

## WHITE PAPER

# PROTECTING MICROSOFT® EXCHANGE

Bob Roudebush,  
Director of Engineering  
Solutions

Published: May 2006

## Executive Summary

E-mail, shared calendars and contacts are used to power some of your most important business-critical applications. In fact, these systems have gone from being a "nice to have" to being business tools that are relied on by the entire company from the warehouse to the executive boardroom. Regardless of your job responsibilities, you most likely have an interest and dependence on e-mail. Without it, productivity literally comes to a crawl and can even stop completely. While it was once just a convenient way for employees to communicate internally, today e-mail systems like Exchange are tightly integrated with other important business applications and are one of the primary methods for communicating with current and prospective customers. Protecting Exchange systems against costly downtime has become a top priority for most IT departments. So then, the question becomes **"How do I ensure that my Exchange environment is always protected?"**

Though the technological reasons to protect Exchange systems may be self evident, there are quantifiable fiscal reasons to protect these messaging systems as well. The dollar value of any given data-set may be difficult to calculate, but the cost-savings of avoiding even a single Exchange outage can easily be determined. In most organizations, there are at the very least one or two subsets of end-users who cannot continue to work without these systems functioning. Even if these groups might not regularly produce revenue in the form of direct sales or billable engagements, salaries, benefits and fixed costs still accrue during an outage. Therefore, the loss of the messaging systems for even a few hours could easily result in thousands of dollars in budget outlay without recouping a single dollar in productivity. For revenue-generating groups, the cost of this downtime is even more easily quantifiable. Avoiding even one of these outages is not only a good idea for the IT department, but for the CFO's office as well.

Complete protection of Exchange requires a lot more than management of on-site and off-site tape backups. While traditional tape backup is an excellent tool for long-term archiving, true recovery for the sake of business continuity requires real-

time data protection which enables disaster recovery and high availability. Having a solution that is cost-effective, hardware independent and scalable is something every IT manager should seriously consider.

This whitepaper is meant to provide a brief technical overview of Microsoft® Exchange Server 2000 and 2003 survivability requirements as well as present how a solution such as Double-Take® can meet your company's availability and data protection needs for Exchange. The need to protect systems and data is readily apparent.

The remainder of this document will cover:

- What Exchange data needs to be protected for business continuity
- How Double-Take protects Exchange data
- How to ensure Exchange availability
  - With Stand-Alone Exchange Servers
  - With Front-End/Back-End Exchange systems
  - With Microsoft Cluster Services and Exchange
- Other considerations for Exchange

## What Exchange data needs to be protected for survivability?

As of this writing, there are two supported versions of Exchange in use (2000 and 2003) and those versions of Exchange can run on various configurations of Windows® 2000 and 2003. For each of these Exchange/OS permutations, one must also consider the additional complexity of service packs and hardware platforms available. The result of these permutations of configuration and deployment options is a wide variety of systems to be protected. The only common denominator in all of these configurations is that the various Exchange files are stored on Microsoft Windows file systems.

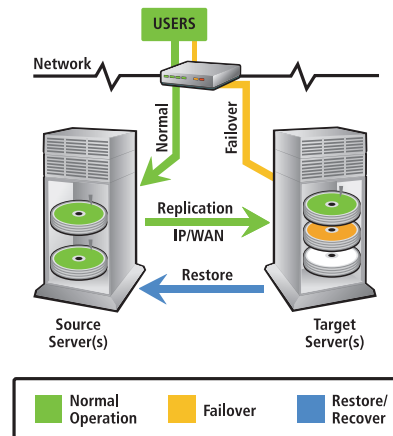
Each Exchange system is actually a complex configuration of multiple databases that are used to store and manipulate data along with a message transport system to move e-mail and other information into and out of these databases. Protection of the database files, along with their log files and checkpoint files, is critical to the recovery of any Exchange server. Generally speaking, each group of databases (Storage Group) will have a set of log files and a checkpoint file. They are identified by the extensions .LOG and .CHK, respectively. Each database unit (Mail or Public Folder Store) will have an e-mail database (.EDB) and a streaming data file (.STM). Only by protecting all of these files can you be sure you can resurrect an Exchange system that has suffered a disaster.

