

Continuous e-mail Archiving



Introduction

E-mail preservation and retention related to businesses is one of the primary focuses of regulatory compliance. Laws such as the Sarbanes-Oxley, HIPPA and SEC Rule 17 A-4 establish retention requirements for e-mail communications. With an Exchange Disaster Recovery solution in place, it will become necessary, from time to time, to failover from the Exchange production server to the Disaster Recovery site server. When the failover takes places, it is imperative the system continues to archive e-mails from the Disaster Recovery server to remain in compliance, as well as to insure overall business continuity.

Traditional Approach

Usually, an organization has e-mail archiving software from one vendor and replication software, which helps them to create a standby server at the Disaster Recovery site, from another vendor. With this approach, there is no integration between the two applications. This results in the e-mail archiving software being unaware that a failover has occurred. Upon failing over to the DR site, that site has now become the primary exchange server location. Because the e-mail archiving software is unaware of the new primary server location, new e-mails which arrive at this new primary server location don't get archived, which makes an organization non-compliant from a regulatory compliance perspective.

Also, most of the replication software uses a byte or block level approach to create a standby server at the Disaster Recovery site, which is offline all the time during the replication cycle. This approach is not application aware and no additional archiving configuration can be done during the replication as the standby server is offline. When the standby server takes the role of the primary e-mail server, archiving configuration needs to be done at that time, which results in a loss of some incoming e-mails during that period of time.

Additionally, with byte or block level replication, chances of transferring physical corruption from primary e-mail server to the standby e-mail server increases. As the standby server is offline during replication, it will not realize if any corrupt data has been replicated until the standby server is required to take the primary e-mail server. Even if a single byte or block is corrupted, then standby e-mail server will not be started and hence old backups will be required to restore the primary e-mail server. Restoring backups can take anywhere from hours to days and e-mails sent/received during this period will not get archived.

MarketStor Approach

MarketStor is the only company in the industry which provides backup/recovery, disaster recovery and e-mail archiving all integrated, and a unique approach for creating standby e-mail server at the Disaster Recovery site. MarketStor takes an approach of replicating e-mails between primary and standby e-mail server to create standby server at the Disaster Recovery site. In this case, the standby server is live and running all the time. No chance of propagating physical corruption as replication is performed at the application layer.

MarketStor uses Microsoft's journaling mechanism to archive e-mails which ensures every e-mail gets archived even if an end user deletes it from his/her mailbox. Upfront primary and standby e-mail servers are configured for Microsoft journaling and the MS eArchiver is installed on both servers. So, in case the primary Exchange crashes or goes down, then the standby e-mail server takes over the role and new e-mails start getting copied to journal mailbox from where the MS eArchiver, which is already running on the standby server, picks up and archives those e-mails to the archive server.

Conclusion

Businesses of all sizes must take backup and disaster recovery seriously. Who knows what can happen? In recent years, information and data has become a vitally important corporate asset essential to business continuity all around the world. The ability to recover critical data quickly after a disaster is a fundamental requirement of economic viability. Microsoft SQL, Exchange and Windows servers are being increasingly used in mission critical environments and hence recovering them from a disaster is crucial for business continuity.

It is very important to have a disaster recovery plan that is easy to follow, well documented and known by employees. Relying on one employee or a non-documented process will only leave a company vulnerable, especially in a disastrous scenario. It is imperative to have proper processes and software implemented and tested to recover quickly from a disaster.



MarketStor Corporation
42400 Nine Mile Road
Novi, MI 48375

Phone: (248) 912-0396
Fax: (248) 347-8894

www.marketstor.com

COPYRIGHT NOTICE

No part of this document may be reproduced, recorded or stored in a magnetic or electric system or transmitted, in any form or by any means, or photocopied, without prior written consent of MarketStor. No patent liability is assumed with respect to the use of the information contained herein. While every precaution has been taken in the preparation of this document, MarketStor assumes no responsibility for errors or omissions. This document and features described herein are subject to change without notice.

Copyright © 2009 MarketStor Corporation. All rights reserved. 20-000020-001

All other products or services mentioned in this document are covered by the trademarks as designated by the companies who market those products.