



Ensuring Protection and Availability for Microsoft Exchange



2 Hudson Place – suite 700
Hoboken, NJ 07030

800-674-9495
www.nsisoftware.com

Powered by  **Double-Take**

"I am sorry but our mail system is down.

Could you call back later?"

The above quote may sound over dramatic, but chances are it also rings true. E-mail has gone from being "nice to have" to being the one application that is shared and demanded from the warehouse to the executive boardroom. Not CRM. Not even file services. But e-mail.

Whether or not your responsibilities include the I/T department, you have an interest and dependence on e-mail. For many of us, that is Microsoft Exchange. So then, the question becomes "**How do I ensure that my Exchange environment is always protected?**"

This document is not meant as a technology discussion on Exchange survivability, but as an executive overview of the options available for protecting Exchange. For more technical information, please visit www.nsisoftware.com/Exchange.

The remainder of this document will cover:

- How to protect Exchange data
- How to achieve disaster preparedness
- How to ensure Exchange availability
 - Without existing Exchange clusters
 - With existing Exchange clusters
- How to quantify Exchange outage vulnerability
- Other considerations for Exchange
- Why use NSI Software

Suggestion to Team > in the final release (and starting on 2nd page of text), let's add one quote per page regarding protecting Exchange. One from maybe Evergreen. Perhaps one from a European/Sunbelt customer. At least one from a US customer like USI (preferably a Financial, a Government, and a Healthcare). Etc.

Protecting Exchange starts with the data. Regardless of availability goals or disaster preparedness, all efforts start with insuring the resilience of the Exchange data.

As of the writing of this document, there are three major versions of Exchange in use (5.5, 2000, and 2003/"Titanium") - and those are running on a combination of Windows NT4, 2000 and 2003. For each of the above permutations, consider the addition of service packs and hardware platforms, and what we find is a wide variety of systems to protect. On top of that, consider that many different tape backup programs offer widely varying Exchange backup capabilities. The

only common denominator in all of these configurations is that the various Exchange files are stored on Microsoft Windows file systems.

NSI Software ® has been protecting file-system-based data since before Exchange 5.5, or even Windows NT 4, began shipping. One of the strengths of NSI's replication technology is that it protects files at a byte-level, regardless of the application. In this case, when the mail application (or any other application) changes any file, the actual byte-strings are sent to another Windows server. Once the data is protected to another server, multiple solutions are available for achieving availability goals. But it all starts with the data, and that means it starts with NSI Double-Take ®.

It is important to note that the NSI Software offers two product lines – Double-Take and GeoCluster™.

- Double-Take protects data on any Windows server to any other Windows server across TCP/IP. If two Windows platforms (including servers, NAS, and clusters) have IP connectivity, Double-Take can protect your data.
- GeoCluster is an add-on to Microsoft cluster services. In a typical MSCS configuration, the nodes share one storage solution. GeoCluster uses the same replication technology found in Double-Take to provide each node with its own copy of the data. Without the single point of failure in a shared storage array, the cluster nodes can be separated between buildings or across town.

"NSI's Double-Take software helps ensure our Exchange systems are protected and available, giving us the peace of mind necessary to focus on running our business."

James A. Hayes
Network Operations Manager
Peoples Bank & Trust Company

But because both products use the same NSI replication technology, most of this paper will focus on capabilities, not products. And the first capability to note is a truly hardware-independent, version-independent, and OS-independent data protection solution. Simply put, Exchange resides on a Windows file system; and NSI Software can protect those file systems.

How to Achieve Disaster Preparedness of Exchange. "Disaster Recovery" means different things to different people. In a broad sense, it includes changes to corporate culture, additional processes and documentation, identifying key personnel and their emergency roles, and equipping an alternate infrastructure. To the more focused IT executive, it all starts with the protection of the data.

One of the presumptions of disaster recovery is that the only two technologies are tape and synchronous hardware.

- With tape, one might routinely ship cartridges to a storage facility or vaulting service. This can be expensive to the bottom line and still leaves large windows of data exposure.

