# HP OpenView Storage Data Protector 5.5

# Microsoft Windows Server 2003

# Cluster Server Integration



# Executive Summary

This white paper provides complementary information for how to configure and maintain HP OpenView Storage Data Protector 5.5 in Microsoft Windows Server 2003 Cluster Server environments.

# Solution Description

As a part of its high-availability functionality and support, Data Protector provides an integration solution with the Microsoft Cluster Server (MSCS).

## MSCS Components

The MSCS consists of the following components:

- Cluster nodes
- Local disks
- Shared disks
- Groups
- Resources

Cluster nodes are computers that compose a cluster. They are physically connected to one or more shared disks.

The shared disk volumes contain mission-critical application data as well as specific cluster data needed to run the cluster. A shared disk is exclusively active on only one cluster node at a time.

A group is a collection of resources that are needed to run a specific cluster-aware application. Each cluster-aware application declares its own critical resources. The following resources must be defined in each group:

- Shared disk volumes
- Network IP names
- Network IP addresses
- Cluster-aware application services

## High Availability of the Data Protector Cell Manager

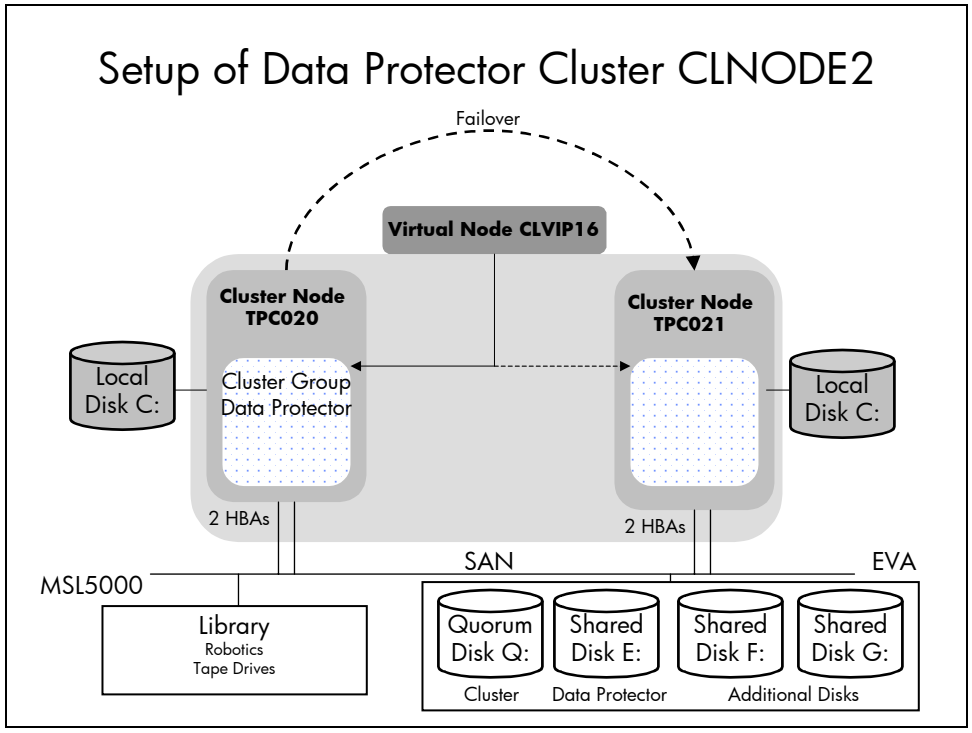
A cluster-aware Data Protector Cell Manager, that is responsible for running the Data Protector Internal Database (IDB) and managing backup and restore operations, has many major benefits over non-cluster versions. All Cell Manager operations are always available. Data Protector services are defined as cluster resources within the cluster and are automatically restarted when a failover occurs.

## Example Setup of Data Protector Cluster

The following figure describes a cluster-aware Data Protector Cell Manager, which will be used as a reference in the next chapters.

Cluster CLNODE2 is configured with two nodes: TCP020 and TPC021. The cluster-aware Cell Manager can be accessed by the virtual node CLVIP16. The cluster group Data Protector keeps its data on a disk array (EVA), which provides disks for MSCS Quorum (Q:), Data Protector (E:) and for future use (F:, G:). The HP MSL5000 tape library is connected with both nodes.

**Figure 1.** Example Setup of Data Protector Cluster




The setup of clustered applications outside a cluster-aware Cell Manager can be considered as a subset and is therefore not described.

# Installation

## Support Matrices

Before installation, please check the latest support matrices for Data Protector and Microsoft Cluster Server at the following links:

HP OpenView Storage Data Protector
http://www.hp.com/go/dataprotector

Products Designed for Microsoft Windows – Windows Catalog and HCL
http://www.microsoft.com/whdc/hcl

## Software Removal

If a system in the cluster has the Data Protector software already installed, you need to uninstall it before the setup.

## Cell Manager

Data Protector has a cluster-aware, fully automated installation of the Cell Manager. When Data Protector is installed on one single node, it is simultaneously installed to every other node.

The installation succeeds with the following screen:

**Figure 2.** Successful Installation Status of Cell Manager Cluster


The installation procedure, which was started on TPC020, imported cluster node TPC021 and virtual node CLVIP16. After this, all physical and virtual nodes are known to Data Protector and can be used for configuration.

## Client

The Data Protector client software cannot be push-installed to the nodes of a Microsoft Cluster Server. Therefore, the client software must be locally installed.

The Data Protector client installation does not propagate to other cluster nodes. The installation procedure requires client installations on every cluster node.

