WHITE PAPER

ULTRABAC SOFTWARE

BARE METAL DISASTER RECOVERY

Filling the Gap in Backup Protection

INTRODUCTION

Since the beginning of the computing age, it has been universally understood that backup is a critical element in protecting against data loss. With the mountains of data being entered in today's online environment, the ability to recover lost data is not a luxury, but a fundamental part of doing business.

Bare Metal Recovery (BMR) is most often considered a supplemental layer of protection that can help insulate an organization against unnecessary downtime. While file-by-file backup and restore software is excellent at protecting against data loss, there is an inherent disadvantage in being able to quickly return an unbootable machine to a fully operational state. The shortcomings are the many steps required to perform a file-by-file recovery, and the lack of guarantee that every operating system (OS) change has been reinstated even after a restore. Thus, BMR should actually be a vital part of any company's disaster recovery plan, not just an afterthought.

THE HISTORY OF BARE METAL RECOVERY

In the early days, the cost of storage was so high that individual transactions were printed on punch cards, paper tape, or ledger cards. Customer transaction totals were stored on a magnetic stripe on the back of a ledger card, tape cassette, or, for those who could afford big iron, disk. Because of the high expense for tiny amounts of storage, and since hardware frequently failed, systems were designed to allow companies to limp along using paper as a fall back during what were often long repair periods.

As technical advances in storage brought the cost per byte down, more data could be kept online. This meant that backup vendors had to keep pace by creating better technology. In some cases advancements were a requirement, and not just produced out of a desire to invent the next big thing. A good example of a necessary development was bare metal disaster recovery.

BMR was a mandatory function for Digital Equipment Corporation VAX users, back when DEC was a major player in the minicomputer market. This was because a VAX only supported one OS. Computers from other manufacturers often supported multiple OS drives so, if one failed (for any reason), you could simply boot from another drive. BMR was a technology born of a requirement by VAX end users to quickly and easily restore a "dead" machine that had lost its ability to boot. This is also often referred to as "cold" booting a machine.

When Microsoft developed Windows NT, they too designed a machine that only supported one OS drive. Windows end users had the same problem as VAX users – it was no easy task to re-install an OS and get a machine restored to the same point it was before an unbootable type of failure. It wasn't long before VAX users, who had converted to Windows NT, started asking for a BMR equivalent.

The third party software community that specializes in backup was slow to understand the significance of BMR. For many users, an OS failure had never been a large issue for the equipment they supported before moving over to NT. However, as more sophisticated end users moved to the new OS, demand for a method to quickly and easily restore a failed machine gained momentum. In order to create this solution, vendors were required to think beyond the

traditional file-by-file backup and restore methods that were so prevalent up until just a few years ago. Therefore, the BMR products available in today's market have been greatly influenced by the success of Windows in the business environment.

Over the past five years there has been an explosion of new hardware and software options for end users that offer better protection. Due to the amount of choices available, it is not surprising many end users are unsure as to which data protection approaches are critical and should be funded, versus what might be optional for their unique environment. Computer down-time is a leading contributor to overall business failure so it is prudent to minimize this risk. However, a major problem is balancing a viable solution cost against acceptable levels of down-time since it is extremely costly to buy and implement a non-stop computing system.

THE WINDOWS NT ERA

When Microsoft released Windows NT, nearly the entire user population regularly backed up to tape using the built-in backup product. As third party backup solutions began to emerge, UltraBac Software introduced the first Windows server backup product that not only backed up to tape, but was actually designed to write to disk as a storage option. As the price of disk storage continued to fall in the late 1990's, every competitive backup product in the Windows market released some type of disk-to-disk functionality. Consumer demand had inspired this move to a different and more stable form of backup media, as tape had often proved to be less than completely reliable. These requests for alternate storage only accelerated as the price of disks continued to fall.

As end users became more reliant on the faster disk-to-disk backups, they realized there was a huge hole in their file-by-file restores. The ability to back up to disk more rapidly than tape created the expectation of faster restores. However, with traditional restore methods this was not possible. When it took five hours to back up to tape, recovering a failed machine in five hours as well was considered normal if not outstanding. When backup times were cut in half, the technology to restore a totally failed machine in a timely manner had to be created.

Once Windows NT was released, customers frequently experienced what was labeled "The Blue Screen of Death." A blue screen event normally did not cause any data loss; the machine just became unbootable and therefore was unusable until recovered. To recover, an administrator had to install a temporary operating system, install the backup software, use the backup software to restore the operating system partition, and then reboot. Backup and restore was almost always performed to and from tape with a common problem – a restored backup often did not have key information that had been layered on the machine since installation. Aside from how long a restore took, the fact that a failed machine typically was not completely restored to the full status at which it failed, initiated the demand for a better way to recover. This led to the development of BMR for Windows. Unfortunately, many end users initially resisted investing in this software technology because of perceived lack of functionality and high cost assumptions.

