

DOUBLE-TAKE SERVER RECOVERY OPTION: FULL-SERVER PROTECTION AND RECOVERY IN REAL-TIME

BUSINESS VALUE WHITEPAPER

Double-Take Software, Inc.

Published: July 2007

Abstract

The complexity of traditional recovery solutions compounds an already difficult situation and heightens the opportunity for human error. Speed and quality of recovery are extremely important when customers and employees are relying on access to critical data, but the average restoration takes hours at best. With solutions like tape backup, even a successful recovery results in the loss of any data that has changed since the backup was made. The Double-Take® Server Recovery Option is a whole-server data protection product that, when combined with the real-time data replication capabilities of Double-Take® for Windows, simplifies the restoration process and reduces the time and effort involved with server recovery. .

The Trouble with Tape

Have you ever recovered a production server using traditional backup solutions such as tape? The complexity of traditional recovery solutions compounds an already difficult situation and heightens the opportunity for human error. Speed and quality of recovery are extremely important when customers and employees are relying on access to critical data, but the average restoration takes hours at best. And, with solutions like tape backup, even a successful recovery results in the loss of any data that is new or has changed since the backup was made.

The problems with tape backup are well known; companies have been dealing with them for decades. For starters, tape backup requires a significant investment. Tape hardware and backup software are expensive, as is the labor required to set up and maintain them. Tape cartridges are a continuing cost and completing daily tape backups requires heavy administrative intervention.¹ If you have multiple branch or remote offices (a recent census bureau survey indicates the average company has 50 locations) you have to set up tape equipment and allocate administrative supervision for each. The only other option in these situations is to forego protecting data in branch office locations which becomes a problem all of its own.

Even once the equipment in place, making backups is inconvenient — bordering on impractical. Tape backup can involve downtime, known as backup windows, since the system being backed up cannot be used during the process. Given the ever-increasing demand for around the clock data access, it gets harder and harder for companies to complete nightly backups within the time window provided. In many cases, it is so hard that the once-nightly backup goal often slips to every other night for many machines. Foregone backups are even a common problem in remote branch offices where backing up is left to non-IT staff.

The Cost of Lost Data

Most companies don't understand how vulnerable their data and business remain to disaster — even after they've made a huge up-front and ongoing investment in tape-based disaster recovery. An article in SearchSecurity reports that in a survey of 500 IT departments, as many as 20% of routine nightly backups fail to capture all data. Among participants of another survey cited in this article, 40% of IT managers were unable to recover data from a tape when they needed it.² This is a significant concern for corporations that are regulated by industry or government requirements as they can face the risk of being out of compliance if they cannot produce required data when they need it.

Tape backup also places limits on your recovery point objective (RPO), the point in time to which you can recover your systems should disaster strike. Periodic tape backup guarantees hours of lost data in the event of a disaster. Suppose, for example, that a critical system fails anytime today; the best you can do is recover to yesterday's data, which will be at least twelve hours old. The later in the day disaster strikes, the older the data from which you'll recover. In addition, recovering from a disaster, any data not backed up is lost for good — unless you recreate it.

The cost of permanently lost data is high and includes the cost of the revenue that the data represents, the business value you can extract from it, and the cost to recreate it. Consider:

- *How much money would your company lose if you lost all your transaction data for the last twelve hours, or even the last ten minutes?*
- *What is the value of the knowledge contained in your company's last twelve hours worth of e-mails and e-mail attachments? What would it cost to have your engineers recreate the last twelve hours worth of original or edited CAD/CAM drawings?*
- *What's your exposure if you can't produce this data in compliance with Sarbanes-Oxley, HIPPA, SEC and other regulations?*

In *The Cost of Lost Data*, a Pepperdine University report updated in 2003 - before the advent of Sarbanes-Oxley - Dr. David Smith estimates the average cost of irrecoverably lost data at more than \$10,000 per megabyte lost.³ But if the data lost is business transaction data or data that's especially expensive to reproduce and key to your company's regulatory compliance, your costs could be much, much higher.

