WHITE PAPER: ENTERPRISE SOLUTIONS

symantec™

Veritas NetBackup™ Bare Metal Restore™ by Symantec

Best-of-Breed Server Recovery Using Veritas NetBackup™ Version 6.0

White Paper: Enterprise Solutions

Veritas NetBackup™ Bare Metal Restore™

Contents

Introduction

This paper describes Veritas NetBackup Bare Metal Restore (BMR), an option to NetBackup 6.0 that eliminates the need for disparate bare metal recovery methodologies and greatly improves the speed and simplicity of system recovery by providing a common methodology utilizing the normal backup data within NetBackup. When we say a solution is capable of bare metal recovery, we mean that the hardware onto which the system is being recovered can be devoid of an operating system or initialized disks.

Veritas NetBackup is the industry's leading enterprise data protection solution, providing customers with fast, reliable, backup and recovery strong enough for the data center. NetBackup can store client backup data on a large variety of tape and disk devices, and can protect that data by encryption, duplication, and off-site vaulting. NetBackup provides a variety of recovery capabilities for single files, groups of files, entire volumes, and specialized applications such as databases. And now, with the Bare Metal Restore option, NetBackup is able to easily recover the entire system from the normal backups.

With the Bare Metal Restore option, NetBackup 6.0 has become the first enterprise backup solution with a true integrated bare metal recovery option.

Bare Metal Restore avoids the common issues that other bare metal recovery solutions must face. In this paper, we will assess the common methods employed for bare metal system recovery and examine several key problems with these methods. We will then describe the Bare Metal Restore option to NetBackup and how it avoids these issues in a highly automated fashion.

The challenges of bare metal recovery

Why do we back up data? We back up data so that it can be recovered when we need it. Whether that is to fulfill requests for lost data, or for regulatory compliance, the data is backed up solely for the purpose of recovery.

When a server must be recovered from bare metal, the recovery process presents several challenges to the IT staff. Most IT staff would agree on the following major challenges to bare metal recovery:

- System recovery takes too long
- Non-integrated methods for system recovery are complex and require highly skilled staff
- Recovery of Windows® systems to different hardware is very difficult

- Recovery procedures and tools vary from platform to platform
- System configurations and changes are often not tracked

The bottom line is that system recovery is very complex and is often unsuccessful.

The problem with non-integrated methods

Enterprise data protection solutions like NetBackup have traditionally been very good at backing up and securing data. NetBackup uses a variety of backup methods, application agents, and advanced techniques. It provides a remotely available central management console to administer backup schedules, view reports, and monitor daily activity. NetBackup can scale to protect thousands of systems throughout the enterprise. It can store the data in a large variety of tape and disk devices, and protect that data through data duplication and off-site vaulting. Enterprise data protection solutions like NetBackup were designed to recover one or more, or even all, of the files within a file system. But for bare metal recovery capabilities, this is not sufficient. To use the data in the enterprise data protection solution to recover the system, you need a minimum of two basic elements:

1. The containers, such as the file systems or volumes, must be present to hold the recovered data
2. An operating system environment is required so that the recovery agent can function

With the Bare Metal Restore option, NetBackup easily fulfills these two basic needs. More than that, NetBackup has raised the bar for system recovery. It is a single solution that will automatically re-create the data containers and then populate those containers with the backup data. There is no special backup image other than the normal backup data. This integrated approach is so important for system recovery. Let's examine why.

There are several approaches to complete system recovery that can use the data in NetBackup or any enterprise data protection solution to recover the system; however, they do not integrate well with these solutions. Let's take a closer look at how this lack of integration will cause problems. These approaches can be summarized as follows:

- The operating system and application re-install, followed by a restore from the enterprise data protection solution
- Restoration from an image, followed by the restore from the enterprise data protection solution
- Homegrown or hybrid solutions that employ custom techniques

When you re-install the operating system and applications, you must re-introduce the customizations and configurations that were implemented for the system. This includes, but is not limited to, the following:

- Changes made to tunable OS parameters required for performance or application functionality
- Application license keys
- Application user and group IDs
- OS and application hot fixes
- Non-default customizations

Even with careful inspection and documentation of the production systems, it is difficult to identify these application and OS modifications. Without the re-introduction of these modifications, the system may not perform well, and applications may not function properly or may not function at all. The re-install and recovery process is technically tedious and time-consuming, and it requires very specific OS and application skills. It is difficult to scale during both normal daily operation and at recovery time.

