



NSI Double-Take and VMware ESX Server & GSX Server Virtual Machines

NSI Software, Inc.
Two Hudson Place Suite 700
Hoboken, NJ 07030
www.NSISOFTWARE.com

VMware, Inc.
3145 Porter Drive
Palo Alto, CA 94304
www.VMWARE.com

No part of this document may be reproduced or transmitted in any form or by any means, electronic, or mechanical, for any reason, without the express written permission of NSI Software. The information in this document is subject to change without notice.
Companies, names and data used in examples herein are hypothetical and/or fictitious unless otherwise stated.

Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

Due to the use of third-party tools described in this document, these concepts are offered to the reader for consideration only. These techniques are not supported by NSI service or support organizations – and should be tested for your environment before implementing into production.

“How would you protect 11 production applications (or clients) with one disaster recovery server?”

NSI® Double-Take® and VMware Technologies provide proven protection for multiple production applications with one disaster recovery server. Simply put, VMware virtual machine enables Double-Take to replicate all production applications to the target as part of the virtual machines disk file. This document describes how VMware products can be used with Double-Take from NSI® Software, Inc. to provide solutions for challenging high availability and disaster recovery cases.

NSI Double-Take is the undisputed leader in Windows® based replication software. And for most business continuity solutions, protecting the data is the lynchpin that all other recovery aspects rely on.

What is the VMware Virtual Infrastructure?

Virtual infrastructure provides a layer of abstraction between the computing, storage and networking hardware, and the software that runs on it. Virtualization simplifies IT so that companies can leverage their storage, network, and computing resources to control costs and respond faster. In a virtual infrastructure, users see resources as if they were dedicated to them while the administrator is able to manage and optimize those resources globally across the enterprise.

Why is Virtual Infrastructure Important?

VMware's virtual infrastructure architecture enables businesses to lower IT costs through increased efficiency, flexibility and responsiveness. Managing a virtual infrastructure enables IT to quickly connect computing resources with business needs. With a virtual infrastructure, IT organizations can provision new services and change the amount of resources dedicated to a software service. With solutions from VMware, the data center can be treated as a single pool of processing, storage and networking power.

VMware Virtual Infrastructure Nodes (comprising ESX Server, VMware Virtual SMP, VMotion and a VirtualCenter Agent) can be deployed and managed with VMware VirtualCenter to transform an IT infrastructure into a virtual infrastructure. These software solutions allow IT organizations to respond faster to business demands with instant provisioning of virtual machines and dynamic resource (such as virtual disks for data) allocation to those virtual machines as business needs change.

VMware® ESX Server™ is datacenter-class virtual infrastructure software for partitioning, consolidating and managing systems. ESX Server and VMware Virtual Infrastructure Nodes provide a highly scalable virtual machine platform with advanced resource management capabilities which can be managed by VMware VirtualCenter. ESX Server runs directly on x86 hardware, providing high performance and complete hardware resource control.

VMware® GSX Server™ is enterprise-class virtual infrastructure software for x86-based servers. It is ideal for server consolidation, disaster recovery and streamlining software development processes. Support for all x86-based platforms makes VMware GSX Server, the most flexible server virtualization product available, and tight integration with VMware VirtualCenter, delivers unrivalled manageability and scalability. In contrast to ESX Server, GSX Server runs as an application within an operating system installed on the x86 system.

A Primer on Server Virtualization Technology

Server virtualization technology, as pioneered by VMware, allows one physical platform to run multiple virtual machines simultaneously. Each virtual machine has its own processor(s), memory, disks and network interfaces.

VMware GSX Server runs as an application within an existing host OS as shown in Figure 1. The operating system running in each virtual machine is referred to as a “Guest”.

Functionally, each virtual machine is autonomous and, in fact, unaware that the hardware is being shared. This allows multiple servers (even of different operating systems or versions) to run on one hardware platform.

One solution that this enables is for a single physical machine to support three different virtual machines:

- Windows NT 4 and Exchange 5.5
- Windows Server™2003 and Exchange Server 2003
- A Domain Controller

The third virtual machine in the example above, a virtualized domain controller (DC), is particularly popular with largely distributed branch offices that require a local DC but do not wish to pay for the physical asset. It is also useful for disaster recovery sites for the same reason.