During installation, Data Protector will recognize the cluster and install the client in the cluster-aware mode. The cluster integration component is selected by default.

The following figure shows the finished installation process with a message that the cluster node has not been imported:

**Figure 3.** Successful Installation Status of Cluster Client


After installing the client software on all cluster nodes, the complete cluster can be imported with the Client GUI and the Import Cluster feature.

## Password Change of Data Protector User Account

If it is needed to change the user password after the installation, the following steps are required:

1. Set the cluster resources OBVS_VELOCIS and OBVS_MCRS offline.
2. Change on all cluster nodes the password of the Windows services “Data Protector Inet” and “Data Protector CRS”.
3. Restart on all cluster nodes the Windows service “Data Protector Inet”.
4. Set the cluster resources OBVS_VELOCIS and OBVS_MCRS online again.

## Debug and Log Files

Setup.exe (csetup.exe) automatically writes a detailed installation log to “OB2DBG*.TXT”. These log files contains complete information on setup except on the part where dialogs are being displayed (technical limitation of MSI itself).

**Details:**

<TEMP>\OB2DBG_<DID>__setup_<HOST><DEBUG_NO>.txt

<DID> (debugging ID) is the process ID of the first process that accepts the debugging parameters. This ID is used as an ID for the debugging session. All further processes will use this ID.

<HOST> is the name of the host where the trace file is created.

<DEBUG_NO> is a number generated by Data Protector.

The location of the <TEMP> directory is specified by the Windows TEMP environment variable. To examine the value of this variable run the set command in a DOS box.

# Patches

## Cell Manager

Cluster patches must be locally installed. It's the same procedure as the Data Protector software installation. Patches can be installed on any node, which will be simultaneously distributed to any other node.

**Note:** CORE and CS patches may require a reboot, which could result in a failover of the Cell Manager. Please check the patch description in advance.

## Client

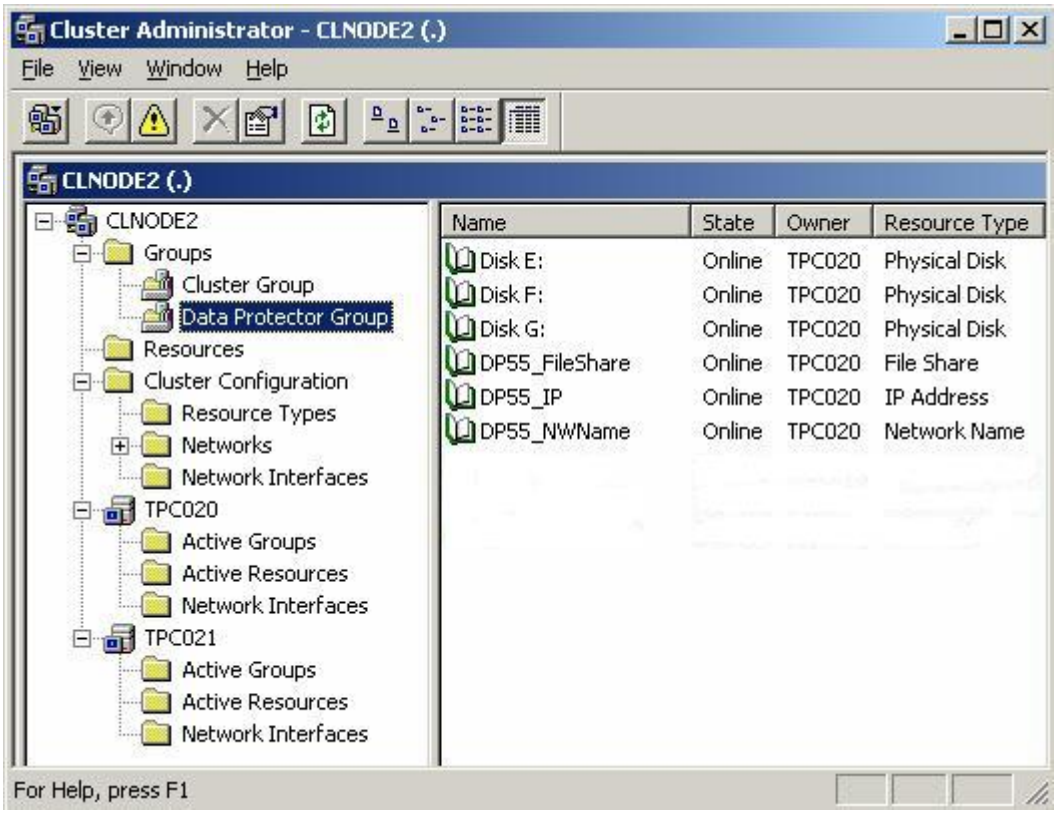
It is the same procedure as for the Data Protector client software installation, which must be executed on every cluster node separately. Afterwards, the cluster must be re-imported.

# Configuration

First, please check chapters Pre-Installation Requirement of File Share Resource and Post-Installation Check of Resource Dependencies for known issues. Then, follow the instructions in the *HP OpenView Storage Data Protector 5.5 Installation and Licensing Guide.*

The following figure shows the two-node cluster CLNODE2 with belonging resources. Please note that "Disk E:" is destined to hold the shared Data Protector software and configuration. "Disk F:" and "Disk G:" are optional disks for future use in the same cluster group.

**Figure 4.** Cluster Administrator View of Data Protector Cluster Configuration




## Automatic Restart of Backups

If a failover of the cluster-aware Data Protector Cell Manager occurs during backup, all running and pending backup sessions will fail. In the Data Protector GUI and in the backup specification, you can set one of the options that define automatic backup session restart at failover of Data Protector.