TIME IS MONEY

While the definition (and monetary value) of a timely recovery of a failed machine can vary from organization to organization, one unarguable fact is that downtime costs money. Actual system downtime loss is an expense that is usually not well perceived in most organizations – it can even

vary by the time of day. Downtime for Company A might cost $5,000 an hour while the cost for Company B could be $100,000 an hour. Even the rate between individual servers within a company can be vastly different depending on the critical nature of the applications being run. Here is a very simple formula to estimate downtime:

(Employee costs per hour) x
(Fraction of employees affected by outage + Average income per hour) x
(Fraction of income affected by outage)
= ***Estimated average cost of one hour of downtime***

*A Simple Way to Estimate the Cost of Downtime – David A. Patterson, Computer Science Division, UC Berkeley.

Downtime costs fall into two broad categories: tangible and intangible. Calculating tangible costs such as employee wages, operating costs, and office expenses are straight forward and can be estimated with great accuracy using a simple formula like the one provided above. The difficultly lies in factoring all of the potential intangible costs such as lowered employee morale, missed opportunities, forgone sales, and loss of customer goodwill. These are hard to assign accurate costs. The bottom line is all companies recognize computer downtime means lost money. Regrettably, most don't realize how much it truly costs.

DECREASING RESTORE TIMES – INCREASING AVAILABILITY

Organizations can significantly decrease server downtime by implementing a quality bare metal recovery solution. Standard file-by-file recovery methods simply cannot bring a server back online quickly or easily. BMR software offers an economical way to eliminate unnecessary downtime, making machine failures less expensive. In some cases, the first use of a BMR solution can provide the user their full return on investment.

There are many expensive hardware and software products on the market that are designed to offer non-stop computing. They do a fine job, but do not eliminate or even help with unbootable events. For example, no matter the quality of a RAID device, or how reliable a cluster server or replication product, none of these can help overcome installing a bad driver that causes a blue screen. In a situation such as this, replication software simply becomes 'double trouble' because the bad driver is replicated to the fail-over machine, making it unbootable as well.

DEFINING BARE METAL RECOVERY

Organizations can significantly decrease server downtime by implementing a quality bare metal recovery solution. Standard file-by-file recovery methods simply cannot bring a server back online quickly or easily. BMR software offers an economical way to eliminate unnecessary downtime, making machine failures less expensive. In some cases, the first use of a BMR solution can provide the user their full return on investment.

Bare metal recovery is essentially the process of taking a low-level snapshot of a machine's operating system partition and storing it where it can be quickly and easily accessed when required. A BMR solution has two parts. The first is a program that is set up to periodically snapshot an OS partition using image backup technology. This is installed as a service and comes with a scheduler. The scheduler is then programmed to take backups of the live machine without any requirement to shut down services, close applications, or go offline. Image backups

are normally stored to a UNC path, SAN, or NAS device for online storage and quick access when needed.

The second part of a BMR solution is the process used to boot a dead machine. This enables users to connect to the online location where the image backups have been stored and initiate a restore. Once the OS partition has been restored (which can take between 5 to 30 minutes), the only remaining steps necessary to complete the disaster recovery are to remove the boot media and reboot the machine. This latter phase takes approximately two minutes before the machine is back to the exact state at which the image backup was performed.

Static image backups are typically performed every 24 hours, with options for incremental and differential backups between full backups. The newest functionality for BMR is continuous image protection, or CIP. CIP can also be referred to as CDP, or continuous data protection, but the term CDP does not differentiate between block or file protection. Many CDP products on the market today only provide continuous data protection for applications such as SQL or Exchange, whereas CIP offers comprehensive protection for all applications on a disk. The advantage both CDP and CIP do offer is the ability to restore a machine to a closer point-in-time to the actual root cause of an unbootable failure, as opposed to a standard image backup that might be 23 hours old.

Using regular file-by-file backup software, restoring a failed server takes most organizations anywhere between two hours to two days to accomplish. By implementing a BMR solution, restoring the same OS partition that took hours using a regular file-based restore might be accomplished in under 10 minutes. Not only is BMR fast, but it is simple when compared to a file-based restore. A sophisticated BMR product can also be fully scripted – even a security guard on the night shift could recover a strategic 24x7 server.

