XactCopy™

Immediate Disaster Recovery Software

WHITE PAPER

_____

System Recovery when Minutes Count

DuoCor ® Incorporated

Storage Device Backup and Disaster Recovery Solutions

Summary

The purpose of this white paper is to provide an overview of a new technology approach toward fast system recovery for servers and mission critical workstations running the Windows NT Operating System (OS). The paper illustrates a simple and inexpensive way of recovering from OS and hard disk failures in minutes instead of hours. Implementation requires a second hard disk and DuoCor's *X*actCopy software.

Contents

Overview of Backup Methods

Most full-system backup products take hours to restore a failed system to normal operation. In many environments, downtime is intolerable, yet striking a balance between backup time and restore time is an issue that is unique to each environment. All of the backup and restore options given below are analyzed to indicate how the new DuoCor technology is most suitable where system downtime, due to either backing up data or restoring it, is intolerable.

There are three different types of backups: full backup and two types of partial backup called incremental and differential.

- **Full Backup -** A full backup usually includes all of the system and data files contained on the system drive. The best form of full backup is a sector-by-sector copy to the target storage device because the single copy provides the fastest system recovery. Most disaster recovery plans recommend performing a full backup at least weekly.

- **Incremental Backup -** With incremental backup, the operation includes only those files changed since the last full or incremental backup. Incremental backups take less time to perform because of the reduced amount of data being written to the target storage device. A full system recovery takes longer to accomplish because the process begins with the last (most current) full backup followed by all subsequent incremental backups.

- **Differential Backup -** With differential backup, every file that has changed since the last full backup is backed up each time. Compared to an incremental backup, it is much faster to restore from a differential backup because the last full backup and the last differential backup are the only copies necessary for the task.

With any of these three backup types, either individual file or disk image methods may be used for the backup process:

- **File-by-File Method -** The file-by-file method requests each individual file and writes it to the backup device. For full-system backups, the backup time is much longer using the file-by-file method over a sector-by-sector disk image method.

- **Disk Image Method -** The disk image method is a sector-by-sector identical copy of the entire system disk. The image backup process typically does not care what is on the system disk or even what it is doing at the time of backup. Disk imaging is much faster than the file-by-file method. If an operating system or disk failure occurs, restoring the system from the duplicate image medium (often a tape cartridge) offers the fastest method of recovery.

The primary reason why system administrators perform full-system backups is for their use in recovering a system after operating system failure, hard disk failure, or significant data loss. Full-system backups differ from archive, which is the method of long-term or legally required storage of certain data files from day-to-day.

Tape backup systems are the predominant choice for the various backup methods. Although tape backup offers the best solution for archiving files on a periodic basis, its use for full-system backups is less desirable because the time to recover from a failed system is relatively long.

Overview of DuoCor Technology

XactCopy's primary function addresses full-system backups for the purpose of immediate system recovery. There are two important differences between *X*actCopy and other full-system backup methods:

1. *X*actCopy's routine full-backups are very fast (typically under 3-minutes), which promotes more frequent use.

2. *X*actCopy utilizes a dedicated disk drive as the backup medium, which offers instant recovery from OS or drive failures—the backup drive is bootable directly.

*X*actCopy makes an identical sector-by-sector copy of the system drive to the backup drive. In the *X*actCopy program and in this paper, we refer to the dedicated secondary drive as the Data Protection/System Recovery (DPSR) drive. **The DPSR drive remains invisible to the operating system at all times**, rendering data safe from alteration or corruption

Following a system drive or OS failure, the DPSR drive is booted directly without having to rely upon floppies, partial OS restore, slow full-system restore from tape (after disk drive replacement or repair), or complicated and time consuming incremental tape restores. *X*actCopy places the system back into operation almost immediately, which enhances productivity with system up time.

After the initial sector-by-sector backup, which occurs during program installation, subsequent (routine) full backups are similar to an incremental backup. Only those files changed since the last backup are a part of the periodic update. The ability to use incremental updates, which enhances the speed of the backup, is unique to the choice of backup medium used. Because the backup device is similar to the hard drive that it is protecting, it is possible to compare data between the drives to search for all changes made since the last full backup. This incremental disk backup results in a full backup of the system drive to the DPSR drive.

*X*actCopy DPSR is a fast alternative method to performing full system backups without tape, for immediate system recovery when needed. It is

not a replacement for incremental tape backups, which companies generally use for legal and other reasons.

All backup operations with *X*actCopy occur from within the operating system, which means that the server or workstation remains live. Most all other disk-to-disk-based copying programs require the administrator to shutdown the server or workstation and boot from a DOS prompt to run them.

