

System Recovery—Breaking through the Dissimilar Hardware Restore Challenge

System Recovery—Breaking through the Dissimilar Hardware Restore Challenge

Contents

Hardware Failure is Inevitable	1
Hardware-Independent Restore—A Critical Component of System Recovery.....	2
Restore Anywhere for Hardware Migration and Hardware Repurposing.....	5
Preparing a New System for Migration.....	5
New Option for Meeting Strict Recovery Time Objectives (RTO) and Upping Disaster Tolerance	7
Conclusion.....	9

Hardware Failure is Inevitable

To combat data erosion and system failures, backup procedures must be designed to address a hardware failure in a timely, cost-effective manner. When hardware must be replaced, a rapid recovery solution is critical. In the event of hardware failure, a bare-metal recovery can be automated or manual. Each approach has distinct advantages.

Automated system recovery

Automated bare-metal recovery is designed for rapid, systematic recovery. With automation, procedures are more likely to be predictable and simple. The user will not require as much training, so this approach should also be more reliable than manual recovery. Automated recovery of a Windows® system does, however, have limitations. Because an operating system, with its unique configuration, is designed at the time of installation for a specific hardware device, a traditional automated recovery cannot take into account the dissimilar hardware components that are at the core of the new computer system.

The most problematic components are the Windows hardware abstraction layer (HAL), the kernel, and the mass storage controllers. When a Windows system boots, these three elements must be correctly assigned to the hardware otherwise Windows will not boot. It is less critical to resolve conflicts with other devices because, once loaded, Windows makes those devices easy to detect and install.

Manual system recovery

Because of the limitations of automated recovery regarding restoration to dissimilar hardware, many users choose to reinstall the operating system manually. In fact, in the past, when a key hardware component (storage controller, motherboard, processor, or HBA) failed, manual recovery was the only viable approach. When the operating system is reinstalled manually, each of these items is detected and installed in a clean environment. The drawback is that the system must be configured entirely from scratch, wasting precious resources - and service packs and hot fixes must also be applied.

Before data restoration can begin in a manual system recovery, applications must be installed and configured and system settings set to match company standards. The complexity of this process is beyond ad hoc management techniques, and it requires strict controls and procedures.

When preparing for bare-metal recovery to dissimilar hardware, users commonly keep a journal to account for the changes that have occurred on the computer. This manual method of record-keeping not only is tedious, but it often fails to account for many system changes, as well. In addition, some administrators make the effort to capture a system's most recent "cold image" on the rare occasion when that system can be taken offline. These steps amount to a significant effort in planning; moreover, the recovery process is extremely slow (see figure 1).

