VERITAS Backup Exec™

for Windows NT/2000

Intelligent Disaster Recovery

VERITAS

BUSINESS WITHOUT INTERRUPTION™

Table of Contents

Whom to contact
If you have questions regarding Backup Exec, please contact:

VERITAS® Software Corp.
North American Sales Headquarters
400 International Parkway
Heathrow, FL 32746
1-800-327-2232 (US and Canada)
407-531-7501 (Outside the US)

Overview

When a network server fails, due to human error, hardware failure or a major disaster, the system must be carefully recovered before the applications and backed-up data can be restored.

Disaster recovery technology strategically complements backup/restore technology. Whereas the primary purpose of backup/restore is to restore applications and data, the primary purpose of disaster recovery is to restore the computing environment itself. Backup/restore assumes that a computing environment exists that will support data recovery. Disaster recovery ensures that the environment is available and minimizes the amount of time required to bring network systems back to full functionality.

Prior to the development of automated disaster recovery technology, manual disaster recovery had been labor intensive, vulnerable to human error, and a lengthy process, costly in both productivity and loss of revenue. Moreover, manual disaster recovery often fails because of a lack of preparation, poorly documented configuration data, and lack of a formal process to complete the task. Now, changes in the operating system increase the need for a uniform, automated process to secure the operating environment. Windows 2000 has several components that must be backed up together that are easiest defined as System State. Critical to the system recovery is the restoration of the System State, which should replace boot files first and commit the system hive of the registry as a final step in the process. Backup Exec™ provides full protection for Windows 2000 System State, which includes:

- Registry
- COM+ Class Registration database
- Boot and system files
- Certificate Services database (if the server is operating as a certificate server)
- Active Directory (if the server is a domain controller)
- SYSVOl- System Volume (if the server is a domain controller)
- Cluster quorum

Proper handling of backup and restoration of System State is key to the successful recovery of any Windows 2000 system; therefore an automated disaster recovery solution is ideal for the complex process of recovering any Windows 2000 or Windows NT 4 system.

Point-in-Time Disaster Recovery

Through the development of specialized applications for Microsoft Windows NT/2000 networks, VERITAS® has simplified and automated the process of preparing for and recovering from a point-in-time disaster. Using the VERITAS Backup Exec for Windows NT/2000 Intelligent Disaster Recovery™ (IDR) Option, network servers and application servers, such as those used for Microsoft Exchange or SQL Server, are quickly and easily recovered to the point of the last backup, complete with the identical configuration of the operating system, user profiles, applications and data. Unique to IDR is the ability to recover to the last incremental, differential or working set backup, not just the last full backup, as is the case with other disaster recovery products. As a result, local and remote systems and data are recovered to a point in time closer to the actual disaster than other products, and the recovery process takes less time.

IDR also provides a simple and flexible way to modify system configuration during recovery for customized configurations of fault-tolerant disk mirroring, disk volumes and others. This includes Backup Exec's unique ability to deal with hardware changes during the disaster recovery procedure. With Backup Exec, there is no requirement to have like hard drives, adapters and such for a completed Intelligent Disaster Recovery operation.

IDR is ideal for both pure and mixed Windows NT and Windows 2000 environments. It allows users to recover Windows NT 4.0 with Service Pack 3 or later Enterprise, Server, Small Business Server, Terminal Server, and Workstation editions and Windows 2000 Professional, Server, Advanced Server and Datacenter editions.

By empowering system administrators to quickly recover network servers to the point of the last incremental, differential or working set backup, Intelligent Disaster Recovery improves data integrity, increases overall system reliability and reduces total cost of ownership.

This paper first compares a manual disaster recovery process with an automated and integrated (thus, "intelligent") disaster recovery approach, then presents the steps required to prepare for and recover from a disaster using the Backup Exec Intelligent Disaster Recovery options for Windows NT/2000.

