ZANTAZ®
Trusted. Proven.™

DISASTER RECOVERY
AND ZANTAZ EAS

On August 28, 2005 the hurricane Katrina beat a path through the Gulf of Mexico directly toward New Orleans. Not one month later, Hurricane Rita, on record as being the strongest measured hurricane to ever have entered the Gulf of Mexico left behind a trail of damage estimated in the billions of dollars to a region still reeling from Hurricane Katrina.

The disastrous conditions left behind by Katrina and Rita reminds us that preparation can be key to survival. And for businesses of all types and in all industries, a tried and tested contingency plan is essential in order to ensure that business operations can be recovered in the wake of a major disaster.

Email is a Critical Business Component

One critical component that is often overlooked in disaster recovery planning is email. The importance and complexity of email has evolved from a few simple text messages into a multitude of mission-critical documents. Negotiations, bids, proposals, contracts, legal agreements, regulatory forms, and a host of other vital correspondence now find form in electronic messaging systems.

According to U.S. News & World Report, Americans send and receive well over 7 trillion email messages each year, compared with only about 300 million pieces of first class mail. Nearly every key business process relies on email as a critical component. As a result, suffering a system outage is a significantly damaging event for most, if not all, organizations.

Email Recovery

While many companies have various disaster recovery and business continuity plans, many also find that their programs fall short when it comes to email. Messages are often widely dispersed in network servers and on individual hard drives throughout the enterprise. When backups are performed, email data is often stored on tape drives or optical discs without a cohesive management mechanism. Indeed, many organizations leave email archive management in the hands of end users, making recovery in times of outage or disaster a hit-or-miss proposition.

This lack of focus on email can spell disaster when it comes time to recover from a catastrophe. Firms that overlook email in their business continuity plans will find that recovering after a disaster may be a fatal impossibility.

The Challenges of Email Archival

In the early 1990's, most email messages were between 1Kb and 3Kb in size, but basic electronic messages have grown over time, to a current average of 75 Kb In addition, a decade ago file attachments were rare, but today over 20 percent of email comes with attachments. Graphic files, spreadsheets and Word documents are common. As a result, email messages with attachments average around 100Kb today, and analysts predict that this super-sizing will continue at a growth rate of 35 percent per year.

The trouble with this exponential growth is that email servers are designed to be transport vehicles, not archive repositories. Their ability to store data over time is limited, and as servers become overburdened by the volume system performance suffers. The result is slow response times, or worse, system outages when the servers themselves become unstable.

To combat the ever-growing demand on server storage, system administrators often limit the allotted size of their users email store. Today, the average size of a message store allotment is between 45 and 100 Mb. If a typical user sends and receives 70 messages per day (at an average of 5Kb) and 20 percent of those messages have attachments (at an average of 100Kb), we can predict that users will quickly exceed their allotted storage space. As a result, most are forced either to begin deleting messages or find other places to store important email.

In response to the imposition of mailbox quotas, email users often create personal archive folders (PST or NSF files) to which they automatically migrate email from their online message store as messages age (i.e., older than "x months"). The trouble is that PST/NSF files are notoriously unstable; especially as they grow in size, and this can foil attempts to recover critical information. In addition, these files are distributed around the network in an ad-hoc fashion and are generally not centrally managed or controlled. Should a company require access to old email messages for litigation or regulatory purposes, messages stored in personal mail archives are extremely difficult and expensive to locate and produce.

ZANTAZ EAS' Resiliency in the Face of Hurricane Rita

One of the largest integrated energy companies in the world maintains seamless email operations in the face of the nation's largest national disaster ever

In August and September of 2005, the United States was hit by two destructive hurricanes: Katrina and Rita. The oil industry suffered a shutdown of 25 percent of all U.S. crude oil production, more than 14 percent of U.S. natural gas production and a significant portion of refinery production capacity at facilities in the Gulf of Mexico region.

As a member of the Gulf Coast community for more than a century, one of the largest integrated energy companies in the world was determined to help speed the recovery from the devastating affects of Hurricanes Katrina and Rita. In addition to making a commitment of millions of dollars to support recovery efforts in the communities affected by Hurricanes Katrina and Rita, and implementing relief programs geared toward rebuilding efforts, the company worked around the clock to ensure the safety of its employees and restore normal operations at its refineries, offshore production facilities and offices in the Gulf region.