¹ See Double-Take whitepaper "Reducing Costs and Risks of Branch Office Data Protection"

² Regan, Keith. "Concerns Raised on Tape Backup Methods." SearchSecurity.com 15 April 2004

³ Smith, David M. "The Cost of Lost Data." Graziadio Business Report Vol. 6 No. 3

The Cost of Downtime

When a large-scale disaster strikes, with tape backup you're out of business until you can restore your systems and your data from your tapes. This kind of restoration takes a minimum of several hours, and can easily take days or even weeks.

Gartner Group estimates that the average cost of network downtime for larger corporations is \$42,000 per hour; Contingency Planning Research pegs the average hourly downtime costs for small businesses at roughly \$18,000. But the cost of downtime can be significantly higher depending on the business. In fact, it can be in the hundreds of thousands per hour for health care, consumer products and banking businesses, and in the millions per hour for brokerage, energy, manufacturing and telecommunications companies.⁴

The key to a successful disaster recovery plan is to focus not just on the data (RPO) but also on the applications that end users run to gain access to that data. Recovery Time Objective (RTO) is generally defined as the amount of time it takes to regain access to business-critical data. Solutions like tape backup, which have an RTO of hours or days, don't provide the level of recoverability that most companies require.

A Better Solution: Data Replication with System State Protection

"Half of the Protection Battle: RPO"

Data replication has long been considered an impractical solution to the data protection problem. Historically, it required expensive hardware and large investments in bandwidth to protect data in real-time. The evolution of software-based, asynchronous replication has dispelled this long-held belief that continuous data replication isn't feasible – especially for small or medium-sized business with limited resources.

And this new breed of data replication offers benefits that more traditional solutions such as tape-based periodic backup cannot:

- Data replication provides a continuously updated copy of critical data at a remote site which minimizes data loss should a recovery be necessary.
- Disk-based recovery is more reliable, less complex and takes less time, improving the RTO of the disaster recovery solution.

Even within the realm of software-based data replication, there are opposing approaches: synchronous and asynchronous replication. It's important to understand the benefits and drawbacks of each.

In synchronous replication, the replication software intercepts data being written to disk and sends it to both the primary and secondary disk arrays at the same time. Only when both arrays confirm receipt of the data does the software accept another write. Asynchronous replication can deliver recovery point objectives (RPOs) measured in minutes, and recovery times measured in seconds.

With synchronous replication, data loss approaches zero because both the primary and secondary disk arrays must contain the same data. But the confirmations required for each data write can cause performance problems, especially in applications that process lots of transactions. Acceptable performance often requires connecting the arrays with high-bandwidth fibre channel, which is very expensive and which has an effective range of about ten miles. As a result, synchronous replication is not ideal for remote disaster recovery, and is most often used to create a local backup of data in situations where having an exact copy of the data is essential.

In asynchronous replication, the replication software grabs data once it is written to disk, and rewrites it to a second array. In asynchronous replication, the application doesn't have to wait for any confirmations and can continue to operate. As a result, it has little or no impact on application performance, and can work effectively and economically over low bandwidth connections and long distances.

While it can't deliver the zero data loss available through synchronous replication, it can be configured to deliver RPOs measured in minutes, and recovery times measured in seconds, both of which are more than acceptable for most businesses. This combination of excellent data protection, minimal performance impact, long-distance effectiveness and low-cost deployment makes asynchronous replication an ideal solution for backing up data to a remote recovery site.

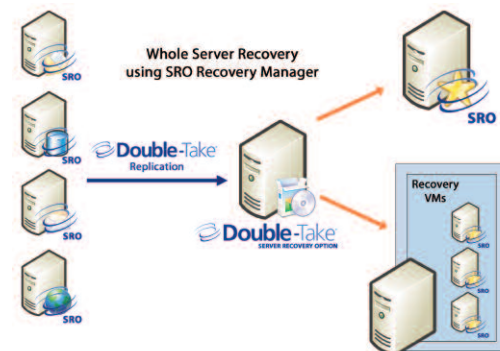
⁴ Meta Group 2000 data

“The Other Half of the Protection Battle: RTO”

Data replication solutions have traditionally been limited to protecting critical data and not the applications associated with that data or the systems on which it resides. When a Windows server fails, however, simply having access to a copy of the data is not enough. It’s the application and the underlying operating system it runs on that provide customers and end users access to the data. This information – the operating system files, registry information, application binaries, settings and other system-related information -- is collectively referred to a server’s “system state”. Left unprotected, recovery of these components can take hours or days to accomplish. In fact, in many cases, the recovery point of the system may not match the system state prior to the failure, requiring system, applications, service packs, settings, drivers, hot fixes, etc., to be re-installed or recovered. Without a way to easily recover the data and system state information, companies risk not being able to meet their Recovery Time Objectives (RTOs).

