WHITE PAPER

VERITAS™

Intelligent Disaster Recovery

VERITAS Backup Exec™ 9.1 for Windows Servers

Intelligent Disaster Recovery™ Option

VERITAS™

TABLE OF CONTENTS

VERITAS Backup Exec™ 9.1 *for Windows Servers* Intelligent Disaster Recovery™ Option is a separately licensed and priced option designed to run with VERITAS Backup Exec 9.1 *for Windows Servers*. The Intelligent Disaster Recovery Option eliminates the need to manually re-install the entire operating system after a system crash. Using bootable media, the Intelligent Disaster Recovery Option allows an administrator to get back online fast by restoring data from the last complete backup set including full, differential, incremental, working set and modified file backups.

INTRODUCTION

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 and restore technology. Whereas the primary purpose of backup and restore is to restore applications and data, the primary purpose of disaster recovery is to restore the computing environment itself. Backup and 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.

Before 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 an inadequate 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 and recovery of business critical data.

SOLUTION: POINT-IN-TIME DISASTER RECOVERY

Through the development of specialized applications for Microsoft Windows networks, VERITAS has simplified and automated the process of preparing for and recovering all data and system information from a point-in-time due to a disaster. Using the VERITAS Backup Exec 9.1 *for Windows Servers* 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 software's unique ability to deal with hardware changes during the disaster recovery procedure. With Backup Exec, restoring exact hardware, such as like hard drives and adapters, is not required in order to complete an IDR operation. Intelligent Disaster Recovery is the only disaster recovery solution allowing users to specify new hard-disk information, RAID configurations and network configuration cards.

IDR is ideal for both pure and mixed Windows environments. It allows users to recover Windows NT 4.0 with Service Pack 6a or later Enterprise, Server, Small Business Server (NT 4 only), Terminal Server, and Workstation editions; Windows 2000 Professional, Server, Advanced Server and Datacenter editions; and Windows Server 2003. 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 presents the disadvantages of the manual disaster recovery process when compared with automated and integrated (thus, "intelligent") disaster recovery approach, then offers the steps required to

prepare for and recover from a disaster using the Backup Exec *for Windows Servers* Intelligent Disaster Recovery Option

COMPARISON: MANUAL DISASTER RECOVERY PROCESS VS. INTELLIGENT DISASTER RECOVERY

DISADVANTAGES TO THE MANUAL DISASTER RECOVERY PROCESS

There are three major disadvantages to the manual disaster recovery process. First, the manual disaster recovery process is open to human error. Secondly, without an automated, integrated solution, the unprepared user or system administrator faces a lengthy and laborious course of action to revive a failed system. Moreover, are the many hours of valuable time for the user, system administrator or consultant to first recover and then restore a network server, adversely affecting productivity. Thirdly, the manual disaster recovery method is technically complex.

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-entered.

Manual Disaster Recovery is Time Consuming

As we have discussed, the disaster recovery 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.

Manual Disaster Recovery is Technically Difficult

The manual disaster recovery 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 is 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

Mistakes made at any point can prevent the recovery of the system causing the administrator to have to re-start the manual process from the beginning.

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 and 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 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.

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

- Alleviates system administration by integrating two typically separate processes
- Minimizes downtime through intelligent and automated system recovery
- Eases the impact on personal productivity and business processes
- Reduces the total cost of ownership
- Simplifies the highly complex technical procedure of disaster recovery

Unlike the manual process described previously, with the Intelligent Disaster Recovery Option, 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, the Intelligent Disaster Recovery Option ensures that the system is recovered accurately.

HOW INTELLIGENT DISASTER RECOVERY WORKS

VERITAS has developed the Intelligent Disaster Recovery Option to be used with the Microsoft Windows operating systems. There are unique challenges in protecting these environments that we will discuss in the section entitled “Intelligent Disaster Recovery for Different Windows Operating Systems”.

