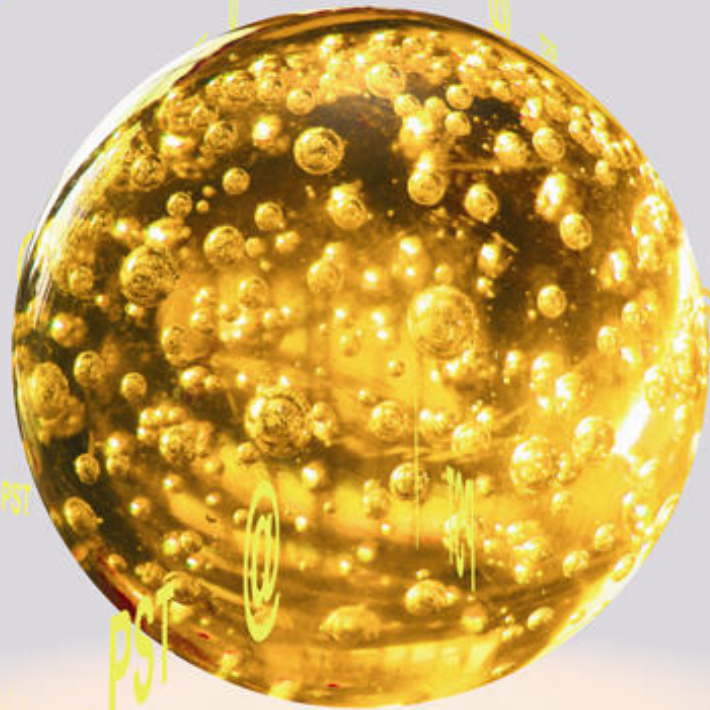


PAM for EXCHANGE email archiving at its best

Whitepaper

Disaster Recovery with **PAM for EXCHANGE**



CONTENT

The Hierarchical Storage Management integrated into PAM for EXCHANGE advances email archiving in the new era of Disaster Recovery.

Author: Adam Surch

All Rights Reserved, including all rights concerning reproduction, copying or any other use or transmission of this document and its contents or parts of it. No part of this publication may, no matter in what form, be reproduced without written permission by H&S Software AG, passed on to third parties, edited by electronic retrieval systems, copied, distributed or used for public presentations. H&S Software AG reserves the right to change and update the content at any time. All data shown on screenshots is solely for demonstration purposes of the software. H&S is not responsible for this content.

PAM-STORAGE® is a trade mark of H&S AG. Microsoft®, Microsoft Windows® and the names of other Microsoft Products are registered trademarks of Microsoft Corporation. All Rights Reserved. Other product names are being used for identification purposes of products and can be registered trademarks of the according manufacturers. Doc.No. exp-wp-0704-001

H&S Heilig und Schubert Software AG
A-1150 Vienna, Staettermayergasse 30

Tel. ++43.1.21555
Fax. ++43.1.21555-200
email: issteam@hs-soft.com | support@hs-soft.com

URL: www.hs-soft.com
URL: www.hs-soft.com/email-archiving



Disaster Recovery with PAM for EXCHANGE

The Hierarchical Storage Management integrated into **PAM for EXCHANGE** advances email archiving in the new era of Disaster Recovery.

Since the turn of the new millennium disaster recovery has slowly grown into a challenging issue for businesses worldwide. In recent years, growing occurrences of natural and man-made catastrophes have emerged and businesses face major repercussions if precautionary steps are not taken.

Email archiving is certainly central to any recovery strategy in the business continuity plan. Growth in archiving in the coming years is likely to mirror the growth in data recovery planning. The important connection between archiving and recovery is retrieval. Administrators and managers both want the speediest recovery possible when their system fails. Archiving can store the data but the ability to retrieve the emails stored on different storage media's to various users in the shortest amount of time is the desired solution.

Email continuity is fundamental in supporting a solid communications network for all businesses. Almost all employees have some interaction with email in their working day, from the CEO to the manufacturer supervisor. If this contact is lost for an unpredictable amount of time then routine business processes become irregular and dysfunctional.

Identifying the risk

The first step to protecting Email systems is identifying the various risks that could cause system damage or failures. Many factors can feature in a system failure, from devastating weather conditions as a result of climate change to system administrators making human errors. Every possible risk requires analysing and attention in each individual company.