The steps listed below illustrate a full system recovery following an operating system or drive failure:

1. *Remove the failed or non-bootable System disk, or change the boot sequence as applicable to the installation.*

2. *Reboot the system from the secondary DPSR drive.*

Applications of the Technology

One of the most frequent questions about *X*actCopy is its application with hardware mirroring, NT mirroring, and RAID. An important distinction about mirroring and RAID is that deleted or corrupted files on the system drive concurrently write to the secondary drive or drive array. Random disk arrays and mirroring only protect against drive failure: they do not protect against file problems.
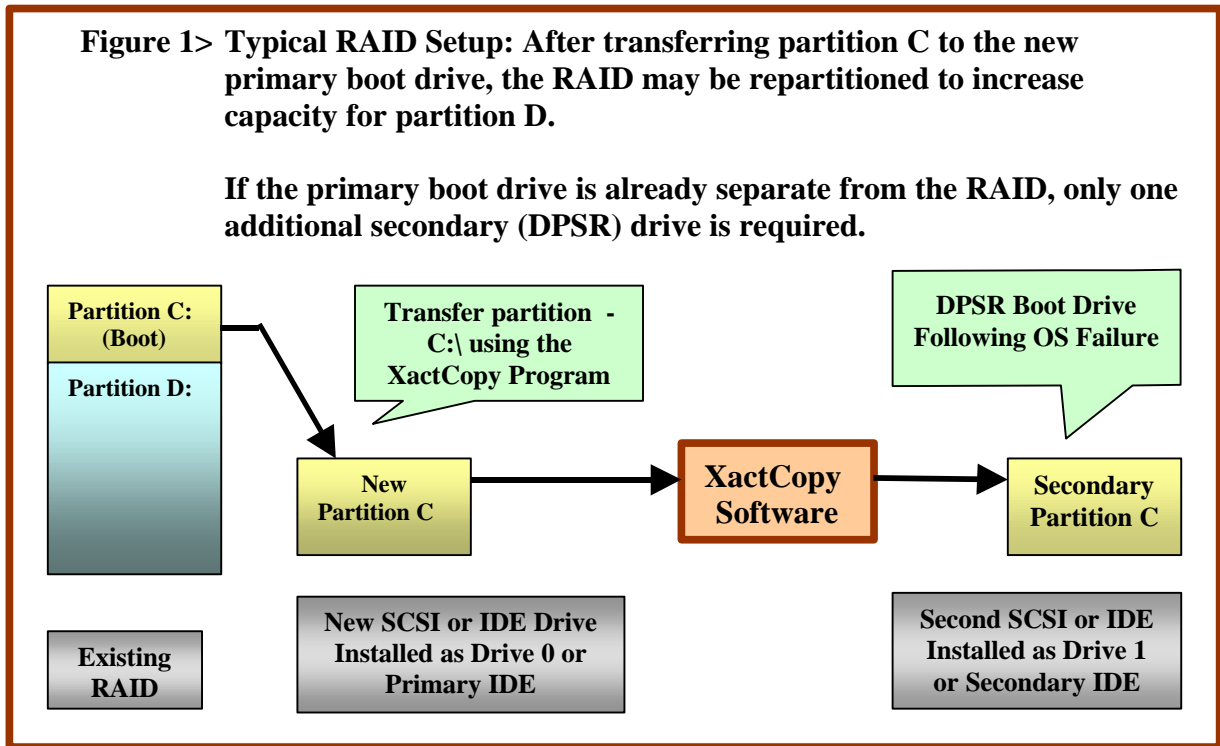
When a critical system file becomes corrupted, such as with the NT "Blue Screen of Death," the disk array offers no benefit for system recovery. Typically, operating system failures occur more frequently than drive failures and protection from OS failures with *X*actCopy is possible because the user decides when to write to the DPSR drive. Even when a routine backup is scheduled, the backup cannot occur if the operating system has failed.

NT Servers with RAID:

In this configuration, **XactCopy provides almost instant recovery of the NT server following non-recoverable operating system failure**. If the boot partition is located on the RAID, the application entails transferring it from the RAID onto a separate small SCSI or IDE drive. After successfully moving the boot partition, a second installed drive becomes the DPSR drive, which protects the new system (boot) drive. *X*actCopy is used to transfer the primary boot partition from the RAID to the new system boot drive and also to copy its contents to the secondary drive on a periodic basis determined by the system administrator.

