



# Intelligent Disaster Recovery

## Symantec Backup Exec™ 11d *for Windows® Servers*

### Intelligent Disaster Recovery Option

Symantec Backup Exec IDR Option provides basic system recovery and automates the process of manual server recovery. For business-critical systems, Symantec recommends Backup Exec System Recovery, which is a stand-alone and complementary product to Backup Exec 11d *for Windows Servers* and is optimized for system recovery. Backup Exec System Recovery combines the speed and reliability of disk-based, bare-metal Windows system recovery with revolutionary technologies for hardware-independent restoration and lights-out operation.

# Intelligent Disaster Recovery

## Symantec Backup Exec 11d

### *for Windows Servers*

#### **Contents**

<b>Executive summary</b> .....	<b>4</b>
<b>Disaster Preparation Plan (DPP)</b> .....	<b>4</b>
Key elements of a Disaster Preparation Plan (DPP) .....	5
Solution: Point-in-time disaster recovery .....	6
<b>Manual disaster recovery process vs. intelligent disaster recovery</b> .....	<b>7</b>
Disadvantages to the manual disaster recovery process .....	7
Intelligent disaster recovery automates and integrates the process .....	8
<b>How intelligent disaster recovery works</b> .....	<b>9</b>
1. Creating disaster recovery files .....	10
2. Running full backups .....	11
3. Preparing disaster recovery media .....	11
4. Creating recovery media after a disaster .....	12
5. Recovering a Windows system .....	12
<b>Intelligent disaster recovery for different platforms and Windows operating systems</b> .....	<b>13</b>
Windows 2000 .....	14
Windows XP, Windows Server 2003, Windows Server 2003 R2 .....	14
<b>Backup Exec options and agents support</b> .....	<b>15</b>
Using IDR with the Central Admin Server Option .....	15
Using IDR with Veritas Storage Foundation™ <i>for Windows</i> .....	16
<b>Intelligent Disaster Recovery Option requirements</b> .....	<b>16</b>
<b>Intelligent Disaster Recovery Option licensing</b> .....	<b>16</b>
Using an evaluation version of the IDR Option .....	16
Intelligent Disaster Recovery license .....	16
<b>Summary</b> .....	<b>17</b>

## Intelligent Disaster Recovery: Symantec Backup Exec 11d *for Windows Servers*

### Executive summary

Symantec Backup Exec 11d *for Windows Servers* Intelligent Disaster Recovery Option is a separately licensed and priced option designed to run with Symantec Backup Exec 11d *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, restoring the system by pulling 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 of server recovery, reducing the time to recovery, and helps get 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, DVD+/-R, or bootable tape, the Intelligent Disaster Recovery Option quickly recovers 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 the Microsoft® Automated System Recovery (ASR) functionality in Windows Server® 2003 and Windows XP to provide comprehensive disaster recovery on Windows servers. With Backup Exec 11d, the Intelligent Disaster Recovery Option can use either physical tapes or backup-to-disk folders as the data source. These media can be local or remote.

### Disaster Preparation Plan (DPP)

When a network server fails due to human error, hardware failure, or a major disaster, the operating 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 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 helps ensure 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, time-consuming, 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 absence 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 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

### Key elements of a Disaster Preparation Plan (DPP)

The DPP you put in place 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 these items are not already 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.
- **Offsite storage of backups.** It is imperative that backed up data be moved offsite 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 offsite storage facilities. Several companies provide offsite storage services that include picking up and delivering tapes when they are to be rotated.
- **Protecting data as well as systems.** Backup software like Backup Exec is optimized to back up your data. You need to go a step beyond that and use a separate option such as IDR or Backup Exec System Recovery. Automated system recovery eliminates the manual process of re-installing the operating system, applications, drivers, and so on, before you can access the data.
- **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 offsite regularly. Also, it is a good idea to document your DPP for reference purposes.

## Intelligent Disaster Recovery: Symantec Backup Exec 11d *for Windows Servers*

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

Before you begin, 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 the key. Equally important to understand is the recovery time objective (RTO), or time in which a server must be recovered in order to keep businesses 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 Symantec Backup Exec.

### **Solution: Point-in-time disaster recovery**

Through the development of specialized applications for Microsoft Windows networks, Symantec has simplified and automated the process of preparing for and recovering all data and system information from a point in time, in the event of a disaster. With the Symantec Backup Exec 11d *for Windows Servers* Intelligent Disaster Recovery (IDR) Option, network servers and application servers 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. For business-critical servers, including Exchange, SQL, and others, Symantec recommends Backup Exec System Recovery, which is a stand-alone product optimized for bare-metal Windows system recovery to same or dissimilar hardware or virtual environments *in minutes*.

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.