One might also run one virtual machine with Microsoft SQL Server™ and other virtual machines with Oracle® and/or Lotus® Notes. Normally, these applications mandate separate hardware to avoid incompatibility issues and to maximize performance.

The key to these solutions is in the complete autonomy between virtual machines and their respective operating systems and applications.

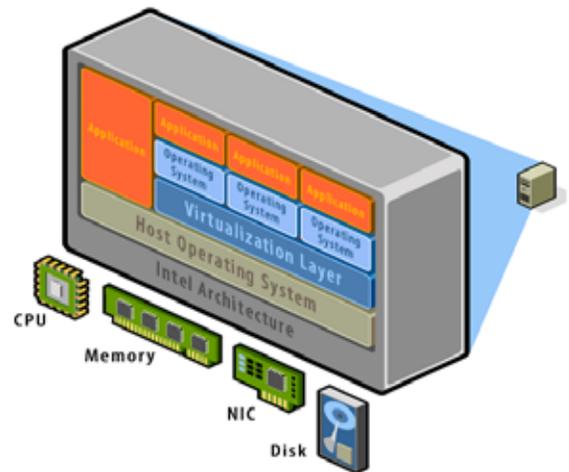


Figure 1 – VMware GSX Architecture

Using Double-Take with VMware Server Virtualization

One of the unique challenges with protecting virtual machines, versus physical servers, is in the storage methods used within virtual machines – namely virtual disks and raw disks. With virtual disks, a group of related virtual disk files exists on the host server and presents itself as storage devices to the virtual machine OS. This causes encapsulation of the entire file set, which provides benefits in its autonomy, but also complexity in its protection. Alternatively, the raw disk method allows for virtual machines to access a physical partition on the host server directly.

Protecting virtual machines and their associated disk files created with ESX Server or GSX Server requires the specific capabilities and data protection innovation found in Double-Take from NSI Software. As a result, some customers have realized the value of using Double-Take with VMware GSX Server and ESX Server for high availability and disaster recovery in virtualized environments.

Double-Take is uniquely able to address these challenges due to its patented architecture and feature-set. Most notably, Double-Take is able to protect the virtual disks, regardless of whether they are configured as virtual disk images or “raw disk” partitions. Because the virtual machine data is encapsulated into “.dsk” files, the queuing model and options within Double-Take allow for flexible configurations that enable the protection of disk I/O created by virtual machines.

By combining Double-Take and VMware virtual machine solutions, some exciting solutions are possible:

- Isolating customers’ data into secure locations and restricting unauthorized access is a priority for outsourcing providers and their customers that are looking for outsourced disaster recovery hot-site services or other off-site vaulting of data. This can be a significant challenge without purchasing separate physical machines for each client. By using designated virtual machines for each customer, data can be isolated from other customers while still allowing the hot-site provider to use their physical servers and floor space in the most efficient way possible.
- Similarly, some enterprise customers also have a need to segment servers, perhaps for security reasons, by business unit. This can be accomplished by designating separate virtual machines as independent Double-Take targets. In both of these cases, the server virtualization software from VMware ensures autonomy, while Double-Take provides the most efficient data replication to the alternate data sites.
- The most common customer need is to protect unique and sometimes conflicting applications on multiple servers to a single recovery server. While Double-Take inherently supports this “many to one” model for data replication, certain applications cannot co-exist on the same server due to conflicts or operational requirements, thus limiting the High Availability options. By leveraging virtual machines on the target platform, each failed source can be protected and made available by an independent virtual machine target.

How does Double-Take protect a Virtual Machine?

One can enable Double-Take replication within a guest OS or on the host OS, as long as either is running a Windows Server OS.

If replicating from a guest OS (Windows NT4, 2000 or 2003), the process is just like replicating from a traditional physical server so no special considerations are necessary. In this configuration, Double-Take, will replicate just as efficiently as it does in NSI's 55,000 other implementations (as of June 2005). *This approach offers the flexibility of providing file-level selection for replication of individual files within the virtual disks belonging to a virtual machine.* Replicating from the Guest can be used anytime the guest is a Windows Server and is the only option when there is not a Windows Host OS.

If the Host OS is Windows Server, Double-Take can be run directly on the host server. From a Double-Take perspective, GSX Server and virtual machines running on it are like any other application which resides on top of the operating system, file system and hardware components of the server.