Manual Disaster Recovery is Time-Consuming and Technically Difficult

Without an automated, integrated solution, the unprepared user or system administrator faces a lengthy and arduous process to revive a failed system. The process is complex and can take hours because it involves a series of manual steps:

- Repairing or replacing the failed hard disk or equipment
- Collecting critical system configuration information (assuming it's documented) and recovery media
- Manually re-partitioning and formatting the hard disk
- Manually reinstalling the operating system
- Manually reinstalling updates, drivers, profiles, etc.
- Manually reinstalling the backup application
- Identifying and finding the last backup tapes
- Re-cataloging the backup tapes
- Restoring the data and applications on the backup tapes

Manual Disaster Recovery is Prone to Human Error

Any manual process is prone to human error. Pitfalls along the way to disaster recovery threaten to extend this painful process even further. Mistaken steps can nullify all the work up to that point, forcing the user, system administrator or consultant to spend even more time.

For example, the administrator may not realize that the hard disc(s) has been re-partitioned incorrectly until the very end, when the backup tapes need to be restored. Then they may realize that restoring the data would cause data errors, or applications to crash. There is no choice but to repeat the entire process, this time partitioning the drive correctly. Or, the administrator may not realize until after the data has been restored that the wrong backup tape was used. Even worse, backups may not have been kept current, and data must be re-input.

Disadvantages of Manual Disaster Recovery Process

There are many disadvantages to the manual process. Not least are the many hours of valuable time for the user, system administrator or consultant to first recover and then restore a network server. As we've discussed, the process is riddled with complexity and prone to unexpected results.

More importantly, during the recovery/restore process, the server is unavailable. When the failed system is a mission-critical server running business applications that the organization depends on daily, this can seriously impact the business and its revenue, not to mention individual productivity of all those who rely on the server. Even if the failure affects only a single workstation, the productivity impact on the user and the business can be significant.

Intelligent Disaster Recovery Automates and Integrates the Process

VERITAS takes a new approach with Intelligent Disaster Recovery: automating the disaster recovery function and closely integrating it with the backup/restore functions of Backup Exec. Integration with Backup Exec provides a more intelligent solution that enables quick and easy recovery of local and remote Windows NT/2000 servers to the point of the last backup. Failed systems are fully recovered, complete with the identical configuration of the operating system, user profiles, updates, applications and data.

Integrated Automation Minimizes Human Error

Since Intelligent Disaster Recovery is highly automated, it minimizes human intervention, and therefore the possibility of human error. Moreover, Intelligent Disaster Recovery integrates recovery and backup/restore to provide an automated solution that:

- reduces system administration by integrating two typically separate processes
- minimizes downtime through intelligent and automated system recovery
- reduces the impact on personal productivity and business processes
- reduces the total cost of ownership
- simplifies the highly complex technical procedure of disaster recovery

For example, unlike the manual process described previously, the system administrator does not need to know the details of network configurations, volume partition sizes, user profiles, etc. All configuration data is automatically protected by the backup function and is available to the disaster recovery engine when needed. By eliminating the need for human intervention, Intelligent Disaster Recovery ensures that the system is recovered accurately.

How Intelligent Disaster Recovery Works

VERITAS has developed the Intelligent Disaster Recovery Option to be used with Backup Exec for Windows NT/2000 and Microsoft's Windows NT and Windows 2000 operating systems. There are unique challenges in protecting these environments that we will discuss. First we will describe the three basic phases of implementing IDR in the Windows NT or Windows 2000 environment, and then we will describe the simple steps required to implement and recover from a disaster using IDR.

Intelligent Disaster Recovery is implemented in two phases, the first being preparation of the disaster recovery media. This media can be diskettes, CD-R/W or bootable tape (supported h/w only*), then, in the event of a disaster, recovering the network server to the point of the last backup. Upon initial release of Backup Exec for Windows NT/2000 version 8.0, support for CD-R/W and bootable tape will be for Windows NT 4 environments only, due to boot sequence differences with Windows 2000. A future update of Backup Exec for Windows NT/2000 will incorporate support for CD-R/W and bootable tape for recovery of Windows 2000 servers and workstations.