System imaging technology addresses some if not most of these concerns, but the system images themselves are not well protected, tracked, or cataloged, nor are they performed often enough to meet the required recovery point objectives (RPOs). (Data created after the image was taken is lost.) It is not practical to use image backups on a daily basis to reduce the recovery point, because they are often full backups, and the data in the image is also protected by data protection solutions like NetBackup.

However, the image can be used to re-create a system with its containers so that an enterprise data protection solution can be used to bring the system up-to-date, thus reducing the recovery point objective to a more reasonable level. So restoration from an imaging solution, followed by a recovery from NetBackup, is often a method used to fulfill the system recovery needs. In general, imaging solutions preserve the user IDs and unique system configuration changes that have been performed, and in some cases they can recover the applications as well, avoiding the application installation steps. However, there are serious issues with this approach as well.

First, imaging technology has very limited capabilities. It cannot be used to recover all of the different file systems and volume managers used in the enterprise. You must also use different imaging solutions to cover all of the operating systems in the enterprise. Examples include the mksysb and savevg commands on IBM® AIX®, Flash Archive on Solaris™, or make_recovery on HPUX. There are several similarly capable imaging solutions for Windows. But, as stated earlier,

many imaging solutions do not protect or track the images, nor do they provide the means to ensure that the images are available in a timely fashion when required.

Second, and more importantly, the image itself is not coordinated with the enterprise backup. The two backups need to be coordinated or you will be faced with a number of issues during recovery.

The imaging solution will recover the system to the point in time when the image was taken. This includes the file systems, their mount points, and their sizes. File systems that were expanded after the image backup return to their original size. Likewise, file systems that were removed after the image backup reappear. Files and directories that were moved or deleted since the image was taken are back in their original locations. And finally, any files, directories, or file systems that were created after the image backup was taken will not be re-created.

Attempts to bring the system up-to-date with the latest backup can result in full file systems, out-of-date files, and multiple file copies in different locations. Cleaning up the mess afterward requires knowledge of when files or file systems were created or deleted, moved, and renamed. This is virtually impossible. The result is a system that is most certainly not the same, and the differences can cause problems that may not be known immediately. When this happens, we say the system is not coherent.

Finally, these imaging solutions are also platform-specific, requiring specialized skills and therefore preventing the use of common tools and processes to lower costs and reduce human error.

There are data protection solutions that provide a means to store these images inside the enterprise backup solution. In these solutions, the image is stored as an object in the enterprise data protection solution. While this addresses the availability and protection issues, it is not truly integrated and it does nothing to address the coherency issue.

The fact is that there is no way to ensure a coherent recovery of a system when it has been patched together with data that was backed up at different times with different backup applications that have no insight into each other's data or recovery methodologies.

With the problems presented above, it is perfectly understandable that companies with a sufficiently large IT staff or budget would develop their own bare metal recovery solutions to meet their unique requirements. These "homegrown" solutions require a great deal of expense and expertise to develop and maintain. The solutions must be evaluated when new versions of the OS are deployed or when new applications are installed. Documentation of the procedures and processes required must be maintained as well. The development staff must be available should situations arise in disaster recovery. However, disasters such as the World Trade Center

destruction on September 11, 2001, or the devastation of New Orleans by Hurricane Katrina in 2005 have shown clearly that it is not always possible to count on the availability of the development staff. All the expense of developing in-house solutions could be for naught if the solution cannot be made to work during
a major disaster.

Process maintenance

Regardless of the solution, to guarantee the recovery process, detailed recovery procedures must be created and maintained. This is a crucial point to consider. In general, as the amount of information required at recovery time increases, so does the difficulty of gathering, maintaining, and protecting this information, and the complexity of the procedures based upon this information.

This process maintenance places an extra burden on the IT staff. System changes are sometimes made due to specific problems after lengthy troubleshooting sessions in which several parameters may have been changed. These changes are too often done without thought given to the recovery process. Process maintenance is, therefore, difficult to enforce.

