Title: Method and System for Processing Email During an Unplanned Outage

This non-provisional application claims priority based upon prior U.S. Provisional Patent Application Serial No. 60/408,755 filed September 6, 2002 in the names of Michael I. Rosenfelt and Satin Mirchandani, entitled "System For Providing Backup Electronic Messaging Services During Unplanned Outages."

BACKGROUND OF THE INVENTION

Technical Field of the Invention

The present invention relates generally to a method and system for processing email during an unplanned outage. More particularly, the present invention provides for the redirection of email during an unplanned outage, notifies users that alternative access is available to said email, and restores messages received during the unplanned outage into the users' original email system to maintain the integrity of the email file.

Description of Related Art

Everyday more and more companies are concluding that email messaging is a mission critical application worthy of inclusion in a business continuity plan. Previously, companies that made this decision had no alternative but to implement expensive and complex systems. Traditionally, the solution has been to replicate the company's entire email system, such as a Microsoft Exchange database, in a remote datacenter on hardware similar to that owned by the company. Because of the complexity of such system, such as Microsoft's Exchange architecture, replication strategies have focused on real-time database replication of disks at the byte level or,

alternatively, on transferring offline database backups on a server-by-server basis.

Even in cases where a company implements complete replication of its databases, it is not uncommon for there to be gaps in email continuity due to, for example, database corruption, the presence of viruses, denial of service attacks, security breaches and other factors. Some of the most often cited problems with replication are:

1. High Cost. The cost involved in replication can be staggering. In order to implement an effective replication system, the company must purchase third party replication software, acquire network bandwidth, secure server capacity, retain administrative support and then monitor each of these systems.
2. Replication of Only a Subset of the Servers. As a result of the costs inherent in providing a replicated database, such as, for example, the cost of hardware, software, bandwidth and support personnel, it is common for only a few of the most critical servers to be replicated.
3. Database Corruption. Because replication technology by its very nature mirrors the files from one server onto another, a corrupt file on the original server will be mirrored in its corrupt form on the backup server. There is currently no efficient means for preventing the mirroring of corrupt files.
4. Incapacitation Due to Virus. Similarly, if a virus occurs in a file on the original server, it will be transported to the second server. Server corruption due to viruses can cause email outages for days.

5. Transactional Inconsistency. Because replication solutions typically perform byte-level replication of the disks, they do not provide integrity for the Exchange transaction boundaries. For example, a single transaction on Microsoft Eschange may consist of ten sequential writes to the disk. If the replication software has only replicated eight of those ten at the time of an outage, then the backup will be incomplete, resulting in a corrupt file which may fail to mount.

6. No Vendor-Supported Replication Solution. Currently no system that replicates systems like the Microsoft Exchange database is readily available at an economical price.

7. Complexity of Replication. The complexity of making an efficient, effective replication solution causes the system to be more prone to failure and thereby require greater resources to maintain.

For all of these reasons the existing technology fails to provide an adequate method for processing email during an unplanned outage. There is a need, therefore, for an improved method and system for processing email during an unplanned outage.

SUMMARY OF THE INVENTION

The present invention relates generally to a method and system for processing email during an unplanned outage and substantially departs from the conventional concepts and designs of the prior art. More particularly, the present invention comprises the steps of managing users' email; redirecting inbound email messages from a primary server to a secondary server when said primary server is unavailable;

notifying said users that the redirection of inbound email messages has been implemented; providing the users with access to the email addresses on a secondary server while the primary server is unavailable; notifying users when the primary server is again available; and incorporating the email messages received while the primary server was unavailable into the software for managing users' email so as to create a complete email history.

BRIEF DESCRIPTION OF THE DRAWINGS

The disclosed invention will be described with reference to the accompanying drawings, which show important sample embodiments of the invention and which are incorporated in the specification hereof by reference, wherein:

FIG. 1 is a flow diagram of a typical prior art replication process;

FIG. 2 is a diagram showing the preferred method of the present invention for processing email during an unplanned outage; and

FIG. 3 is a diagram showing a method for replicating email addresses on a secondary server.