Email Disaster Recovery has been thoroughly analysed and evaluated ever since the first email was saved to file. Archiving solutions have adapted to growing compliancy and recovery issues as email archiving becomes more popular. Knowledgeable businesses are now realising the importance of archiving especially because of disaster recovery. The major damage a system failure can have on communications is a developing reality. What a company classes as a risk and how they assess them depends on aspects like cost, time and resources.

Natural Disasters

Generally, first impressions of disaster recovery pertain to natural disasters; hurricanes, tsunami's, earthquakes, floods. In the last five years, many more cases have appeared worldwide and frequently. The controversial conclusion that climate change is the predominant factor in the increase leads us to believe that things will only worsen.

The consequence for the business world is a higher percentage risk of a system shutdown due to these disasters. The impact on maintaining business continuity relates to enlarged risk management strategies and finding new solutions. Location is obviously an important factor when assessing company risks; southern parts of North America and the Caribbean have high threat levels especially in the hurricane season. In 2005, the world sadly looked upon in astonishment at the immeasurable destruction hurricane Katrina created.



Although these natural disasters cause shattering outcomes to companies without solid contingency plans, they only make up a small percentage of disaster recovery examples. The majority of cases where recovery of data is needed occur because of technological failures such as human-computer error, data corruption, database and storage errors, software configuration or failure, site failures, poor network management and mass hard drive crashes. Especially power outages are a high telecommunications risk, fires, either accidental or man made but also mundane tasks such as relocating to a new site will require system continuity plans. These categories all fall under 'disaster recovery' therefore strategic and contingent plans must be in place to prevent them from happening.

Hurricane Katrina 2005

Vulnerability of Email

Specifically with email systems, all the above failures would affect email management greatly. Special considerations should be contemplated for email recovery because it is generally far more vulnerable than any other application especially when it is put under high volume stress. Email systems are continuously susceptible to viruses, decentralised systems can be unstable platforms and the diverse configuration of many users causes inconsistencies and problems when dealing with third party applications.

Preparation, Impact and Continuity

Successful Disaster Recovery Management involves careful planning and a complete understanding of the operative business processes. The impact a system failure can have on a business is substantial but with the suitable continuity plan in place, little disturbance will manifest.

When a company experiences a system shut down they have many considerable inconveniences to cope with, some businesses do not ever recover in the long term after a serious failure.

The major issue is cost, if you have no functional business you have no profit. Banking, Brokerage and media companies run particularly high turmoil risks when they are down because of their constant struggle with time. Large sums of money and perhaps more importantly damage to reputation can cause havoc in the short and long term.

The main objective in Disaster Recovery management is to start normal business operating as quickly as possible, have the shortest Recovery Time Objective (RTO) as possible. Many factors effect this common goal; technological, financial, timing, resources and regaining correct information systems.

There is a vast difference between small and large enterprises when deciding upon a recovery strategy. Large organisations can afford the time, resources and cost in building strategic continuity plans with data centre switch over, staff working contingency plans, extensive off site back up storage and retrieval mediums. Where as smaller businesses struggle to afford the resources for any backup system at all.

Continuity also ranges from firm to firm; getting the right balance after a failure can affect the long term business recovery. For example, when employees attempt to continue working after a failure, it can cause high risk security problems with sensitive data being transmitted from home or Internet cafes etc. The data then becomes highly inaccessible, out of the office network. This emergency initiative undertaken by the employee can cause more difficulties than solving the problem. For compliancy reasons employees that start saving emails onto their home systems run the risk of losing delicate information. Their received mails should be archived when the office system returns to full functionality.

Continuity plans can be developed internally, with the help of IT consultants or through a contracted consultancy firm. Software solutions such as H&S's **PAM for EXCHANGE** play an important role in the full business disaster recovery plan.

Email Continuity with PAM for EXCHANGE

H&S simplify the email lifecycle management process for IT Administrators and End Users. Email retrieval through the integrated HSM store is a straightforward procedure that requires little effort and little time.