Ensuring outage-free operations for its email archive during Hurricane Rita was a five minute task thanks to its centrally managed email archival system, ZANTAZ EAS.

"With the advantages of a ZANTAZ EAS' parent-child architecture, disaster recovery preparations took this multinational energy company only five minutes to implement a disaster recovery plan for its email archive when faced with a category 5 hurricane," said a representative of the energy company. "By simply redirecting email reads from our parent servers to point to our replica data in our child servers, we were able to efficiently and transparently maintain outage free operations. Good thing it only took five minutes, because when Rita hit category 5, we weren't sticking around!"

Another issue with personal mail archives is that they inevitably result in the storage of email in multiple places (often multiple times). As each user independently creates their local mail archive, there is no mechanism to apply any storage optimization of email messages enterprise-wide. Consequently, email takes up residence in a hodge-podge of hard drives, laptops, and network servers of all sizes and types. Analysts indicate that overall space consumed by these unmanaged emails can be enormous – 10, 15, 20 terabytes, or more – and estimate that upwards of 80 percent of stored email records and their attachments can be eliminated because they are redundant copies.

Centrally Managed Email Archive

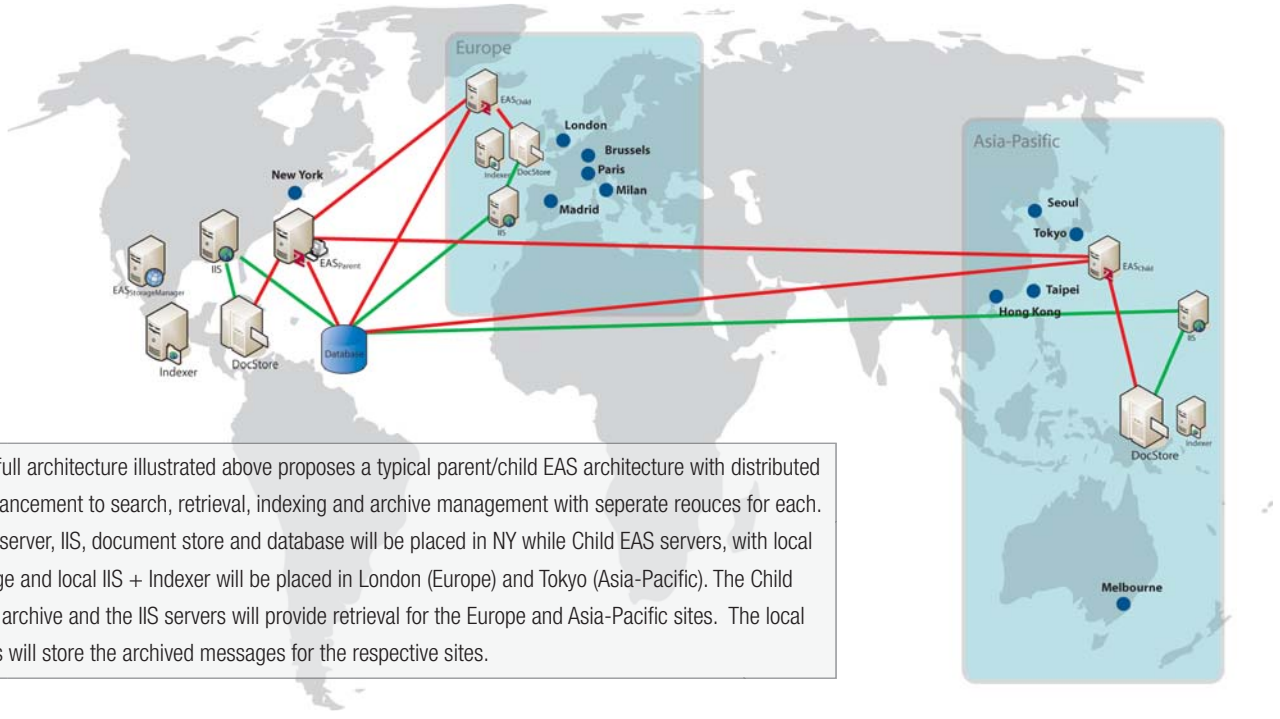
Instead of allowing users to create ad-hoc email archives or continuing to dump messages into unmanaged PST files, a better administrative approach is to create centrally managed archive designed to store large volumes of email data and allow those messages to be retained and accessible at all times. This approach not only enables IT administrators to offload the burden on email servers, improving their stability and performance, but it can ensure redundancy and access to critical messages in the event of a system outage or disaster.