DETAILED DESCRIPTION OF THE EXEMPLARY EMBODIMENTS OF THE INVENTION

The numerous innovative teachings of the present application will be described with particular reference to the presently preferred exemplary embodiments. However, it should be understood that these embodiments provide only a few examples of the many available embodiments and advantageous uses of the innovative teachings described herein. In general, statements made in the specification of the present application do not necessarily delimit any of the various claimed inventions. Moreover, some statements may apply to some inventive features, but not to others.

FIG. 1 is a flow diagram of a typical replication process. Inbound email messages **101** are received and processed on the primary server **102**. On a periodic basis, the information on the primary server **102** is replicated on a secondary server **103**. The replication process can occur at the byte level, the file level or the disk level. In some cases, the replication system is configured such that only files or disks to which changes have been made are replicated. In the event of an outage of the primary server, the secondary server is activated. However, because the primary server **102** and the secondary server **103** do not act in concert, it is necessary to take the primary server **102** completely offline before activating the secondary server **103**. Moreover, it is not possible to test the efficacy of the replication system by transferring only a few users from the primary server **102** to the secondary server **103**. Also, because of the complexities in transferring from the primary server **102** to the secondary server **103**, it can take as long as 30 to 60 minutes to complete a transfer at the time of an outage.

FIG. 2 shows a diagram outlining the preferred method for processing email during an unplanned outage. In general, inbound email messages **201** are redirected from a primary server **220** to a secondary server **230** when said primary server **220** is unavailable. Users are notified that email messages **201** have been redirected and those users are provided access to their email messages **201** via the secondary server **230**. Users are again notified when the primary server **220** is available. Thereafter, the email messages 201 that were received while the primary server **220** was unavailable are synchronized with the preexisting email messages **201** on the primary server **220** to create a continuous email history.

In an exemplary embodiment of the invention, inbound email messages **201** are sent to a server gateway **210**. In a corporate environment, inbound email messages may be sent from customers, vendors, partners, suppliers and the like. In a typical environment, inbound email messages are routed to an email application **240** residing on the primary server **220**. A registry of all email addresses residing on the primary server **220** is kept either on the primary server **220** or on the server gateway **210**. In some cases, the method of determining the email addresses that reside on the primary server **220** utilizes functionality inherent within the email application **240**. In other cases, the method of determining the email addresses that reside on the primary server **220** may be an independent program operating autonomously.

Next, email addresses that are redundant to the email addresses residing on the primary server **220** are created on the secondary server **230**. The secondary server **230** can be located remotely from the server gateway **210** and may be connected, for example, through the internet. In most cases, a message will be employed whereby the email addresses on the secondary server **230** will be updated on a periodic basis to replicate the email addresses on the primary server **220**. This creation of redundant email addresses on the secondary server **230** is continued on an ongoing basis.

A method is next employed to detect whether email addresses that reside on the primary server **220** are detectable to inbound email messages **201**. In some cases, this detection can be as simple as monitoring the email flow for error messages indicating a delivery failure. In other cases, an automated method may be employed which continually monitors a flow of inbound messages **201** to determine whether they are received on the primary server **220** as intended.

At such time as the email addresses that reside on the primary server **220** are not detectable to inbound email messages **201**, the inbound email messages **201** are redirected from the primary server **220** to the secondary server **230**. The transition from the primary server **220** to the secondary server **230** can be done automatically to determine that the email addresses on the primary server **220** are not being detected by inbound email messages **201**. It is also possible to direct only a portion of the inbound email messages **201** from the primary server **220** to the secondary server **230** in cases where only a portion of the email addresses residing on the primary server **220** are undetectable to inbound email messages **201**. Similarly, a decision may be made to transfer all inbound email messages from the primary server **220** to the secondary server **230** even though only a portion of the email addresses on the primary server **220** are undetectable to inbound email messages **201**. In those cases, for example, where it appears that primary server **220** may be prone to additional failure. It may also be desirable in those cases where the transition from the primary server **220** to the secondary server **230** is performed manually, to implement a password protection scheme whereby ability to effectuate the transition requires the entering of a password.