While Microsoft Windows and leading backup applications provide a degree of protection against failures by allowing users to back up critical system state information to tape media, it is on a scheduled, versus real-time, basis. This means there is good likelihood of system state information loss since system changes are likely to occur between tape backups. Also, this type of approach often requires recovery to similar server hardware — something many organizations may not have on-hand in the event of a major disaster.

The Double-Take Server Recovery Option (SRO) addresses this “recovery gap,” providing real-time replication and hardware-independent recovery of system state information. Real-time head-to-toe protection of system, application and data are delivered when SRO is combined with Double-Take Software’s core replication solution: Double-Take. Recovery can be done to a physical server or, more importantly, virtual environments like VMware ESX Server or Microsoft Virtual Server 2005.



Double-Take Server Recovery Option

The Double-Take Server Recovery Option is a whole-server data protection solution that, when combined with Double-Take real-time replication simplifies the restoration process and reduces the time and effort involved with server recovery. Using Double-Take with the Server Recovery Option, the entire production server – its operating system, applications and data – can be protected and easily recovered to a new system quickly.

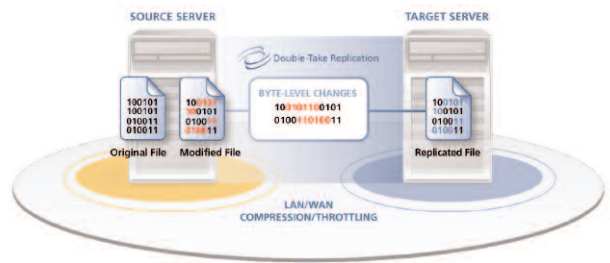
Double-Take, when combined with the Double-Take Server Recovery Option (SRO), provides a single solution to continuously protect and recover an entire server. Protection is provided by the industry-proven real-time replication of Double-Take while recovery is performed by the Server Recovery Option. The Recovery Manager, provided as part of the Double-Take Server Recovery Option, presents the task of server recovery as a series of easy-to-understand steps. Because Double-Take replication protects the entire production server – its operating system, applications and data, restoring the server encompasses as few steps as possible and provides a significantly better recovery time than existing solutions such as tape backup.

Built on Proven Double-Take Technology

The Double-Take Server Recovery Option is used in conjunction with Double-Take and its replication technology, the world’s most relied-upon solution for accessible and affordable data protection solutions for disaster recovery and centralized backup. Double-Take utilizes patented replication and failover technology that continuously captures byte-level changes as they happen and replicates those changes to one or more secondary servers at any location - locally or at a recovery site miles away.

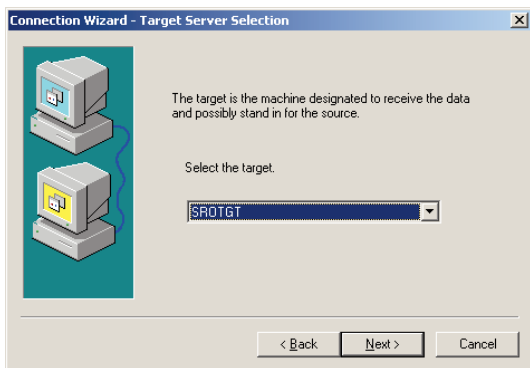
Double-Take from Double-Take Software integrates with the Windows kernel I/O sub-system which provides a serialized view of all I/O operations before they are passed to the file system layer. This is a standard integration point where applications such as anti-virus and open file agents integrate and provides a fully consistent transactional view of all system writes. It monitors the system I/O and replicates the write activity for user-defined volumes, directories or files. I/O operations that are exposed at this layer reflect the actual byte-level changes by the applications while they are writing to the files, so Double-Take replication does not require the database to be taken off-line or placed in a quiescent state before determining which changes have taken place.

