

## Intelligent Disaster Recovery

### **VERITAS Backup Exec™ 10 for Windows Servers**

#### *Intelligent Disaster Recovery™ Option*

## TABLE OF CONTENTS

Executive Summary .....	3
Disaster Preparation Plan (DPP).....	4
Key Elements of a Disaster Preparation Plan (DPP).....	4
Solution: Point-in-Time Disaster Recovery .....	5
Manual Disaster Recovery Process Vs. Intelligent Disaster Recovery.....	6
Disadvantages to the Manual Disaster Recovery Process.....	6
Manual Disaster Recovery is Prone to Human Error .....	6
Manual Disaster Recovery is Time Consuming .....	6
Manual Disaster Recovery is Technically Difficult.....	6
Intelligent Disaster Recovery Automates and Integrates the Process.....	6
How Intelligent Disaster Recovery Works .....	7
1. Creating Disaster Recovery File.....	7
2. Running Full Backup.....	8
3. Preparing Disaster Recovery Media.....	8
5. Recovering a Windows System.....	9
Intelligent Disaster Recovery for Different Platforms and Windows Operating Systems.....	10
Windows 2000 .....	10
Windows XP and Windows Server 2003.....	10
Backup Exec Options and Agents Support .....	11
Using IDR with the Central Admin Server Option .....	11
Intelligent Disaster Recovery Option Requirements .....	12
Intelligent Disaster Recovery Option Licensing.....	12
Summary .....	13

## EXECUTIVE SUMMARY

VERITAS Backup Exec™ 10 *for Windows Servers* Intelligent Disaster Recovery™ Option is a separately licensed and priced option designed to run with VERITAS Backup Exec 10 *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 bring a Windows-based system back online fast by restoring data from the last complete backup set including full, differential, incremental, working set, and modified file backups.

The Intelligent Disaster Recovery Option saves recovery time by automating the traditional manual, error prone process. This option automates server recovery, reducing the time to recovery and gets you back into business fast. Implement a server recovery solution for both local and remote Windows servers, eliminating the need to first reload the entire operating system of crashed servers.

Using either diskette-based, CD-R/CD-RW or bootable tape, the Intelligent Disaster Recovery Option will quickly recover downed servers enabling restores from the last complete backup set including full, differential, incremental, and working set backups. The Intelligent Disaster Recovery Option integrates directly with Microsoft's Automated System Recovery (ASR) functionality in Windows Server 2003 and Windows XP to provide complete disaster recovery on Windows servers. The comprehensive protection is available for remote, LAN-based computers that use Intel 64-bit Itanium processors.

### KEY BENEFITS

- Minimized recovery with the only point-in-time recovery process of local and remote systems
- Complete recovery of any Windows server or workstation including all partitions, registry, and configuration information
- Flexible recovery that is not limited to the same hardware or configuration
- Automated step-by-step wizard system that easily walks the user through the recovery process

## DISASTER PREPARATION PLAN (DPP)

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, a lengthy process, and costly in terms of loss of both productivity and 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 and recovery of business critical data.

### KEY ELEMENTS OF A DISASTER PREPARATION PLAN (DPP)

The DPP you put in place with your Backup Exec system should be tailored to your network environment. While environments vary in different organizations, there are five elements to consider when creating a comprehensive DPP.

- *Hardware protection.* The hardware devices on your network (CPUs, drives, video) are susceptible to damage from many disaster situations. Uninterruptible power supplies (UPS), surge protectors, and security monitoring devices are the equipment most often used today to protect hardware. If you do not already have these items in place, you should consider installing them. In the event of a disaster, the initial investment could be justified many times over.
- *The ability to maintain business operations during a disaster period.* Make sure that proper precautions are taken by everyone to implement plans for network interruptions. For example, the phones in the sales department won't stop ringing because the server is down, so orders may have to be handwritten until the server is up again. Each department should work out strategies for such occurrences. If the proper precautions are taken, the server can be rebuilt quickly and operations can still continue.
- *A sound backup strategy.* A well-designed backup strategy that includes a strong media rotation scheme plays a key role in quickly restoring your file server.
- *Off-site storage of backups.* It is imperative that backed up data be moved off site regularly. This ensures that, if something happens to your facility, all of your backups will not be destroyed. Depending on the importance of your data, you may choose to use several off-site storage facilities. Several companies provide off-site storage services that include picking up and delivering tapes when they are to be rotated.
- *Effective DPP management.* The last element — and possibly the most important — is proper management of your DPP strategy. A person or a group of people should be charged with constantly supervising your organization's disaster preparation efforts. Someone should install and maintain hardware protection devices, make sure all departments have a plan if the server goes down temporarily, and make sure that backups are made and rotated off site regularly. Also, it is a good idea to document your Disaster Preparation Plan for reference purposes.