When a recovery from tape is attempted, the tape systems will replace these files onto the original server or a new server, at which point management tools can be invoked from within the Exchange System and from the command line to re-constitute the databases back to the state they were in when the tape backup was taken. This is an acceptable way to recover from something like a virus attack or human error where a point-in-time copy is needed to restore a good copy of the data. For a majority of outages like hardware failures and site-wide disasters, however, it is not the most effective means of restoring a failed server.

In many environments, solutions such as e-mail archiving are also deployed as an integral part of a company's e-mail architecture. These tools are designed to remove attachments and outdated e-mails from the Exchange server in order to free up disk space and enhance overall performance. This should be considered as part of any company's recovery plan for Exchange as it may be possible that not all of your vital data actually resides on the Exchange server itself. These additional systems will also need to be adequately protected in order to fully restore services to end-users. The same theory applies to Blackberry, GoodLink and other mobile information systems which also integrate with Microsoft Exchange to provide additional functionality such as remote access to e-mail. Without a Disaster Recovery (DR) plan that accommodates these systems, restoring the Exchange server itself is only one step on the road to recovering the entire messaging system.

Finally, as with many other database systems, Exchange requires that each transaction it writes to disk is performed in an explicit order. This is tracked continuously so that Exchange can maintain which changes have been requested and which have actually been committed to the physical database files. Generally referred to as a "transactional database system" and specifically called the JET database engine in Exchange, these databases do not tolerate replication or a backup system that cannot guarantee that write-order integrity of the data is maintained.

## How Double-Take Protects Exchange Data



Double-Take Software has been protecting messaging systems and other business-critical data since before Exchange 5.5 and even Windows NT Server 4.0 began shipping. One of the strengths of the Double-Take replication technology is that it protects files at the byte-level regardless of the application. In this case, when Exchange writes data to any of its files, the actual byte-level changes it makes to the Windows file system are sent to another Windows server. Once the data is protected to another server, multiple options are available for achieving availability and disaster recovery goals. The important point to consider, however, is that it all starts with the data - and that means it starts with Double-Take.

The first capability this method of data protection offers is a truly hardware-independent, version-independent, and OS-independent data protection solution. Simply put, Exchange resides on a Windows file system and Double-Take can protect those file systems.

Additionally, by leveraging its patented set of replication technologies, Double-Take can ensure that each Windows I/O transaction for a protected data-set is not only sent to one or more DR systems with full data integrity, but also that it will be committed in the exact same order that the original Exchange server committed the changes. Double-Take affords both data and write-order integrity, allowing the Exchange and the JET database system to immediately recognize a consistent copy of the data on the recovery system(s).

## An Overview of Double-Take Application Manager for Exchange.

Double-Take Manager for Exchange is designed specifically for the configuration and management of Double Take for the protection of Microsoft Exchange environments. It automates the setup and configuration of replication and failover monitoring of Exchange servers for rapid and successful deployment. Features such as auto-discovery of servers and key Exchange data files simplify the process down to just four steps and reduces the risk of human error.

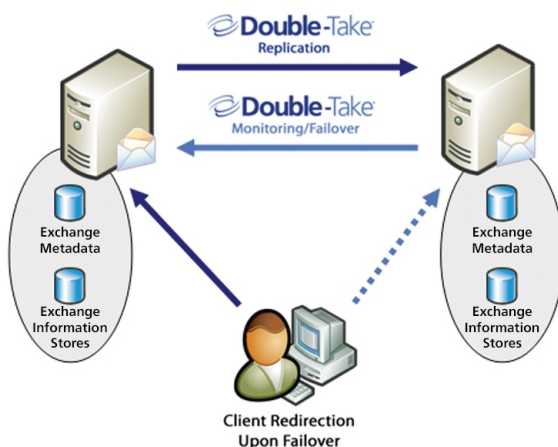
Exclusive features such as the pre-flight check help to ensure that all necessary settings within the environment are configured correctly for replication and failover of Exchange. Any errors identified are listed along with suggestions for resolution. Double-Take Manager for Exchange checks over 65 different configuration criteria and can automatically correct a majority of them on the administrator's behalf. This helps achieve a seamless, error-proof deployment.