PAM for EXCHANGE confronts disaster recovery by using its revolutionary designed Hierarchical Storage Management (HSM). The HSM store is integrated into the PAM server and redirects archived mails into various storage media's. When mails are directly archived the administrator can decide to simultaneously/parallel archive mails into two or more storage devices. Therefore if one storage media malfunctions, the mails continue to be archived and stored safely onto the secondary storage device. The system can be repaired without any loss of communication to the users (See Figure).

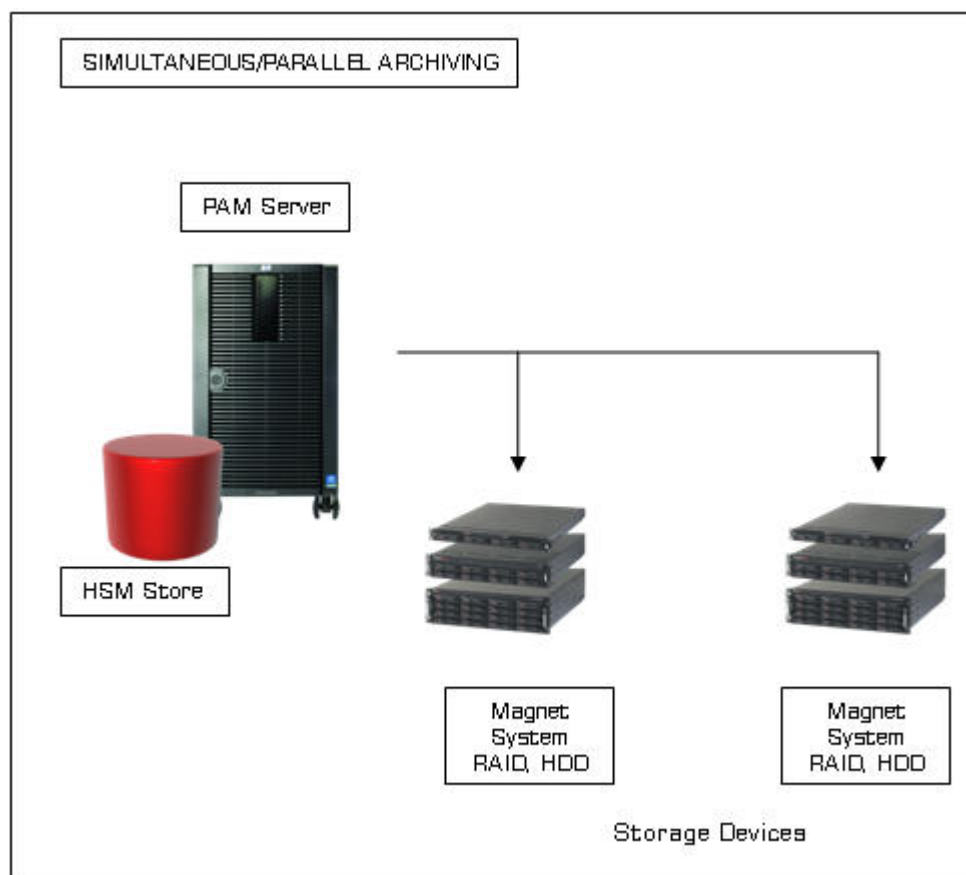


Figure 1 Simultaneous/Parallel Archiving

PAM for EXCHANGE is designed specifically to compliment the MS-Exchange Server. If the MS-Exchange Server crashes for any reason, the archived mails remain stored on the storage media and the **PAM for EXCHANGE** server blocks any further emails from being received until the MS-Exchange Server is back running. Once again, no emails are misplaced or lost whilst the network is down. Finally, **PAM for EXCHANGE** has the ability to function with POP3 and the web archive if the MS-Exchange fails. This quick fix solution helps users stay connected and communicating in disastrous situations. In conjunction with the Direct Archiving feature users can access and edit their archived messages and attachments through the Web Portal.

Retrieval is Critical

The key element to **PAM for EXCHANGE** archiving solution for disaster recovery is the integration of H&S’s HSM store with the PAM Server. Archiving has proven to cut storage costs and relieve pressure from Outlook but in the event of a system failure what good are stored emails on hardware devices if they cannot be retrieved proficiently.

