



System Recovery

Meeting the Dissimilar Hardware
Restore Challenge

System Recovery

Meeting the Dissimilar Hardware

Restore Challenge

Contents

Hardware failure is inevitable	4
Automated system recovery	4
Manual system recovery	4
Duplicate hardware for disaster recovery	5
Hardware-independent restore—a critical component of system recovery	6
Restore Anywhere capability enables recovery to dissimilar physical computers	6
Using the Restore Anywhere Capability	7
Recovering with Restore Anywhere	7
Restore Anywhere and recovery to virtual computer environments	8
Restore Anywhere for hardware migration and hardware repurposing	9
Hardware migration strategies	9
Preparing a new system for migration	9
Repurposing hardware for optimal resource utilization	11
New option for meeting strict RTOs and upping disaster tolerance	12
Defining disaster tolerance	12
What is your recovery time objective?	13
Restoring an Active Directory domain controller and Exchange Server	13
Best practices for Backup Exec System Recovery and Active Directory	14
Conclusion	15

System Recovery: Meeting the Dissimilar Hardware Restore Challenge

Hardware failure is inevitable

To combat data erosion and system failures, backup procedures must be designed to address the eventual failure of a computer's hardware, which is finite and transitory, as it is juggled from one storage device to another. System failures that involve hardware must be addressed in a timely, cost-effective manner. Even if the hardware must be replaced, the need for a rapid system recovery solution does exist. In the event of hardware failure, a bare metal recovery can be automated or manual, with each approach having 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. Automated Windows® system recovery does, however, have limitations. Because an operating system, with its unique configuration, is designed at the time of installation for a specific hardware device, an automated recovery cannot account for dissimilar hardware components at the core of the new computer system.

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

Manual system recovery

Because of the dissimilar hardware limitations of an automated recovery, many users choose to reinstall the operating system manually. In the past, when a key hardware component failed (storage controller, motherboard, processor, or HBA), 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 be applied.

Before data restoration can begin, 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 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 bookkeeping is tedious and often fails to account for many system changes. In addition, some administrators capture the most recent "cold image" of the system during the infrequent occasions

System Recovery: Meeting the Dissimilar Hardware Restore Challenge

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).

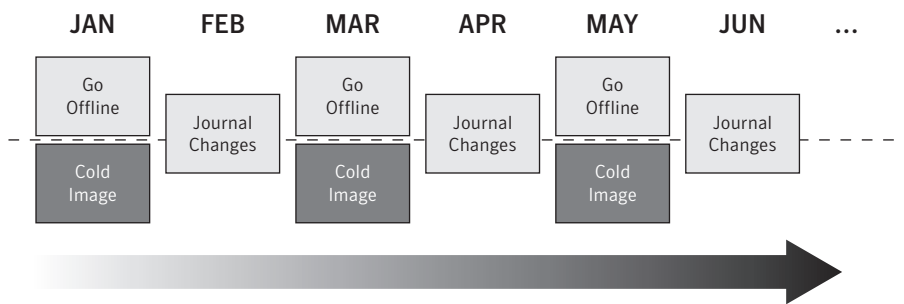


Figure 1. Manual recovery method

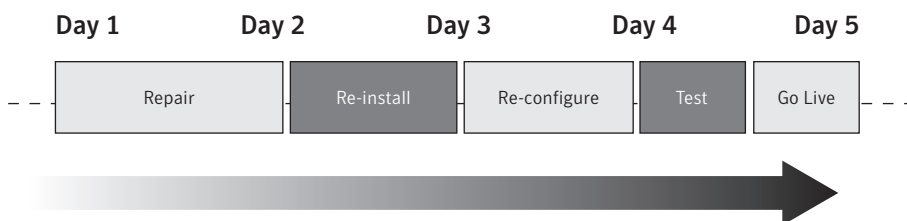


Figure 2. Typical recovery steps and time

Manual recovery relies on multiple steps following a layered approach that is meant to restore the system as close as possible to its pre-failure state. If cold images were captured, the most recent one can be recovered as a starting point, but all changes since the last image 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 computers. Imagine working under a recovery time objective (RTO) that dictates full site recovery at an alternate site within a week, three days, or even sooner. While this is not a universal condition, dissimilar hardware recovery is a concern for every administrator. As the RTO becomes 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 systems can justify it.