Backup Exec plays a major role in your DPP by offering an easy, reliable way of backing up and restoring your files. The rest of this paper describes tools to make restoration as straightforward as possible in the event of a disaster.

Prior to beginning, it's recommended that an overall disaster recovery assessment be made for all servers and applications in a user's environment. Systems with business-critical data and applications are prioritized first for recovery using tools essential to meeting uptime and regulatory requirements.

Determining a recovery point objective (RPO), to which an application must be recovered in order to minimize data loss and resume operations, is key. Equally important to understand is the recovery time objective (RTO), or time in which a server must be recovered in order to keep business or users from being negatively impacted. Downtime costs are measured in lost user productivity, an inability to conduct business operations, or even a loss of user files or business transactions.

The right solution enables performing backups frequently enough to meet recovery times while capturing system-specific configuration and backup catalogs with each full backup. This means that if a disaster occurs on a remote computer before you create the recovery media for it, you can still create recovery media if you made a full backup of the computer before the disaster.

Integrating the operating system recovery process with the backup and restore operations allows these two interdependent procedures to leverage key technologies in Microsoft Windows and VERITAS Backup Exec.

## **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 10 *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 what is offered by 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 that allows 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 an 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

## MANUAL DISASTER RECOVERY PROCESS VS. INTELLIGENT DISASTER RECOVERY

### DISADVANTAGES TO THE MANUAL DISASTER RECOVERY PROCESS

The manual disaster recovery process has three major disadvantages. First, the manual disaster recovery process is open to human error. Second, 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, the many hours of valuable time for the user, system administrator, or consultant to first recover and then restore a network server can adversely affect productivity. Third, 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 on the recovery process.

For example, the administrator may not realize that a hard disc 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 manual 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 to complete 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 (system and data recovery)
- Minimizes downtime through guided and automated system recovery operations
- Eases the impact a downed server has on personal productivity and business processes
- Reduces the total cost of ownership
- Simplifies the highly complex technical procedure of disaster recovery

And the product is extremely cost effective, with the user realizing a return on investment (ROI) in a single use. 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 Platforms and 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 through the steps necessary in preparing for disaster recovery and in recovering a local or remote Windows system to its pre-disaster state. After you have performed these steps for each computer you want to protect, you are prepared to recover those computers 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.

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 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 bootable media also contains a text file called <computer name>-diskconf.txt, which contains information about the computer's hard disk layout.

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 on another computer or a different physical drive in case the media server's hard drive is damaged.

Backup Exec automatically creates or updates the \*.dr file during a backup and stores it in the specified location during a backup. During a recovery, you can copy the \*.dr file from the alternate path to a diskette to recover the target computer if the media server's hard drive is unavailable. If you are specifying a remote computer's hard drive as the alternate data path, it is recommended that you map a drive letter to the remote computer. When mapping the drive letter, be sure to select the Reconnect at Logon option so that you can reconnect to the drive letter every time you log on. Check the directory later to make sure that the \*.dr files were copied.

## 2. Running Full Backup

After setting up an alternate data location for the \*.dr file, run full backups for the hard drives. When running full backups for IDR preparation, make sure that volumes (C, D, etc.) have been backed up. The \*.dr files are not created or updated if only individual directories are backed up.

- Make sure that if utility partitions are present on the computer, they are selected for backup. Utility partitions are usually small partitions installed on the hard disk by OEM vendors and contain system diagnostic and configuration utilities.
- Do not include or exclude files from the backup using the Advanced File Selection feature.
- Make sure that if the computer is a remote computer, a compatible version of the Remote Agent has been installed on it. To determine if the Remote Agent is installed on a remote computer, from Windows Explorer right-click the remote server and then from the shortcut menu, click **Properties**. The status of the Remote Agent, if installed, is displayed.

## 3. Preparing Disaster Recovery Media

The process of installing the Intelligent Disaster Recovery Option results in the creation of a series of diskettes, a CD, or a 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)

When selecting the type of bootable media to create, consider what type of Windows computer is being protected, the available hardware, and the system BIOS. 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.