System Recovery—Breaking through the Dissimilar Hardware Restore Challenge

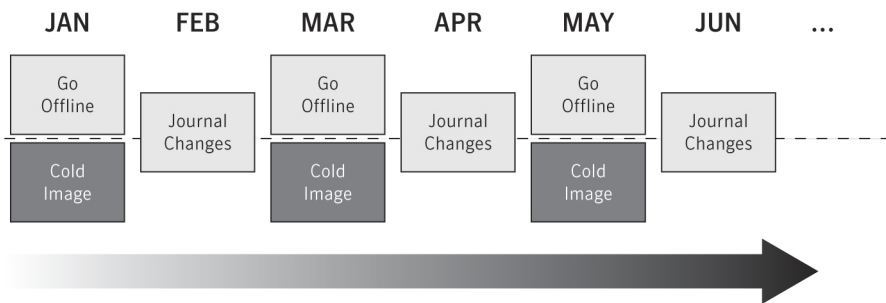


Figure 1. Manual recovery method

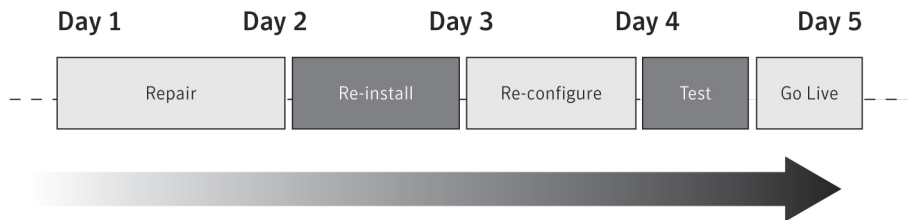


Figure 2. Typical recovery steps and time

Manual recovery is a multi-step process following a layered approach that is meant to restore the system as closely as possible to its pre-failure state (see figure 2). If cold images have been captured, the most recent one can be recovered as a starting point—but all changes since the last image capture must still be accounted for manually.

Duplicate hardware for disaster recovery

To hedge against hardware failure and still allow for automated system recovery, many organizations purchase duplicate hardware for the most critical computer systems. Imagine working under a recovery-time objective (RTO) that dictates full site recovery at an alternate site within a week, three days, or even faster. While this is not a universal condition, dissimilar hardware recovery is a concern for every administrator. As the RTO becomes more and more compressed, the problem of dissimilar hardware is compounded, and the cost is increased. Maintaining duplicate hardware for an entire site is so cost-prohibitive that only the most critical (and smallest percentage) of organizations can justify it.

When duplicate hardware is purchased, many system vendors cannot guarantee that even the same model will have the same components from one batch to the next. It is common for a manufacturer to put in a new storage controller or other components as updated versions become available. This practice has significant implications for corporate purchasing policies, because the only way to ensure that all of a company's computer systems have the same hardware components is to purchase all of them at once.

Hardware-Independent Restore—A Critical Component of System Recovery

As stated previously, restoration through layered reinstallation is a time-consuming process. Reinstallation of a typical Microsoft® Small Business Server with a small database application would take more than four hours (under constant vigilance and barring any mechanical setbacks). With Symantec Backup Exec™ System Recovery, the automatic process is just a couple of clicks away and can take 30 minutes or less. Backup Exec System Recovery protects against business

System Recovery—Breaking through the Dissimilar Hardware Restore Challenge

downtime and disaster with rapid, reliable backup and recovery and includes Restore Anyware™ technology, which allows organizations to quickly and easily restore systems to dissimilar hardware.

With the Restore Anyware capability in Symantec Backup Exec System Recovery, it doesn't matter what hardware the downed device is restored to. There is no need to layer a restoration because of hardware incompatibilities that may be detected during the restoration process. Restore Anyware technology properly replaces all critical system drivers during a routine restoration-and it launches Windows native plug-and-play capabilities to detect additional non-critical devices and peripherals. The result is a fully functioning computer system installed on whatever hardware is available at the time of recovery. The system can be restored to new hardware-or even to a virtual environment.

Restore Anyware capability enables recovery to dissimilar physical computers

When Symantec Backup Exec System Recovery was first released, it literally changed the way bare-metal system recovery was performed for Windows systems, making the process rapid, simple, and reliable. It offered the first image-based system recovery to dissimilar hardware on the market. With the Restore Anyware capability, recovery to dissimilar hardware is simple and reliable, so even the most problematic elements of a system are easy to handle. For example, a single-processor computer can be recovered to a multi-processor computer; SCSI storage can be recovered to SATA or SAS; and recovery to different HAL, chipset, and kernel models can be performed quickly and easily without manual intervention.

Using the Restore Anyware capability

Symantec Backup Exec System Recovery captures an entire system image - called a recovery point - that can be set up to occur automatically on a scheduled basis without any ongoing administrative intervention. These recovery points are captured "hot", meaning they occur while the Windows operating system is running and functioning normally, without the need to down the server first or boot into a pre-operating system mode. Two types of recovery points "base only" or "base with incremental" can be scheduled. Best practices suggest that a full system recovery point, called a base, be run during non-production hours or during times of lower system resource use. An incremental recovery point can be scheduled to run during production, depending on the size of the incremental file and the resource utilization settings for Symantec Backup Exec System Recovery.