Double-Take captures disk-writes at the host's file system layer while all applications (including virtual machines writing to virtual disks) operate above the actual file system layer. This allows Double-Take to transparently and reliably protect that data, by replicating the data via its normal mechanisms to a target server running another copy of Double-Take.

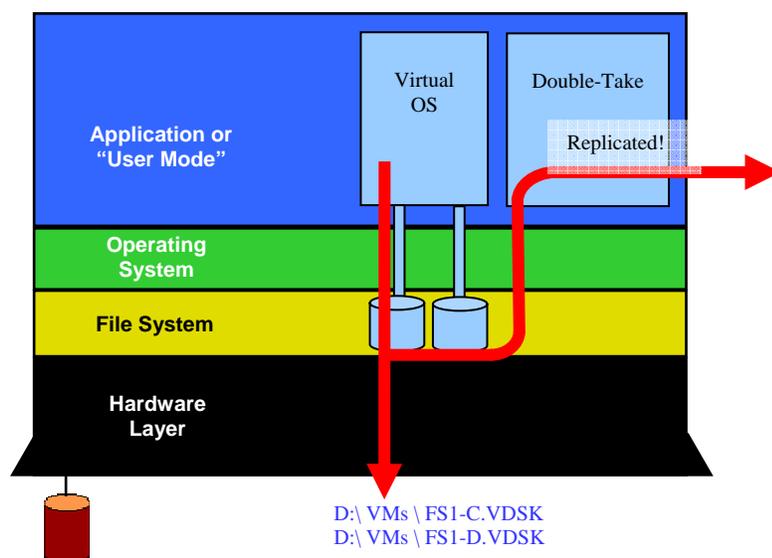


Figure 2 – How Double-Take replicates virtual disks

In addition, replicating from the host OS (running VMware GSX for Windows) offers the benefit of replicating non-Windows guest operating systems (e.g. Linux, Solaris x86, or NetWare). This allows customers to extend the protection of Double-Take to operating systems that do not have a reliable replication technology available to them.

On the target side, Double-Take simply applies the same file update commands to the duplicate files that reside on the target server – sending only real-time byte-level changes across any IP connection.

How can System State and other registry information be protected?

By design, Double-Take does not normally attempt to replicate the Source server's registry or system state information. This is due to the "Many to One" design of Double-Take that allows customers to gain cost-effective economies of scale – protecting multiple heterogeneous servers to a single target.

To maintain server integrity, Double-Take does not replicate hardware-specific and OS-specific information. Consider, for example, three Double-Take Source servers replicating to one Double-Take Target server:

- HP® ProLiant running Windows 2003 and Exchange 2003
- Dell® PowerEdge running Windows 2000 for SQL 2000
- IBM® xSeries running Windows NT4 and Exchange 5.5

Which registry areas should Double-Take replicate to the target? Which drivers? Which OS files and hives?

Even without replicating the potentially dangerous or at least conflicting system-specific information, Double-Take *does* work in these environments and is still able to protect the applications and data on these systems . By running a separate and fresh OS on the target and assuming the names, IP addresses, file shares and services of each and every source server should a failover situation occur.

For most current "BackOffice"-type applications, the registry simply points to applications' data areas and maintains their configurations. This type of information stays relatively static and would not benefit from real-time replication. This model is warranted because it makes the application "portable" for clustering and other fault-tolerant approaches.

However, for application servers where the registry or OS binaries are not static, encapsulating the OS within a VMware virtual machine enables Double-Take to replicate the actual and entire OS to the target as part of the virtual machines disk file(s). Then, the target server simply needs to mount that virtual disk in a new virtual machine to recover the server.

Which Virtual Infrastructure implementation should be used?

VMware GSX Server runs as an application on a Windows or Linux host OS. By using the Windows-server based solution, users have the choice of replicating data from within the guest operating systems or from the host operating system's perspective.