System Recovery: Meeting the Dissimilar Hardware Restore Challenge

When purchasing duplicate hardware, system vendors often 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 change a storage controller or other component as updated versions become available. This practice has implications for corporate purchasing policies because computers must be purchased all at once to assure that they have the same hardware components.

Hardware-independent restore—a critical component of system recovery

As stated previously, restoration through layered reinstallation is a time-consuming process. A typical Microsoft® Small Business Server with a small database application would take over four hours to reinstall (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 is the gold standard in complete Windows system recovery and includes Restore Anyware technology, which allows organizations to quickly and easily restore systems to dissimilar hardware.

With the Restore Anyware™ capability in Backup Exec System Recovery, it doesn't matter which hardware the downed device is restored to. There is no need to layer a restoration because of hardware incompatibilities detected during the restoration process. Restore Anyware technology properly replaces all critical system drivers during a routine restoration and launches Windows native plug-and-play capabilities to detect additional non-critical devices and peripherals. The result is a fully functioning computer system on whatever hardware is available at the time of recovery. The system can be restored to new hardware as well as 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 it rapid, simple, and reliable. It offered the first image-based dissimilar hardware system recovery 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 multiprocessor computer; SCSI can be recovered to SATA or SAS storage; and recovery to different HAL, chipset, and kernel models can be performed quickly and easily without manual intervention.

System Recovery: Meeting the Dissimilar Hardware Restore Challenge

Using the Restore Anyware Capability

Backup Exec System Recovery captures an entire system image, called a recovery point, which can be set up in a scheduled job to occur automatically without any continuous administrative intervention. Two types of recovery points—base only or base with incrementals—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. Incrementals can be scheduled to run during production times, depending on the size of incrementals and the resource utilization settings for 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 computers in the user's environment. It contains all the storage, HAL, and kernel drivers that Windows Server® 2003 and Windows XP use when performing a new installation. Symantec has also included a large number of drivers on the CD that are not part of the standard Windows installation media. In addition, the new customizable SRD with Backup Exec System Recovery 7.0 automatically harvests system drivers not already included on the SRD and allows administrators to add additional drivers for a customized recovery environment tailored to meet your unique hardware needs if necessary.

Recovering with Restore Anyware

When Backup Exec System Recovery performs a bare metal restore, at boot-up the SRD loads the necessary storage controller, HAL, kernel, and network drivers into a Windows-based environment. Users then select the desired recovery point and destination and select the option to restore to dissimilar hardware. The recovery proceeds to restore the entire system to unallocated space on the selected hard drive. Near the end of the recovery, the Restore Anyware process automatically updates the storage controller, HAL, kernel, and other critical drivers for the system that was just restored. 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. From there, users 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

System Recovery: Meeting the Dissimilar Hardware Restore Challenge

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 Anywhere and recovery to virtual computer environments

Server and storage consolidation go hand in hand in today's data centers. Not only is central storage necessary for clustering and backup purposes, but also centralized and consolidated servers are reducing the hardware complexity of clustered systems. The only way to consolidate servers in a realistic way is through virtual server technology. Virtual server technology such as VMware is a software layer that enables several virtual servers to be positioned on a single physical server so that each can 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 number of servers. 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
Hardware Architecture	Virtual Server Virtualization Layer		
	Windows for Physical Server		
	Hardware Architecture		

With Backup Exec System Recovery 7.0, users can convert to virtual environments seamlessly (and back again) using VMware ESX, VMware Server (formerly GSX Server), VMware Workstation, and Microsoft Virtual Server, allowing greater flexibility in managing recovery environments.

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.