**Note:** If the Cell Manager and another application are installed in the same cluster, its cluster critical resources need to be configured in the same cluster package or group as the application being backed up, in order to automatically restart failed backup sessions that failed due to a failover. Otherwise, the failed backup sessions must be restarted manually.

## Load Balancing at Failover

If a failover causes a move of applications to that system where the Data Protector Cell Manager is running, it can result in a very high load on that system. Therefore, it might be necessary to abort running backup sessions in order to have enough system resources for the applications.

It is possible to:

- Abort all running backup sessions.
- Abort specific running backup sessions.
- Inhibit the Data Protector cluster Cell Manager for a specific timeframe.

The belonging feature is provided by the command line utility “omniclus.exe”.

## Autoconfiguration of Backup Devices

The autoconfiguration wizard enables easy and automatic configuration of libraries in cluster environments. The devices are configured as virtual and floating drives.

Floating drives are devices that are configured on a virtual host, using virtual hostnames. Floating drives should be configured for the backup of cluster-aware applications. This ensures that no matter on which node in the cluster the application is currently running, Data Protector always starts a media agent on that same node.

Before executing Autoconfigure:

- Verify that drive hardware paths are identical on every node.
- Autoconfigure runs only on the active node without checking the inactive nodes. Therefore, drive hardware paths are only determined on the active node.

During execution of Autoconfigure:

- Choose the appropriate virtual hostname.
- Select required devices.
- Enable option “Automatically discover changed SCSI address”, which could help in case of changed backup device paths (this is a well known problem in Windows environments, which can be detected by Data Protector).

After execution of Autoconfigure:

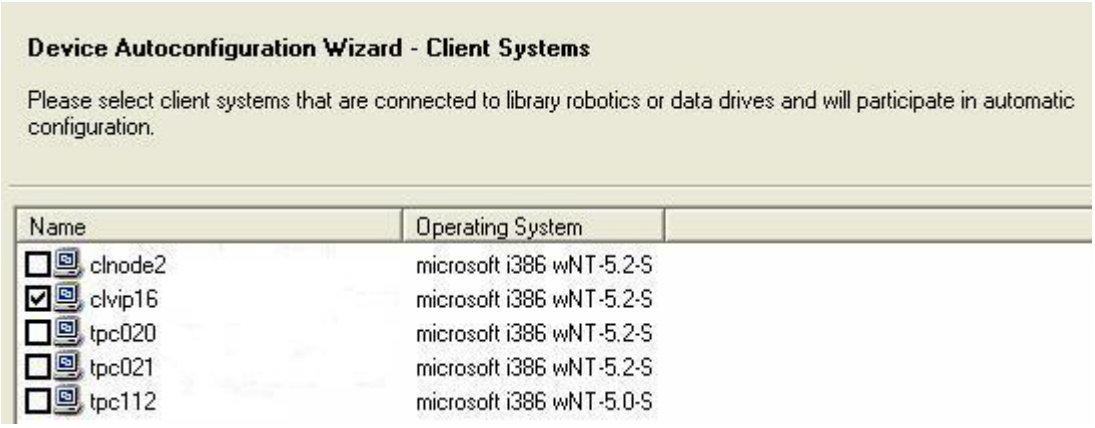
- A failover test is imperative for checking that all paths are matching.

The next figures show an example how to autoconfigure a HP MSL5000 library. In the Scoping Pane, right-click Devices and click Autoconfigure Devices to open the wizard:

**Figure 5.** Device Autoconfiguration Wizard - Start

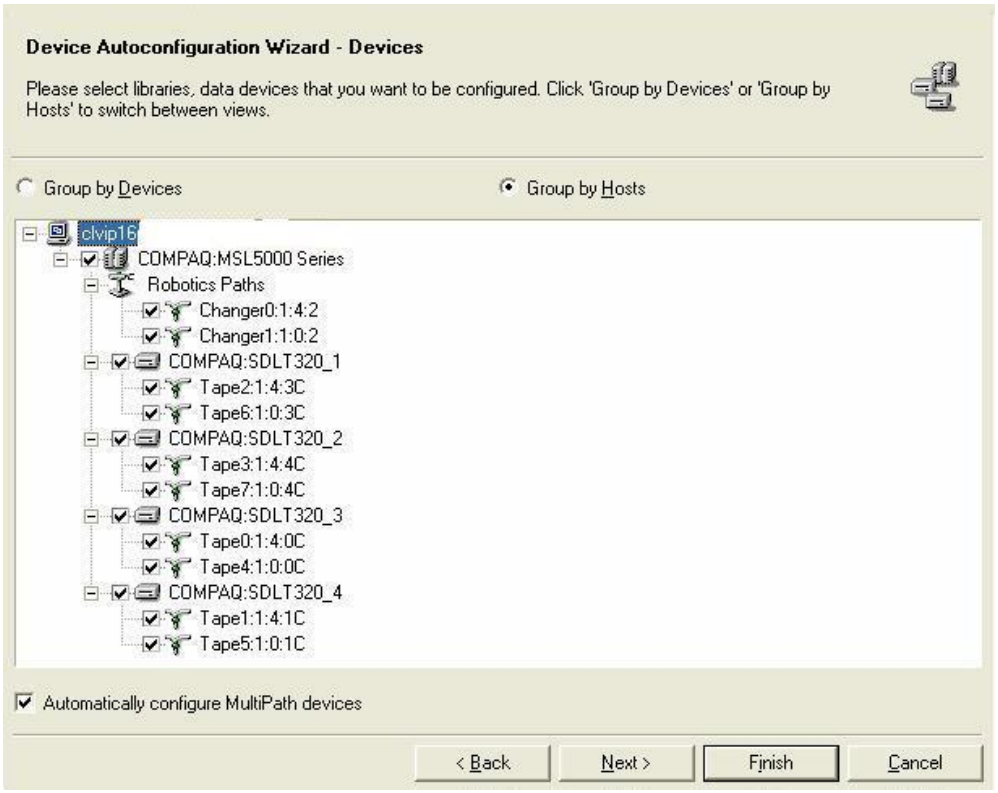

Select the client system by its virtual hostname, which will execute the autoconfiguration on the active node:

**Figure 6.** Device Autoconfiguration Wizard – Client Systems



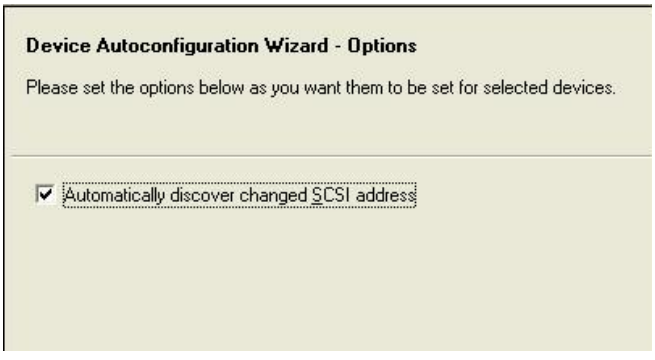
Please note that any device can be accessed from two paths, which is caused by two installed host bus adapters (HBA). Select the tape library with all required tape drives:

**Figure 7.** Device Autoconfiguration Wizard - Devices



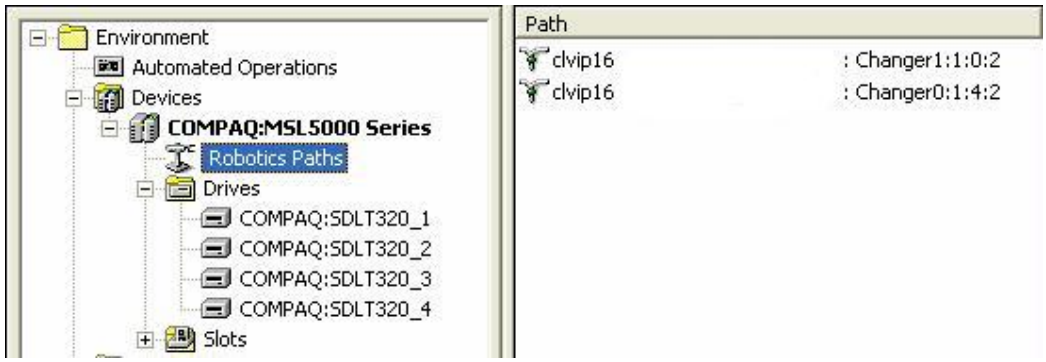

Please enable wizard option "Automatically discover changed SCSI address":

**Figure 8.** Device Autoconfiguration Wizard - Options



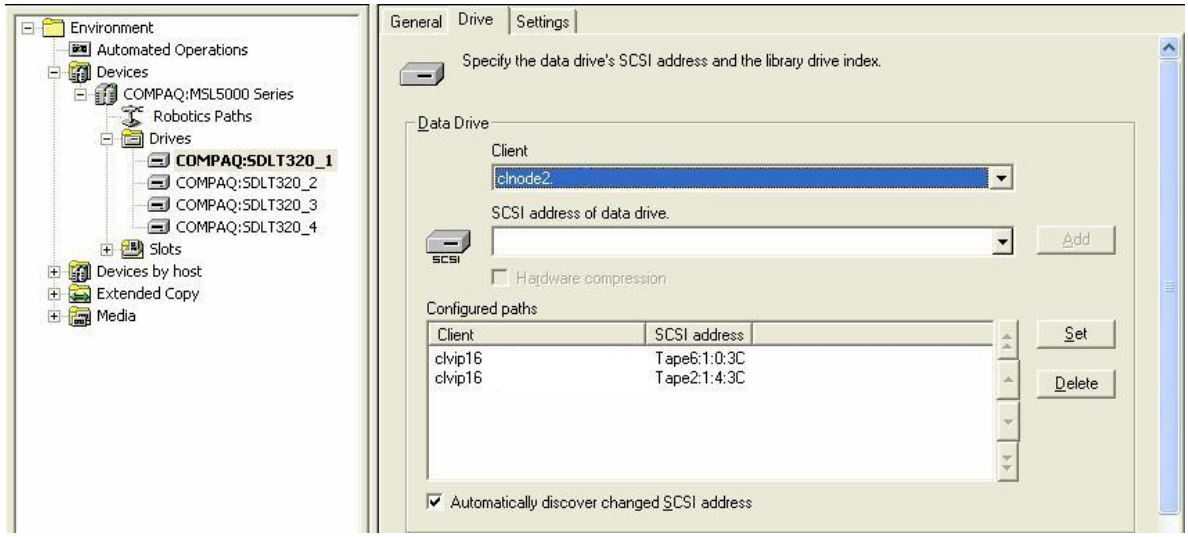
The following figure shows the final library robotics configuration. The robotics can be accessed via the virtual hostname and two different paths (multipath).

**Figure 9.** Final Library Configuration




The next figure shows the final configuration of library drive COMPAQ:SDLT320_1. The drive can be accessed via the virtual hostname and two different paths (multipath).