- With synchronous hardware, the data is protected but at a solution-cost that often exceeds many annual IT budgets. And due to the nature of those solutions, both copies of data are typically in the same power grid, weather zone, and municipality. In fact, some industries have started mandating that synchronous hardware does not provide enough distance and must be supplemented.

This brings us back to asynchronous software replication. NSI can replicate your Exchange data to any location across the city or across the country. By taking advantage of its built-in bandwidth control and extended queuing features, DoubleTake can use your current infrastructure to protect your existing Exchange servers to any other location.

If you already maintain multiple data centers, one can simply deploy redundant servers at key locations. This allows the local IT teams to maintain the platforms and conduct disaster preparedness exercises (*see figure 1*).

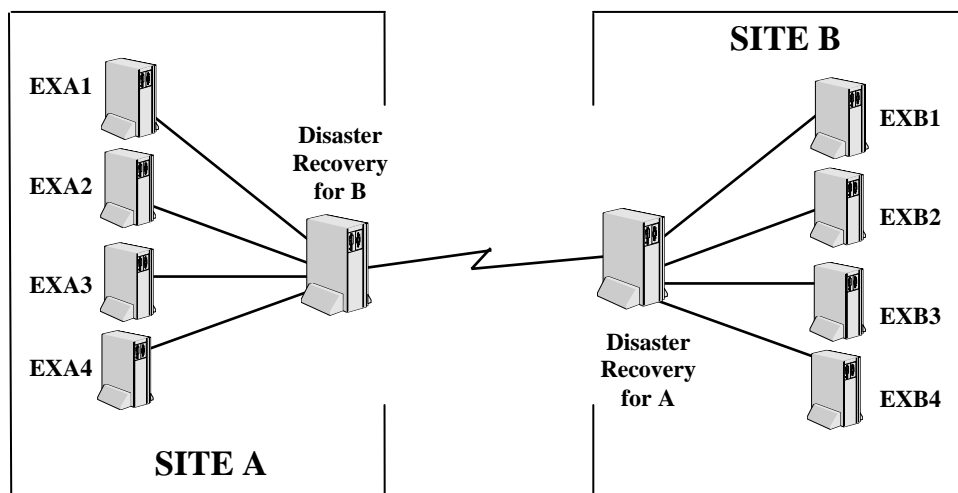


Figure 1 – Exchange Servers, bow-tied bidirectional between company sites

Or if you already have a relationship with a disaster recovery vendor (e.g. SunGard) or an SSP (storage service provider), chances are that they already have a relationship with NSI and can serve as the "target" for your data (*see figure 2*).

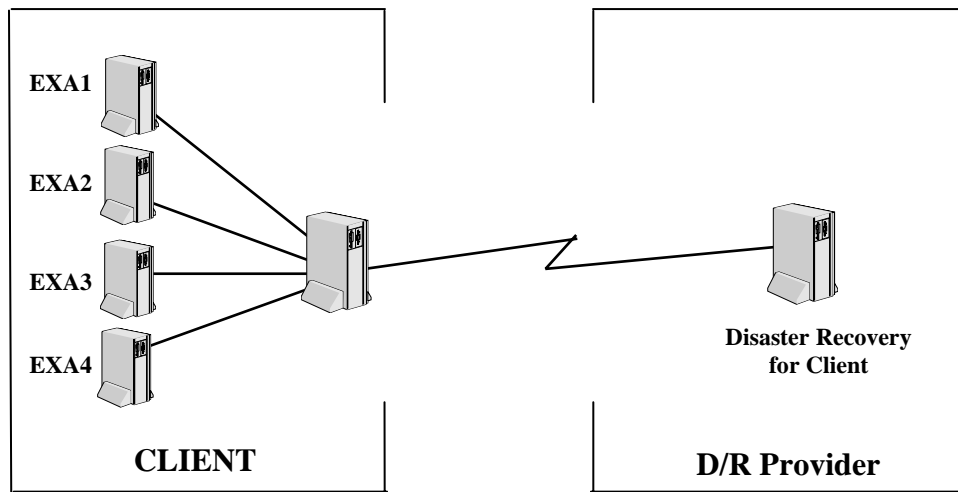


Figure 2 – Exchange DR to an SSP/hotsite

How to Ensure Exchange Availability. This is the one that matters most, right? How does one ensure that in all scenarios, the Exchange system continues to be available to the users?

