INTELLIGENT DISASTER RECOVERY

DELL POWERVAULT DL 2000
POWERED BY SYMANTEC

Intelligent Disaster Recovery

The PowerVault DL2000– Powered by Symantec Backup Exec offers the industry's only fully integrated backup-to-disk solution with software factory installed. Dell and Symantec have co-developed this offering to give you easier management capabilities of the backup-to-disk environment. It's an ideal way for any IT department to achieve faster, more reliable backups and restores. In addition, the appliance includes system level disaster recovery capabilities designed to recover failed systems no matter the cause.

When a network server fails due to human error, a 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. In today's environments, changes in the operating system increase the need for a uniform, automated process to secure the operating environment and recovery of business critical data.

The PowerVault DL Backup to Disk Appliance features disaster recovery capabilities powered by Symantec Backup Exec Intelligent Disaster Recovery Option. The Intelligent Disaster Recovery Option eliminates the need to manually re-install the entire operating system after a system crash. Using the created 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.

Intelligent Disaster Recovery

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 recover and gets business back into production fast.

Using either a 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.

How Intelligent Disaster Recovery Works
The Intelligent Disaster Recovery Option is designed to protect Microsoft Windows operating systems. There are unique challenges in protecting these environments that are discussed in the section, "Intelligent Disaster Recovery for Different Platforms and Windows Operating Systems". The Intelligent Disaster Recovery Configuration Wizard appears the first time Backup Exec is launched from the Dell Appliance Management Console. The wizard systematically guides a user through the steps necessary in preparing for a disaster recovery and in recovering a local or remote Windows system to its pre-disaster state. A complete Intelligent Disaster Recovery Operation consists of the following 3 steps:

1. Creating a Disaster Recovery file that contains specific information about the protected computer.
2. Making a full backup of the system being protected.
3. Creating bootable Disaster Recovery media for the protected system.

Step 1: Creating a Disaster Recovery File
The Disaster Recovery File contains specific information about the individual system that is being protected. This information includes:

- Hardware specific information for each system including hard disk partition information, mass storage controller information, and Network Interface Card information.
- The list of catalog entries that identify the backup media and sets needed to recover the system in the event of a disaster.
- Windows Automated System Restore (ASR) configuration for Windows XP and Windows Server 2003 systems.

1. On the Backup Exec Getting Started screen, select "*Configure Intelligent Disaster Recovery*" to start the wizard. When the Welcome screen appears, click *"Next"* to continue.

Backup Exec automatically creates a *.dr file for the IDR-protected computer when it is backed up and stores it in the default location on the media server's hard drive, which is:
C:\Program Files\Symantec\Backup Exec\idr\Data\<computer name>.dr.

The *"Enter an Alternate Data Path"* screen allows you to specify an alternate location for storing a copy of the *.dr. This allows the *.dr file to be available even if the media server has been damaged.

2. Enter the alternate location where a copy of the *.dr file will be stored, and then click *"Next"*.

Best Practice: Symantec recommends that the alternate location be on another computer or on a different physical drive than the default location.

3. The IDR configuration is now complete. You are ready to run backups and create bootable media. Click *"Finish"*.

Step 2: Running a Full Backup
After creating the Disaster Recovery File, a full backup of the hard drives on the protected system needs to be performed. Make sure that the full volumes are selected (C, D, etc.) for the backup. By selecting the full volumes, the disaster recovery file for the specific machine will be updated with the latest system information. In addition to selecting the full volumes, make sure the following Best Practices are followed:

- Select the utility partitions, if present, for backup on the protected system.
- Do not utilize the*" include or exclude files"* feature. This is located in the Advanced File Selection of the backup job properties.
- If a remote system is being protected, make sure that the Agent for Windows Systems is installed on the remote system.

1. On the Backup Exec interface, select the drop down from the **Backup** Tab and choose "**New Backup Job…"**

2. The Backup Job Properties page will appear. Verify that the remote agent is installed by right-clicking on the system name in the View by Resource tab and select **Properties**. The status of the remote system is displayed. Verify that the following appear for the Remote Agent status:

   - Installed: Yes
   - Status: Running
   - Version: 12.5.x.x

   If the Remote Agent is not installed or running, refer to the Backup Exec Administrator's Guide for steps to install the Remote Agent for Windows Systems.