When creating bootable tape or CDs, you must provide the Windows operating system files. In releases of Backup Exec prior to version 10, IDR only accepted the standard Windows operating system installation CD as a source for the Windows OS. In Backup Exec 10 and later, you can use MSDN-style CDs, and you can enter a path to the Windows operating system files on the network or to existing .iso image files as well.

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

#### 4. Creating Recovery Media After a Disaster

If a disaster occurs on a remote computer before you create the recovery media for it, you can still create recovery media if you made a full backup of the computer before the disaster. When you create a full backup of a remote computer, IDR creates a \*.dr file that contains system and catalog information. IDR uses the \*.dr file to create the recovery media needed to recover the remote computer.

#### 5. 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 such as 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.

The hardware must be identical to the original computer except for hard disks, video cards, and network interface cards (NICs). If you plan to change the hardware in the computer being recovered, note the following:

- *Hard drives* — Any hard drive you use should be the same size or larger than the original drive; otherwise repartitioning problems may occur.
- *Processors* — The computer you want to recover should have the same number of processors as the original, and should be the same type of processor.
- *SCSI cards* — Install SCSI cards on the computer before running the IDR recovery process so that the cards can be incorporated during the restore. Only SCSI cards that are running during the recovery process are integrated into the restored Windows computer. To install OEM third-party SCSI drivers, select the Custom Setup option during IDR and then add the drivers manually.
- *NIC cards* — If using IDR to recover a computer that has different network interface cards (NIC), run the Windows Network Control Panel to remove old NIC driver and install new drivers.
- *Video hardware* — If you install different video hardware, install the video driver for that hardware after the original Windows operating system boots into VGA compatibility mode. IDR will not install new video drivers.

After following the first three steps above, 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 PLATFORMS AND WINDOWS OPERATING SYSTEMS**

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

IDR can protect 32-bit computers and 64-bit Intel Itanium computers. On 32-bit computers, IDR supports both local and remote restores; however, on 64-bit computers, IDR supports only remote restores. Also, only bootable CD images can be created for 64-bit computers. For a 64-bit Intel Itanium computer, you can use IDR to restore the Extensible Firmware Interface (EFI) system partition data, which contains the files necessary to boot the computer.

### **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 Windows 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, such as 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