With Exchange 5.5, a wide variety of availability solutions exist, including those provided by NSI Double-Take and GeoCluster. But with the release of Exchange 2000, it is clear that the best way to “fail over”, or provide a redundantly available instance of Exchange, is through Microsoft clustering. Due to Exchange 2000’s reliance on Active Directory and other technical concerns, Exchange behaves best when the name/IP/mailboxes/etc. are abstracted into a “virtual server” within MSCS. Then, MSCS handles moving the virtual server between physical machines – for availability.

Unfortunately, MSCS has some inherent architectural limitations, such as a shared single storage solution and node/distance limitations.

- All MSCS nodes must share the same physical storage. If the storage technology were to fail, none of the nodes would be able to function. This means that the shared data solution becomes a single point of failure.
- Because the nodes are assumed to share the solution, the existing MSCS technology does not provide for the nodes to be geographically separated. This means that if a single building (or even just the computer room) were to be impacted, the entire solution would be affected.

To address these limitations, NSI’s replication technologies can be used to significantly increase the availability of Microsoft Exchange.

If you don't already have clusters, then several NSI solutions are possible.

To eliminate the liability of the single instance of storage failing, one can integrate GeoCluster into the solution for redundancy of the storage. GeoCluster allows each of the clustered Exchange nodes to have its own copy of the Exchange data. Any failure of the application or OS (of the active clustered node) would be handled by the cluster. But now, the storage would be equally fault-tolerant (see figure 3).

To eliminate the potential of a building-wide crisis (which would negate all the nodes of a traditional cluster), the GeoCluster'ed nodes can be a significant distance away. Since each node has its own a local copy of the data, the cluster would continue to service clients throughout the environment.

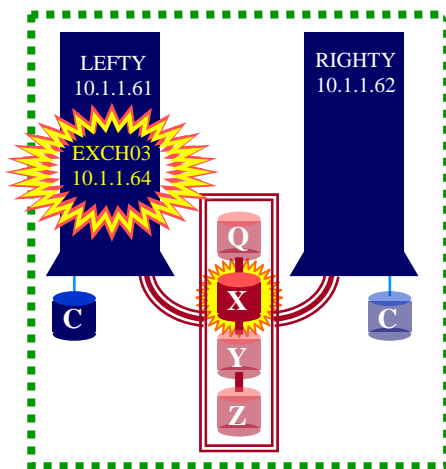


Figure 3a – Exchange on MSCS
(shared storage = single point of failure)

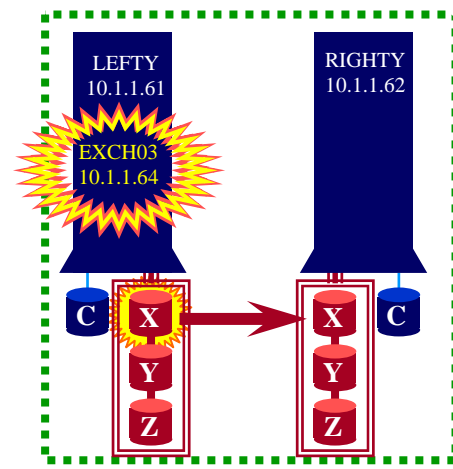


Figure 3b – Exchange on MSCS - with GeoCluster
(each node with independent storage)

Collectively, this provides not only "local" high availability, but actually metropolitan-wide protection. Whether it is simply a node that fails, a computer room crisis, or even any building-wide catastrophe - the surviving node (with its independent storage) will ensure that your Exchange services continue to function. For most NSI Exchange customers, the GeoCluster'ed nodes are across town, across a river, or in neighboring cities (e.g. Manhattan/New Jersey, Minneapolis/St. Paul, or Tampa/Orlando). But what about a regional crisis?

Or, if you already have clusters, then you already have a local availability solution (although with shared storage). But what happens if the computer room or building (that contains both Exchange nodes and the shared-storage were to suffer an outage)?