**An example would be HP's OBDR (One Button Disaster Recovery) DDS-3/4 drives*

Users should be aware that backup servers cannot completely protect remote Windows 2000 servers or workstations unless the Backup Exec Agent Accelerator for Windows NT/2000 is installed and running on each remote Windows 2000 server or workstation to be protected.

Phase One: Initial Preparation of Disaster Recovery Media

The process of installing Intelligent Disaster Recovery results in the creation of a series of diskettes, CD or tape that contains a recovery engine, required operating system components and configuration data. Together, this information will be used to boot a failed system and initiate the automated disaster recovery process.

Phase Two: Recovery of the Failed Server Following a Disaster

Faced with a failed server, the system administrator or consultant repairs or replaces the failed system or components; then uses IDR in conjunction with Backup Exec's restore function to restore system applications and data to the point of the last backup. The recovered server includes the identical configuration of the operating system, user profiles, updates, applications and data. If desired, configuration modifications like fault-tolerant disk mirroring, and partition sizing can be changed, resulting in a recovered system with an updated configuration. (Note: It is always best to consult with your system administrator before modifying system configurations.)

Implementing Intelligent Disaster Recovery

IDR automates and simplifies the process of Windows NT/2000 disaster recovery far beyond manual recovery or other disaster recovery products. Table 1 below describes the simple steps required to install IDR, create the disaster recovery media, and integrate with regular system backup.

Table 1: Implementing IDR using floppies, CD-R/W or bootable tape

Using Disaster Recovery Floppies	Using CD-R/W+	Using Bootable Tape+
Format recovery media: 4 diskettes	Format recovery media: CD-R/W*	Format recovery media: bootable tape with disaster recovery header
Run IDR from a Windows NT/2000 Server	Run IDR from a Windows NT/2000 Server	Run IDR from a Windows NT/2000 Server
IDR creates new Windows NT/2000 start-up diskettes; copies all setup, system partition configuration information, fault tolerance attributes, registry and directory account info and tape device driver to the recovery files on disk 4	IDR creates files and places them into the user defined directory for the CD burner software; copies all setup, system partition configuration information, fault tolerance attributes, registry and directory account info and tape device driver to the recovery files	IDR automatically detects bootable tape drive and media; creates the image on a tape header and copies all setup, system partition configuration information, fault tolerance attributes, registry and directory account info and tape device driver to the header
IDR creates command parameters with which to invoke Backup Exec and required restore components	IDR creates command parameters with which to invoke Backup Exec and required restore components	IDR copies command parameters with which to invoke Backup Exec and required restore components
System prepared to recover in the event of failure	Burn recovery files to CD*	System prepared to recover in the event of failure
	System prepared to recover in the event of failure	

Recovering From Disaster Using IDR

System recovery is a fully automated process using IDR in the Windows NT/2000 environment as Table 2 describes below. After repairing or replacing the failed system or hard disc, the user or system administrator uses the IDR recovery media to boot the system and initiate the disaster recovery session.

Table 2: Initiating Disaster Recovery using Intelligent Disaster Recovery

Traditional Method	Using DR Floppies	Using CD-R or CD-RW+	Using Bootable Tape+
Repair Hardware	Repair Hardware	Repair Hardware	Repair Hardware
Collect All Necessary Media Together	Collect All Necessary Media Together	Collect All Necessary Media Together	REBOOT in DR Mode and Restore System
Reload OS (updates, drivers from profiles, etc.) CD-ROM or Floppies	REBOOT Using DR Floppies	REBOOT Using CD-R or CD-RW	REBOOT
REBOOT	Load Recovery Tape and Restore System	Load Recovery Tape and Restore System	
Reload Backup Software from CD-ROM	REBOOT	REBOOT	
REBOOT			
Load Recovery Tape, Re-Catalog the Tape and Restore System			
REBOOT			

+ Currently supported on Windows NT only
** CD-R/W requires a drive that is ISO9660 compatible*

Altering Hard Drive Partition Sizes for Windows NT/2000

There are many real-life examples as to why you might want to resize your hard drive partitions during a recovery process which competing disaster recovery solutions simply do not support. If the pre-disaster computer hardware contained a 4 GB hard drive with two 2 GB partitions, and you have replaced it with a 9 GB model, IDR (using the DR file) will rebuild the hard disk partition table using the partition information found on the original 4 GB hard drive. As a result, only 4 GB of space will be allocated on the new 9 GB hard drive, with a partition map consisting of two 2 GB partitions.