Replicating from a Windows host OS using Double-Take and VMware GSX Server provides the following capabilities:

- The ability to replicate non-Windows OS virtual machines because the replication software on the host OS sees only the virtual disk files or has access to the actual Windows partition(s) that may be mounted by guest operating systems.
- Allows multiple guest operating systems to be protected with a single license of NSI Double-Take because the replication license is based on the host OS instead of requiring an additional license for each guest OS.
- Complete failover capability of the guest OS because everything in the virtual machine's system volume (including the registry, INIs, DLLs, etc.) is encapsulated within virtual machine mounted disks or virtual disks that can be replicated. Failover of the virtual machine to an alternate machine running VMware GSX Server is simply a matter of recovering the virtual machine's configuration files.

VMware ESX Server runs directly on x86 systems without using a host OS. ESX Server uses a proprietary kernel written by VMware to maximize virtual machine capabilities and performance. However, because the ESX Server kernel is not Windows or a commercial version of Linux, Double-Take cannot be installed in the ESX Server kernel. However, Double-Take can still be installed within any Windows-based guest operating systems.

Replicating from the Windows guest operating system(s) by running Double-Take provides the following capabilities:

- Selection of individual files/directories for replication because the guest OS sees the actual files instead of the the host's encapsulated virtual disk image files.
- The ability to replicate Windows servers that are now virtualized onto other ESX Server (or GSX Server on Linux) platforms.

SCENARIO 1 – Fully-Integrated VMware/Double-Take Solution (Virtual to Virtual)

VMware customers are deploying virtual machines on standard x86-based hardware to provide standardization of software and support tools, and ease deployment of new platforms.

In this case, the production server platform might run Windows 2003 Server as the host OS and VMware GSX Server. The guest OS (running in a virtual session) might be Windows NT4 with Microsoft SQL 7. The guest OS “hard drive” is actually a file on the host OS drive (e.g. c:\VMs\svr\C-DRIVE.VMDK), while the host’s other data drive(s) might contain other virtual disk files or be used to store other types of data on the host OS.

In order to provide fault tolerance across any IP network (LAN or WAN), Double-Take can be installed to replicate the bytes of data that change to another Windows server somewhere in the enterprise.

- Solution 1A – Double-Take can be installed within the guest OS. This allows Double-Take to replicate any part of the logical files or directories within the virtual machine disks. The target server has no recognition that the source server is a virtual machine and not “real hardware”. Upon failover, the Double-Take target server would assume the name, IP, shares and services of the failed guest OS.
- Solution 1B – Double-Take can be installed on the host OS and maintain replicas of all of the VMware virtual disk files on the target server. The target server would “monitor” the guest OS for failure but instead of actually assuming the name, IP, file shares and services, it would simply invoke a script that would initialize GSX Server on the target server. The GSX Server instance would utilize the replicated virtual disk files which hold the actual configuration and data from the guest OS. This is the most common solution. *See Figure 2.*
- Solution 1C – While the guest OS system partition is a virtual disk, the actual data drives may be allocated partitions of the host OS. In this case, Double-Take would be installed on the host OS of the source platform and replicate both data from the allocated partitions as well as any virtual disk files being used by the guest OS(s). Similar to Solution 1B, the target server, in the event of a failure on the source machine, would invoke GSX Server on the target. After GSX Server starts, the virtual machine could be started using the replicated virtual disk file(s) and data replicated from the allocated partitions on the Source server.

Solutions 1B and 1C also illustrate how the entire guest OS, including its system state and other key settings, can be captured to the target server. *See earlier section on protecting system state.*

SCENARIO 2 – Enhanced “Many to One” Failover (Physical to Virtual)

Because the target server might be used for the failover of multiple source servers, some care should be taken to prevent compatibility issues. An example of this scenario (outlined below) illustrates four Double-Take Source servers replicating and failing over to one target:

- Database server SQL1 running NT4 and SQL 7 for Sales department
- Database server SQL2 running NT4 and SQL 7 for Marketing department
- Database server ORCL2 running Windows 2000 and Oracle 9i
- Database server NOTES01 running Windows 2003 and Lotus Domino Server

One potential problem would be if SQL1 and SQL2 both experienced an outage simultaneously. Microsoft SQL 7 was not intended to run multiple instances on one machine. While there might be a way to mount both datasets, this would complicate the high availability solution.

Also, while each of these applications may run fine as the only application on each server, compatibility issues may arise by having three database applications (SQL, Notes and Oracle) installed and running on the same target server.