The Intelligent Disaster Recovery Configuration Wizard appears the first time Backup Exec is started after the IDR Option is installed. The wizard systematically guides an administrator in preparing for disaster recovery and in recovering a local or remote Windows system to its pre-disaster state. A complete Intelligent Disaster Recovery operation consists of 4 steps:

1. Specifying a location where a copy of the computer-specific disaster recovery file will be stored
2. Running full backups of the hard drives on the Windows system to be protected
3. Running the IDR Preparation Wizard to create bootable media and recovery diskettes for each computer
4. Recovering a Windows system using the IDR Recovery Wizard and the recovery media

1. Creating Disaster Recovery File

During initial startup, a wizard guides the user through the setting of an alternate data path for the computer-specific disaster recovery file, called a “*.dr” file, in which the asterisk (*) represents the name of the Windows system for which the file was created. The *.dr file contains specific information for the system you are protecting, including:

- Hardware-specific information for each computer, such as hard disk partition information (Windows 2000 and NT only), mass storage controller information, and Network Interface Card information.
- A list of catalog entries that identify the backup media used to recover the computer.
- For Windows XP and Windows Server 2003 computers, Windows Automated System Recovery (ASR) configuration information. The ASR files are necessary to recreate partitions on Windows XP and Windows Server 2003 computers during the recovery process.

The default data path for the *.dr file is on the media server's hard drive, but it is a recommended best practice to specify an alternate data path to store another copy of the *.dr file in case the media server's hard drive is damaged.

2. Run Full Backup
After setting up an alternate data location for the *.dr file, run full backups for the hard drives.

3. Prepare Disaster Recovery Media
The process of installing the Intelligent Disaster Recovery Option 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. The IDR Preparation Wizard guides the user through the preparation of bootable media used to recover protected computers and copies the *.dr file and other recovery information to the Intelligent Disaster Recovery diskette. You can create three types of bootable media with the IDR Preparation Wizard:

- Diskettes (not supported for Windows XP or Windows Server 2003)
- CD-R (CD-Recordable) or CD-RW (CD-Rewritable)
- Bootable tape (the tape device must support bootable specifications)

Consider what type of Windows computer is being protected, the available hardware, and the system BIOS when selecting the type of bootable media to create. Media can be combined to make updating the *.dr files easier. If you are using bootable CD-R or CD-RW, or tape, you can still back up the *.dr files to diskette using the IDR Preparation Wizard so that you can easily update them when required.

Backup Exec creates the *.dr file during a full backup and stores it in the default and alternate storage locations. Catalog entries from subsequent backups are automatically added to the *.dr file as these backups are completed.

Note: When creating a bootable tape image, the bootable tape image must be created before running full backups.

4. Recovering a Windows System
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 software'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.)

After following the first three steps, an administrator will be prepared to successfully recover local or remote systems using any of the following recovery methods:

- Restore a media server (Backup Exec server) using a locally attached storage device
- Restore a Windows computer by moving the media and the storage device to the computer being restored, and then restoring the computer through the locally attached storage device
- Restore a remote Windows computer using a network connection to the media server

Recovering a Windows system is composed of several discrete steps:

- Creation of the partitions
- Creation of volumes
- Creation of file systems by formatting volumes

- Installation of the Operation System
- Placing of original data back onto the system

Backup Exec carefully guides an administrator through these processes and automates these tasks.

INTELLIGENT DISASTER RECOVERY FOR DIFFERENT WINDOWS OPERATING SYSTEMS

Some Windows operating systems have certain caveats that need to be understood before implementing an Intelligent Disaster Recovery solution.

Windows 2000

Windows 2000 has several components that must be backed up together that are 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 server.

