July 26, 2007

Augmenting the Disaster Recovery Approach of Microsoft Vista with Acronis True Image

Introduction

Every IT manager understands the importance to back up a computer system. They also recognize it is even more crucial to be able to restore the backed up server or workstation. This critical practice ensures the ability to recover from any number of problems, including catastrophic events such as fire, flood, or earthquake, as well as other "disasters" such as viruses, failed software installs, and, of course, the dreaded Blue Screen of Death. The key to surviving a disaster is having a transportable backup - a backup that can be restored to a new system without regards to its hardware configuration. The only requirements: the system must be x86- based and running Windows.

Small- to mid-size business owners, as well as users in corporate environments, are likely to recognize this importance of data restoration as there is a personal stake in the survival of business data. Additionally, there is an ownership feeling about data, as in "my data", "my business accounting records", and "my mission-critical applications and configuration files". Effective users and IT managers take a personal interest in the health of the IT systems that might make a difference between business continuity and business interruption - and business failure.

If you are in business, it can be argued that there is an ethical mandate to protect data integrity and assure the survivability of your critical business data. Policies and procedures need to exist if the implied ethical agreement between business and data user is to be honored, not to mention compliance with government regulations. Preparation and regular testing go hand in hand to establish flexibility, reliability and data integrity.

Without solid data protection systems for backup and recovery of data, other aspects of disaster recovery planning make little sense. Transportable systems backups are the foundation of any comprehensive disaster recovery strategy, as it is the only technology that will allow an organization to go back to any point in time and retrieve the data from that point, exactly as it was at that point in time, regardless of the existing hardware platform.

Microsoft Vista, the newest and most powerful operating system from Microsoft for desktop systems, opens new opportunities for power computing, but these new opportunities also open up new requirements for transportable backups.

Transportable backup and recovery using disk imaging is the only technology that provides:

- Protection against complete data loss - Traditionally, file-based data backups cover 100% of data but not necessarily the operating system, configuration files and applications. Other strategies, such as continuous data protection, cover the entire system, but are typically cost- and storage-prohibitive and only appropriate for transaction-based servers. Disk imaging allows you to create a snapshot of the entire server or workstation hard disk, including open

Windows files and all applications and data, without compromising on speed, cost or performance.

- Protection against viruses and data corruption - With a transportable backup in conjunction with incremental and/or differential backups, you are able to go back to any point in time and retrieve a corruption- or virus-free data set from before the corruption event. With the right imaging software, it also is possible to edit an image to remove corrupted data after the fact.
- Integrated desktop/laptop protection - 60% of all data stored in an enterprise is on laptops and desktops, according to International Data Corp., a leading market research firm, providing data protection to mobile or remote locations is more critical than ever. Organizations need a flexible approach to protecting data, regardless of where it is. In the case of laptops, it is critical to protect the data even when the user is traveling and not connected to the corporate LAN.
- Managed multiple point-in-time copies of data - Image-based transportable backups, which are usually done daily, provide point-in-time copies of data going back in time much longer than many other data protection strategies.

Disaster Recovery and Image Backup

In day-to-day computer system management, the requirement to restore from a backup will most likely be to recover a strategic file that has become corrupted or accidentally deleted. Less frequently, an entire drive is lost and must be restored as soon as possible. This typically creates a big problem when the lost drive is also the operating system (OS) drive.

Normal file-by-file backups work well for restoring data files, except when the failure occurs on a Windows OS disk. Here are a few common failures that can cripple a Windows server or workstation:

- Registry file corruption
- Deleting strategic files
- A failed OS hard drive

Any of these problems will render a system unbootable. If the system is unbootable, a regular fileby-file backup cannot be used until a temporary OS has been installed; partitions set; device drivers installed; and when used, third-party file-based backup software installed. Only then can a file-based backup recover files to the failed machine, and then, the backup would not include open Windows system files and some hidden system files.

A file-based OS recovery can take anywhere from two hours to two days or more depending on the degree of difficulties encountered. Because of these limitations, other methods of backup have been developed to better recover a failed OS. The fastest and easiest to use method is based on disk image technology.

Disaster recovery and business continuity planning moved to center stage in IT planning issues in the past few years following both natural and man-made disasters. While these subjects deservedly command the attention that they get, firms too often do not find the time and assets necessary to pay full attention to all the issues and execution of good plans often remains a problem. One reason for this is that often too much focus is put on "major" disasters, while too little is placed on business interruptions due to such mundane occurrences that we'll look at later.

One of the foundations of disaster recovery is data recovery from failed IT assets, and some have been looking to operating system vendors to do some of the disaster recovery job for them, especially in terms of backup and recovery. Look at Windows.

