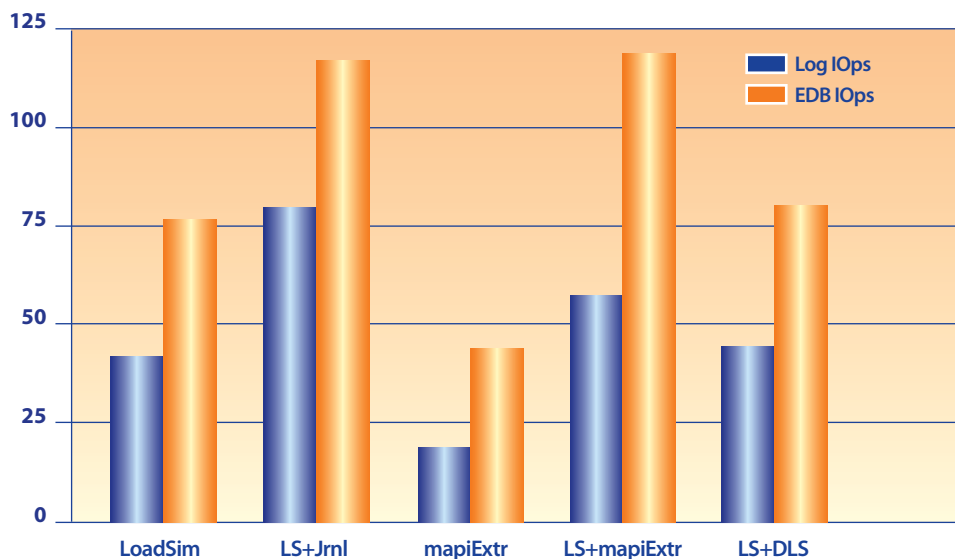
Tests Performed

- Test 1** 1,000 Mailbox Loadsim Medium Load
- Test 2** 1,000 Mailbox Loadsim Medium Load with Envelope Journaling
- Test 3** 1,000 Mailbox Loadsim Medium Load with Envelope Journaling and MAPI Archiving
- Test 4** 1,000 Mailbox Loadsim Medium Load with Mimosa Dynamic Log Shipping

Test Results

Envelope journaling costs significantly more in disk resources. Disk I/O rates went up 51 percent and 95 percent on the EDB and log drives, respectively, compared with just LoadSim running. For normal dynamic log shipping functioning, the impact is minimal (less than a five percent increase) because Mimosa NearPoint is copying newly created 5MB log files during dynamic log shipping and periodically truncating the logs. The following table and chart depict the relative disk I/O costs:

	LoadSim Only	LoadSim + Envelope Journaling	LoadSim + Envelope Journaling + MAPI Extraction	LoadSim + Dynamic Log Shipping
Exchange EDB Disk IOPS	75.98	114.51	157.37	80.53
Exchange Disk IOPS	41.29	80.56	98.92	44.18



CPU utilization impact was minor. Tests show that CPU usage increased from 1.9 percent for LoadSim to 6.2 percent for journaling, an increase of more than 300 percent, but still low and within the healthy thresholds of the host.

One marked difference between envelope journaling and log shipping is the breadth and depth of Exchange Items captured.

	LoadSim + Envelope Journaling + MAPI Extraction	LoadSim + Dynamic Log Shipping + Smart Extraction
Exchange Items Captured	263,469	1,074,224

Envelope journaling captures only inbound and outbound mailbox messages, whereas Mimosa log shipping with Mimosa Smart Message Extraction is a lossless archival technology that captures all Exchange items (notes, calendar, contacts, conversational threads, and so on), as well as all historical changes to those objects (object move, attribute change, deletion, and so on). It is important to note that all of these items that journaling does not capture are discoverable; not being able to produce them in eDiscovery could lead to major sanctions. The overall conclusion of the performance tests was that while log shipping with Smart Extraction captured four times as much data from the Exchange mailboxes, the performance impact of log shipping on Exchange was negligible.

Creating the Solution

Creating a successful archiving deployment is a task that requires planning and preparation. A successful email archiving implementation will:

1. Establish robust email archive procedures:

- Ensure that *all* emails and IMs (if required) are archived.
- Enable IT to certify to stakeholders and the court that the email archive technology, processes, and procedures capture all email content (emails, IMs, and attachments) and show that emails have not been changed.
- Ensure that the archive system is resilient and reliable, so it will not be a drain on IT and will allow the IT staff to do their normal day-to-day tasks.
 1. IT no longer has to worry about long backups.
 2. IT no longer has to do legal searches that keep them from doing IT duties.
- Ensure that data cannot be deleted before its retention period has expired. (This time period can be many decades for some types of content.)
- Ensure that data can be checked for readability and migrated to new technology as it become available.
- Comply with industry standards and applicable regulations.
- Allow emails to be retrieved within the statutory period (e.g., 48 hours for SEC Rule 17a).

2. Allow the archive to be exploited by upstream applications to reduce risk:

- Allow easier and quicker internal and external auditing of emails.
- Significantly reduce the risks from “ill-advised” emails.
- Allow the data to be accessed “directly” from other applications. (The data should belong to the organization, not the email archiving vendor!)

3. Does not degrade with the current email system:

- Ensure that sufficient additional resources are budgeted to deal with additional email processing and additional bandwidth.
- Be able to handle the company’s changing email archiving needs.⁴

⁴ Source http://wikibon.org/Email_archiving.

Conclusion

It is clear that email archiving plays a huge role in ensuring litigation readiness and adherence to compliance regulations. Without an automated approach to archiving, organizations risk time-consuming and costly eDiscovery projects and may also disrupt end-user access to information—a huge problem in today’s information-driven economy.

While most archiving vendors leverage MAPI for archiving capture, Exchange log shipping offers a far more compelling solution. Mimosa NearPoint is a complete Exchange data management solution that supports compliance archiving, eDiscovery, recovery, and storage optimization in a single integrated solution. Log shipping is the only data capture method that can ingest the complete set of Exchange email and metadata that is relevant to eDiscovery, archiving, and recovery. NearPoint complements and extends the value of the Exchange messaging server to ensure compliance and efficient legal discovery.

Related Links

- www.microsoft.com/exchange
- www.mimosasystems.com
- www.archiving101.com
- www.sedonaconference.org
- www.wikibon.org

About Mimosa Systems

Mimosa Systems, Inc., delivers next-generation information management solutions with Mimosa NearPoint, providing a live content archive for Microsoft® Exchange Server. NearPoint unifies archiving, eDiscovery, recovery, and storage management in a single solution, assuring email continuity and regulatory compliance.



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



© 2008 Mimosa Systems, Inc. All rights reserved worldwide. Mimosa, Mimosa Systems, 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. NPWP_0408_NA