Using VMware virtualization, Double-Take can provide for failover for all of these servers to one physical machine. During failover, the target server would be configured to start a virtual machines corresponding to each source server. This would allow the target to provide high-availability for each of the protected servers without running the workloads on the same instance of Windows on the host.

“We have 25 Windows servers including 5 SQL servers in production in San Francisco, replicating with Double-Take to a VMware server in New York.

I can’t imagine how we could have implemented anything else as effective for disaster recovery.

NSI and VMware are true solution providers, not just software companies. Our executives demanded the best in disaster protection for our organization. This combination was it.”

Kenny Tam
Network Manager, Shorestein Realty Services, LP

A Virtual Machine Customer Example

One NSI customer had seven production servers with a variety of hardware manufacturers, operating systems and applications. Despite these differences, they still needed to provide the same level of recovery across all Windows platforms while utilizing only one physical target server:

- Windows NT4 and SQL 7
- Windows NT4 and Exchange 5.5
- Windows 2000 Domain Controller
- Windows 2000 and Custom Application
- Windows-Powered NAS File Server
- Windows 2003 and IIS Web Server
- Windows 2003 File Server

This is a common request from customers and highlights why byte-level file replication technology like Double-Take is an ideal, cost-effective solution. While Double-Take does support “Many to One” solutions, the variety of applications in some customer situations warrants keeping each application separate during failover.

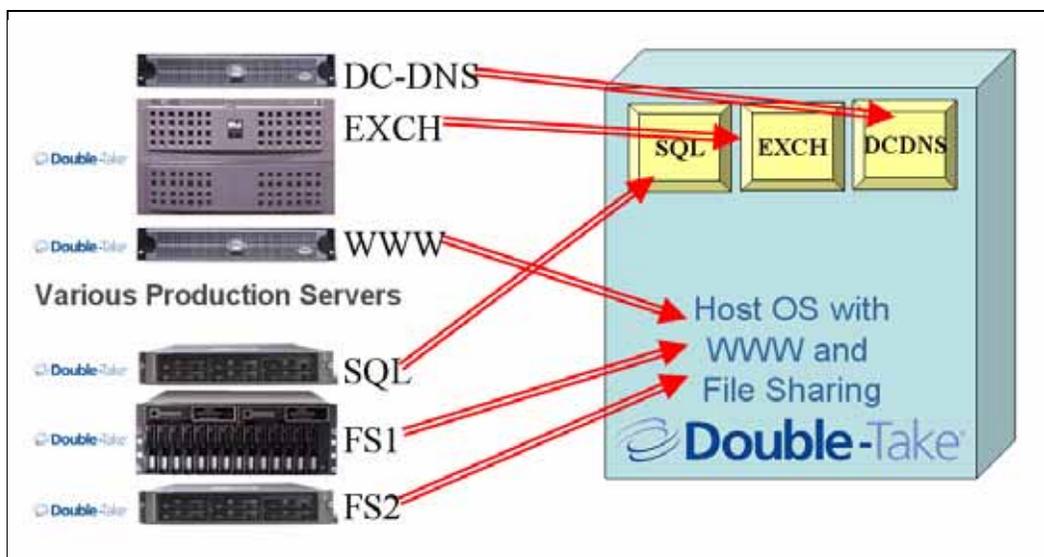


Figure 3 – “Many to One” with virtual machines on the Target

To accomplish this, the Windows 2003 target server was configured with Double-Take and VMware GSX Server. A copy of Double-Take was also installed on each of the production servers. Then, seven VMware virtual machines and their respective guest operating systems were configured - with the guest OS data drives being mounted on the host OS.

Failover of any one or more failed servers is accomplished by simply starting the appropriate virtual machine running a similarly configured OS, mounting the appropriate data sets and starting the appropriate services. This failover process is achieved quickly and allows the application to continue to serve the user community.

A Virtual Machine Hot-Site / SSP Example

A Disaster Recovery company wished to maximize the use of its hardware assets across multiple client companies while still insuring that each customer's data was isolated for security purposes. Below are the three customers' lists of protected applications.

Acme, Inc.