Double-Take Manager for Exchange performs recovery and failback of Exchange servers with a minimal window of downtime. By performing recovery tasks while users remain online, Exchange downtime is reduced to just the few moments that it takes for Double-Take to stop and start the necessary Exchange services and relegate processing back to the production server.

Double-Take is at the core of our Exchange solutions, making available the extensive set of features and functions it offers. All advanced Double-Take features including intelligent data compression and flexible bandwidth scheduling are available for fast and efficient replication of Exchange data. Double-Take Application Manager for Exchange 4.0 further integrates the management of the Exchange protection environment into a single console with increased automation, speed, and efficiency for improved recovery times and higher levels of Exchange availability.

### How to ensure Exchange availability:

*With Stand-Alone Exchange servers:*



Exchange systems can come in a variety of flavors and configurations to meet nearly every business need and budget. By far the most common system employed today is the Stand-Alone Exchange server (SAES). SAES systems are a single server running all components of the Exchange system on the same physical or virtual system. This means the server acts as a mail-transport system, routing system, SMTP server and gateway and mail and public folder database server. It may also provide spam filtering, anti-virus scanning or any other function related to Exchange.

The end result of this configuration is that you have a single server that must be protected - all your eggs are quite literally in one basket. Double-Take can provide you with data replication of all key information for the Exchange system and any other systems running on the production server. In addition, the Double-Take Application Manager (DTAM) for Exchange can help you prepare a secondary server to take over in the event of a loss of the primary. DTAM for Exchange provides application-specific configuration, availability and management features and is a free toolkit available as part of Double-Take.

DTAM for Exchange will select the appropriate directories and volumes on your production machine which need to be protected, configure Double-Take replication, and configure the secondary server's Exchange configuration to match that of the production machine. It will also prepare the secondary server to execute the necessary commands to start Exchange services during an outage and allow failover to occur. During this configuration process, you can specify what network path the replication systems should use, if data should be compressed for transmission and if you wish to manually initiate the failover process ("one-click failover") or have it happen automatically after a timeout you define.

During an outage, DTAM will either automatically initiate a failover if the production server is unreachable for the amount of time you set, or alert you and wait for you to initiate the failover manually. Alerting for either type of failover scenario is available via SNMP, SMTP and the Windows Event Log, in addition to the native Double-Take management tools. Regardless of which failover methodology you choose, the procedure for restoring services for end-users is the same.

First, Double-Take's DNS Fail Over (DFO) component will update Active Directory DNS servers to re-route end-users to the recovery server. You may specify any and/or all DNS record types for update, depending on what systems you need re-directed. Double-Take Software Professional Services can also assist you with providing automated failover for customized DNS or Exchange deployments as well.

After DFO re-routes the end-users, the Double-Take Exchange Failover (EFO) component will dynamically re-assign all mailboxes and Public Folders from the failed server to the recovery server. This will allow end-users to regain access to their information the next time they attempt to connect to Exchange. Internal testing and real-world feedback has revealed that this failover process is very fast and creates a relatively small load on your existing DNS and Active Directory infrastructure - approximately 14,000 users can be moved to secondary server in around 7 minutes. In fact, while conservative failover estimates are suggested to be placed at 45 minutes for total failover, most Double-Take customers report being able to failover in less than 20 minutes - even when performing the failover across a WAN connection.

Finally, DTAM will prepare and start the appropriate Exchange and 3rd party services (anti-virus, mobile mail, archiving, etc) on the recovery server. This last step re-establishes a live Exchange server for your end-users to connect to. Outlook clients may need to be re-started, but no end-user configuration will be required. In addition, other components such as Outlook Web Access (OWA) and other e-mail integrated system will simply pick up where they left off.