Dissimilar restore on Windows

Companies wishing to recover their Windows systems to different hardware face a daunting task. When a Windows system fails and needs to be replaced, the replacement hardware can differ in a number of ways:

- CPU speeds and number of CPUs
- Motherboard chipsets
- HAL (Hardware Abstraction Layer)
- Mass storage drivers
- Network interface cards

Recovery to hardware that differs in these ways can be difficult to impossible to perform—especially in a disaster recovery scenario. Solutions that do not handle recovery of Windows systems to different hardware cannot seriously be considered for use in disaster recovery. Sometimes, even two systems of the same exact model can be manufactured using different hardware.

Veritas NetBackup Bare Metal Restore

Bare Metal Restore was created to solve all of the issues described above. It allows NetBackup customers to completely recover their systems from their normal backups, without requiring separate system backups or reinstalls. In the event that a server loses its boot disk or suffers some other catastrophic failure, the Bare Metal Restore option will allow NetBackup to restore it to the exact configuration that existed as of the latest full or incremental backup. It can, in fact, recover to any point in time for which a valid backup image exists—either full or incremental, including synthetic backups.

The Bare Metal Restore configuration editor makes it possible to view and change the system configuration to automate recovery to completely different disk layouts or to recover Windows systems to completely different hardware using a common interface on the NetBackup administrative console.

Bare Metal Restore External Procedures extend flexibility by allowing user-supplied scripts or programs to be run at different points in the recovery. Recovery using Bare Metal Restore is swift and sure, with nothing left to chance or human error. Bare Metal Restore was developed with real-world functionality in mind.

Bare Metal Restore overview

Bare Metal Restore is integrated with NetBackup. During the scheduled backup, the NetBackup client runs the BMRSave process at the start of the backup. The BMRSave process automatically discovers the state of the system configuration a very small amount of data and stores this configuration in the Bare Metal Restore database. The BMRSave process is immediately followed by the normal NetBackup backup operation. The BMRSave process and the backup are thus tightly coupled.

At recovery time, the configuration information collected by BMRSave is pulled from the BMR database and is used to generate the recovery procedures that that will re-create the volumes and file systems and then populated them using the NetBackup backup data. No separate system image is used. As ordinary NetBackup data, they can be stored on a large variety of tape and disk devices, can be protected by duplication and off-site vaulting, and can be used for individual or multiple file restores.

Restoring a system with Bare Metal Restore is easy and highly automated. The entire process consists of running one command on the NetBackup master server and rebooting the client.

The following sections describe the Bare Metal Restore components and their functions, specifically, enabling Bare Metal Restore protection of the NetBackup clients, daily operations, creating a recovery environment, and finally, recovery scenarios.

Components of Bare Metal Restore

Bare Metal Restore master server component—The master server component is installed on the NetBackup master. It is the component that houses the Bare Metal Restore database where the client configurations are stored. The Bare Metal Restore master server component will generate the client-specific restore procedures to automate the recovery of the NetBackup client. The Bare Metal Restore master server component controls the recovery environment, allocating and de-allocating recovery resources for the restore process. It is also the component that provides for centralized Bare Metal Restore administration through the NetBackup Administration Console, and houses any user-provided external procedures.

The Bare Metal Restore Boot Server—One or more Bare Metal Restore Boot Servers are installed in the NetBackup environment. These can be installed on existing NetBackup clients or servers. The Boot Server component houses the Shared Resource Trees (SRTs), which provide the recovery environment for the client restorations. The SRT provides the client with the programs, libraries, and configuration data it needs to execute the recovery procedure.

The NetBackup client—The NetBackup client component collects the NetBackup client's configuration information when directed to do so by the NetBackup policy.

Figure 1 summarizes the NetBackup and Bare Metal Restore environment.