2000 DC
2000 IIS Web *
2000 Exchange 2000 *
2000 File Server *

Spacely Sprockets

2003 DC
2003 Exchange 2003 *
2003 SQL 2000 *

XYZ Widgets

NT4 PDC
NT4 SQL7 *
NT4 File *

* - All non-Domain Controllers run a copy of Double-Take

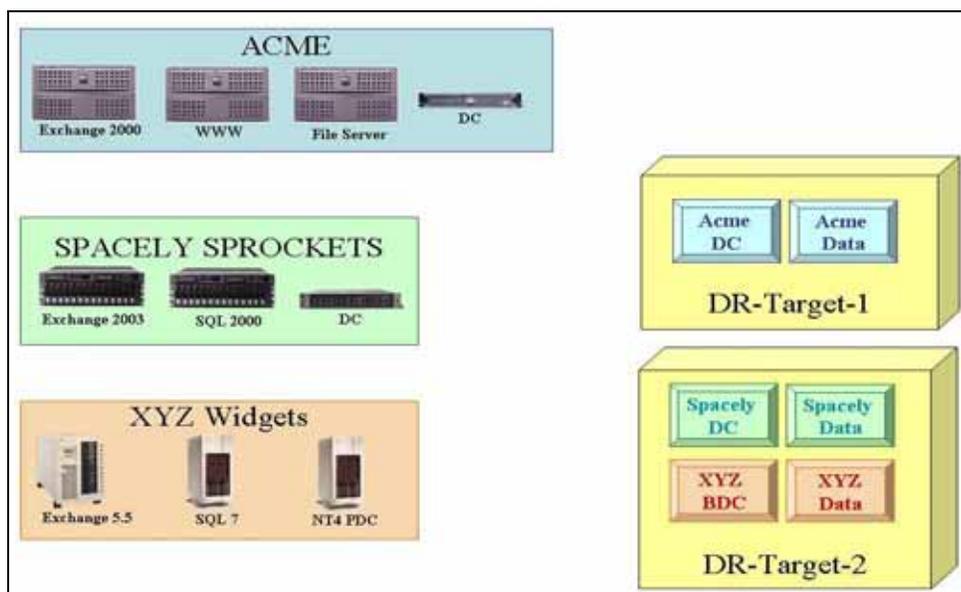


Figure 4 – Hot-Site server, supporting multiple clients

At the hot-site, two physical platforms were configured with a base-OS and a copy of VMware GSX Server.

- A virtual machine was built for each client's domain controller (DC), and the native Domain and/or Active Directory process populated and maintained the DC's.
- A virtual machine, running a license of Double-Take, was built as the "data target" for each client. This allows each client to manage their own replication solution and maintains security.

To maximize hardware resources, Spacely's and XYZ's virtual machines and data sets are actually maintained on one physical server. If any client's data becomes too large, their virtual machines can be moved to larger or faster equipment without significant effort or end-user impact.

Additional Double-Take Solution Examples

In addition to the solutions described earlier, Double-Take replication empowers other possibilities – some of which can be enhanced even further by virtual machine technology.

1. NAS to SAN storage migration
2. Branch office server backup to centralized data center
3. Small office Server to Server protection
4. Consolidated Backup Operations
5. Multiple site replication – Fan-Out or Fan-In

Example 1 – NAS or SAN storage migration. As more environments move from local storage-based servers to NAS/SAN, the question of how the actual migration will occur becomes more frequent. Using the same techniques outlined above, one can migrate from local storage to a NAS, a server utilizing a SAN, or even a NAS-gateway to a SAN. In all cases, the fundamental requirement is that the data is moving from one Windows platform (with local storage) to another Windows platform with more manageable storage such as a Windows Storage Server (or Windows-Powered NAS).

Example 2 – Branch office server backup to centralized data center. Even in enterprises where protecting the corporate data has become a standard, branch offices tend to still be isolated to tape solutions. This forces non-IT personnel to be responsible for tape rotations and cleanings; and the result is higher manpower costs and less reliable restores. By efficiently replicating the byte-level changes within the data using Double-Take, one can bring the branches' data back to a centralized data center. This provides disaster recovery for the branches and allows backups to be done at the centralized facility by IT personnel using more advanced tape technologies.

Example 3 – Small office Server-to-Server protection. Whereas large enterprises may have multiple data centers and a myriad of server technologies, the small office relies heavily on perhaps one or a few server resources with limited IT resources and personnel. When the primary server fails, the office productivity can grind to a halt. Double-Take provides a simple and cost-effective way to fail over to a second machine in the same office or perhaps at an employee's home. The result is rapid recovery of the server and expedited return to "business as usual" for the small office.