At the time, or immediately after, inbound email messages **201** have been redirected to the secondary server **230**, a notification is sent to users alerting them that email messages are available on the secondary server **230**. The notification method may consist, for example, of the automated delivery of notification messages **250** to an alternate email address for each of the users. Each of the users **231, 232** and **233** will have access to the secondary server **230** over the internet or a wide area network. The aforementioned

notification messages **250** can be sent to, for example, cellular telephones, personal digital assistance, pagers and the like.

During the period that inbound email messages **201** are directed to the secondary server **230**, continual assessment is underway to determine when email addresses, residing the primary server **220**, are again detectable to inbound email messages **201**. This activity may take the form of, for example, periodically pinging the email addresses residing on the primary server **220** and evaluating whether a response is received.

Once the primary server **220** is again available, inbound email messages **201** that had been directed to the secondary server **230** can be redirected back to the primary server **220**. At that time, users can be notified that the primary server **220** is again operational and that their traditional email application **240** is functioning. The notification to users can again be in the form of a notification message delivered to each user's alternate email address.

Once inbound email messages **201** are successfully redirected to the primary server **220**, inbound email messages **201** that had been received on the secondary server **230** during the outage can be synchronized into the email application **240** thereby creating a comprehensive email history within the email application **240**.

It is important to understand that in this preferred embodiment there is no need to take the primary server **220** completely offline in order to test the efficacy of the secondary server **230**. In addition, there is no significant cost inherent in testing the efficacy or functionality of the secondary server **230**. In addition, the ability to transfer only a portion of the email addresses residing on the primary

server **220** to the secondary server **230** provides a tremendous benefit. For example, if only a limited number of email addresses residing on the primary server **220** are affected, then only the inbound email messages **201** intended for those email addresses can be redirected to the secondary server **230**. In another example, after an outage has occurred, it is possible to redirect the inbound email messages **201** back to the primary server **220** on a limited basis to test the viability of the primary server **220** without the need to transfer all of the addresses on the secondary server **230** to the primary server **220**. This functionality permits a gradual transition back to the affected primary server **220**. Also, redirecting inbound email messages **201** from the primary server **220** to the secondary server **230** can be effectuated in less than two minutes compared to the 30-60 minutes required in traditional replication systems.

FIG. 3 is a diagram showing a method for replicating email addresses on a secondary server. In the initial step, email addresses that reside on a primary server are monitored using a means independent from the email application used to process email messages to create a registry of existing email addresses **301**. Periodically, a query **302** is sent to the primary server to determine changes to the registry. More specifically, the query will seek to determine whether email addresses exist in the registry **303**, if there are email addresses that do not exist in the registry **304**, or whether the email addresses are currently being updated in the registry **305**. If the email address exists in the registry **303**, then no further action is taken and the system repeats the query on a **302** on a periodic basis. If the email addressed does not exist in registry **304**, then the email address is added to the registry **306** and the address is

updated on a secondary server **308**. Thereafter, additional queries **302** are run on a periodic basis. Finally, if the email address is being updated in the registry **305**, that status is noted in the registry **307** and the added queries are run in the future to determine the updated status.

WE CLAIM:

1. A method for providing backup electronic messaging services during unplanned outages, comprising the steps of:

redirecting email messages from a primary server to a secondary server when said primary server is unavailable;

notifying intended recipients of said email messages that the redirection of said email messages has been implemented;

providing said intended recipients with access to said email messages on a secondary server while said primary server is unavailable;

notifying said intended recipients when said primary server is again available; and

incorporating said email messages received while said primary server was unavailable into said intended recipient's primary email file so as to create a continuous email history.

2. A method for providing backup electronic messaging services during unplanned outages, comprising the steps of:

retrieving an organization's email directory prior to an unplanned outage;

managing said email directory across multiple platforms;

restoring emails to said organization's production email system;

managing said restoration across multiple platforms;

notifying said organization's employees of the occurrence of said unplanned outage; and

populating an alternative back-up messaging system.