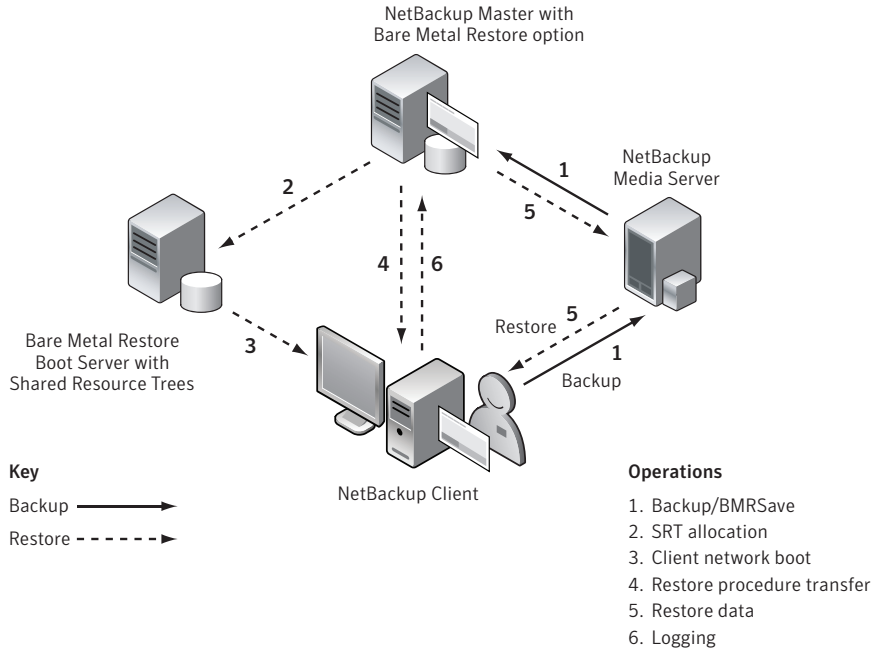

Figure 1. NetBackup with Bare Metal Restore

Enabling Bare Metal Restore protection of the NetBackup clients

License the Bare Metal Restore option on the NetBackup server, then either install the Bare Metal Restore master server component (UNIX/Linux) or initialize the Bare Metal Restore database (Windows). Next, edit the existing NetBackup policy, or create a new one for the clients to be protected. Perform a server-directed backup with the Bare Metal Restore-enabled policy. When the backup is completed, the client is protected.

Daily operations

There are no manual operations needed to protect the clients. The following automated operations occur whenever a scheduled backup is initiated from a policy where the Bare Metal Restore attribute is enabled:

1. A scheduled backup begins
2. The NetBackup client collects the configuration information, storing it locally on the NetBackup client
3. A copy of the NetBackup client configuration is then transferred to and stored on the NetBackup master server in the Bare Metal Restore database, replacing the previous configuration in the database
4. The normal backup is performed

The information gathered by BMRSave is also stored on the client and is backed up during the NetBackup backup that immediately follows. In this way, Bare Metal Restore ensures that the client's configuration data is synchronized with the corresponding NetBackup backup in cases when it is desirable to perform a point-in-time restore.

The restoration process

The Bare Metal Restore recovery process is highly automated and efficient. Bare Metal Restore is a single solution that performs system restoration across the major enterprise server platforms. The process involves two steps:

1. A prepare to restore operation
2. A network or media boot of the system

During the prepare to restore operation, a client configuration is selected. The NetBackup master digests the selected client configuration information and uses it to generate a custom restore procedure. This procedure is then executed by the client in the repair environment provided by the SRT or CD-based SRT. The restore procedure partitions and formats the disks and recovers the data from NetBackup onto the newly created file systems. The operating system being used in the recovery environment is running in a different location from the operating system being recovered. It is therefore not overwritten in this process, and does not interfere in the recovery of the original operating system and applications. After this process is complete, the client system is fully restored.

Bare Metal Restore speeds effective and efficient system recovery

The entire Bare Metal Restore process can be completed in minutes. No manual intervention is required, other than the initial boot, so many systems can be recovered by a small number of administrators and/or operators.

Bare Metal Restore imposes no requirements for additional network bandwidth beyond normal NetBackup requirements. The time required for the restoration is largely determined by network speed, NetBackup server performance, tape access times, and other environmental factors. With proper design of the network and NetBackup server configuration, Bare Metal Restore can scale up to completely restore very large sites in one or two days.

Bare Metal Restore imposes little or no additional storage requirements since it can use the normal NetBackup incremental backups for recovery.