WHAT TO LOOK FOR IN A BARE METAL RECOVERY SOLUTION

When image-based disaster recovery first appeared in the Windows environment, the majority of users were astonished at how fast and simple recovering failed servers became. Unfortunately, certain restrictions applied. In order to restore the saved backup image files, they were required to be restored to the same or nearly identical hardware. As BMR software has evolved, key features were introduced to make this solution truly flexible.

The technology has become an integral disaster recovery application for more and more enterprise level businesses, and now the SMB market is realizing that it is as vital to them as it is for larger companies. When considering which software application is right for a company, here are some key features to look for in a bare metal recovery solution:

1. Dissimilar hardware restore
2. Virtual consolidations and disaster recovery
3. Restore to larger partitions and disks
4. Restore to smaller partitions and disks
5. The ability to safely restore Active Directory and Domain Controllers
6. Full, incremental, and differential options
7. Continuous image protection (CIP)

8. Fully scripted backups and restores
9. Remote management
10. Backup and restore using FTP/SFTP
11. Backup and restore using IBM Tivoli Storage Manager
12. Backup and restore using any local or remote tape drive
13. Backup and restore using any local or remote library
14. Backup and restore using any local disk, UNC path, SAN, NAS, USB, or FireWire device
15. Backup and restore using CD, DVD, USB Key, or PXE/RIS
16. Backup and restore through tightly locked down firewalls
17. Disk-to-disk-to-tape options for redundant and off-site storage

HOW BARE METAL RECOVERY SAVES MONEY

Every minute of machine downtime costs an organization time and money. Therefore, everyone should be able to agree that limiting downtime is highly desirable, particularly if it is reasonably affordable. To demonstrate the return on investment (ROI), here is a BMR scenario:

If the national average for Windows server downtime is $15,000 an hour (and this is a fairly modest sum), then this would mean that every minute of downtime equals $250. If it then takes a standard bare metal disaster recovery solution approximately 20 minutes, as opposed to 40 minutes using file-by-file backup and restore, the 20 minute savings using the BMR solution equates to a $5,000 dollar savings in downtime cost with its first use.

Expanding on this, if the price of a premium BMR solution is $1,000 per server, an organization could subtract the price of the BMR software from the money they saved on restore times. Bottom line, the company would still be left with a $4,000 cost savings. Not many products offer a ROI like this, particularly after just a first time use. In a real production environment, the time savings is more like a 6-to-1 ratio, leading to even greater savings as opposed to the 2-to-1 ratio used in this example.

THE BARE METAL RECOVERY STEPS

To give organizations a better understanding of how the two backup methods differ, we have provided a procedure comparison between using file-based backups and restores versus image-based backups and restores.

File-by-file restore example:

1. Install EISA Partition (53 minutes)
2. Install Windows OS (45 minutes)
3. Install Backup Software (5 minutes)
4. Create Data Partitions (10 minutes)
5. Restore System 4GB drive (35 minutes)
6. Restore System State/Registry (1 hour)
7. Reboot Server (2 minutes)

Total Restore Steps = 7 Restore Time = 3 ½ hours

Bare Metal Recovery example using UltraBac Software's UBDR Gold:

1. Boot server using UBDR Gold Restore Media (5 min)
2. Connect to a UNC path and initiate a 10GB OS partition restore with a conservative 2GB/minute transfer rate (8 minutes)
3. Reboot Server (2 min)

Total Restore Steps = 3 Restore Time = 15 minutes

As the example demonstrates, a BMR solution can easily restore a failed machine's 10GB OS partition in 15 minutes using a conservative 2GB/minute restore speed on a Gigabit network connection. Fast systems can experience over 5GB/minute restore speed. Organizations using the BMR process now "complain" that the machine boot time takes longer than the physical restore. When comparing file-by-file methods with BMR, there simply is no comparison.

SUMMARY

Buying and implementing a BMR solution has become a priority for many organizations – and it should be. BMR is a key part of any formal disaster recovery plan. It not only offers a fast means of restoring a failed server, but also offers extraordinary benefits to expedite recovering from a catastrophic event. With the ability to recover to dissimilar hardware and/or virtual environments, organizations can provide a clear path to recovering lost servers by taking off-site backups to any number of service companies who can provide temporary equipment. Rather than attempt to locate exact hardware matches or conduct laborious file restores to new equipment, users can restore an image of a Dell server to an HP or IBM server. Using the right BMR solution, companies also have the ability to restore multiple physical servers to a VMware ESX host machine, and be up and running in literally minutes.

With the technology available today, it is no longer acceptable to have a file-by-file backup solution as the only means of protecting data. Whether an organization has a single server, or over a thousand, a bare metal recovery solution is a necessary preventative measure against expensive and unnecessary downtime. BMR should be an integral part of every disaster recovery plan.