System Recovery: Meeting the Dissimilar Hardware Restore Challenge

Restore Anyware for hardware migration and hardware repurposing

Migration is part of the life cycle for Windows servers and desktops. When hardware becomes outdated and is replaced, the system must be migrated, a process 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 Backup Exec System Recovery with the Restore Anyware capability is an ideal solution to hardware migration woes; moreover, if it is already being used for bare metal system recovery, it is a natural centerpiece for any hardware migration strategy.

Hardware migration strategies

Any migration procedure should define the reasons for migration, steps involved, fallback precautions, and other important factors that can influence the migration process. Two conflicting philosophies influence technology upgrades. The first is, "If it ain'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 having 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 invaluable to a hardware migration plan. Hardware failures and upgrades are 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 planning a short interval for rollbacks, if necessary. Following are a few key steps in the process, which demonstrate 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 Backup Exec System Recovery

System Recovery: Meeting the Dissimilar Hardware Restore Challenge

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, you can easily create a customized recovery CD tailored for your environment using a wizard-driven interface; or if necessary, send a request to Symantec Support, which will update the CD or provide you with the steps to follow.
3. With an updated customized SRD, create a base recovery point of the new server and then store it in the recovery point warehouse, along with the suggested configuration information worksheet for the server.

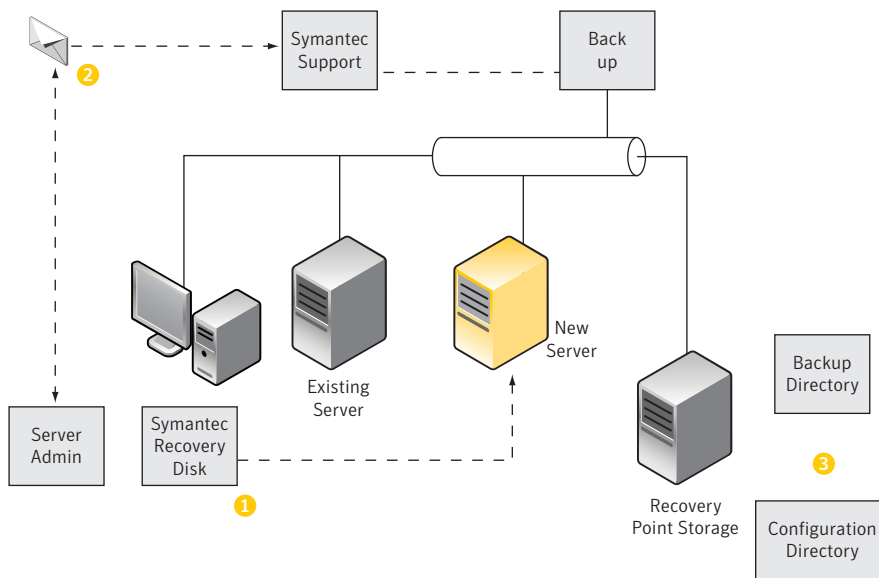


Figure 3. Planning process for system migration

By preparing the new system in this way, you can boot up from the CD if necessary, access configuration data for rebuilding any portion of the system, and revert to an established baseline recovery point if problems are encountered during migration.

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

System Recovery: Meeting the Dissimilar Hardware Restore Challenge

Repurposing hardware for optimal resource utilization

Similar to hardware migration, repurposing can be a valuable exercise when some servers are being underutilized and others overutilized. Most IT organizations have to repurpose hardware at one time or another to optimize their use of existing resources.

Integrating Backup Exec System Recovery and its Restore Anywhere capability into the hardware repurposing process helps ensure that your time for migrating from one platform to the next will be minimal. As mentioned previously, manual reconfiguration of a server is a multilayer process (involving possibly 90 steps) that can demand several hours of an administrator's time. Backup Exec System Recovery's four-step process reduces this time by up to 80 percent. More important, the steps do not have to be journaled and can be replicated identically every time with no special training (see Figure 4):

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 from the server from which you are migrating and restore it to the new server.
4. Back up the new server to a new directory, creating a recovery point in case you need to revert to this point on the new server. Do not delete the old recovery point before confirming successful migration.