When considering regional-type outages (e.g. September 11th, the August 2003 blackouts or even annual hurricanes and tornados), city-wide measures may not be adequate.

To eliminate a city-wide or larger impact, Double-Take can replicate the data from the cluster to another platform, anywhere in the world. In fact, Double-Take can protect traditional MSCS clusters and GeoCluster'ed clusters (see figure 4).

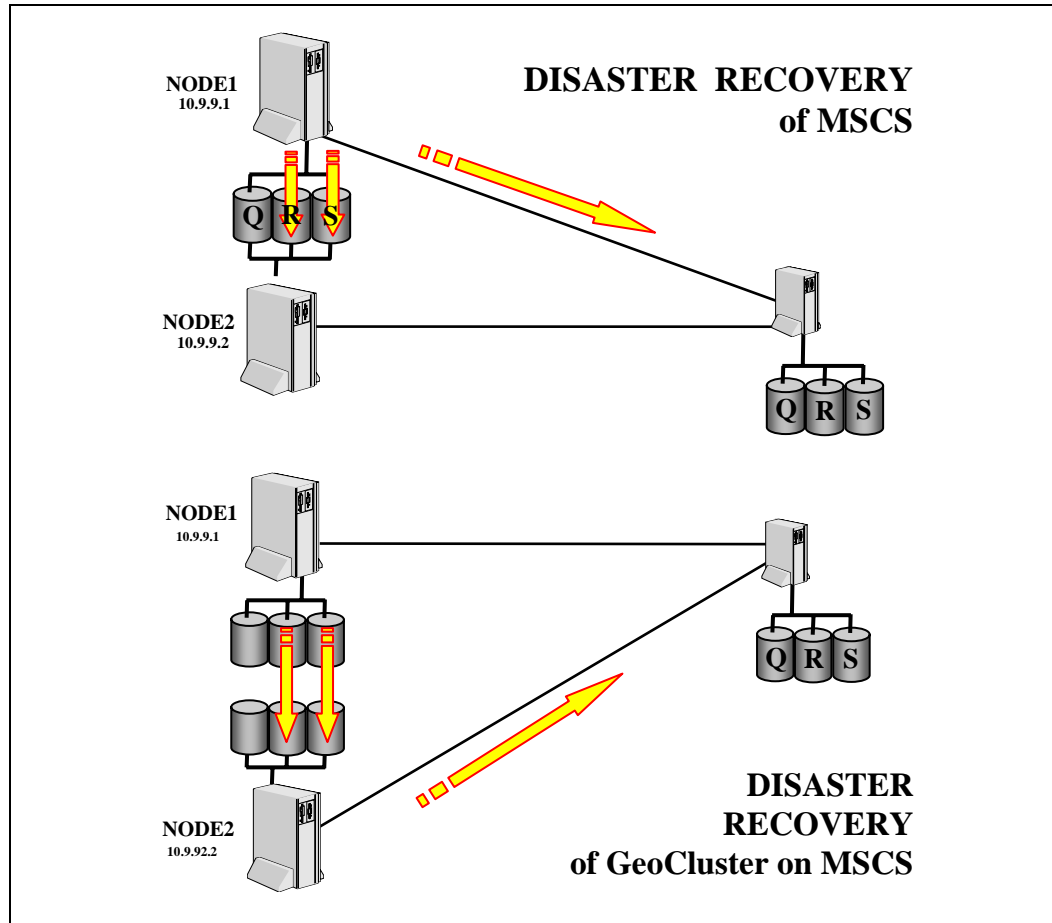


Figure 4 – Disaster Recovery of any cluster (with or without GeoCluster)

Using these tools, the target platform (anywhere in the world) can then be brought online to stand in for a failed production Exchange instance.

How to Quantify Exchange Outage Vulnerability. After recognizing that higher levels of resilience are possible for one's Exchange environment, we must now try to understand the business impact of an Exchange outage; so that we can decide what level of protection is adequate.

There are commonly two processes for quantifying outages and business impact. And really, the two build on each other.