Windows XP and Windows Server 2003

Windows XP and Widows Server 2003 systems include Windows Automated System Recovery (ASR) technology. Developed by Microsoft, ASR enables disaster recovery of the operating system. ASR provides tools for third party vendors, like VERITAS, that help add functionality to their recovery products. For example, the Intelligent Disaster Recovery Option uses ASR for reconfiguring the physical storage to its original state following a disaster. This information includes:

- OS version
- Time Zone
- Buses
- MBR disks and partitions
- Guide Partition Table disks and partitions
- Recovery commands
- Removable media information
- LDM Volume state
- Device instances
- Class keys
- Device instance hash values

BACKUP EXEC OPTIONS AND AGENTS SUPPORT

Backup Exec 9.1 *for Windows Servers* Intelligent Disaster Recovery Option works in conjunction with all agents and options. The only exception is running IDR on a local machine that is utilizing the Backup Exec Tivoli Storage Manager Option.

INTELLIGENT DISASTER RECOVERY OPTION REQUIREMENTS

The Intelligent Disaster Recovery Option has the following requirements:

- VERITAS Backup Exec 9.1 *for Windows Servers*
- The VERITAS Backup Exec *for Windows Servers* Remote Agent must be installed on any remote computers to be protected with the Intelligent Disaster Recovery Option
- Windows NT 4.0 with Service Pack 6a or later Enterprise, Server, Small Business Server (NT 4.0 only), Terminal Server, and Workstation editions; Windows 2000 Professional, Server, Advanced Server and Datacenter editions; Windows XP Professional; and Windows Server 2003
- Windows NT recovery requires at least 40 MB of hard drive space to hold the minimal recovery system, as well as sufficient space for the data that is being restored. The required hard drive space for a 2.0 GB partition storing 1.8 GB of data is 1.8 GB plus 128 MB plus 40 MB for a total of 1.97 GB
- Windows 2000/XP/Windows Server 2003 recovery requires sufficient hard drive space to hold an entire Windows installation (600 MB to 2 GB)

Note: Disaster recovery from virtual devices requires a Remote Intelligent Disaster Recovery Option license using a media server with access to the virtual device.

INTELLIGENT DISASTER RECOVERY OPTION LICENSING

The Intelligent Disaster Recovery Option has two different licenses. The first license is for the first Backup Exec server using IDR and the second license is for additional resources that need Intelligent Disaster Recovery.

1. **Intelligent Disaster Recovery License**
   The license can be used on the same server that Backup Exec is currently installed on, becoming the "primary" IDR license, or it can be used to protect a client on the network. If a client is to be protected, the Remote Agent Client Access License (CAL) for Windows must be installed as well.

   Licensed: Per the first Backup Server

2. **Intelligent Disaster Recovery Additional Client Access License (CAL)**
   This option enables administrators to provide disaster recovery for any additional servers on the network that are being protected from a Backup Exec server that already has a "primary" Intelligent Disaster Recovery license installed. The features are identical to the Intelligent Disaster Recovery Option, but at a discounted rate.

   Licensed: Per Additional Protected Server or Workstation
   Prerequisite: Remote Agent for Windows must be installed on the client and a single License of Intelligent Disaster Recovery Option deployed on the Backup Exec server

SUMMARY

The Intelligent Disaster Recovery Option truly is a strategic complement to routine backup procedures. By automating and integrating the disaster recovery process with backup and restore technology, IDR protects against system disasters and reduces the time required to recover critical network servers. A summary of the benefits of IDR include:

- Minimized 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
- Complete recovery of any Windows 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

Furthermore, IDR provides a simple set of steps to prepare for a disaster and to recover, should a disaster strike:

1. Specifying a location where a copy of the computer-specific disaster recovery file will be stored
2. Running full backups of the hard drives of the computers to be protected
3. Running the IDR Preparation Wizard to create bootable media and recovery diskettes for each computer
4. Recovering a computer using the IDR Recovery Wizard and the recovery media

As a world leader in the protection of Windows 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.

VERITAS Software Corporation
Corporate Headquarters
350 Ellis Street
Mountain View, CA 94043
650-527-8000 or 866-837-4827

For additional information about VERITAS Software, its products, or the location of an office near you, please call our corporate headquarters or visit our Web site at www.veritas.com.