白書

ULTRABAC SOFTWARE

ベアメタル・リカバリ

-- バックアップ保護やＢＣＰ（事業継続計画）の改善 --

[The English version appears after the Japanese translation.]

コンピュータ時代の始まり以来、バックアップはデータ損失を防ぐための重要な要素であると広く知られてきました。今日オンライン上に蓄積されていくデータの山を考えると、失われたデータを復旧する技術は余分な贅沢ではなく、むしろビジネスを行う上で基本となる要素です。

ベアメタル・リカバリ（BMR）は 、企業を不要なダウンタイムから守る追加的な保護層であると一般的に考えられています。ファイル事バックアップと復元のソフトウェアはデータ損失を防ぐことにかけては優れていますが、その一方で起動していないコンピュータを完全な動作状態に素早く戻すことにおいて特有の欠点を持っています。それは、ファイル事バックアップ実行のための手順が多いことや、復元してもOSの変更を全て回復できる保証がないことです。したがって、BMRはどの企業のディザスタリカバリ計画においても単なる付録ではなく、実際に重要な要素となるべきなのです。

ベアメタル・リカバリの歴史
始めのころはストレージ費用が非常に高額だったため、個々のトランザクションはパンチカード、紙テープ、または台帳カードに印刷されていました。顧客トランザクションの総計は、台帳カード裏の磁気ストライプ、テープカセット、または超高速大型コンピュータを使用している場合はディスクに保存されていました。 わずかなストレージにも高額の費用がかかることやハードウェアが頻繁に故障してしまうことから、改善までの長い間、企業が紙を頼りにもたつくようなシステム設計がされていました。

ストレージの技術が進歩するにつれてバイトごとの費用が下がり、より多くのデータがオンラインで管理できるようになりました。これによってバックアップ製品のベンダーはさらに良い技術を生み出して、この技術の進歩に対応しなければならなくなりました。時として進歩はそれそのものが必要であり、画期的な新発明への情熱が生み出すものではありませんでした。必要な進歩の良い例がベアメタル・リカバリです。

デジタル・イクイップメント・コーポレーション(ＤＥＣ)がミニコンピュータ市場の中心だった時代、BMRはDEC社のVAXユーザーにとっては必須機能でした。これは1台のVAXは1つのOSのみサポートしていたためです。他の製造業者のコンピュータは複数のOSドライブをサポートすることが多かったので、 その内の1つが（理由はどうあれ）機能しなくなっても、他のドライブから起動させることができました。BMRは、起動ができなくなった「故障した」マシンを迅速かつ簡単に復元させたいというVAXエンドユーザーの要求を受けて生み出された技術で、 よく「コールド」ブートと呼ばれています。

Microsoft社がWindows NTを開発したとき、やはり1台のOSドライブのみをサポートするマシンを設計しました。Windowsエンドユーザーは VAXユーザーと同じ問題を抱えました. つまり、OSを再インストールし、起動できなくなるような故障のあった直前と同じ時点の状態にマシンを復元するのはそう簡単なことではありません。
Windows NTを使い出したVAXユーザーは、すぐに相当するBMRを求めるようになりました。

バックアップに特化する第三者ソフトウェアコミュニティは少しずつBMRの重要性を理解し始めました。多くのユーザーにとって、NTに移る前はOSの不具合は大きな問題ではありませんでしたが、高度なエンドユーザーが新しいOSに移行するに従って、迅速で簡単な復元方法に対する需要が高まりました。このようなソリューションを生み出すため、ベンダーはほんの数年前まで広く普及していた従来のファイルバックアップと復元方法を超えるものを考える必要に迫られました。つまり、現在市場で販売されているBMR製品にはビジネス環境でのWindowsの成功が大きく関わっているのです。

過去5年間で、より優れた保護機能を提供する新しいハードウェアとソフトウェア製品が急増しました。当然ながら多くのエンドユーザーは、その選択肢の多さのため、どのデータ保護アプローチが重要で費用をかけるべきか、また、個々の環境においてどのアプローチがオプションとなり得るのか判断をつけられなくなりました。コンピュータのダウンタイムはビジネス全体が失敗する最大の要因となるため、このリスクを最小限にすることが賢明と言えます。しかし、一番の問題は支出可能なソリューション費用とダウンタイムの許容レベルのバランスを保つことです。なぜなら無停止型のコンピュータシステムを購入し実装するには非常に高額な費用がかかるからです。