### How to ensure Exchange availability:

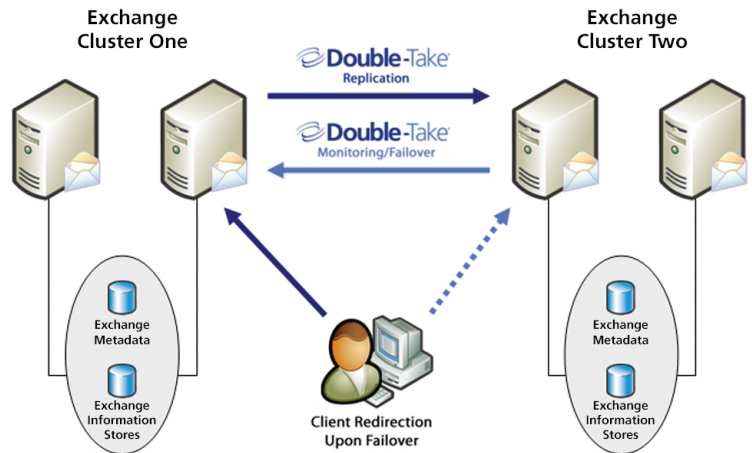
*With Front-End/Back-End Exchange servers:*

Front-End/Back-End (FE/BE) configurations for Exchange servers are becoming more and more popular as spam filters, virus firewalls and other solution sets make putting those systems on a non-database server much more effective. Front-End servers house mail routing and transfer systems, third-party tools for mail management and often the Outlook Web Access component of Microsoft Exchange. In these configurations, Back-End servers function as repositories for mailbox and public folder data used by end users.

In many ways, the method by which Double-Take protects FE/BE systems is very similar to the method employed with SAE systems described earlier. By leveraging the inherent load balancing capabilities of Exchange services such as Outlook Web Access or the load balancing feature of other Exchange-related solutions, a second Front-End server can be configured to accept mail and perform other functions either when the primary Front-End server fails or dynamically as additional resources are needed. Double-Take with the Double-Take Application Manager for Exchange is then deployed to the Back-End servers to provide disaster recovery and high availability for the Exchange databases used by the Front-End services. All options available for protecting SAE systems with DTAM are also available for protecting Back-End systems.

### How to ensure Exchange availability:

*With Microsoft Cluster Services and Exchange Server:*



In some cases, even a 20 minute failover time is simply too long to withstand. Microsoft Cluster Services (MSCS) can provide your organization with faster failover times in some cases - often failover occurs in a matter of just a few minutes. Though MSCS provides some benefits in terms of failover for Exchange, there are also potential drawbacks to be considered that may affect your decision to implement the technology. Firstly, MSCS requires hardware that is certified to be compatible with MSCS and also requires the purchase of shared disk array. Secondly, the MSCS architecture (two servers, a shared disk array, etc) may not be ideal for situations where you wish to separate the nodes of the customer across great distances. Lastly, due to the nature of MSCS and the shared-disk configuration it uses, two servers will alternately use the same copy of the data. This makes MSCS an exceptionally good system for local availability, but potentially introduces a single point of failure if an entire site experienced a disaster or other outage.

Double-Take used in combination with MSCS, however, allows for the protection of an Exchange Cluster to either another single- or multi-node Exchange cluster at a remote recovery location. By integrating seamlessly into the MSCS component of Windows Server, it does this without adding additional complexity to cluster administration. This is a best-of-both-worlds solution, offering MSCS failover in the event of a single-server failure, but still allowing for a redundant copy of the data on another system and the ability to fail over via DTAM for Exchange to that secondary system in the event that the entire production cluster is lost.