After accomplishing the reconfiguration, *X*actCopy performs periodic copies of the entire contents of the primary boot drive without booting from DOS, which means that the server continues to operate. All routine backups are incremental (changed files-only) and result in a full backup to the secondary small DPSR drive.

When the server encounters a non-recoverable operating system failure, the system administrator can immediately boot the backup drive to restore system operation. Total downtime is typically less than a few minutes and because of its simplicity, a non-skilled technician can handle the recovery. If the primary drive is housed in a removable bay, the recovery procedure is to physically remove the primary drive. If the primary drive is not in a removable canister, changing the boot address recovers the system. Figure 1 illustrates adapting the configuration for optimal OS failure recovery in a RAID environment.

Figure 1> **Typical RAID Setup: After transferring partition C to the new primary boot drive, the RAID may be repartitioned to increase capacity for partition D.**

If the primary boot drive is already separate from the RAID, only one additional secondary (DPSR) drive is required.

NT Servers with Mirroring

There are two basic types of mirroring: hardware mirroring (with an installed special hardware card) and the software mirroring available in the Server version of Windows NT, and other third party vendors. If a system configuration is set up under NT or another brand of software mirroring, discontinue using the second drive under the software or hardware mirroring scheme and substitute this drive as the DPSR drive with *X*actCopy.

With *X*actCopy installed, system recovery is possible from both types of failure—disk drive and operating system problems—where the latter was not previously available. An additional benefit from this configuration is that of gaining protection from non-system file corruption, deletions, and possibly virus infections.

NT Servers without RAID or Mirroring:

In this application, the DuoCor technology provides fast recovery from both OS and hard drive failures. **Periodic full backups of only those files changed since the last backup, take place from within the operating system in approximately one to three minutes—while the system is running**. The system administrator has the option to perform periodic full backups automatically by using the *X*actCopy Scheduler Service (an NT Service) or manually at any time.

The technology offers a low cost alternative to RAID for drive failure protection plus the addition of OS failure protection.   Frequent updates of the system drive ensures up-to-date DPSR drive data, which minimizes data loss and enhances fast system recovery. This configuration also protects from corruption and loss of data files, which are other than critical system files.

*X*actCopy also restores files, folders, and complete partitions very quickly. The main screen of the program displays the contents of both drives in a side-by-side Explorer-like fashion. To aid in quickly identifying file differences between the System and DPSR drives, the program places a red colored not-equal sign next to the file. Files deleted since the last backup appear in the DPSR drive panel and not in the System drive panel.

By highlighting the file or folder and clicking the **Restore Files** button, the program instantly restores the file or the entire contents of a selected folder. Using the full-partition restore command of the program quickly restores an entire partition.

Mission Critical Workstations and Stand-alone PCs:

The application of *X*actCopy at a mission critical workstation is identical to that of its application on a non-RAID or mirrored server system. The technology offers protection from loss of mission critical data and its immediate recovery without the need to search through a tape library or network server. Like its server counterpart, the program offers fast system recovery from OS or system drive failures.

In many instances, backing up data at the workstation level has the added benefit of reducing network traffic. Another advantage afforded by the fast system recovery feature of *X*actCopy, is that of productivity for

the workstation user. With different schemes for servicing a failed workstation, which range from replacement to complete rebuilding, *X*actCopy's instant recovery feature does not noticeably interrupt the workflow of the user. The administrator or third party service organization can delay repair of the system to off-hours or when time permits.