3. A method for providing backup electronic messaging services during unplanned outages, comprising the steps of:

managing an organization's email directory across multiple platforms prior to an unplanned outage;

upon the occurrence of said unplanned outage, restoring emails to said organization's production email system wherein said restoration occurs across multiple platforms;

notifying said organization's employees of the occurrence of said unplanned outage; and

populating an alternative back-up messaging system.

4. A method for processing email during an unplanned outage comprising the steps of:

managing users' email activity through a software application residing on a primary server;

determining the email addresses that reside on said primary server;

creating on a secondary server email addresses redundant to said email addresses that reside on said primary server;

determining if said email addresses that reside on said primary server are detectable to inbound email messages;

redirecting said inbound email messages addressed to said email addresses that reside on said primary server from said primary server to said email addresses that reside on said secondary server at such time as said email addresses that reside on said primary server are not detectable to said inbound email messages, thereby providing continuous access for said users' to said

inbound email messages and a means for generating outbound email messages from said users' existing email address;

notifying said users' that said email messages are available on said secondary server;

assessing the time at which said email addresses that reside on said primary server are again detectable to said inbound email messages;

redirecting said inbound email messages sent to said email addresses that reside on said secondary server from said secondary server to said email addresses that reside on said primary server after said time at which said email addresses that reside on said primary server are again detectable to inbound email messages;

notifying said users' that said inbound email messages are again available on said primary server; and

synchronizing said inbound email messages received on said secondary server from said time as said email addresses that reside on said primary server are not detectable to said inbound email messages until the time said email addresses that reside on said primary server are again detectable to inbound email messages with the existing messages in said software application, thereby completing the email message history within said software application.

5. The method of Claim 4, wherein said primary server is located remotely from said secondary server and is interconnected to said secondary server through the Internet.

6. The method of Claim 4, wherein said method of determining the email addresses that reside on said primary server utilizes functionality inherent within said software application.

7. The method of Claim 4, wherein said step of creating a secondary server of said email addresses redundant to said email addresses that reside on said primary server is repeated periodically so as to maintain a current registry of redundant email addresses on said secondary server.

8. The method of Claim 4, wherein said step of detecting if said email addresses that reside on said primary server are detectable to inbound email messages is performed manually by assessing whether an error message has been received indicating an inability to deliver said inbound email message.

9. The method of Claim 4, wherein all of said inbound email addresses on said primary server are automatically redirected to said secondary server at any time said email addresses on said primary server are undetectable to said inbound email messages.

10. The method of Claim 4, wherein all of said inbound email addresses of said users on said primary server are redirected to said secondary server after some, but less than all, of said inbound email messages are undetectable.

11. The method of Claim 4, wherein said step of notifying said users that said inbound email messages are available on said secondary server further includes the automated delivery of a preexisting notification email message to an alternate email address for said users.

12. The method of Claim 4, wherein said users' access to said inbound email messages on said secondary server is over the Internet.

13. The method of Claim 4, wherein said users' access to said inbound email messages on said secondary server is over a wide area network.

14. The method of Claim 4, wherein said step of assessing the time at which said email addresses that reside on said primary server are again detectable to said inbound email messages further includes periodically pinging said email addresses and evaluating whether a response is received from said email addresses.

15. The method of Claim 4, wherein said step of notifying said users that said inbound email messages are again available on said primary server consists of the automated delivery of a preexisting notification email message to an alternate email address for said users.

16. The method of Claim 4, wherein the ability to redirect said inbound email messages from said primary server to said secondary server is password protected.

17. A system for processing email during an unplanned outage comprising:

means for managing users' email activity through a software application residing on a primary server;

means for determining the email addresses that reside on said primary server;

means for creating on a secondary server email addresses redundant to said email addresses that reside on said primary server;

means for detecting if said email addresses that reside on said primary server are detectable to inbound email messages;

means for redirecting said inbound email messages addressed to said email addresses that reside on said primary server from said primary server to said email addresses that reside on said secondary server at such time as said email addresses that reside on said primary server are not detectable to said inbound email messages, thereby providing continuous access for said users' to said inbound email messages and a means for generating outbound email messages from said users' existing email address;

means for notifying said users' that said email messages are available on said secondary server;

means for assessing the time at which said email addresses that reside on said primary server are again detectable to said inbound email messages;

means for redirecting said inbound email messages sent to said email addresses that reside on said secondary server from said secondary server to said email addresses that reside on said primary server after said time at which said email addresses that reside on said primary server are again detectable to inbound email messages;

means for notifying said users' that said inbound email messages are again available on said primary server; and

means for synchronizing said inbound email messages received on said secondary server from said time as

said email addresses that reside on said primary server are not detectable to said inbound email messages until the time said email addresses that reside on said primary server are again detectable to inbound email messages with the existing messages in said software application, thereby completing the email message history within said software application.