Windows NTの時代

Microsoft社がWindows NTをリリースした頃、ほとんどのユーザーは内蔵されたバックアップ製品を使用して定期的にテープにバックアップしていました。第三者が開発したバックアップソリューションが現れ始めたころ、UltraBac Software社が始めてのテープにバックアップするだけではなく、ストレージ選択技としてディスクに書き込みができるように設計されたWindows Server Backup製品を発売しました。ディスクストレージの値段は90年代後半に下がりつづけ、 Windows市場では競合するあらゆるバックアップ製品が何らかのdisk-to-disk機能を搭載して発売されました。
テープはあまり信頼できないことが証明されるようになり、マーケットの需要によってこの市場の動きが刺激され、別のより安定したバックアップメディアの形態に向かわせました。代わりのストレージに対する要求はディスクの値段が下がるにつれてますます高まりました。

エンドユーザーがより高速なdisk-to-diskバックアップに以前よりも頼るようになると、彼らはファイル事の復元に大きな欠点があることに気づきました。テープよりも早いディスクへのバックアップはより早い復元を期待させましたが、従来の復元方法ではこれは不可能だったのです。テープへのバックアップに5時間かかっていたときは、故障したマシンの復旧にも5時間かかるのは際立っているとまではいかなくても普通だと思われていました。バックアップの時間が半分に短縮されたとき、完全に故障したマシンを直ちに復元できる技術を生み出さなければならなくなりました。

Windows NTがリリースされると、ユーザーはいわゆる「死のブルースクリーン」をしばしば経験しました。ブルースクリーン状態は通常はデータ損失の原因にはなりません。これはマシンがただ起動不可能になり、その結果として復旧するまで使えなくなっただけです。復旧するには管理者が臨時のOSをインストールし、バックアップソフトウェアをインストールし、そのバックアップソフトウェアを使用してOSパーティションを復元し、そして再起動する必要がありました。 バックアップと復元はテープとのやりとりにおいて、大抵同じ問題を抱えていました。それは、復元したバックアップは, インストール以来マシン上に蓄積されてきた重要な情報を含 んでいないことがよく

あることでした。復元にかかる時間に加え、不具合を起こしたマシンが大抵は完全に元の状態に復元されないという事実から、リカバリ方法の改善という需要が生まれ、Windowsに対応したBMRの開発につながりました。
あいにく、機能性に欠けるという認識と高額な費用がかかるという思い込みが原因で多くのエンドユーザーが最初はこのようなソフトウェア技術への投資に反対していました。

タイム・イズ・マネー
不具合を起こしたマシンを直ちにリカバリすることの定義（および金銭的価値）が企業によって異なる一方、ダウンタイムには費用がかかることは疑いのない事実です。ダウンタイムによる実際の損失費用は、1日の時間帯によってさえ変化するため、ほとんどの企業において大抵は十分に把握されていません。ダウンタイムによる損失がA社では1時間につき5,000ドルの場合、これに対してB社では100,000ドルかもしれません。企業内における個々のサーバー間の比率でさえ、実行されているアプリケーションの本質によって大きく変わります。下記の式はダウンタイムの費用を見積もることができる、とても簡単な計算式です。

（1時間あたりの従業員費）×
（機能停止によって影響を受ける従業員の割合＋1時間あたりの平均収入）×
（機能停止によって影響を受ける収入の割合）＝
ダウンタイム1時間あたりの推定平均費用
「ダウンタイム費用を見積もる簡単な方法」より
（デイビット A. パターソン作, コンピュータ　サイエンス学部,
カリフォルニア大学バークレー校）

ダウンタイム費用には大きく分けて有形と無形の二つのカテゴリがあります。従業員の賃金、運営費、および事務費のような有形費用の計算は分かりやすく、上記のような簡単な数式を使用してかなり正確に見積もることができます。難しいのは、従業員の士気の低下、機会の喪失、売上放棄、そして顧客の信頼喪失など潜在的な無形費用も全て考慮に入れて正確な費用をあてがうことです。肝心なことは、全ての企業がコンピュータのダウンタイムは金銭の損失であると認識することです。しかし残念なことに、多くは実際にどれほどの費用がかかっているか理解していません。

復元時間の短縮－有効性の向上
企業は質の良いベアメタルリカバリソリューションを実行することでサーバーダウンタイムをかなり短縮することができます。標準的なファイルごとの復元方法ではどうしても、素早く簡単にサーバーをオンラインに復帰させることはできません。BMRソフトウェアを使うと経済的な方法で不要なダウンタイムを減らし、マシンの故障による費用を安くすることができます。場合によってはBMRソリューションの初回の使用で投資を全額回収することもできます。