## Intelligent Disaster Recovery: Symantec Backup Exec 11d *for Windows Servers*

IDR is ideal for almost all aspects of the Windows computing environment. It allows users to recover Windows 2000 Professional, Server, Advanced Server, and Datacenter editions; Windows Server 2003 and Windows Server 2003 R2; 64-bit versions of Windows Server 2003/Windows Server 2003 R2; and 64-bit Itanium® servers. By empowering system administrators to quickly recover network servers to the point of the last incremental, differential, or working set backup, IDR improves data integrity, increases overall system reliability, and helps reduce 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 repartitioned incorrectly until the very end, when the backup tapes need to be restored. At that point, restoring the data would cause data errors, or applications could 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.

## Intelligent Disaster Recovery: Symantec Backup Exec 11d *for Windows Servers*

### ***Manual disaster recovery is time-consuming***

As 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 (and rebooting several times along the way):

- Repairing or replacing the failed hard disk or equipment
- Collecting critical system configuration information (assuming it is documented) and recovery media
- Manually repartitioning 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
- Recataloging 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 restart the manual process from the beginning.

### **Intelligent disaster recovery automates and integrates the process**

Symantec 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.

## Intelligent Disaster Recovery: Symantec Backup Exec 11d *for Windows Servers*

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
- Helps reduce 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, and so on. 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**

Symantec 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 titled “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 you 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 media server (Backup Exec server) using a remote backup-to-disk folder
- 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

## Intelligent Disaster Recovery: Symantec Backup Exec 11d *for Windows Servers*

A complete Intelligent Disaster Recovery operation consists of four 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. With Backup Exec 11d, either a tape device or a backup-to-disk folder can be used as the target for these full backups.
3. Running the IDR Configuration Wizard to create bootable media and/or recovery diskettes for each computer.
4. Recovering a Windows system using the IDR Recovery Wizard and the recovery media.

### **1. Creating disaster recovery files**

During initial startup, a wizard guides the user through the setting of an alternate data path for the computer-specific disaster recovery file. Depending on the choices selected, this can be a “\*.dr” file (in which the asterisk [\*] represents the name of the Windows system for which the file was created), an IDRCD.ISO image, or a bootable tape image. These files contain specific information for the system you are protecting, including:

- Hardware-specific information for each computer, such as hard disk partition information (Windows 2000 or Windows Server 2003 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 re-create 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 recovery files is on the media server’s hard drive, but it is a recommended best practice to specify an alternate data path. Doing so enables you to store a copy of the recovery files on another computer or a different physical drive in case the media server’s hard drive is damaged.

During a backup, Backup Exec automatically creates or updates the recovery files file and stores it in the specified location. During a recovery, you can copy the recovery files 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 recovery files were copied.

## 2. Running full backups

After setting up an alternate data location for the recovery 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 recovery 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 is 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. With diskettes, the process automatically copies the recovery file and other recovery information to the Intelligent Disaster Recovery diskette. With a CD, an IDRCD.ISO image file is created in a path specified by the user. This image can be burned to CD or DVD and used when recovering a downed system. You can create three types of bootable media with the IDR Preparation Wizard:

- Diskettes (not supported for Windows XP or Windows Server 2003/2003R2)
- CD-R (CD-Recordable) or CD-RW (CD-Rewritable), or DVD+/-R
- Bootable tape (the tape device must support bootable specifications)

Note that third-party CD- or DVD-burning software will be needed to burn the recovery file created by Backup Exec to CD-R, CD-RW, or DVD+/-R media.

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. If you are using bootable CD-R or CD-RW, or tape, you can still back up the recovery files to diskette using the IDR Preparation Wizard. Doing so enables you to easily update the recovery files when required.

## Intelligent Disaster Recovery: Symantec Backup Exec 11d *for Windows Servers*

Backup Exec creates the recovery 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 recovery 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 11d, IDR only accepted the standard Windows operating system installation CD as a source for the Windows OS. In Backup Exec 11d, you can use MSDN-style CDs and 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 recovery file that contains system and catalog information. IDR uses the recovery 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.

## Intelligent Disaster Recovery: Symantec Backup Exec 11d *for Windows Servers*

- **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.
- **NICs**—If using IDR to recover a computer that has different NICs, run the Windows Network Control Panel to remove the 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 media server (Backup Exec server) using a remote backup-to-disk folder
- 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 entails several discrete steps:

- Creation of the partitions
- Creation of volumes
- Creation of file systems by formatting volumes
- Installation of the Operation System
- Placement 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 and 64-bit Windows computers, as well as 64-bit Intel® Itanium computers. Only bootable CD images can be created for Itanium 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.