3. After verifying that the remote agent is installed and running, select the remote system for backup at the system name node. In addition, a selection list name and description can be specified so that the selection list can be reused in additional backup jobs.

4. The destination for the backup job can be specified from the Device and Media tab. The default device is "All Virtual Disk". The backup job will target any available virtual disk as the backup destination.

5. Name the backup job from the General tab. Naming the backup job provides an ease of use mechanism for remembering the purpose of the backup job in the future.

6. A schedule can be created so that a backup job repeats on a periodic basis, ensuring that a system is protected with the latest information. For the purpose of this article, the backup job will run immediately with no schedule set. Select "**Run Now"** and select "**Ok"** from the Job Summary to run the backup.

The backup job status can be monitored from the **Job Monitor** tab on the Backup Exec interface. The backup job has completed successfully when the backup job appears under the Job History and is listed as Successful.

Step 3: Preparing Disaster Recovery Media

1. From the Tools Menu, Select *"Wizards"* and then select the *"Intelligent Disaster Recovery Preparation Wizard."*
2. Select *"Next"* to continue the wizard.
3. Select the type of media that will be used to create the DR media:
    - Bootable CD Image for Use with CD Writers (ISO 9660)
    - Bootable Tape Image for use with bootable tape devices
    - Non-bootable disaster recovery CD Image

    Or Copy
    - Disaster recovery information (.dr) files

BEST PRACTICE: Creating a bootable CD image provides the quickest methodology for performing the recovery of a failed system. Backup Exec will create an image that must be burned to CD using third party software. A blank CD, third party software, and a writable CD device must be available. For the purpose of this article, a bootable CD Image will be used.

4. Select *"Bootable CD Image"* for Use with CD Writer (ISO 9660) and select Next.
5. Select *"Next"* to continue the CD Image Creation Wizard.
6. Select the systems that you want use for recovery with the bootable CD Image. Move each system from the list of Available Computers to the list of Selected Computers. ***NOTE:*** *All of the selected computer must be running the same version of the Windows operating system.* Select *"Next"* to continue.
7. Specify the location that Backup Exec will create an ISO 9660 CD image. Select *"Next"* to continue.
8. Backup Exec utilizes the Windows operating system installation files in the creation of the IDR recovery media. The Windows operating system files provided must match the version and language of the systems being protected. Specify the location of the Windows operating system installation files and select *"Next"* to continue.
9. The Intelligent Disaster Recovery Wizard will create the bootable CD image. This may take a few minutes. When complete, the ISO image will be stored in the location specified in step 7. Select *"Next"* to continue.
10. The ISO image must be burned to a CD using third party software before it can be utilized as part of the disaster recovery process. Select Finish to complete the IDR Preparation Wizard.

Recovering a System

In the event that a protected system experiences a disaster or system crash, it can be recovered in the following 2 steps:

- Boot the failed system with the Disaster Recovery CD Media that was created with the IDR Preparation Wizard
- Recover the system and data to utilizing the Disaster Recovery Wizard

STEP 1: Boot the Failed System

1. Boot the failed system using the Bootable CD Image created as part of the disaster recovery preparation wizard.

2. Once the system boots select the disaster recovery task to be performed:
   - Select "*Automated Recovery"* if the disaster recovery (.dr) file is available from Step 1 in the disaster recovery creation process.
   - Select "*Manual Recovery"* is the disaster recovery (.dr) file is not available from Step 1 in the disaster recovery creation process.

   NOTE:*For the purpose of this article, the Automated Recovery Process will be used.*
3. The Disaster Recovery Wizard will detect the SCSI, RAID, and USB Tape Device Controllers connected to the system. The Drivers for all of the controllers should be loaded. If the drivers are missing, click "Have Disk" to install the required drivers and click "Ok". Click "*Next"* to continue.

4. Select the disaster recovery file (.dr) for this system that will be used for the recovery.
   - If the file is available locally, select "*Browse for Disaster Recovery files…"* and specify the file location.
   - If the disaster recovery file is available on the network, select "*Install Network"* and the required network services will be installed. You most likely will need to map a network drive to the location containing the disaster recovery (.dr) file.