Users should know which drivers their systems are using and whether they are supplied on the default Symantec™ Recovery Disk (SRD). The SRD is designed to recover all the computer systems in the user's environment. It contains all the storage, HAL, and kernel drivers that Windows Server 2008, Windows Server 2003, Windows 7, Windows Vista, and Windows® XP use when performing a new installation. Symantec has also included on the disk a large number of drivers that are not part of the standard Windows installation media. And in addition, the customizable SRD with Backup Exec System Recovery automatically harvests system drivers that are not already included on the SRD and allows administrators to add any necessary additional drivers to tailor a customized recovery environment to their unique hardware needs.

Recovering with Restore Anyware

When Symantec Backup Exec System Recovery performs a bare-metal restore, the SRD loads the necessary storage controller, HAL, kernel, and network drivers into a Windows-based environment at boot-up. Users then indicate the

System Recovery—Breaking through the Dissimilar Hardware Restore Challenge

desired recovery point and destination and select the option to restore to dissimilar hardware. The recovery proceeds to restore the entire system to the selected destination. Near the end of the recovery, the Restore Anyware process automatically updates the storage controller, HAL, kernel, and other critical drivers for the newly restored system. This process adds about 30 seconds to the recovery. If these drivers or components are not already on the CD, users will be prompted to supply them. The driver can then be placed in the same location as the recovery point, because the SRD already has access to this location, or they can be placed on a USB device which, when inserted, will be automatically detected by the Windows-based environment in which the recovery process is running. Accordingly, users can simply browse to the drivers and install them as they would in a native Windows driver installation.

After recovery, the newly restored system boots up on the new hardware. Restore Anyware initiates Windows Plug and Play to run during this first boot. Plug and Play takes approximately 10 to 15 minutes. Once it is completed, users can log in with either domain or local credentials and check the Device Manager for any non-critical components that Plug and Play did not detect.

Restore Anyware and recovery to virtual computer environments

In today's data centers, server and storage consolidation go hand in hand. Not only is central storage necessary for clustering and backup purposes, but centralized and consolidated servers are reducing the hardware complexity of clustered systems as well. The only way to consolidate servers in a realistic way is through virtual server technology. Virtual server technology - such as VMware, for example - is a software layer that enables several virtual servers to be positioned on a single physical server so that they can all share the same physical resources without affecting one another. Up to 64 virtual servers per physical server can be accommodated, reducing hardware costs for hot standby servers and controlling the total number of servers required. Instead of having multiple servers at a remote site, a single (albeit larger and faster) server can be deployed with multiple "virtual" hot standby servers running inside it (see table 1).

Table 1. Physical and virtual server comparison

Normal Server	Virtual Server		
Exchange	Exchange	SQL Server	Web Server
Windows	Windows	Windows	Windows
	Virtual Server Virtualization Layer		
Hardware Architecture	Windows for Physical Server		
	Hardware Architecture		

With Symantec Backup Exec System Recovery, users can convert seamlessly to virtual environments (and back again) using VMware ESX, ESXi or vSphere, VMware Server, VMware Workstation, Microsoft Virtual Server, and Microsoft Hyper-V 1.0 or Hyper-V Server 2008 R2 for greater flexibility in managing their recovery environment. Support for Citrix XenServer 5.x is also now available in Backup Exec System Recovery. Additionally, IT administrators can set a schedule for having physical recovery points (backups) converted to virtual systems, enabling immediate recovery.

Virtual conversion also provides a new world of flexibility in performing pre-flight testing of patches, application installations, configuration changes, and driver updates in the virtual environment before applying changes to production systems.