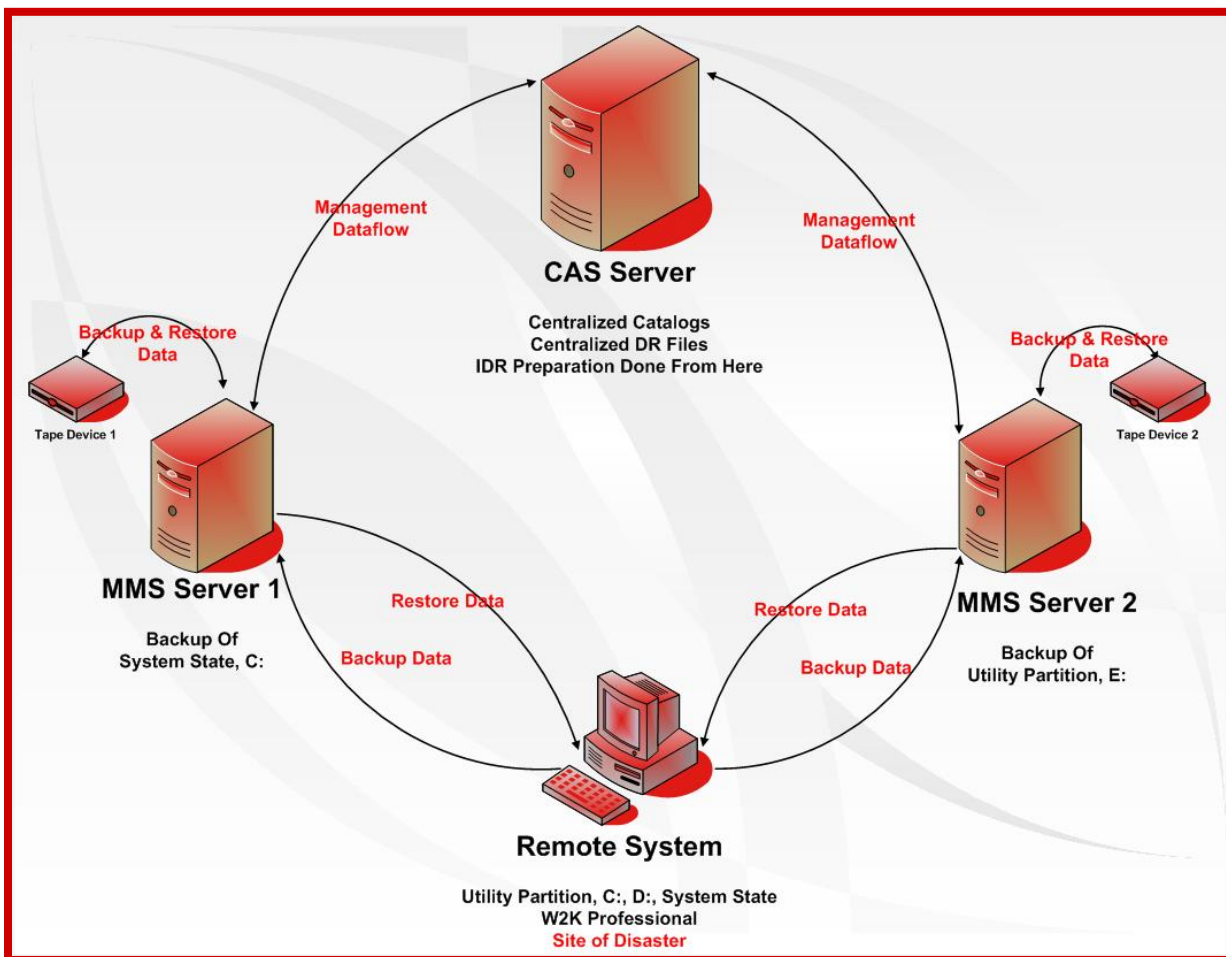
- Device instance hash values
- For Windows 2003, back up Shadow Copy components
- For 64-bit systems, back up EFI system partition

## BACKUP EXEC OPTIONS AND AGENTS SUPPORT

Backup Exec 10 *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.

### Using IDR with the Central Admin Server Option

If you have purchased and installed the Centralized Administration Server Option (CASO), you can perform IDR of the managed media servers (MMS) in a CASO environment. To prepare recovery media for the managed media servers, you must run the IDR Preparation Wizard on the Central Admin Server (CAS). The \*.dr files are stored on the CAS. During IDR recovery of an MMS, all restore jobs are submitted from the CAS. The CAS will then send the restore jobs to the appropriate managed media server.



### Using IDR with VERITAS Storage Foundation for Windows

If you use VERITAS Storage Foundation for Windows on Windows 2003, IDR can restore the dynamic volumes. During backup, IDR gathers the components necessary to restore the dynamic volumes and adds them to the recovery media. After the dynamic volumes are recovered, the data recovery on the volumes proceeds as usual.

## **INTELLIGENT DISASTER RECOVERY OPTION REQUIREMENTS**

The Intelligent Disaster Recovery Option has the following requirements:

- VERITAS Backup Exec 10 *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
- Microsoft Windows 2000 family of products; Windows XP Professional SP1 or later; and Windows Server 2003 family of products
- 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**

### **Using an Evaluation Version of the IDR Option**

Backup Exec and the Intelligent Disaster Recovery option can be installed without a license key and evaluated for up to 60 days. However, once Backup Exec and IDR licenses are purchased and installed, the user must recreate the IDR recovery media that includes the boot media and the Intelligent Disaster Recovery diskette.

Using the IDR Recovery Wizard to recover a computer after the evaluation period has expired will result in the user being prompted to enter a valid IDR serial number to continue the recovery process. This will continue to occur unless you recreated IDR recovery media after IDR was licensed.

### **Intelligent Disaster Recovery License**

The Intelligent Disaster Recovery Option license is purchased only for the Backup Exec media server and allows the user to benefit from IDR on every server and workstation on the network that is protected by that specific Backup Exec server. If a server is to be protected over the network, the Remote Agent Client Access License (CAL) for Windows must be purchased and installed as well.

*Licensed: Per Backup Exec Media Server*

## SUMMARY

The Intelligent Disaster Recovery Option is a key and 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 that 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 that 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 solutions 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](http://www.veritas.com).