5. Once the disaster recovery (.dr) file has been specified, select *"Next"* to continue.

6. The Disaster Recovery Wizard will perform the following operations:
   - Repartition the Hard Drives
   - Mount the drives
   - Format the local drives

   Note: *You will need to acknowledge the format operation for the hard drives by selecting Ok.*

7. Once the Hard Drives have been prepared, select "*Next"* to continue.

8. The Hard Disk partitioning can be modified from the original layout if desired. Make the necessary changes and select *"Next"* to continue.

9. The Disaster Recovery wizard is now ready to automatically restore the data. A method must be selected for accessing the DL2000 containing the data. The methods are:
   - Use locally attached media device
   - Use the network, and restore from remote backup-to-disk folders
   - Use the network to restore from a remote media server

   Note: *Since this is a remote protected system, the PowerVault DL2000 containing the data will be used for restore.*

10. Select *"Use the network"* to restore from a remote media server and then select "*Next"* to continue.

11. The media server containing the data must be specified to complete the restore. Enter the required information for the media server and select *"Next"* to continue:
    - Server Name:

- Domain Name:
- User Name:
- Password:

12. A summary of the data sets and media is presented. Select *"Next"* to continue the restore.
13. Once the data has finished restoring, the disaster recovery process will be completed. If the restore was performed to a different system, it may be necessary to specify the correct hard drive to boot the operating system. This can be done by editing the *BOOT.ini* file. If no changes are needed, select *"Finish"* to complete the disaster recovery process. The system will now reboot.
14. The disaster recovery process is complete.

Important Considerations

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.

Windows 2000

Windows 2000 has several components that make up the System State and these components must be backed up together. Critical to the recovery of the system is the restoration of the Systems State, which replaces boot files first and commits the system hive of the registry as the 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 for systems operating as a certificate server
- Active Directory for Domain Controllers
- SYSVOL – System Volume for Domain Controllers
- Cluster quorum for Cluster Servers
- 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 system.

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. The Intelligent Disaster Recovery Option works with 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
- GUID Partition Table disks and partitions
- Recovery commands
- Removable media information
- LDM Volume State
- Device instances
- Class Keys
- Device instance hash values
- Backup Shadow Copy Components for Windows 2003

PROTECTING YOUR POWERVAULT DL2000WITH INTELLIGENT DISASTER RECOVERY

Intelligent Disaster Recovery can be used to protect your PowerVault DL2000and minimize the amount of time required to restore the appliance in the event of a system failure. Full system backups as part of the IDR process protect all software components on the appliance including the Windows Operating System, Backup Exec, and all configuration information. When performing a full system backup, make sure that the full volumes are selected (C Drive) for the backup. By selecting the full volumes, the disaster recovery file for the specific machine will be updated with the latest system information. In addition to selecting the full volumes, make sure the following Best Practices are followed:

- Select the utility partitions for backup on the appliance.
- Do not utilize the*" include or exclude files"* feature. This is located in the Advanced File Selection of the backup job properties.

12. On the Backup Exec interface, select the drop down from the **Backup** Tab and choose "**New Backup Job…"**
13. Select your backup to disk appliance at the system name node. In addition, a selection list name and description can be specified so that the selection list can be reused in additional backup jobs.
14. The destination for the backup job can be specified from the Device and Media tab. The default device is "All Virtual Disk". The backup job will target any available virtual disk as the backup destination.
15. Name the backup job from the General tab. Naming the backup job provides an ease of use mechanism for remembering the purpose of the backup job in the future.
16. A schedule can be created so that a backup job repeats on a periodic basis, ensuring that a system is protected with the latest information. It is recommended that a full system backup be performed at least once a month for the appliance. Set the desired schedule for the full system backup For the purpose of this article, the backup job will run immediately with no schedule set. Select "**Submit"** and select "**Ok"** from the Job Summary to run the backup.
17. The backup job status can be monitored from the **Job Monitor** tab on the Backup Exec interface. The backup job has completed successfully when the backup job appears under the Job History and is listed as Successful.

SUMMARY

The Intelligent Disaster Recovery Option is a key beneficial feature to routine backup procedures. IDR protects against systems disasters and reduces the time required to recover critical network systems by automating and integrating the disaster recovery process with backup and restore technology. Key benefits of IDR include:

- Minimize the recovery process with point-in-time recovery
- Automated step-by-step wizards simplify the recovery process
- Complete recovery of any Windows system including all partitions, registry, and configuration information.