Restore Anyware for Hardware Migration and Hardware Repurposing

Migration is part of the lifecycle for Windows servers and desktops. When hardware becomes outdated and is replaced, the system must be migrated-using a process that is equivalent in many ways to a bare-metal recovery. It is even likely that a user's current migration strategy closely resembles that for bare-metal system recovery. The two processes share many of the same shortfalls. Using Symantec Backup Exec System Recovery in combination with the Restore Anyware capability offers an ideal solution to hardware migration woes; moreover, if it is already being used for bare-metal system recovery, this combination is a natural centerpiece for any hardware migration strategy.

Hardware migration strategies

Any migration procedure should define along with the reasons for the migration-the steps involved, the fallback precautions, and any other important factors that can influence the migration process.

Two conflicting philosophies influence technology upgrades. The first is, "If it isn't broke, don't fix it." Obviously, if an organization has a functional, easy-to-use, well-designed server infrastructure, the idea of upgrading may not be so appealing. The second philosophy is, "Those who fail to upgrade their technologies perish." But that means restoring each server to new hardware with new drivers that have their own peculiarities, and then cascading hardware upgrades "down the line" until all servers on the list are upgraded to the next highest level, with the bottom server being "dropped out of the pool."

No matter which approach is taken, Restore Anyware is an invaluable aid to a hardware migration plan. Hardware failures and upgrades are both inevitable - but with the Restore Anyware capability of Backup Exec System Recovery, users are well prepared to deal with either.

Preparing a New System for Migration

Any migration procedure involves planning and pilot-testing the migration, executing it, and allowing a short interval for rollbacks, if necessary. Following are a few key steps in the process, demonstrating how Symantec Backup Exec System Recovery with Restore Anyware can help (see figure 3):

1. Ensure that the SRD recognizes the storage controller(s) and NIC(s) in the new server and that there is a backup of the native state of the new server. Install the Symantec Backup Exec System Recovery software onto the new server. During this process, the new computer's hardware can be checked for any drivers that the SRD CD may lack.
2. If new drivers are needed, it's easy using a wizard-driven interface to create a customized recovery CD tailored to the specific environment.
3. With an updated, customized SRD, create a base recovery point for the new server and then store it in the recovery point warehouse, along with the suggested configuration information worksheet for the server.

System Recovery—Breaking through the Dissimilar Hardware Restore Challenge

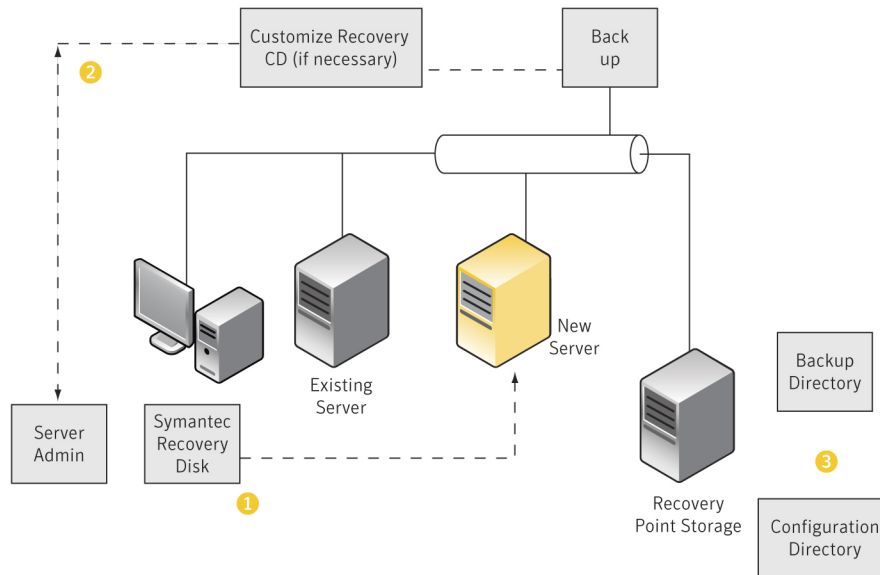


Figure 3. Planning process for system migration

With the new system prepared in this way, it is possible to boot it from the CD if necessary, access configuration data for rebuilding any portion of the system, or revert to an established baseline recovery point if problems are encountered during the migration.