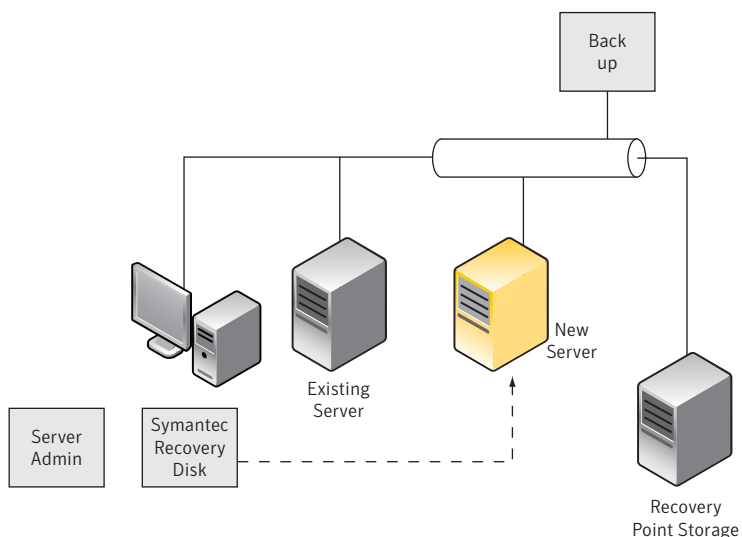


Figure 4. Upgrade planning sketchbook—server repurposing

System Recovery: Meeting the Dissimilar Hardware Restore Challenge

New option for meeting strict RTOs and upping disaster tolerance

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

Defining disaster tolerance

For many organizations, recovery time objectives are too short and do not allow for the time it takes to order new computers and wait for them to arrive. To shorten recovery time, the system's disaster tolerance (its ability to survive a disaster, most often from multiple points of failure—perhaps 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.

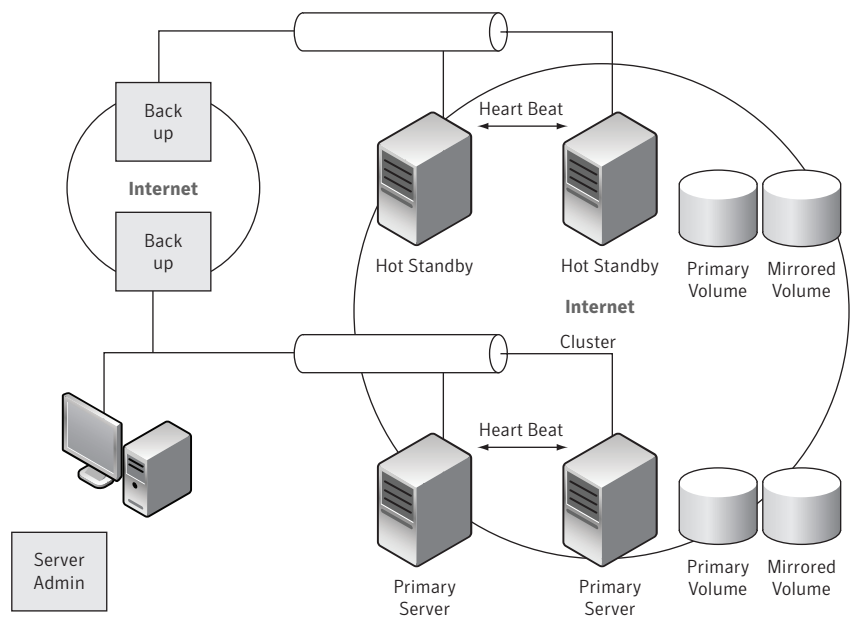


Figure 5. Server backup sketchbook—backing up the mirrored server

System Recovery: Meeting the Dissimilar Hardware Restore Challenge

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 versus cost

Criticality	Recovery time frame	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. 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 Backup Exec System Recovery, administrators can achieve medium-criticality objectives while maintaining costs that are comparable to low-criticality approaches (after factoring in the manpower needed for manual reinstallation).