Backing-up Open Database Files

When performing backup operations with *X*actCopy, it copies all open database files on a sector-by-sector basis. With several workstation users changing information and using a sector copy technique, the database would normally be uncoordinated resulting in a "dirty backup." To solve the problem of "dirty backups," the server version of XactCopy NT contains an Open Transaction Manager (OTM), which provides a "clean backup" of all open files while users are changing information on the open files.
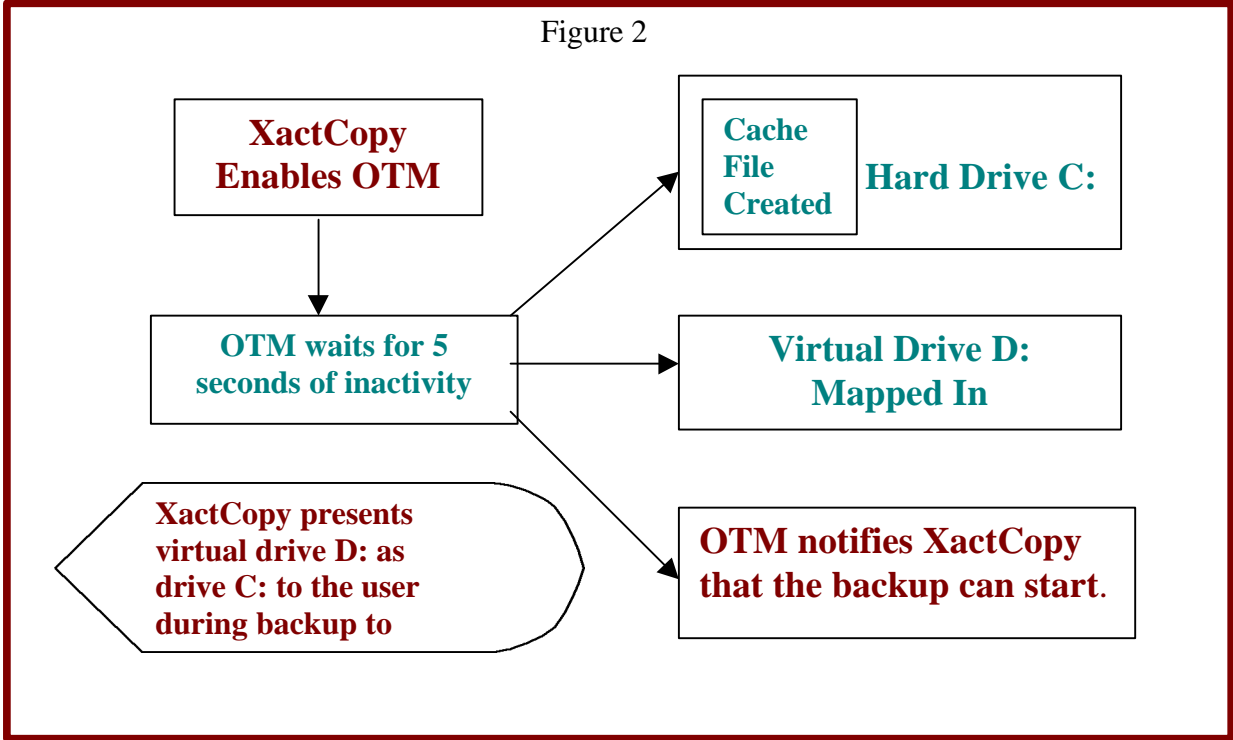
How XactCopy and OTM work Together

OTM presents a stable, non-changeable picture-in-time of any system hard drive to the DPSR drive by creating an alternate "virtual drive," or static copy of the drive to be backed up. When OTM is started by XactCopy, it waits for a short period of inactivity (5 seconds) where no writes are occurring to any of the volumes or drives that have been selected for backup. Once this quiescent period is obtained, OTM is enabled and maps-in a virtual drive letter for each volume selected to be backed up. XactCopy accesses this static virtual volume, instead of the original volume, which is changing during the backup.

When a write command occurs on the original volume, OTM pauses it and copies the old corresponding data to its cache file and immediately sends the original write data to the system drive. This action keeps the system drive current and unaffected at all times during the backup. Read requests from all applications except the backup are passed directly to the system drive with no intervention. Read requests from XactCopy are passed to the OTM filter driver, which determines if the requested data is already in cache. If data is in cache, OTM passes the cached data to the DPSR drive. If not, the data is passed directly from the system drive. Since OTM only needs to preserve the original data, additional writes to the same sector are not cached and are passed directly to the system drive. (For additional information and details, see the OTM White Paper on DuoCor's Website.)

Figure 2

XactCopy Enables OTM	**Cache File Created** **Hard Drive C:**
OTM waits for 5 seconds of inactivity	**Virtual Drive D: Mapped In**
XactCopy presents virtual drive D: as drive C: to the user during backup to	**OTM notifies XactCopy that the backup can start**.

The Benefits of Increased Backup Frequency

By performing frequent backups of the database or other applications, data is kept more current resulting in less data lost in the event of a catastrophic failure. In any backup environment, a need to restore non-current data after a critical failure exists because of the difference in time between the failure and the last backup. The data loss equation is:

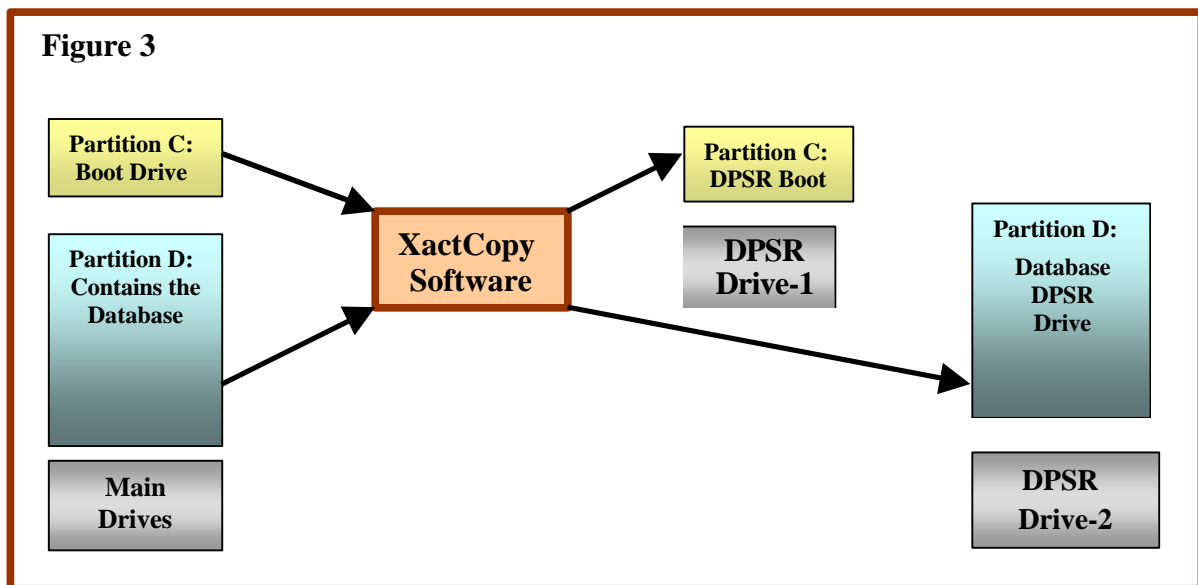**Data Loss = Time of Failure - Last Backup**

To minimize data loss, the system partition should be physically separated from the data partition(s). The system partition should only be backed up when new applications are installed, new users are added, or any other changes that affect the operating system's registry. Other than for the purpose of duplicating these registry-type changes, frequent backups of the operating system partition are not needed.

Protecting data partitions through frequent backups is another matter. According to the data loss equation, frequent backups of the data partition(s) results in less information lost after a critical failure occurs. XactCopy allows partition selection for manual or automatic backups to accommodate this scheme for minimizing data loss.

An Alternate Scheme for Zero Data Loss when OS Failures Occur

Systems configured with the operating system and data partitions on the same physical disk drive, as discussed in the previous section, still remain vulnerable to data loss. Suppose that 45-minutes after a backup operation, the operating system fails and becomes non-recoverable. Booting the DPSR drive will recover the system, but the last 45-minutes of data will not be on the DPSR drive. These data can be copied from the drive where the operating system failed, but the process will consume time to accomplish.

By separating the system partition from the main data drive (as in the RAID application discussed above) and placing it on a separate small IDE or SCSI drive, system recovery issues become separate from rapidly changing data activity on the main data drive. Figure 3 illustrates a typical configuration maximized for fast system recovery and zero data loss.

Figure 3

For maximum data protection (zero data loss) and minimum downtime, the scheme requires the addition of three hard drives:

- One small IDE or SCSI drive to house the primary system partition.
- A second small IDE or SCSI DPSR drive to protect the primary system drive.
- A third DPSR drive to protect the main data drive.
- A Single XactCopy license.

In this configuration, if the operating system fails and becomes non-bootable, system recovery is accomplished by booting the DPSR drive for immediate system recovery. With the system back in operation, the data drive is current and the result is zero data loss.

Technology Benefits Summary

- In the network server, workstation, and stand-alone PC environment, the technology does not require shutting down the system to run manual full backup copies of everything on the system drive. The result is more frequent use and less data lost.

- Offers almost instant system recovery; reboot from the DPSR drive without the use of DOS utilities, OS reloads, floppies, or complicated and time consuming incremental tape restores. The result is increased productivity and reduced costs in system downtime.

- Provides a low cost alternative to RAID servers for protection against both system disk and operating system failures. This results in cost savings and increased disaster recovery protection.

- "Hidden" secondary DPSR disk drive cannot be altered by the user or corrupted (or changed) by the operating system. No drive letter conflicts to worry about.

- Protects against lost or corrupted files by allowing for immediate restoration of files, folders or full partitions. The result is increased productivity.

- Significantly reduces or eliminates data loss trauma and its associated affect on business efficiency.

Conclusion

With the ever-decreasing cost of disk drives combined with the ever-increasing cost of downtime and reconstruction of lost data, the DuoCor DPSR Immediate Disaster Recovery technology has a place in most enterprise systems.