Perhaps most important, Bare Metal Restore eliminates the need to manage multiple backup and restore methods. With Bare Metal Restore there is no need to perform redundant system backups or maintain client configuration information. As long as the normal NetBackup backups are taken, any Bare Metal Restore client can be completely recovered without additional effort, which results in a substantial savings of an administrator's time.

Advanced concepts and features

There are some unique and exceptionally practical features that are standard with Bare Metal Restore. These include point-in-time recovery, dissimilar disk restore (DDR), Windows dissimilar system restore (DSR), and External Procedures.

Point-in-time recovery

The default recovery is set to the latest backup. The Bare Metal Restore recovery uses the true image recovery capabilities of NetBackup to restore the file systems. NetBackup maintains the true image state of the system for each backup performed. To perform a recovery to a point in time of another backup, the Bare Metal Restore node of the NetBackup administrative interface is used to recall the Bare Metal Restore client configuration from NetBackup. A dialog is presented, allowing the administrator to choose the point in time from a list of known backup points. NetBackup then retrieves the Bare Metal Restore client configuration associated with this backup point. It places this configuration under the Bare Metal Restore client information in the administrative interface. This retrieved configuration is then used in the prepare to restore operation just as you would use the default (current) configuration.

Dissimilar disk restore

It often happens that the disks on the replacement system will differ from the disks on the original system. You will want to use dissimilar disk restore when:

- A physical disk was replaced with a different one
- The size of one or more disks has decreased and cannot contain the same volume arrangement
- The location of one or more disks has changed
- The number of disks has decreased and the original volume arrangement cannot be restored
- You need to change the layout and volumes for the restored system
- You want to restore only some of the disks or leave some of the volumes off during the system restore

You can also use dissimilar disk restore to:

- Resize a volume to place it on a larger or smaller disk
- Move a volume onto another disk
- Change the volume type—for example, change it from mirrored to a RAID 5 volume
- Create but not restore a volume

Windows dissimilar system restore

The recovery of Windows systems to different hardware is a very difficult task, and is fraught with error. Bare Metal Restore allows you to recover a system to hardware that is very different from the source system. The destination hardware can differ in a number of ways:

- Manufacturer and model
- Number and type of processors, motherboard chipsets, and associated changes such as different Hardware Abstraction Layers (HALs)
- Number and brand of video adapters
- Number and brand of network interface cards (NICs)
- Number and type of Fibre Channel Host Bus Adapters (HBAs)
- Number and type of mass storage controllers (MSDs)
- Number and size of disk drives (dissimilar disk restore—DDR—rules apply)
- TCP/IP and network configuration

Bare Metal Restore is frequently used to migrate Windows systems to new hardware. It can also recover a virtual system to physical hardware or to restore a physical system onto virtual hardware.

Bare Metal Restore External Procedures

Bare Metal Restore External Procedures offer opportunities to insert user-supplied custom processes to meet special needs during recovery of the system. There are specific points during the Bare Metal Restore recovery where an administrator can have Bare Metal Restore execute commands via a script or a program. This greatly enhances the functionality and flexibility of Bare Metal Restore. For example, it allows Bare Metal Restore to use a script supplied by the database administrator to recover a database that was excluded from the normal NetBackup backups, or it can be used to recover an exchange server using the NetBackup exchange agent in an external procedure.

Bare Metal Restore configuration concept and the Bare Metal Restore configuration editor

The DDR and the Windows DSR capabilities are made possible by a feature unique to NetBackup Bare Metal Restore known as the Client Configuration—commonly referred to as the "config." The Bare Metal Restore client config can be thought of as an abstraction of the system. It is stored as an entity on the NetBackup master server in the Bare Metal Restore database. The client's config maintained at backup time is named "current." The client config can be extensively edited using the Bare Metal Restore configuration editor. Windows disk and network drivers, client IP addresses, network routes, NetBackup client configuration, and disk volumes can be easily changed using the Bare Metal Restore configuration editor accessed through the NetBackup Administration console.

Since the configs are stored as independent entities in the Bare Metal Restore database, the original client need not be available for the editing to occur. As mentioned earlier, client configs are also saved in the backup data for each system, and can be retrieved from NetBackup to perform a point-in-time restore.