18. The system of Claim 17, wherein said primary server is located remotely from said secondary server and interconnected to said secondary server through the Internet.

19. The system of Claim 17, wherein said means for determining the email addresses that reside on said primary server utilizes functionality inherent within said software application.

20. The system of Claim 17, wherein the operation of said means for creating a secondary server of said email addresses redundant to said email addresses that reside on said primary server is repeated periodically so as to maintain a current registry of redundant email addresses on said secondary server.

21. The system of Claim 17, wherein the operation of said means for detecting if said email addresses that reside on said primary server are detectable to inbound email messages is performed manually by assessing whether an error message has been received indicating an inability to deliver said inbound email message.

22. The system of Claim 17, wherein all of said inbound email addresses of said users on said primary server are

automatically redirected to said secondary server at any time said email addresses on said primary server are undetectable to said inbound email messages.

23. The system of Claim 17, wherein all of said inbound email addresses on said primary server are redirected to said secondary server after some, but less than all, of said inbound email messages are undetectable.

24. The system of Claim 17, wherein said means for notifying said users that said inbound email messages are available on said secondary server further includes the automated delivery of a preexisting notification email message to an alternate email address for said users.

25. The system of Claim 17, wherein said users' access to said inbound email messages on said secondary server is over the Internet.

26. The system of Claim 17, wherein said users' access to said inbound email messages on said secondary server is over a wide area network.

27. The system of Claim 17, wherein said means for assessing the time at which said email addresses that reside on said primary server are again detectable to said inbound email messages further includes periodically pinging said email addresses and evaluating whether a response is received from said email addresses.

28. The system of Claim 17, wherein said means for notifying said users that said inbound email messages are again available on said primary server further includes means for the automated delivery of a preexisting notification email message to an alternate email address for said users.

29. The system of Claim 17, wherein said means for redirecting said inbound email messages from said primary server to said secondary server is password protected.

30. A method for processing email during an unplanned outage comprising the steps of :

using a software means for managing users' email;

redirecting inbound email messages from a primary server to a secondary server when said primary server is unavailable;

notifying said users that said step of redirecting inbound email messages has been implemented;

providing said users with access to said email addresses on said secondary server while said primary server is unavailable;

notifying users when said primary server is again available; and

incorporating said email messages received while said primary server was unavailable into said software means for managing users' email so as to create a complete email history.

31. The method of Claim 30, wherein said primary server is located remotely from said secondary server and interconnected to said secondary server through the Internet.

32. The method of Claim 30, wherein said email addresses on said primary server are periodically replicated on said secondary server so that the transition from said primary server to said secondary server is seamless.

33. The method of Claim 30, further including the step of manually determining the availability of said primary

server by assessing whether an error message has been received indicating an inability to deliver said inbound email message.

34. The method of Claim 30, wherein the step of redirecting said inbound email addresses of said users on said primary server to said secondary server is automatically performed at any time said primary server is unavailable.

35. The method of Claim 30, wherein the step of redirecting said inbound email addresses of said users on said primary server to said secondary server is performed after some, but less than all, of said inbound email messages are undetectable.

36. The method of Claim 30, wherein said step of notifying said users that said means of redirecting inbound email messages has been implemented further includes the automated delivery of a preexisting notification email message to an alternate email address for said users.

37. The method of Claim 30, wherein said users' access to said inbound email messages on said secondary server is over the Internet.

38. The method of Claim 30, wherein said users' access to said inbound email messages on said secondary server is over a wide area network.