Restoring an Active Directory domain controller and Exchange Server

A domain controller running on Windows Server 2003 with Volume Shadow Services (VSS) enabled can be backed up and restored to dissimilar hardware using Backup Exec System Recovery. Backup Exec System Recovery interacts with VSS to prepare the domain controller and the Active Directory database to be backed up. Note: Running with VSS disabled is not supported and will cause domain controller failures upon restoration.

Microsoft states that there are two methods for an Active Directory–aware application to back up a domain controller:

- Use the legacy application programming interfaces (APIs) (Ntbackup).
- Use the VSS APIs to flag the Active Directory as a backup copy, causing it to request a new invocation ID upon restoration.

Backup Exec System Recovery uses the second method for Windows Server 2003 with VSS (see <http://support.microsoft.com/kb/875495/en-us>). Physical and virtual methodology is the same. The steps outlined in the next section can help ensure a successful transition.

System Recovery: Meeting the Dissimilar Hardware Restore Challenge

Best practices for Backup Exec System Recovery and Active Directory

Backup Exec System Recovery follows the best practices and recommended procedures referenced in the Microsoft Knowledge Base and TechNet (such vigilance is necessary to ensure clarification of conflicting messages surrounding this subject).

Backup Exec System Recovery with the Restore Anywhere feature can be used to back up and restore a Windows Server 2003 Active Directory domain controller to its original or a dissimilar hardware configuration. It can also be used to back up and restore a Windows 2000 Server Active Directory domain controller to its original hardware configuration.

Attention to detail is important when performing backup and recovery operations with Backup Exec System Recovery. The following guidelines can help ensure success:

- The domain controller backup image or recovery point cannot be older than the tombstone lifetime (the number of days before a deleted object is removed from the directory services). This helps remove objects from replicated servers and prevents restores from reintroducing a deleted object. The tombstone lifetime is stored in the Directory Service object in the configuration NIC. For Windows 2000 Server and Windows Server 2003, the default tombstone lifetime is 60 days. Active Directory domain images should be taken frequently (more than once a month). See http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adschema/adschema/a_tombstonelifetime.asp.
- The backup image or recovery point of a domain controller cannot be older than two times the maximum machine account password age. A maximum password age determines the number of days a password can be used before the system requires it to be changed. By default, this setting is defined in the Default Domain Group Policy Object (GPO) and in the local security policy of workstations and servers with a value of 30. See <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gp/501.asp%20also%20see%20KB%20175468>.
- Newly promoted domain controllers use a default machine account before they establish a valid unique machine account. Allow the Active Directory domain controller to run for at least 24 hours prior to taking the first backup image or recovery point to help ensure the machine account has been properly established.
- Check a newly promoted or a restored domain controller for consistency before creating the first backup. Contact Symantec Support for more information on performing this check.

System Recovery: Meeting the Dissimilar Hardware Restore Challenge

- An image or recovery point of all the active disk volumes on a domain controller must be created and restored at the same time to preserve the synchronization of the domain controller's data. Select all the domain controller's volumes when creating the backup schedule job.
- When restoring a tree or the entire forest in a server forest environment, be sure to restore from the top down to maintain domain integrity.

Conclusion

The Backup Exec System Recovery Restore Anyware capability can dramatically change the way organizations perform a wide range of IT tasks, including bare metal system recovery, restoration to 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 Anyware functionality, Backup Exec System Recovery provides even greater flexibility in recovering systems, enabling the user to reduce recovery times and save significant hardware investments.

For more information about Backup Exec System Recovery and the Restore Anyware technology, visit www.backupexec.com.

About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world.

The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 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

Copyright © 2007 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and Backup Exec are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Microsoft, Windows, and Windows Server are registered trademarks of Microsoft Corporation in the United States and other countries. Other names may be trademarks of their respective owners. Printed in the U.S.A.
03/07 12067948