The advantage of a migration plan is that all new hardware drivers can easily be added to the master SRD, and the SRD can then be used on all subsequent servers already in place.

Repurposing hardware for optimal resource utilization

Much like hardware migration, repurposing can be a valuable exercise when some servers are being underutilized and others overworked. At one time or another, most IT organizations must repurpose hardware to optimize their use of existing resources.

Integrating Symantec Backup Exec System Recovery and its Restore Anywhere capability into the hardware repurposing process helps to minimize the time it takes to migrate from one platform to the next. Manual reconfiguration of a server is, as mentioned previously, a multi-layer process that may involve up to 90 steps - and demand several hours of an administrator's time.

Symantec Backup Exec System Recovery offers a four-step process that can reduce this time by up to 80 percent:

1. Boot the server to be repurposed.
2. Ensure that the BIOS and RAID configurations are set properly for the new system. (Note: Steps 1 and 2 should take less than five minutes.)
3. Locate the recovery point of the server being migrated from, and restore it to the new server.
4. Back up the new server to a new directory, creating a recovery point in case there is a need to revert to this point on the new server. Do not delete the old recovery point before confirming a successful migration.

System Recovery—Breaking through the Dissimilar Hardware Restore Challenge

Even better, the preceding steps do not have to be journaled and they can be identically replicated every time, with no special training required (see figure 4).

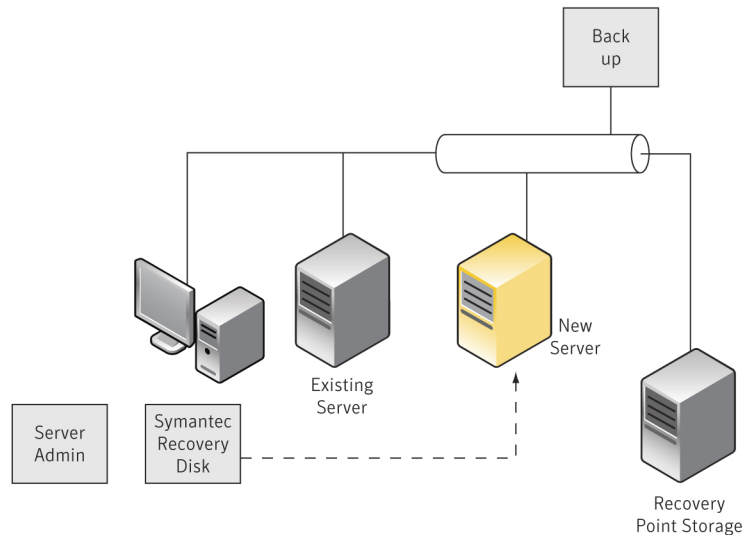


Figure 4. Upgrade planning sketchbook—server repurposing

New Option for Meeting Strict Recovery Time Objectives (RTO) and Upping Disaster Tolerance

Existing technology solutions provide many types of failover for the most critical systems, but rapid system recovery solutions are scarce, and the expense of high-end failover technologies cannot be justified in most cases. Restore Anyware technology offers a new option for meeting stringent recovery-time objectives that do not require immediate failover. This is a much-needed recovery solution for systems that do not warrant the high cost of clustering or mirror sites - but that must nonetheless be recoverable in minutes, not hours or days. One factor in determining the appropriate solution is disaster tolerance.

Defining disaster tolerance

For many organizations, recovery-time objectives are short and do not allow sufficient time to order new computers and wait for them to arrive. To shorten recovery time, a system's disaster tolerance (its ability to survive a disaster, most often from multiple points of failure—perhaps even the loss of an entire data center or facility and all its functions) must be increased. How can a server be made disaster tolerant? The answer depends on the desired degree of tolerance to multiple failures, which in turn has financial ramifications, because the most fault-resilient systems are also the most expensive. Each level of protection has its own requirements and associated costs and benefits. Figure 5 shows a common mirroring scenario.