39. The method of Claim 30, further including the steps of determining the availability of said primary server by periodically pinging said email addresses on said primary server and evaluating whether a response is received.

40. The method of Claim 30, wherein said step of notifying said users that said inbound email messages are again available on said primary server further includes the automated

delivery of a preexisting notification email message to an alternate email address for said users.

41. The method of Claim 30, wherein the step of redirecting said inbound email messages from said primary server to said secondary server is password protected.

42. A system for processing email during an unplanned outage comprising:

software means for managing users' email;

means for redirecting inbound email messages from a primary server to a secondary server when said primary server is unavailable;

means for notifying users that said means of redirecting inbound email messages has been implemented;

means for providing said users with access to said email addresses on said secondary server while said primary server is unavailable;

means for notifying users when said primary server is again available;

means for incorporating said email messages received while said primary server was unavailable into said software means for managing users' email so as to create a complete email history.

43. The system of Claim 42, wherein said primary server is located remotely from said secondary server and is interconnected to said secondary server through the Internet.

44. The system of Claim 42, wherein the email addresses on said primary server are periodically replicated on said secondary server so that the transition from said primary server to said secondary server is seamless.

45. The system of Claim 42, further including a manual means for determining the availability of said primary server by assessing whether an error message has been received indicating an inability to deliver said inbound email message.

46. The system of Claim 42, wherein said means for redirecting said inbound email addresses of said users on said primary server further includes means for automatically redirecting said inbound email addresses to said secondary server at any time said primary server is unavailable.

47. The system of Claim 42, wherein said means for redirecting said inbound email addresses of said users on said primary server to said secondary server operates after some, but less than all, of said inbound email messages are undetectable.

48. The system of Claim 42, wherein said means for notifying said users that said means of redirecting inbound email messages has been implemented further includes means for the automated delivery of a preexisting notification email message to an alternate email address for said users.

49. The system of Claim 42, wherein said means for providing users' access to said inbound email messages on said secondary server is over the Internet.

50. The system of Claim 42, wherein said means for providing users' access to said inbound email messages on said secondary server is over a wide area network.

51. The system of Claim 42, further including means for determining availability of said primary server by periodically pinging said email addresses on said primary server and evaluating whether a response is received.

52. The system of Claim 42, wherein said means for notifying said users that said inbound email messages are again available on said primary server further includes means for automatic delivery of a preexisting notification email message to an alternate email address for said users.

53. The system of Claim 42, wherein said means for redirecting said inbound email messages from said primary server to said secondary server is password protected.

54. A method for replicating email addresses on a secondary server comprising the steps of:

monitoring the email addresses that reside on a primary server and using a means independent from the email application generally used to process email messages to create a registry of said email addresses;

sending a query on a periodic basis to determine which of said email addresses reside on said primary server at any point in time, said query capable of determining if a specific email address exists on said primary server, said specific email address does not exist on said primary server, or said specific email address is in the process of being added to said primary server;

based on the results of said query, updating said registry of said email addresses;

replicating said email addresses on a secondary server upon a change in said registry of said email addresses.

55. The method of Claim 54, wherein said primary server is located remotely from said secondary server and is interconnected to said secondary server through the Internet.

56. A system for replicating email addresses on a secondary server comprising:

means for monitoring the addresses that reside on a primary server and using a means independent from the email application generally used to process email messages to create a registry of said email addresses;

means for sending a query on a periodic basis to determine which of said email addresses reside on said primary server at any point in time, said query being capable of determining if a specific email address exists on said primary server, said specific email address does not exist on said primary server, or said specific email address is in the process of being added to said primary server;

means for updating said registry of said email addresses based on the results of said query;

means for replicating said addresses on a secondary server upon change to said registry of said email addresses.

57. The system in Claim 56, wherein said primary server is located remotely from said secondary server and interconnected to said secondary server through the Internet.

58. A method for synchronizing messages received during an unplanned outage comprising the steps of:

identifying all email messages received on a secondary server during an unplanned outage;

determining which of said email messages have not been previously received at the user's primary email address;

forwarding copies of said email messages from said secondary server to said user's primary email address such that said email messages can be incorporated into said user's primary email application.