市場には高価なハードウェアやソフトウェア製品が数多くあり、継続したコンピュータ使用に対応するよう設計されています。そういった製品は良い働きをしますが、起動不可能な状況を失くしたり助けたりしてくれるわけでもありません。
例えば、RAIDデバイスの品質が良いとしても、またはクラスタサーバーや複製製品が信頼性に優れているとしても、どれもブルースクリーンの原因となる不正なドライバのインストールを解決する助けにはなりません。 このような状況 では、複製ソフトウェ

アは どうしても「二重の問題」となってしまいます。不正なドライバが 復元先のマシンにもコピーされ、同じように起動不可能にさせるからです。

ベアメタル・リカバリの定義
ベアメタル・リカバリは基本的にマシンのOSパーティションの低レベルなスナップショットを取り、必要なときに素早く簡単にアクセスできる場所にそれを保管する処理を行います。BMRソリューションには２つの要素があります。1つはプログラムで、イメージバックアップ技術を使用して定期的にOSパーティションのスナップショットを取るよう設定されています。これはサービスとしてインストールされ、スケジューラーと一緒に搭載されています。 このスケジューラーは稼動しているマシンのバックアップをとるようプログラムされており、サービスを停止したり、アプリケーションを閉じたり、またはオフラインにしたりせずにこれを実行できます。イメージバックアップは通常、オンラインストレージと必要な時に迅速にアクセスできるようにUNCパス、SAN、またはNASデバイスに保存されています。

BMRソリューションのもう1つの要素はダウンしたマシンを起動させるためのプロセスです。これによりユーザーはオンライン上のイメージバックアップが保存されている場所に接続し、復元を開始できます。OSパーティションが復元されたら（5分から30分程度かかります）、あとは起動メディアを取り出して、マシンを再起動するだけです。この2番目の手順によって、マシンはおよそ2分でイメージバックアップを実行したときの状態にそのまま戻ります。

静的イメージバックアップは通常24時間ごとに実行され、任意でフルバックアップの間に増分および差分バックアップが行われます。BMRの最新の機能は継続的なイメージ保護であるCIPです。CIPは別名CDPまたは継続的データ保護（Continuous Data Protection）とも呼ばれますが、CDPという用語はブロックとファイル保護を区別していません。現在市場に出ている多くのCDP製品はSQLやExchangeのようなアプリケーションのための継続的なデータ保護を提供するだけですが、CIPはそれに対してディスク上の全てのアプリケーションを対象とした包括的な保護を提供します。CDPとCIPが提供する強みは、起動不可能な障害にあう直前の、ある特定時点の状態にマシンを復元することができることです。23時間前の状態に戻すこともありえる標準的なイメージバックアップとは対照的です。

標準的なファイルバックアップソフトウェアを使用すると、ほとんどの企業では故障したサーバーを復元するのに2時間から2日間かかります。BMRソリューションを実行することで、標準的なファイルベースの復元では数時間かかるOSパーティションの復元が10分以下で完了することが考えられます。BMRは早いだけではなく、ファイルごとの復元に比べて簡単です。 高度なBMR製品はフルスクリプト化(簡単な指示による確実な復元)もできるため、夜間警備員でも戦略的な24時間稼動のサーバーを復旧できます。

BMRソリューションの見所
イメージベースのディザスタリカバリが初めてWindows環境に登場したとき、ユーザーの多くはそのサーバー復旧の速さと簡単さに驚きましたが、残念ながらいくつかの制限が適用されていました。保存したイメージバックアップファイルを復元するためには、同一またはほぼ同一のハードウェアに復元しなければいけませんでした。 BMR

ソフトウェアが進化するにつれて重要な機能が搭載され、このソリューションはかなり融通のきくものとなりました。

この技術はますます多くの企業レベルのビジネスにおいて、なくてはならないディザスタリカバリアプリケーションとなりました。今日ではSMB(中小企業)でも、大企業と同様にとってもこの技術が重要だと理解しはじめています。企業にとってどのソフトウェアが適切か考える場合、ベアメタルリカバリソリューションには次のような重要な特徴がいくつかあります。

1. 異機種ハードウェア間での復元
2. 仮想統合とディザスタリカバリ
3. より大きいパーティションとディスクへの復元
4. より小さいパーティションとディスクへの復元
5. アクティブディレクトリとドメインコントローラーを安全に復元する機能
6. フル、増分、および差分選択肢
7. 継続的イメージ保護（CIP）
8. フルスクリプト化された（簡単な指示による確実な)バックアップと復元
9. リモート管理
10. FTP/SFTPを使用したバックアップと復元
11. IBM　Tivoli ストレージマネージャを使用したバックアップと復元
12. ローカルまたはリモートテープドライブを使用したバックアップと復元
13. ローカルまたはリモートライブラリを使用したバックアップと復元
14. ローカルディスク、UNCパス、SAN、NAS、USB、またはFireWireデバイスを使用したバックアップと復元
15. CD、DVD、USBキー、またはPXE/RISを使用したバックアップと復元
16. 堅くロックされているファイアウォールを介したバックアップと復元
17. 冗長なオフサイトストレージ用のdisk-to-disk-to-tape選択肢