Double-Take replication technology reduces the window for data loss, is more efficient than tape, and less costly than tape or other replications solutions. Because Double-Take replicates data in near real-time, an up-to-the-second copy of data is always available on the backup server. Double-Take also uses unique compression and bandwidth throttling features that allow an administrator to control the amount and timing of bandwidth used for backup. It can utilize existing infrastructure and is hardware agnostic; there's no large investment or hidden costs standing between you and better backups. Today, Double-Take is the most relied-upon solution for real-time replication of critical data and automated failover for application availability. Double-Take is Microsoft® Windows® 2000 and 2003 certified at all levels, one of the few replication products to have achieved this level of certification. It delivers protection that is better or comparable to many hardware based solutions, but costs tens of thousands less.



- Real-Time Protection - Replicates continuously at the byte level over any shared or private IP network, ensuring that changed data is protected and can be quickly restored at all times
- Application Agnostic - Works with existing hardware to protect applications such as Microsoft Exchange, Microsoft SQL Server, and SharePoint® – any application that runs on Windows Server.
- Easily Installed and Maintained - Allows companies of any size looking for data protection solutions to install and maintain Double-Take.
- Cost Effective - Provides strong data protection at low cost with an accelerated return on investment - paying for itself usually within months.

Easy Implementation and Management



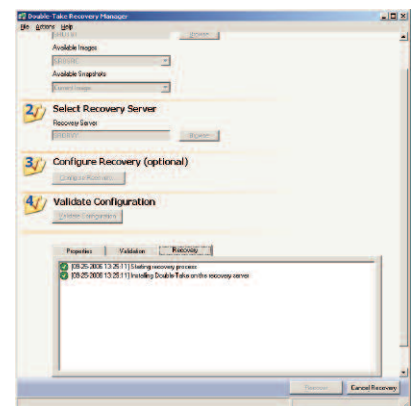
The Double-Take SRO features additions to the Double-Take Management Console that provide an easy-to-follow wizard for creating a connection that protects the entire server. Once installed, Double-Take performs an initial mirror of the server, including data, applications and operating system. When the mirror is complete, Double-Take begins replicating changes made, at the byte level, to the operating system, data and applications. This replication of system state ensures that the entire server can be recovered in the event of a disaster or data loss.

In some cases, not every volume on a server needs protected. The Double-Take Server Recovery Option provides the option to exclude one or more data volumes at either protection or recovery time based on an organization's specific requirements.

Single-Step Recovery with the SRO Recovery Manager

The Recovery Manager console, included with the Double-Take Server Recovery Option, allows you to quickly and easily configure and perform recovery, including validation steps that ensure recovery goes as planned. When a system volume or entire server fails recovery of both system state and data can be performed from the Recovery Manager, reducing the number of steps needed to recover a server to its original state. The Recovery Manager also eliminates many of the steps required by traditional backup and restore solutions by requiring only a standard Windows OS on the new system.

The Double-Take Server Recovery Option provides an easy method for restoring an entire server, including the system state (the server's configured operating system and applications). The process requires you to select the system state image for the failed source from the target image server and identify the replacement server, called the recovery server, where you want to recover the data to. There is no need to select files or remember when data is stored. Double-Take does not even need to be installed on the recovery server. Recovery can be used if the entire source server is lost and you must replace it with a new one. The recovery process will install Double-Take, if necessary, and copy all of the data, including the system state to the recovery server. After the recovery process is complete and the recovery server is restarted, it will have the identity and data of the original failed source.



Snapshot Support

Double-Take and the Double-Take Server Recovery Option integrate with Microsoft Volume Shadow Copy Service to allow you to schedule and recover from up to 512 point-in-time copies of data on your Double-Take target. This allows administrators to easily recover an entire server from problems caused by viruses, corruption or human error. When recovering from a snapshot, the entire server (including the OS, Applications and data) is recovered to a consistent point based on which snapshot is selected.