DTAM for Exchange when used in conjunction with an Exchange cluster failover performs nearly identically to the Stand-Alone or Front-End/Back-End configurations outlined earlier. In the case of Exchange clusters, however, replication is performed from the "owning node" of the cluster. The "owning node" is the cluster node that is currently running the Exchange services. In non-cluster deployments, Double-Take would replicate from a single, physical machine. In a clustered deployment of Double-Take, however, replication occurs from the "owning node" and switches to another node should MSCS failover Exchange to another node in the cluster. Because Double-Take is tightly integrated with MSCS, this happens automatically without administrator intervention.

### **Other Considerations for Exchange**

*and the rest of your environment.*

It is likely that new versions, service packs, hot fixes, and 3rd party add-ons will make protecting Exchange even more difficult in the future. By focusing on the Windows file system and OS, Double-Take Software will continue to provide value to customers with its effective, yet simple, approach to Exchange protection. This approach, along with the stability and scalability of the solution, is a reason for the current leadership position Double-Take Software maintains among Exchange protection technologies.

When considering enterprise technologies, it can be difficult to select vendors that support large areas of complex and heterogeneous organizations. When considering the variety of

applications (such as Exchange, SQL, Oracle, and file services) and the different versions of each of these applications in use, the task is even more daunting. However, because Double-Take Software replication technologies focus on data replication and then assist in the pre-configuration of applications independently, the same level of data protection for Exchange is equally viable for any other Windows based application. More simply put, you can standardize on one Windows availability solution, regardless of the myriad of applications in your environment.

In the same light, while storage technologies will continue to grow and change, Double-Take Software can protect any data on any Windows server. Even if you change server manufacturers or storage-solution vendors, as long as it is running a Windows server OS, Double-Take Software will remain part of your solution.

Double-Take Software has been protecting applications running on Windows file systems since Windows NT 3.51, and other server operating systems longer than that. "Business Continuity through Replication" is the single focus of every person in our company. That focus, and the quality of our products, has helped Double-Take Software forge relationships with HP, IBM, Dell, SunGard, Microsoft and probably your preferred reseller-integrator. Double-Take Software has even been awarded the Advanced Infrastructure Competency Certification for Exchange by Microsoft, proving that our Exchange solutions are not only technically sound, but that they have been battle-tested by real clients in real emergencies.

## About Double-Take® Software

NSI Software, Inc. (NSI®) doing business as Double-Take® Software, provides the world's most relied upon solution for accessible and affordable data protection for Microsoft® Windows® applications. The Double-Take product is the standard in data replication, enabling customers to protect business-critical data that resides throughout their enterprise. With its partner programs and professional services, Double-Take delivers unparalleled data protection, centralized back-up, high availability, and recoverability. It's the solution of choice for thousands of customers, from SMEs to the Fortune 500 in the banking, finance, legal services, retail, manufacturing, government, education and healthcare markets. Double-Take is an integral part of their disaster recovery, business continuity and overall storage strategies. Double-Take Software is privately held and headquartered in Southborough, MA. For more information, please visit [www.doubletake.com](http://www.doubletake.com).

**For more information on Double-Take Software products and services please contact us.**

### Double-Take Software Headquarters

257 Turnpike Road  
Southborough, MA 01772  
Phone: 800-775-4674  
Fax: 201-656-2727

### Double-Take Software Sales

8470 Allison Pointe Blvd. Suite 300  
Indianapolis, IN 46250  
Phone: 800-674-9495  
Fax: 317-598-0187

**Or visit us on the web at [www.doubletake.com](http://www.doubletake.com)**



**Get the standard today: [www.doubletake.com](http://www.doubletake.com) or 888-674-9495**

© 2006 NSI Software, Inc. All rights reserved.

Double-Take®, GeoCluster® and NSI® are registered trademarks of NSI Software, Inc. Balance™ and Double-Take for Virtual Systems™ are trademarks of NSI Software, Inc. Microsoft, Windows, and the Windows logo are trademarks, or registered trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are properties of their respective companies. are trademarks of NSI Software, Inc. Microsoft, Windows, and the Windows logo are trademarks, or registered trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are properties of their respective companies.