BMRによるコスト削減方法
マシンのダウンタイムは企業に対して1分ごとに時間と費用の負担をかけます。したがって、ダウンタイムを抑える方法は、特にそれが手ごろな価格の場合は、非常に価値があることは疑いようもありません。投資回収率（ROI）を証明するために、ここにBMRのシナリオを用意しました。

Windowsサーバーのダウンタイム費の全国平均が1時間あたり 15,000ドル（これはかなり控えめな金額です）だとすると、ダウンタイム1分あたりでは250ドル（約￥27.500）かかることになります。標準的なベアメタルディザスタリカバリがおよそ20分で終了するのに対してファイルバックアップと復元には少なくても40分かかるとすると、BMRソリューションの初回使用によって短縮された20分はダウンタイム費用における5,000ドル分の節約に値します。

これをさらに詳しく説明すると、サーバーごとのプレミアムBMRソリューションの価格を1,000ドルとした場合、企業はこの価格を復元時間の短縮で節約した金額から差し引いて、結果としてまだ4,000ドルを節約できることになります。このような投資回収率を、特に初回使用のみで提供できる製品はそう多くありません。実稼動環境では時間

短縮はむしろ6対１に近く、この例で使用した2対1の比率に対してさらに大きなコスト削減をもたらします。

BMRの手順
この二つのバックアップ方法がいかに違うものか読者により深く理解してもらうために、ファイルベースのバックアップおよび復元とイメージベースのバックアップおよび復元の手順を比較してみます。

ファイルごとの復元の例：
1. EISAパーティションをインストール（53分）
2. Windows OSをインストール(45分）
3. バックアップソフトウェアをインストール（5分）
4. データパーティションを作成（10分）
5. 4GBのシステムドライブを復元（35分）
6. システム状態/レジストリを復元（１時間）
7. サーバーを再起動（2分）

復元手順の合計＝7　　復元時間＝3.5時間

UltraBac社のUBDR　Goldを使用したベアメタルリカバリの例：
1. UBDR Gold復元メディアを使用してサーバー起動(5分)
2. UNCパスに接続して控えめに2GB/分の転送速度で10GBのOSパーティションの復元を行う（8分）
3. サーバーを再起動（2分）

復元手順の合計＝3　　復元時間＝15分

この実例説明のように、BMRソリューションではギガビットネットワーク接続で控えめな2GB/分の転送速度を使用して、故障したマシンの10GBのOSパーティションを15分で簡単に復元できます。早いシステムなら5GB/分の復元速度になります。このBMRプロセスを活用している企業が現在「不満を言う」のは、マシンの起動時間のほうが物理的な復元より時間がかかることについてです。 ファイルごとの復元とBMRソリューションと比較しても、比べ物にならないのは言うまでもありません。

概要
BMRソリューションを購入して実装することは多くの企業にとって優先事項になっており、またそうなるのが当然です。BMRはどのディザスタリカバリ計画でも重要な役割を果たし、故障したサーバーを素早く復元する手段だけではなく、壊滅的な事態からの迅速な復旧によって特段の利益をもたらしてくれます。異機種ハードウェア間および仮想環境間で使用できる復旧機能があれば、企業は一時的にハードウェアを貸してくれる多くのサービス会社に、オフサイトでバックアップを行い損失したサーバーを復元するための明確な道をもたらすことができます。正確に一致するハードウェアを探したり新しい装置への困難なファイル復元を実施する代わりに、ユーザーはたとえばDellサーバーのイメージをHPまたはIBMサーバーに復元できます。適切なBMRソリューションを使用すれば、企業はさらに複数の物理サーバーをVMware GSXホストマシンへ復元し、ほんの数分で再運用できる機能を使用できます。

現在の技術を使うと、もはやファイル事のバックアップソリューションはデータ保護に対する唯一の手段ではありません。企業が持っているサーバーが1台か数千台かに関係なく、ベアメタルリカバリソリューションは高額で不要なダウンタイムに対する必要な予防手段であり、BMRは全てのディザスタリガバリやＢＣＰ(事業継続計画)における重要な役割を担っています。

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 GSX 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.