**Figure 10.** Final Drive Configuration

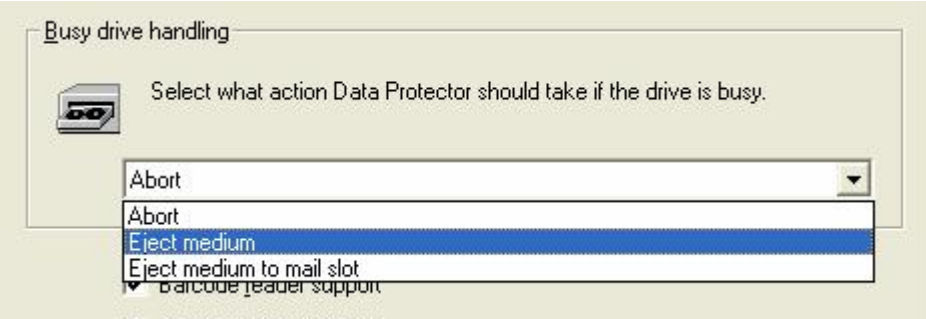


## Busy Drive Handling

Libraries in clustered environments are managed by the active cluster node and the virtual hostname. If the active cluster node fails during a backup, the tape drive could not be unloaded due to an aborted and failing media agent. The next backup going to that drive will recognize an already loaded tape and fail. This can be prevented by setting an appropriate busy drive option.

**Note:** It is highly recommended that libraries configured with virtual hostnames are capable to eject already loaded tapes. This can be achieved by setting the library option "Busy drive handling".

**Figure 11.** Busy Drive Handling – Library Control Option



# Cluster Recovery

This chapter describes some common scenarios, which can be manually fixed and don't require an Automated System Recovery (ASR).

## Cluster Disks

Shared disks use the disk signature to identify a disk and to map the real device to a physical disk resource. When a physical disk resource fails and is replaced, the signature of the newly formatted disk no longer matches the signature stored by the physical disk resource.

Cluster and quorum disks can be recovered with the Microsoft Windows Server 2003 Resource Kit tool ClusterRecovery, which substitutes the newly created physical disk resource for the failed resource. The properties of the failed resource are automatically transferred to the new resource. Any dependencies on the old resource are changed to point to the new resource.

**Note:** In case of a failed quorum disk, the cluster service must be started with parameter "/fixquorum".

The following two figures show a recovery of disk resource "Disk F:". Before executing ClusterRecovery, the new disk resource must be visible to the same set of nodes as the old resource.

**Figure 12.** Server Cluster Recovery Utility – Replace Physical Disk Resource

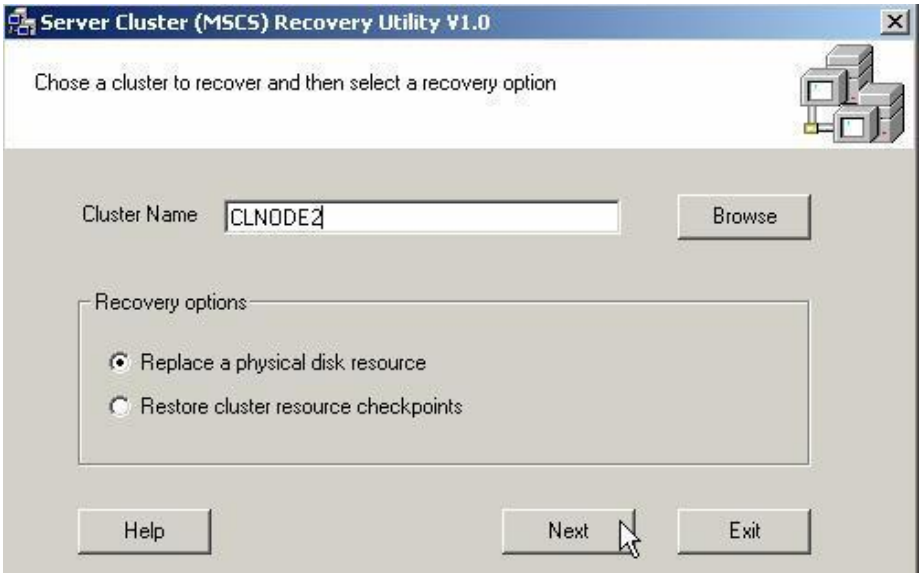


**Figure 13.** Server Cluster Recovery Utility – Select Disk Resources


To complete the replacement, the new disk resource should be brought online and the drive letter should be changed with the disk management snap-in to match the old disk resource (this is necessary because applications typically reference files on the disk via a drive letter).

If the new physical disk resource is successfully validated, the old physical disk resource should be deleted, as it no longer represents a real resource on the cluster.

Once the cluster is configured with the new physical disk resource, the application data can be restored to the disk.

## Debug and Log Files

In case of problems, please check the file "<File Share>\log\Server\cluster.log".

Furthermore, debugs can be created:

1. Take the CRS service resource OBVS_MCRS offline. This will automatically stop the CRS service.
2. Edit the following lines within the trace file in the shared directory (<File Share>\Config\Server\Options\trace):
   — ranges: 1-99
   — postfix: DBG
   — select: <virtual host name>
3. Take the CRS service resource OBVS_MCRS online again. This will automatically start the CRS service.

Another possibility to start the CRS service in debug mode is to add the debug options (-debug 1-99 DBG) to the start parameters of the service resource OBVS_MCRS parameter properties. This is done within the Cluster Administrator GUI.

The debugs can be found in the "$DPHOME\tmp" directory of the active node.