Windows has come a long way since its original introduction as a DOS add-on. Windows-based systems extend into the hundreds of millions of users and have become more feature-rich as the operating system has evolved.

Until recently, operating systems took little notice of the backup and restore functions essential to correcting catastrophic data loss and business continuity. Only the barest software hooks were included to enable third-party packages to backup and restore. OS-based backup and restore was unheard-of.

This lack has always been peculiar. All businesses, great or small, run on information and, more to the point, available information. When this information is lost or access is interrupted, the impact on a business is injurious, sometimes fatal.

Analysts at Gartner report that 40% of businesses that suffer a disaster never recover and fail within 5 years. The US Bureau of Labor Statistics is even more pessimistic; the government claims that 93% of all companies that experience "significant data loss" are out of business within five years. The message here is clear: loose your data, loose your company.

Gartner's report notes that application failures are responsible for 40% of downtime; operator error is responsible for 40% of downtime; systems and environmental problems, such as hardware failures, are responsible for 20% of downtime; and less than 5% of downtime is due to a natural disaster, such as a fire, flood or earthquake, or to terrorist attacks. These statistics demonstrate that the vast majority of downtime - downtime that can turn into a corporate disaster - are not caused by what many people think of as traditional disasters.

Backup is done to provide against unanticipated data loss. As noted earlier, the most dramatic causes for the loss are natural disasters, such as earthquakes, fires and floods. More frequently, however, the reasons for data loss are generally hardware failure, software failure, viruses, worms and human error.

Hesitation of OS vendors to address backup and recovery has been somewhat overcome by customer demand. There are still too many IT managers and users who fail to backup routinely. As a result, Microsoft has been placing backup features in Windows targeted at the core consumer audience.

Windows XP

In Windows XP, the popular predecessor of the recently released Windows Vista, Microsoft shipped what some call a rudimentary solution well hidden in XP iterations. When it was introduced, the backup solution required a technology called Automated System Recovery (ASR) to function fully.

According to Microsoft's Knowledgebase Article 818903, "ASR is a two-part system; it includes ASR backup and ASR restore. The ASR Wizard, located in Backup, does the backup portion. The wizard backs up the system state, system services, and all the disks that are associated with the

operating system components. ASR also creates a file that contains information about the backup, the disk configurations (including basic and dynamic volumes), and how to perform a restore".

It goes on to say: "You can access the restore portion by pressing F2 when prompted in the textmode portion of setup. ASR reads the disk configurations from the file that it creates. It restores all the disk signatures, volumes, and partitions on (at a minimum) the disks that you need to start the computer. ASR will try to restore all the disk configurations, but under some circumstances it might not be able to. ASR then installs a simple installation of Windows and automatically starts a restoration using the backup created by the ASR Wizard". You will note that no where in the document does Microsoft talk about restoring lost data or the state of the computer - just the system files necessary to run Windows. That's because this utility is not intended to restore user files or the system state.

Confusion, unfortunately, was a hallmark of backup under Windows XP. The user had to select individual folders and files from a lengthy tree of checkboxes, trying to find or guess where other users kept their files, predicting where files would be stored at a future time, and the like. All of this discouraged the user and backups went undone. (Have you ever tried to find your Outlook mail files? Windows hides them deep in the system. You first must unhide hidden system folders in order to find these files. Even then, Microsoft doesn't make it easy, forcing you to go seven layers deep into the file tree in order to locate the Mail files if you wish to do a file-based backup).

Backups under Windows XP are maintained in a proprietary .bkf format. The format led to several inconveniences. The backup could not be restored anywhere except on a PC running Windows XP. The format is not a standard; it is neither published nor supported. Users reportedly have historically found it hard to work with, discouraging backup and recovery activity.

Vista

Microsoft's successor to Windows XP originally was slated for introduction in 2003. The schedule was pushed to late 2004 and pushed back again. More and more postponements followed until the latter part of November 2006, when it was released to manufacturers. First customer shipments were at the end of January 2007.

Microsoft Vista, like XP before it, comes in multiple versions from a Basic Home release to a more full-featured Ultimate version. More advanced versions feature a new backup and restore tool called Windows Complete PC backup. This feature stores a version of the entire PC installation, known as an image. This is a snapshot of the PC's configuration at the time the backup is made.

The process is deceptively simple. Run the backup program to create a disk image, then save the result to an external hard disk, a separate volume on an internal local disk (not a network copy) or writeable DVDs. To restore the image, boot from the DVD and follow prompts to the Windows Recovery Environment, where Complete PC Restore is a Menu item. Yes, this is disk imaging, but how Microsoft implements the technology is just as important as which technology it chooses to use.