IDR defaults to restoring the hard drive partition to the same sizes they were before the disaster. There may be unused and unallocated space. If the hard drive in the target computer is larger than the hard drive that was in place before the disaster occurred, run Windows NT's Disk Administrator or Windows 2000 disk management program (within the IDR Recovery Wizard) to alter the partition sizes to reflect the larger hard drive size. Refer to the Microsoft Windows NT/2000 Resource Kit for information on adjusting fault-tolerant RAID configurations.

Conclusion

Intelligent Disaster Recovery truly is a strategic complement to routine backup procedures. By automating and integrating the disaster recovery process with backup/restore technology, Intelligent Disaster Recovery protects against system disasters and reduces the time required to recover critical network servers.

Intelligent Disaster Recovery provides a simple set of steps to prepare for a disaster and to recover, should a disaster strike. These include:

1. preparing the disaster recovery media (diskettes, CD-R/W or tape)
2. automatically updating the disaster recovery information
3. recovering the server to the point of the last backup

VERITAS has developed Intelligent Disaster Recovery as an optional add-on to Version 8 of Backup Exec for Windows NT/2000 for recovery of Windows NT and Windows 2000 systems. Earlier editions of Backup Exec for Windows NT and the IDR option, including versions 7.0 and 7.2, support recovery of systems running Windows NT 3.51 and NT 4. As a world leader in the protection of Windows NT/2000 and NetWare systems and data, VERITAS continues to evolve Intelligent Disaster Recovery in support of customer goals to reduce the administrative burden and total cost of ownership of business networks.

Intelligent Disaster Recovery for Windows NT/2000 - Feature Summary:

- Minimizes recovery with the only point-in-time recovery process of local and remote systems
- Automated step-by-step wizard system easily walks the user through the recovery process
- Completely recovers any Windows NT/2000 server or workstation including all partitions, registry, and configuration information
- Integration with Backup Exec updates disaster recovery information as part of each backup
- Flexible recovery is not limited to the same hardware or configuration
- Compatible with Microsoft Windows NT 3.51; requires Backup Exec for Windows NT v7.0, 7.2 or 7.3
- Compatible with Microsoft Windows NT 4.0; requires Backup Exec for Windows NT v7.0, 7.2, 7.3 or 8.0
- Compatible with Microsoft Windows 2000 Professional, Server, and Advanced Server; Requires Backup Exec for Windows NT/2000 v8.0 or later

VERITAS Software
Corporate Headquarters
1600 Plymouth Street
Mountain View, CA 94043

North American Sales Headquarters
400 International Parkway
Heathrow, FL 32746
800-327-2232 or 407-531-7501
407-531-7730 Fax

Global Locations

United Kingdom
0800-614-961 or
44-(0)870-2431000
44-(0)870-2431001 Fax

France
33-1-41-91-96-37
33-1-41-91-96-38 Fax

Germany
49-(0)69-9509-6188
49-(0)69-9509-6264 Fax

South Africa
27-11-448-2080
27-11-448-1980 Fax

Australia
1-800-BACKUP
612-9955-7682 Fax

Hong Kong
852-2507-2233
852-2598-7788 Fax

Japan
81-3-5532-8217
81-3-5532-0887 Fax

Malaysia
603-715-9297
603-715-9291 Fax

Singapore
65-488-7596
65-488-7525 Fax

China
011-8610-62638358
011-8610-62638359 Fax

Electronic communication

E-Mail:
sales@veritas.com

World Wide Web:
http://www.veritas.com

90-00987-910 • NT01-2KIDRWPR-9902