Broad Application Support

The Double-Take Server Recovery Option protects the entire server so there is no need for specialized application support as is the case with tape backup solutions. The Double-Take Server Recovery Option supports most business-critical applications and replicates between any configuration of physical and virtual systems. The Double-Take SRO also integrates with Microsoft® Volume Shadow Copy Service to allow you to schedule and recover from up to 512 point-in-time copies of protected data. And, with the exception of a matching operating system, the recovery server does not have to be an exact match for the server you are recovering.

Protection Scenarios Using the Server Recovery Option

SRO in a Branch Office Scenario

Well-prepared businesses know that deploying the right resources, processes and technology to protect key information and minimize downtime at their main headquarters is important. But having adequate resources and technology in place for protecting invaluable data in branch offices is just as important, though often overlooked.

In a survey conducted in 2005 by the Ad Council, most businesses agreed that emergency preparedness is important, yet only 39% said their company had a plan in place. In companies with distributed branch offices, data protection strategies may not have kept up with the reality that branch or remote offices now contain customer databases, e-mail servers and financial information that are critical to the company's day-to-day operation. The traditional approach – relying on tape backup for branch-office data protection – is costly and risky. For example, in addition to the initial tape backup hardware, software, and installation costs for each branch, add the continual costs of tape media, maintenance, and off-site transport and storage. Many companies also can't afford to have IT staff in branch offices, so they incur additional IT support costs for the regular technical maintenance and verification of the branch backups.

For untrained non-technical staff in branch offices, being responsible for consistent, reliable backup can be tough. Backups may fail without the branch staff even noticing. Improperly labeling, shortcuts, and rotating and removing tapes can result in lost data and slow recovery. Also, if the branch employees have never tested the recovery process, they won't be familiar with how to execute the recovery when a disruption occurs. As a result, in the event of a disaster the branch could be down for a prolonged period of time and often requires the assistance of the central IT staff.

To begin with, tape hardware and backup software can be a headache even before they fail. Required hardware and software are expensive, as is the labor required to set up and maintain them. Tape cartridges are a continuing cost and completing daily tape backups requires heavy administrative intervention. If you have multiple branch or remote offices, (a recent census bureau survey indicates the average company has 50 locations) you have to set up tape equipment and allocate administrative supervision for each, or try to manage backups with no local IT support.

A common backup solution in a branch-office scenario is to replicate the branch servers to a central location and perform a nightly tape or disk backup. If the Branch 2 server fails, the administrator would have to provision the new server, install applications, then go through the cumbersome recovery process. On average, this would take more than one

SRO for a More Complete DR Strategy

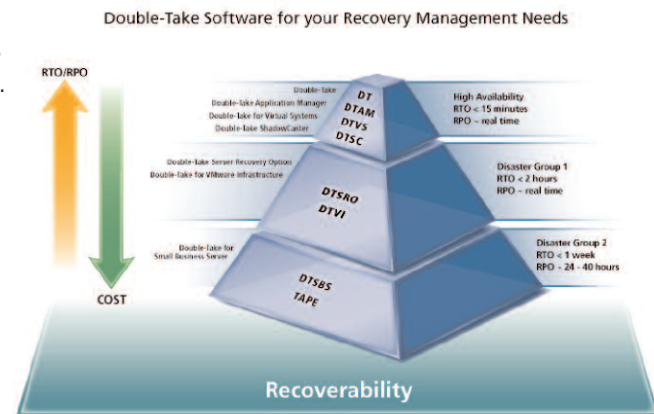
Organizations of all sizes are increasingly dependent on computerized data systems for their operations. Ensuring that these systems keep operating is a critical part of business planning. Business Continuity (BC) is strategy that ensures critical data and systems remain available even if hardware, software or environmental problems interrupt the primary server's normal operation. Gartner research emphasizes that not only do laws and regulations dictate BC planning, but also that organizations are accountable for their systems and processes related to data. "The bottom line is that laws and regulations, as well as shareholders, expect organizations to exercise due care to ensure that necessary data is available."⁶

The simplest approach to business continuance is to treat all data as equal, and equally important to business operations. However, this approach leads to unnecessary cost and complexity; many areas of the Windows infrastructure already have fault resilience. For example, Active Directory's multiple-master replication model means that loss of one or more domain controllers is survivable as long as at least one DC remains. Likewise DNS, WINS, and most other infrastructure servers can handle the loss of one or more participants. Furthermore, the design of these services is such that a failed server can often quickly be replaced or rebuilt, and its data restored via replication from its remaining peers.