Analysts predict that the size and volume of email will grow at a rate of 35% per year.

ZANTAZ EAS is built on a parent-child architecture that can be centrally managed and locally optimized across an organization with multiple domestic and international branches. Regardless of the number of sites or users in an organization, the parent-child architecture of EAS makes it possible to create one logical archive that spans an entire organization.

During disaster recovery, a centralized email archive can be a lifesaver since mission-critical and historical email is no longer spread out among various storage media, local hard drives and laptops. Backup and recovery is achieved more quickly, completely and effectively with a centralized archive.

Establishing a centralized archive is only part of the equation, however. Organizations should be cautious to avoid a single point of failure. It is crucial that the central email archive is included in overall corporate data recovery plans and redundant repositories should be established, preferably in separate geographic locations. To overlook this aspect of disaster planning will put the company at risk.



The distributed-full architecture illustrated above proposes a typical parent/child EAS architecture with distributed storage and enhancement to search, retrieval, indexing and archive management with seperate reouces for each. The Parent EAS server, IIS, document store and database will be placed in NY while Child EAS servers, with local document storage and local IIS + Indexer will be placed in London (Europe) and Tokyo (Asia-Pacific). The Child EAS servers will archive and the IIS servers will provide retrieval for the Europe and Asia-Pacific sites. The local document stores will store the archived messages for the respective sites.

As we see with the Katrina and Rita hurricane disasters – events that impacted a three-state area – it does an organization no good to have an email archive, only to have that archive suffer the same soggy fate at headquarters as other servers and systems. The risk is that during one singular problem – be it an electrical surge, a fire, or an event as catastrophic as a hurricane – the entire email archive will be lost. The same type of business continuity acumen applied to phone networks, corporate data applications or network topology must be applied to email archive management as well.

Another key aspect to making this redundancy work as an effective recovery mechanism is the ability to redirect operations between the redundant archives. If users typically access emails in New Orleans, for example, redirection to a redundant archive, say in Atlanta, is a must for recovery. Many companies on the gulf coast banked their recovery on data tapes or optical discs housed in their headquarters and are now suffering through a prolonged outage and recovery period. Organizations with a broader recovery plan that included backups in separate geographic locations have faired more favorably, incurring a relatively brief interruption of business operations.

Automatic Archival and Redundancy Via EAS

This redundancy and disaster recovery capability is intrinsic in ZANTAZ Enterprise Archive Solution (EAS). No additional replication tools or ancillary products are needed to ensure that email is saved automatically in a centralized archive, and that the data in that repository is ported to one or more redundant storage sites. The EAS archive engine has the flexibility and performance to support archival to multiple document stores simultaneously. This enables EAS system administrators to configure multiple geographically diverse archive storage locations – New Orleans, Atlanta, California, for example. These redundant repositories are updated on the fly by EAS as messages are archived.

> For businesses of all types and in all industries, a tried and tested contingency plan is essential in order to ensure that business operations can be recovered in the wake of a major disaster.

In the event of a disaster, message retrieval is automated as well. EAS utilizes web server technology, with its inherent capacity for redirection, to connect users with the archived email. If users request access to email stored in New Orleans, but the server is down, EAS will automatically and transparently direct the request down another path to the secondary archive in Atlanta. If Atlanta is down also, EAS looks to California, and so on.

This type of automated redundancy and re-routing is transparent to users, and part of the standard feature set of EAS. Administrators do not have to purchase ancillary products or manage additional tools in order to provide redundant protection and recovery capabilities. Users can work with the assurance that they can access important email data via the centralized archive. Executives can rest easier knowing that the company has eliminated a critical point of failure that can put recovery out of reach during times disaster.