System Recovery—Breaking through the Dissimilar Hardware Restore Challenge

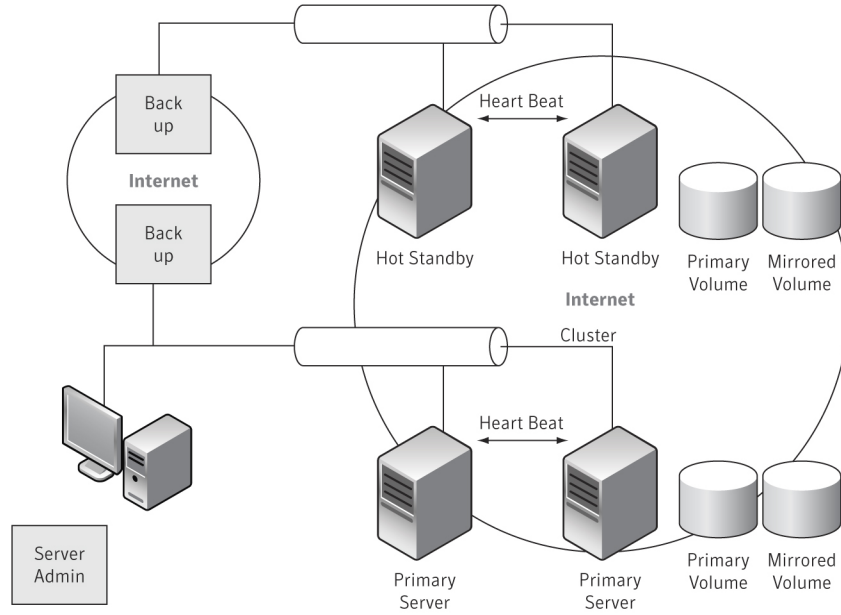


Figure 5. Server backup sketchbook—backing up the mirrored server

What is your recovery-time objective (RTO)?

Your RTO, the maximum amount of time it should take to bring a service back online, will determine which of the approaches presented in table 2 you should consider.

Table 2. Criticality vs. cost

Criticality	Recovery timeframe	Cost
Low	Systems do not need to be available for days or weeks; there is time to perform traditional manual or automated system reinstallation and recovery.	\$
Medium	Systems and replica sites must be available in minutes or hours; hardware does not need to be similar, or virtual systems can be used.	\$\$
High	Systems must fail-over immediately; replica sites with the same or similar hardware must be available for failover.	\$\$\$\$\$

Many systems fit into the medium criticality category but lack a viable technology solution that makes budgetary sense. The missing capability is a full, rapid recovery to dissimilar hardware. Symantec Backup Exec System Recovery, with its Restore Anyware capability, is the answer for systems that must be recovered in minutes, not hours or days, to whatever hardware or virtual system is available. Using Symantec Backup Exec System Recovery, administrators can achieve medium-criticality objectives while keeping costs comparable to a low-criticality approach.

Conclusion

Symantec Backup Exec System Recovery, with its Restore Anywhere capability, can dramatically change the way organizations perform a wide range of IT tasks, including bare-metal system recovery, restoration to dissimilar hardware or virtual environments, hardware migration, repurposing, change management, and site-level recovery. Disk-to-disk technology enables organizations to meet ambitious recovery-time objectives. And, with breakthrough Restore Anywhere functionality, Symantec Backup Exec System Recovery provides even greater flexibility in recovering systems, enabling the user to reduce recovery times and saves significant hardware investments.

For more information about Symantec Backup Exec System Recovery and the Restore Anywhere technology, visit

www.backupexec.com/besr.

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2009 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.
10/2009 12067948-3