The first is to calculate the cost in man-hours due to Exchange downtime. Determine the average annual 'unavailable' time for your exchange servers. "Unavailable" encompasses scheduled outages and unplanned interruptions. Then, after assessing how often each server is down, identify the users that are supported by each Exchange server. You next need to calculate the hourly cost for these groups of users. This information can be obtained from HR/Payroll or by using industry averages. Once you have the hourly costs, multiply that by the 'unavailable' time to determine your average cost of downtime as it applies to lost user productivity. There are other cost factors not accounted for here which you may want to consider, such as the lost business opportunities and transactions during these downtimes. And after doing this exercise, you now understand financially what your Exchange server is worth. And the uptime or downtime becomes a business decision, instead of a technology decision.

The second idea is to simply extrapolate the business impact over the estimated lifespan of technology in your environment. For example, you may assume that server hardware has a 24-36 month value. If so, any technology added to those servers would have the same lifespan. Therefore, one can objectively consider fault-tolerant technologies in an ROI analysis to the cost of the problem.

53 percent of companies have experienced business interruption or monetary loss related to email downtime

Osterman Research, April 2003

What most people find when they have assessed the business/financial implications of downtime, and compared it with more traditional technology alternatives, is:

- Tape backup does not provide enough protection, since it only runs nightly. All Exchange messages on the day of the failure are lost. And often, users are less or non-productive for most of the next business day. When looked at from the "lost manpower" perspective, most companies cannot afford to simply use tape.
- Synchronous mirrored hardware is the other end of the spectrum. When considering the proprietary hardware, software and additional components, most hardware solutions provide zero data loss but at a solution cost which often rivals or exceeds entire IT budgets, much less the cost of being down. Very few Exchange environments can justify this solution.

It is for this reason that Gartner predicted that, by the end of 2003, companies would be mixing tape backup (for weekly/monthly archives) and replication technology "*for more rapid application recovery*" – Gartner, IT Trends for 2002

More simply put, you can't afford to lose days of Exchange messages but most can't afford synchronous hardware. The answer is NSI Software's replication technologies.

Other Considerations for Exchange and the rest of your environment.

It is likely that Microsoft Exchange will continue to grow in dominance in the Windows networking space. It is even more likely that new versions, service packs, hot fixes, and third-party and-on's will make a protecting Exchange even more difficult. By focusing on the Windows file system and OS, NSI Software will continue to hold its leadership position in Exchange protection technology.

When considering enterprise technologies, it can be difficult to select vendors that support large areas of the organization. When considering applications (such as Exchange, SQL, Oracle, and file services) into their various versions, the task is even more daunting. However, because NSI replication technologies focus on files and not applications, the same level of data protection for Exchange is equally viable for one's other Windows-based applications. 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, NSI 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, NSI will remain part of your solution.

NSI Software has been protecting applications running on Windows file system's since Windows NT 3.51, and other server O/S's 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 NSI forge relationships with HP, IBM, Dell, SunGard, EMC, Microsoft and probably your preferred reseller-integrator.



For over 10 years, NSI has been providing the products, services, and support to help you be successful in protecting your most critical applications ... like Exchange.

We'd like the chance to prove it to you.

© 2003 NSI Software. All rights reserved.

Double-Take and NSI are registered trademarks of Network Specialists, Inc., GeoCluster is a trademark of Network Specialists, Inc. and all are used with permission of the trademark owner.

Microsoft, Windows Powered, Windows, Exchange, and SQL Server, are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Our Vision

To be the leading provider of data protection & high availability software solutions for 24x7 business operations

Our Offer to You

We would like to become your partner in ensuring the continuous operations of your business.

Please allow us the opportunity to talk to you about your specific data protection needs and to discuss our products and services that may apply.

Products that Protect your Data

Services that Ensure your Success

For more information on NSI's products and services, please contact NSI.

NSI Software - Corporate Office
Two Hudson Plaza, Suite 700
Hoboken, NJ 07030
800-775-4674 or 201-656-2121
Fax: 201-656-2727



NSI Software – Inside Sales
8470 Allison Pointe Blvd. Suite 300
Indianapolis, IN 46250
800-674-9495
Fax: 317-598-0187

Or visit us on the web at WWW.NSISOFTWARE.COM