## Intelligent Disaster Recovery: Symantec Backup Exec 11d *for Windows Servers*

### **Windows 2000**

Windows 2000 has several components, defined as the System State, that must be backed up together. 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 the 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 the 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, Windows Server 2003, Windows Server 2003 R2**

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 Symantec, 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 Server 2003/2003R2, backup Shadow Copy components
- For 64-bit systems, backup EFI system partition

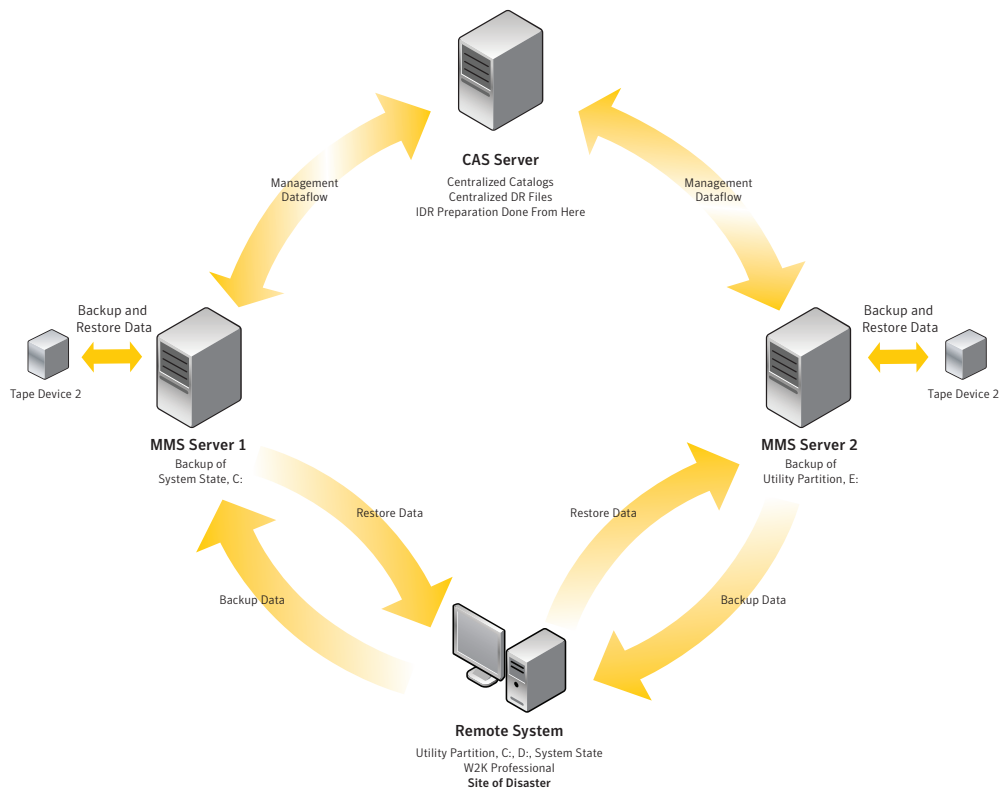
# Intelligent Disaster Recovery: Symantec Backup Exec 11d for Windows Servers

## Backup Exec options and agents support

Backup Exec 11d for Windows Servers Intelligent Disaster Recovery Option works in conjunction with all agents and options.

## Using IDR with the Central Admin Server Option

If you have purchased and installed the Centralized Administration Server Option (CASO), you can perform intelligent disaster recovery 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 recovery 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 Central Admin Server Option

## Intelligent Disaster Recovery: Symantec Backup Exec 11d *for Windows Servers*

### **Using IDR with Veritas Storage Foundation™ *for Windows***

If you use Veritas Storage Foundation for Windows on Windows Server 2003 or Windows Server 2003 R2, 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:

- Symantec Backup Exec 11d *for Windows Servers*
- The Symantec Backup Exec *for Windows Servers* Agent for Windows Systems 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 2003/2003 R2 family of products
- Windows 2000/XP/Windows Server 2003/Windows Server 2003 R2 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 re-create the IDR recovery media that includes the boot media and the Intelligent Disaster Recovery diskette.

Using the IDR Recovery Wizard to restore 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 re-created 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

## Intelligent Disaster Recovery: Symantec Backup Exec 11d *for Windows Servers*

### 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 a quick and reliable point-in-time recovery process of local and remote systems
- Automated step-by-step wizard system that easily guides 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, which 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, Symantec 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.

In addition, if you are looking for system recovery for mission-critical systems to the same hardware, dissimilar hardware, or virtual environments in minutes, we invite you to find out more about Backup Exec System Recovery at [www.backupexec.com/besr](http://www.backupexec.com/besr).

## 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](http://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](http://www.symantec.com)

Copyright © 2007 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, Backup Exec, Veritas Storage Foundation, and Veritas are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Microsoft, Active Directory, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other names may be trademarks of their respective owners. Printed in the U.S.A. 01/07 10753270