Example 4 – Consolidated Backup Operations. As geographic and national boundaries have less impact on effective commerce, today's corporations are lengthening their business day,. Unfortunately, this results in an ever-shrinking backup window. However, the redundant copies of the files on Double-Take target servers can be backed up even when the original copy of the data is in use. Without expensive and application-specific backup agents, the second copy of the data can be protected using existing tape technology attached to the target server. And even more beneficial for companies is the fact that the backup can be done at local disk/tape speeds instead of a media server backing up multiple application servers.

Example 5 – Multiple site replication. Many replication needs are not based around data protection or availability. In the case migration solutions, for example, the business need is simply to get the data to an alternate location. Double-Take can provide a corporation with a master-content server and ensure that all regional locations and branch offices receive the replicated files – regardless of whether it is a custom application or simply a Human Resources directory for vacation forms and business card requests.

NSI Software, Double-Take Products and Services

NSI knows how to protect applications running on Windows file systems. "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®, Microsoft® and probably your preferred reseller-integrator.

When considering the solutions described above, the key to remember is that Double-Take provides the most efficient, byte-level replication of files within a Microsoft Windows server environment. Whatever the business goal (migration, protection, availability or distribution), it starts with having multiple copies of your files. So it starts with Double-Take by NSI Software.

For information on how to migrate your existing servers, how to replicate data for business continuity and how to improve and centralize backup operations, please refer to the NSI contact information on the back of this document.

All of these solutions are based around NSI Software's fundamental philosophy that all business continuity efforts start with protecting the data. From there, it is simply a matter of what you want to do with it.

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

VMware Technologies and Consulting Services

VMware Technologies virtual infrastructure products provide innovative solutions to address your IT requirements. VMware Consulting delivers these solutions while minimizing risk and accelerating deployment to achieve a faster return on investment.

VMware and VMware Authorized Consulting (VAC) partners, have the technical expertise on virtual infrastructure products and the extensive experience needed to apply these technologies into practical business solutions.

VMware Authorized Consulting services and capabilities help ensure the successful implementation of VMware solutions. Utilizing proven VMware Virtual Infrastructure Methodology (VIM) VMware consistently delivers comprehensive end-to-end solutions to assess, plan, build and manage VMware virtual infrastructure. Using the VIM, business needs are properly assessed, deployment is carefully planned, and a robust roadmap to guide you through the virtual infrastructure adoption lifecycle is provided, from the step-by-step procedures for building systems, to well-defined, repeatable processes for the ongoing management of your virtual infrastructure.

For more information on Double-Take replication products and services,



NSI Software, Inc.
8470 Allison Pointe Blvd. Suite 300
Indianapolis, IN 46250
800-674-9495 (toll-free)
317-598-0185 (outside US)

Or visit us on the web at www.NSISOFTWARE.com

For more information on Virtual Machine technology products and services,



VMware, Inc.
3145 Porter Drive
Palo Alto, CA 94304
Tel: 1-877-486-9273 (toll-free) or 650-475-5000
Fax: 650-475-5005
Email: sales@vmware.com

Or visit us on the web at www.VMWARE.com

© 2005 NSI Software, Inc. and VMware, Inc. All rights reserved.

Double-Take, NSI and GeoCluster are registered trademarks of NSI Software, Inc., Balance is a trademark of NSI Software, Inc. and all are used with permission of the trademark owner. All other trademarks are properties of their respective companies.

VMware is a registered trademark and the VMware boxes logo, GSX Server, ESX Server, Virtual SMP, VMotion and VMware ACE are trademarks of VMware, Inc. Protected by one or more of U.S. Patent Nos. 6,397,242, 6,496,847, 6,704,925, 6,711,672, 6,725,289, 6,735,601, 6,785,886, 6,789,156 and 6,795,966; patents pending.

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.

Linux is a registered trademark of Linus Torvalds.

Although we try to provide quality information, NSI makes no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained in this document. Companies, names and data used in examples herein are hypothetical and/or fictitious unless otherwise stated.

All other marks and names mentioned herein may be trademarks of their respective companies.