# Automated System Recovery (ASR)

Automated System Recovery is a complex process and must be well organized. It is not sufficient to backup the environment. To be prepared for the real disaster, the disaster recovery process must be executed and verified in advance. Important issues are complete backups, appropriate network settings and correct drivers for mass storage controllers - particularly missing HBA drivers will prevent ASR from recognizing and recreating shared disks.

**Note:** Only local shared storage (connected to cluster nodes via SCSI) is fully supported in cluster environments for ASR. Shared storage on disk arrays connected to cluster nodes via Fibre Channel (for example: EVA or XP disk arrays) is only supported if appropriate device drivers are provided during the initial phase of ASR recovery (by pressing F6). This enables Windows 2003 Setup to correctly detect shared storage located on disk arrays.

## Cluster Backup

One single full backup session is a prerequisite for a successful ASR, which must include:

- All physical nodes including local disks.
- All virtual nodes including shared disks.
- The IDB virtual node, if Data Protector is configured as a cluster-aware application.

**Note:** Perform a full client backup after each hardware, software or configuration change and update the ASR diskettes. This also applies to any network configuration changes, such as change of the IP address or DNS server.

## Hardware Documentation

It is recommended to create a preparation template, as required for the Assisted Manual Disaster Recovery. It could be useful in case the ASR partly fails and e.g. shared disks must be manually created. Please check the *HP OpenView Storage Data Protector 5.5 Administrator's Guide – Appendix A Further Information – Windows Manual Disaster Recovery Preparation Template*.

Furthermore, the configuration of any cluster-aware tape device should be documented including hardware paths. This is valuable information for the local restore mode.

## ASR Set

An ASR set is a collection of files stored on three (32-bit Windows) or four diskettes (64-bit Windows), required for:

- Proper reconfiguration of the replacement disk (disk partitioning and logical volume configuration).
- Automatic recovery of the original system configuration.
- The user data that was backed up during the full client backup.

These files are stored on the Cell Manager as an ASR archive file in the shared directory "<File Share>\Config\Server\dr\asr" as well as on the backup medium.

**Note:** Create the ASR set for the Cell Manager in advance, because you will not be able to obtain the ASR archive file after the disaster. ASR sets for other systems can be created using Cell Manager when a disaster occurs.

## DHCP and DNS

For online ASR, DHCP must be additionally configured, though Microsoft cluster network interfaces must be configured with static IP addresses. DHCP must enable DNS Server, which resolves exactly all involved servers into correct full-qualified hostnames. E.g., online ASR will even fail if only the domain is different.

If DHCP and DNS fail, the ASR offline restore mode is executed.

## Restore Modes

Data Protector attempts automatic media management operations during ASR, which is called online mode. If the Cell Manager is inaccessible, the offline mode is executed.

**Note:** The recovery of the cluster-aware Cell Manager is always offline.

**Online**

The online mode requires full access to the Cell Manager.

**Offline**

If the Cell Manager is inaccessible, the offline mode attempts to start the media agent including robotics support.

**Local**

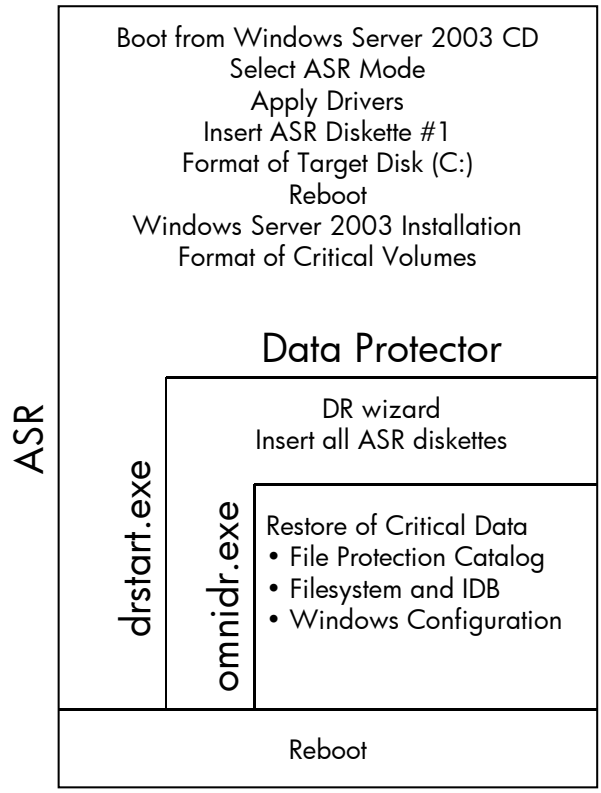
If the online and the offline mode fail, Data Protector executes the local mode. All local devices are scanned and offered in an additional window. In this scenario, it is very helpful to verify the correct device and its hardware path with the latest hardware documentation.

## Process Flow

The following example describes the process flow with all required steps for a cluster-aware Cell Manager configured with two nodes. It is assumed that the active node is completely lost including the shared disks, e.g. that a virus or bad program deleted all volumes with its data. In this case, ASR would restore the disk signatures and partition layouts of all cluster disks. Then, Data Protector would restore all critical volumes (quorum and Data Protector “DPSHARE”). After ASR has finished, non-critical volumes must be manually restored.