Caveat Emptor

While considered an improvement over Windows XP, Complete PC backup has disadvantages worthy of contemplation.

It can be argued that the process is destructive. Microsoft gives you one choice and one choice only: Image the entire drive; Restore the entire drive. More sophisticated disk imaging applications use this only as a starting point, adding significant features and functionality that allow the user to image their drives selectively, storing images where they are most appropriate for that network and then allowing the user to manipulate the image as needed.

With the Vista approach, the backed-up image completely replaces the contents of the drive onto which it is restored. There are no tools to select what you want or how you want the images restored. The Vista approach results in losing any data added to the PC subsequent to the creation of the image. Here's the first of many cautions: if the image is damaged before it is restored, the user will be placing an unusable image over what might be a functionally good drive. Without any way to confirm the reliability and viability of the image, it's a gamble when you run the Restore option.

The process works with full volumes only, and users who require more selective backup and restore operations must find an alternative. Like its predecessor in Windows XP, this backup product was designed with the core consumer in mind. Users requiring more sophistication in backup and recovery will find the Vista backup tools far too rudimentary.

Here's another potential gotcha - how do you know if the image you made is viable at the outset? Microsoft provides no verification tools for after the image is made, let alone before you restore it.

Also, Vista does not allow the user to boot directly from the backup image in order to restore a system, nor does Vista offer a true "one-button restore" that allows the user to restore an entire system, including its state and all user data and configuration files.

According to "Total Data Protection For Small- and Medium-Sized Businesses," a report published by market research firm Peripheral Concepts Inc., "The Perfect Backup" is defined as one that offers the following features:

- Allow Incremental and/or Differential Backup
- Copy Important files - continuously and in real time
- Takes zero time to copy
- Immediate reliable recovery
- Achieve point-in-time-based recovery of any version
- Easy to implement
- Transparency runs in the background

Using Peripheral Concepts' definition, the disk imaging capabilities of Vista fall far short of being the "perfect backup"; instead, users will need to look at a third-party product such as Acronis True Image.

Acronis creates images of the running operating system using a patented snapshot technology. The image is created in the background, so there is no interruption to the server or workstation being imaged.

Once the base image is created, the user (or IT manager in a corporate environment) can add incremental or differential images based on their own schedule. That way, the user can go back to a specific point in time to restore a file, folder or entire disk image.

If Vista's Complete PC creates an image of a hard disk that contains a virus or malware, that problem would still be a factor should the user restore that saved image. That is because Vista does not allow the user to mount the image as a virtual disk and then edit it. However, Acronis True Image does permit the image to be mounted as a virtual disk. Antivirus or antispyware software can then be run on that virtual disk, removing the offending software. When completed, the user can "save" the cleaned version of the disk. The changes - the disk sectors that had the offending software removed - are saved as an incremental image so that when the full image is restored, the virus or malware is gone. Vista's lack of support for incremental images makes this impossible in the native operating system.

Additionally, Acronis offers the Acronis Secure Zone®, a partition where an image of the disk can be stored. Should the user encounter problems, this image can be restored from the partition, even if Vista is somehow damaged and cannot boot. The partition is a FAT32 partition with the EISA partition type. The partition is visible in Windows from the Disk Management screen but a drive letter cannot be assigned.

Acronis True Image allows creating both file-backup (files and/or folders) and image-backup (partitions, hard disks), and stores them into either a local or remote file, burn it to CD/DVD, or in an Acronis Secure Zone®.

Vista can restore file-based backup archive both from working operation system and from Windows Vista Bootable DVD, but Microsoft doesn't support custom recovery from archives.

Vista offers two automatic recovery modes: from the last backup and from the old backup. There is an original database that contains all previously created backups. This helps to optimize the recovery process. Microsoft provides bare-metal recovery and uses Windows Bootable CD/DVD and My Computer Backup, saved on another local HDD, CD/DVD or a network location, to accomplish the task. Vista also provides the ability to fix OS errors using My Computer Backup. All backup archives are stored in a special database. When users want to restore files or volume, they use this database to choose the required backup file.

Vista offers the following ways of restoring:

- Use the File and Folder Restore wizard to restore files and folders from a backup
- Use Complete PC to restore the contents of the computer from a backup image
- Use System Restore to fix system-file problems and undo changes to Windows

In case of File and Folders Restore, the user has the ability to use shadow copies to restore previous versions of files that have been accidentally modified or deleted.

By comparison, the Acronis Restore Data Wizard recovers partitions/hard disks or even separate files from the previously made backup image. All that is needed is to select an archive and determine a location to restore. The rest is done automatically.