In addition, no two workloads within an organization have the same importance to the operation of the business on a day-to-day basis. Line-of-business applications and their associated data, messaging, database, resource planning and other critical systems carry the data that a business cannot operate without, so it's critical to ensure that the data is protected. As part of a Business Impact Analysis (BIA), many companies identify which systems and data are more critical to the organization and apply the appropriate level of protection. But what about workloads which are important enough to be properly protected but don't have an RTO of 15-30 minutes and, therefore, don't really require the real-time replication and failover of Double-Take for Windows and a standby system at a secondary location?

An example a more holistic approach to disaster recovery is Baxter Credit Union, a Double-Take Software customer. Like many organizations prior to working with Double-Take® Software, Baxter Credit Union relied on tape backups for disaster recovery. For decades, tape has reigned supreme as the standard backup medium for many corporations. However, as the company grew over the years, so did the complexity of their systems and the process to protect and recover their data. Though the tape-only approach worked, the entire process was incredibly expensive, time consuming, and challenging for the team.

At the time, the Baxter Credit Union infrastructure consisted of more than 100 physical and virtual machines in production. Their strategy was to place each server into one of four tiers, depending on the importance of the data and application. This approach allowed Baxter Credit Union to determine the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) goals for each application within their infrastructure. Today, Baxter Credit Union is protecting all Tier 1 applications (including file servers, Exchange servers, and SQL servers) with an RTO of 2 hours or less using Double-Take and the Double-Take Application Manager feature for real-time replication and failover to a standby system. Tier 2 and 3 servers (a variety of file servers, IIS Web servers, and other application servers) with an RTO of 24 hours – 3 days, including are protected by Double-Take and SRO. The Double-Take Server Recovery Option allows Baxter Credit Union to quickly configure and perform a full recovery, regardless of whether or not the new server is the same make, model or configuration as the original server. And since the Double-Take and the Server Recovery Option utilize many-to-one replication from multiple source systems to a single target, additional operating system or application licenses are required for every replicated production system.



⁶ Noakes-Fry, Kristen, et. al. "Laws Influence Business Continuity and Disaster Recovery Planning Among Industries." Gartner. 11 July 2005.

Summary

Recovering your production server from backup using traditional recovery solutions can be a cumbersome and stressful process. Complex restoration software and the inability of solutions like tape backup to protect data in real-time don't improve the situation. Double-Take and the Double-Take Server Recovery Option provide a better alternative – real-time data protection with a streamlined recovery process that reduces the time and effort involved with server recovery. Double-Take replication in conjunction with the Double-Take Server Recovery Option protect the entire production server, including system state data, so there's no need to provision a new server or reinstall applications.

About Double-Take® Software

Headquartered in Southborough, Massachusetts, Double-Take® Software (Nasdaq: DBTK) is a leading provider of affordable software for recoverability, including continuous data replication, application availability and system state protection. Double-Take Software products and services enable customers to protect and recover business-critical data and applications such as Microsoft Exchange, SQL, and SharePoint in both physical and virtual environments. With its unparalleled partner programs, technical support, and professional services, Double-Take Software is the solution of choice for more than ten thousand customers worldwide, from SMEs to the Fortune 500. Information about Double-Take Software's products and services can be found at www.doubletake.com.

© Double-Take Software. All rights reserved. Double-Take, GeoCluster, and NSI are registered trademarks of Double-Take Software, Inc. Balance, Double-Take for Virtual Systems, Double-Take for Virtual Servers and Double-Take ShadowCaster are trademarks of Double-Take 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 the property of their respective companies.

Double-Take Software Headquarters

257 Turnpike Road
Southborough, MA 01772
Phone: +1-800-964-0185 or +1-508-229-8483
Fax: +1-508-229-0866

Double-Take Software Sales

8470 Allison Pointe Blvd. Suite 300
Indianapolis, IN 46250
Phone: +1-888-674-9495 or +1-317-598-0185
Fax: +1-317-598-0187

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



Get the standard today: www.doubletake.com or 888-674-9495