This concept of a client config is the key to understanding the capabilities of Bare Metal Restore. For example, it means that the administrator can decide onto which hardware the client will be recovered after the client suffers a catastrophic failure. It means that all of the changes required to bring the system onto new hardware can be done using a common interface in advance of the restore, so that the restore itself can be as automated as possible, requiring only minimal to no manual intervention at recovery time. This design lends itself extremely well to the pressures under which administrators find themselves during system recovery, and allows a single administrator to recover numerous systems simultaneously.

Veritas NetBackup leads the industry with innovative concepts and technologies, the concept of the client configuration as an editable entity alone revolutionizes the way disaster recovery is performed. In addition, it provides the basis of future, more powerful innovations in still further automation in dissimilar recovery and the mass server recoveries required for entire data centers.

Figure 2 is a screen shot of the Bare Metal Restore configuration editor. The navigation area is on the left side of the screen. Selection of one of the nodes in the navigation area displays the corresponding information editing panel to the right, allowing changes to be performed to the client config. The drivers node is shown in the screen shot. This screen allows the Windows drivers to be changed for recovery to dissimilar hardware.

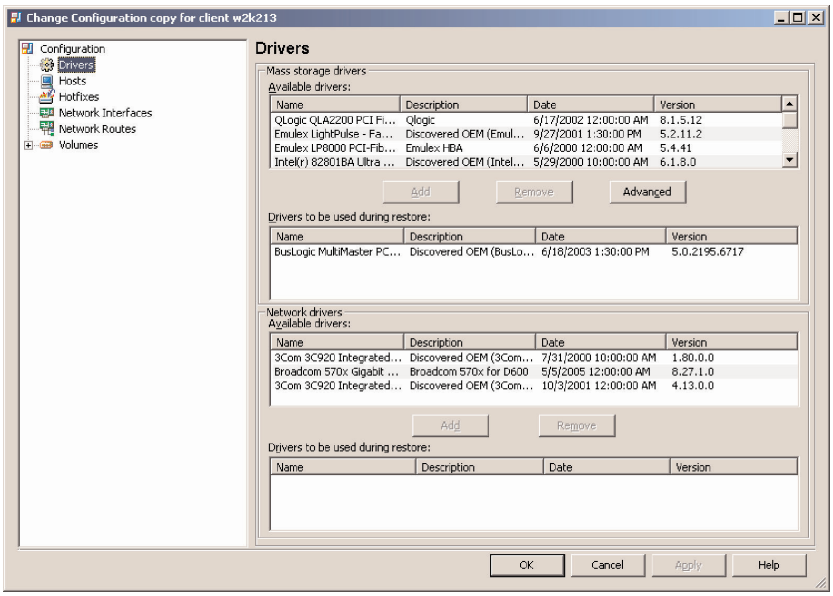

Figure 2. The drivers node in the Bare Metal Restore configuration editor

The Bare Metal Restore configuration editor is a standard feature of Veritas NetBackup Bare Metal Restore, and allows the extensive changes to be made that are necessary for recovery to systems that differ from the original system that was backed up. It allows these changes to be made in the database ahead of time, using a common interface so that recovery is as automated as possible. The resulting configuration is then referenced by the NetBackup master when the restore procedures are generated during the prepare to restore operation.

Summary

Bare Metal Restore provides the key element in extending NetBackup to provide complete system recovery. By allowing any system to be completely recovered from only its NetBackup backup, Bare Metal Restore eliminates redundant network and storage usage, saves labor, and provides users with unsurpassed confidence in their system's recovery capabilities.

The Bare Metal Restore configuration concept removes the complexity involved in recovering the different operating systems to different disks and different hardware. This common interface allows the extensive changes to disk layouts, network settings, and NetBackup configuration for any of the NetBackup clients and allows the insertion of Windows drivers for Windows systems to be recovered to dissimilar hardware.

Point-in-time recovery, in combination with incremental and synthetic backups, provides an unprecedented flexibility in bare metal recovery.

External procedures provide a means of customizing the recovery process to meet the needs of complex recovery scenarios.

The standard features of Bare Metal Restore such as the configuration editor, point-in-time recovery, and External Procedures are unequaled in the market today, and demonstrate the leadership of NetBackup in executing the most important part of backup—the restore.

About Symantec

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

09/06 10747369