Acronis can boot from the bootable rescue media, from Acronis Startup Recovery Manager that allows you to access the Acronis Secure Zone®, or from the image itself. The Acronis Startup Recovery Manager can be installed to the Master Boot Record. When it is installed, users can hit F11 while booting (but before the operating system loads) to restore a system without bootable media.

Users can run Acronis True Image on bare-metal drives (unformatted) or on a crashed computer that cannot boot. Bootable media can be created during Acronis True Image installation or later on - the retail media itself is bootable. It can be a CD, DVD, diskettes, thumb drive, Zip drive or any other bootable media.

Microsoft, rightfully so, is very careful that its operating systems are not pirated. One way it protects its operating systems is to make sure that a user cannot simply remove a disk drive loaded with the OS from one machine and place it in another. While this technology successfully thwarts thieves creating multiple drives with a single version of the OS, it wrecks havoc on users whose systems fail and must migrate to a new hardware platform.

Vista's backup feature set does not address this issue. Acronis, however, does provide a transportable image approach that is hardware-independent. It allows a user to take an image from one hardware platform and restore it to another without violating Microsoft's EULA.

Overview

When comparing Vista's own backup and disk imaging technology to that of Acronis True Image, there are several additional capabilities that Acronis brings to the table:

- Exclusive Acronis Secure Zone® - A partition, not visible to the operating system or applications, except for Acronis True Image and some special disk managing tools. It allows the storing of a disk backup file on the same disk without any risk of that file being corrupted by software
- Exclusive Acronis Active Restore - This feature permits a user to boot the OS on the crashed computer before its image is completely restored, returning the user to work in seconds while the system is still being restored. The user can prioritize the most important application so it can be restored first, allowing the user to get back to work quickly and easily while a complete sector-by-sector disk restoration proceeds in the background
- Image Backup & File Backup - Acronis True Image combines its original sector-based disk imaging backup with a file-based backup option. Users can restore a system in minutes in case of a system crash, hardware failure or software failure
- Full incremental and differential backup - In addition to full and incremental back ups, user can create differential backups. Unlike incremental backup, when every backup procedure saves data changes against the previous backup file in a "chain," a differential backup creates an independent file, containing all changes against the initial full archive. To recover data, user needs only two files: the differential backup itself and the base full backup.
- BartPE plugin and Bootable Backup Media - BartPE helps to create bootable CD/DVD disks with operating system kernel such as Windows 2000/XP/2003. This utility is used only for creation files or ISO archives. It creates a bootable disk containing the operating system and different applications, such as antivirus, antispyware, file manager and e.g. Implementation process for bootable CD/DVD is easy. It needs just the right path for full Windows distribution, a directory for bootable files and then the process launches.

Conclusion

It was not too long ago that the Y2K scare shook up the entire world with the threat of catastrophic data loss. Fortunately, the effects of Y2K were greatly exaggerated. But Y2K did something that no other common-sense argument could have done. It made clear to IT managers and computer users the dependency of their businesses upon information systems. Moreover, it increased the business perception of the threat attached to data loss, both to operations and to potential profits.

From there, it is a matter of due diligence that a user, knowing that a potentially damaging situation exists, take sufficient steps to correct the situation or provide against the consequences. There are choices to be made, and it serves no one to defer or neglect those choices.

For bare bones backup functionality, a handful of users might find the backup tools embedded in Windows Vista a useful choice. But for more sophisticated and flexible options and functionalities, it is necessary to go beyond a tool created for the core consumer market. A third party option like Acronis True Image could make the difference between a responsible choice and a half-hearted one.

Calculating Downtime

Just how much revenue would your company lose if your systems were down and you can't process customer orders? Here's help calculating those losses:

- Multiply the average hourly revenue by the number of hours needed to recover.
- What is the cost of lost productivity?

In calculating lost productivity, consider the payroll, taxes, benefits and overtime for recovery, then multiply the number of employees from all of the affected business units.

- What is the value of IT employee productivity lost while trying to resolve the problem?

Use this for considering the costs associated with the IT employees reassigned to reconstruct and recover the data and systems.

- How much inventory will be lost or spoiled, and how much will it cost to recover or rebalance manufacturing processes.

When calculating this figure, consider materials and labor for handling, rework and/or disposal.

- What fines, fees and/or compensatory payments will you have to pay?

These include the fiscal impact of breach of contract, regulatory fines, late-shipment or late-payment and attorney fees.

- Add the costs of sales and marketing campaigns required to recover revenues, lost customer loyalty, reputation and goodwill.
- Finally, add the costs of legal, health, safety or liability exposures your company will face.

You might well be surprised by the total!