The HSM store is developed to locate and retrieve emails from multiple storage devices and deliver them to multiple mailboxes in the quickest response time. This advantage is ideal in disaster recovery periods (See figure 2). In this scenario, a company has two locations and two archiving systems communicating to each other through an SQL database. Archiving emails from location 1 can be synchronously archived to storage in location 2. If the entire system at location 1 is demolished, the IT administrator can quickly and securely retrieve the duplicate archived emails from the mirrored stores in location 2 and relay them to the users.

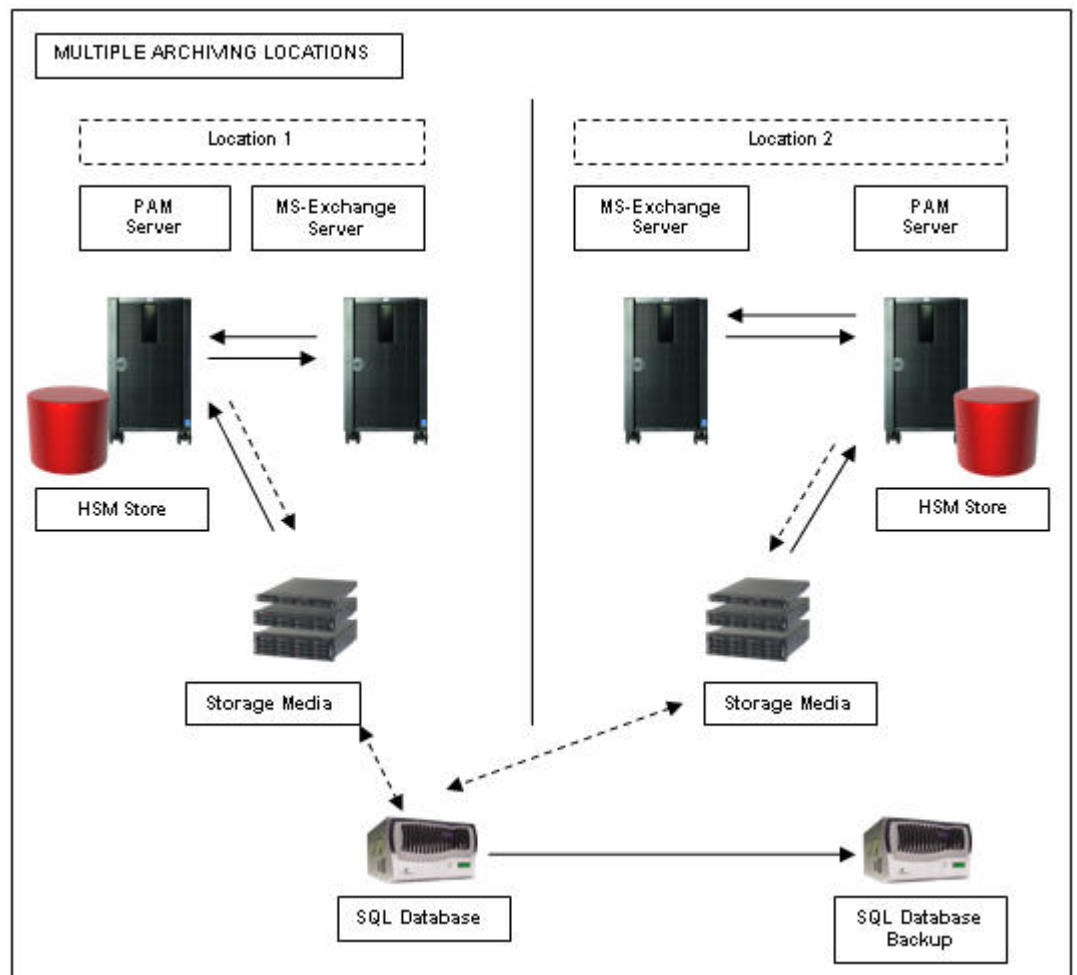


Figure 2 Multiple Archiving Locations

Off-Site Storage

Sufficient distance for off-site storage between the two locations is debatable. Many believe thirty miles is adequate safety but if a power outage or hurricane for instance hits an entire city or area then both locations risk the same outcome. Long distance locations will solve that problem but message transfers require an able capacity IP subnet to function with the amounts of data sent and received. Research into locations and risk management is a key factor to consider and it will differ from business to business. The expense to a small business could be too high to regard as an option but for larger