The following figure describes major steps of ASR:

**Figure 14.** Simplified ASR Process Flow




The next list describes the ASR steps in detail:

1. Make sure that you have the following available:
   - The latest ASR floppy disks (as long as the cell manager is available, they can be created or updated with the disaster recovery wizard).
   - The latest backup media.
   - The original operating system installation CD.
   - If you have a mass storage controller and you are aware that the manufacturer has supplied a separate driver file for it (different from driver files available on the Setup CD), obtain the file (on a floppy disk).
2. Verify that the second node is switched off and does not access shared disk resources.
3. Insert the original operating system installation CD.
4. Restart the computer.
5. If you have a separate driver file as described in step 1, use the driver as part of Setup by pressing F6 when prompted.
6. Press F2 when prompted at the beginning of the text-only mode section of Setup.
7. If required, apply a separate driver file as described in step 1.
8. If prompted, insert the ASR floppy disk.
9. If prompted, confirm the delete and format partitions screen.
10. If prompted, re-apply a separate driver file.

11. If prompted, re-insert the ASR floppy disk.
12. ASR automatically reboots.
13. Remove the ASR floppy disk, which will later cause the DR process to stop and to offer additional options (Registry Editor, Command Window, Task Manager, Debug, Install Only).
14. The ASR starts the preparation of the operating system installation, which takes a couple of minutes.
15. In the preparing installation step and immediately after installing devices and network, all cluster disks are automatically formatted. If not, a problem with mass storage driver could be the reason as mentioned in step 1.
16. The DR wizard starts. Open at least one CMD-window. This enables file system access in case of problems.
17. If prompted, enter the drive letter and path of the SRD-file.
18. Follow the directions on the screen and insert all ASR floppy disks (which are copied to "\WINDOWS\system32\OB2DR\bin").
19. Select wizard option "Finish".
20. ASR starts Data Protector the OMNIDR utility ("omnidr.exe –srd recovery.srd"), which executes the following steps:
    - Start INETD daemon.
    - Check online restore mode, which will fail in this scenario due the DR of the Cell Manager.
    - Attempt offline restore mode. It could fail in case of an outdated SCSITAB or mismatch of robotics and tape drivers (e.g. "scsi5:1:0:2" instead of "Changer0:1:0:2"). The outdated SCSITAB problem and its solution are described in chapter ASR and Outdated SCSITAB and the driver problem in chapter ASR and Mismatch of Robotics and Tape Drivers.
    - If offline restore mode fails, local restore mode is started. A device menu will prompt you to select a device with the loaded tape media. Please make sure that the media is loaded before the appropriate device is selected. Otherwise, ASR will fail and finish.
    - Data Protector starts restore sessions one after the other for the Windows file protection catalog, the operating system volume (C:) in parallel with the Data Protector shared volume (DPSHARE), and the Windows configuration database (registry).
21. ASR reboots automatically.

After the successful ASR, restore all non-critical volumes as described in the HP OpenView Storage Data Protector 5.5 Administrator's Guide.

## Debug and Log Files

Per default, Data Protector creates ASR debug and log files in the following directories:

- \WINDOWS\system32\OB2DR\tmp\debug.log
- \WINDOWS\system32\OB2DR\bin\OB2DBG*.txt

## Additional Support Information

In the past, many questions were asked regarding the support of network card teaming and RAID type of disk arrays. Network card teaming is supported and Data Protector is able to determine the correct IP address, which is saved in the SRD-file.

RAID technology is supported but could cause more effort during disaster recovery due to additional steps with disk array belonging tools. If the disk array is lost, the same volume configuration must be re-established for a successful ASR.

# Known Issues

## Pre-Installation Requirement of File Share Resource

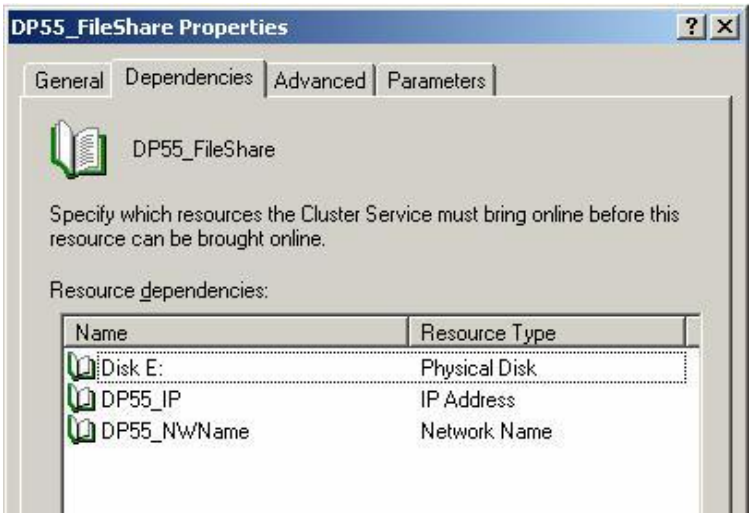
**File Share Dependencies**

The <File Share> resource, where Data Protector has to be installed, must have the following resources set among the <File Share> dependencies (as described in the *HP OpenView Storage Data Protector 5.5 Administrator's Guide* chapter *Installing Data Protector on Microsoft Cluster Server*):

- IP Address
- Network Name
- Physical Disk

Before installation, check the file share resource for the following dependencies:

**Figure 15.** Dependencies of File Share Resource




**File Share Permissions**

Microsoft Windows Server 2003 gives only read access to everyone. Therefore, configuration file "omni_info" cannot be created and installation directory "<File Share>\Config\ Server\install" is empty. At this stage Data Protector needs:

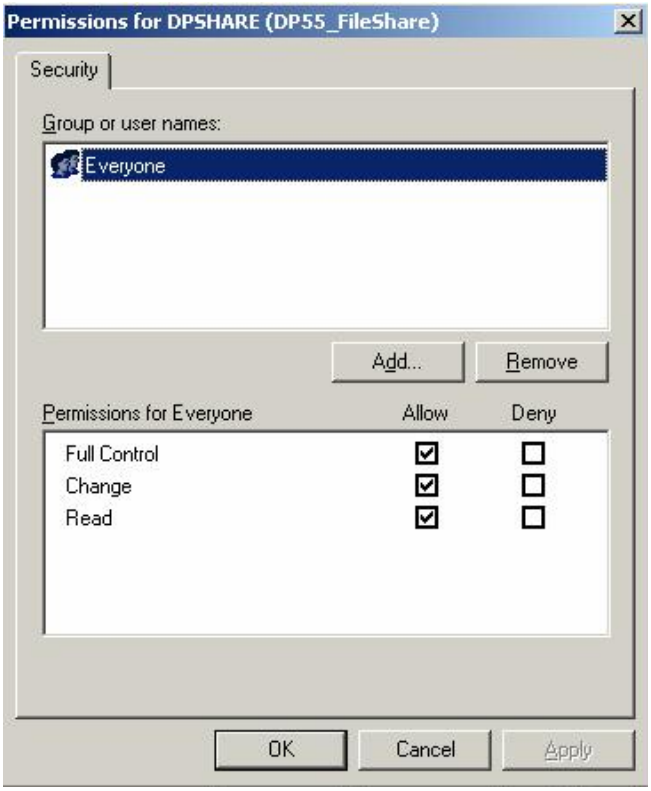
1. To be uninstalled.
2. File share permissions to be fixed.
3. To be reinstalled.

**Workaround:** To avoid this problem before installing Data Protector in a MS Cluster, a Data Protector cluster group containing the future DP folder as file share resource type needs to be created. Then all operations to everyone (or at least the accounts that will write in this folder or subfolders) must be granted.

It is planned to fix this problem in the future. Please check the latest patches.

The following figure shows the corrected permissions for file share resource DPSHARE:

**Figure 16.** Permissions for DPHSHARE



## Post-Installation Check of Resource Dependencies

After installation, check the following resources for correct dependencies:

**Figure 17.** Dependencies of OBVS_MCRS

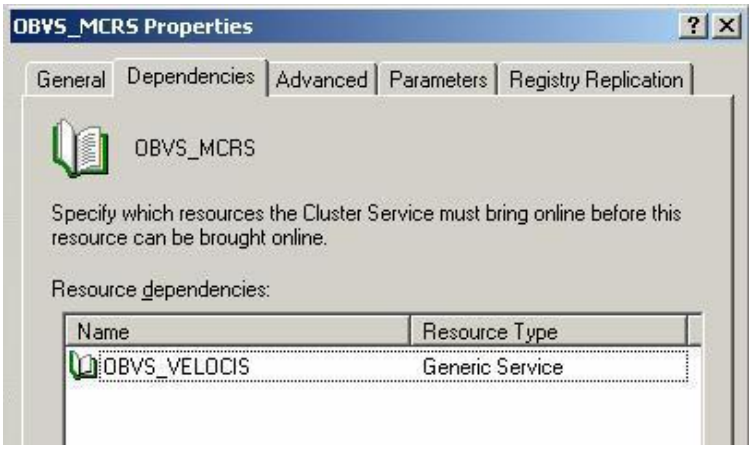



**Figure 18.** Dependencies of OBVS_VELOCIS

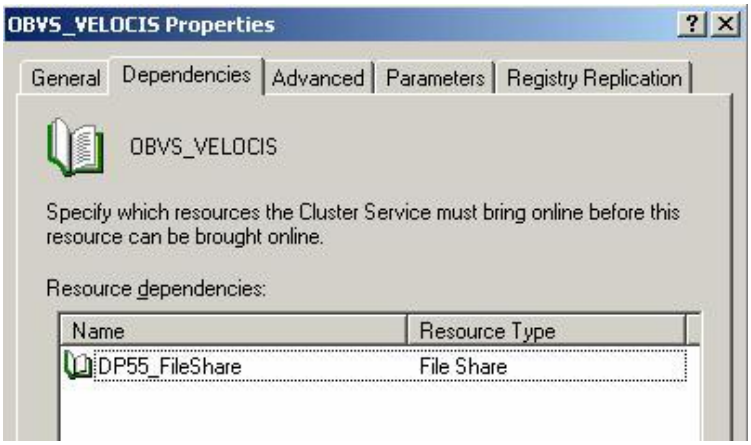


**Figure 19.** Dependencies of OmniBack Share

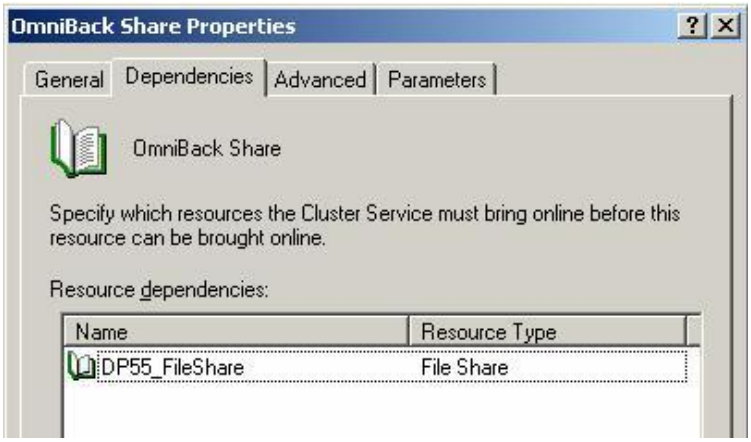
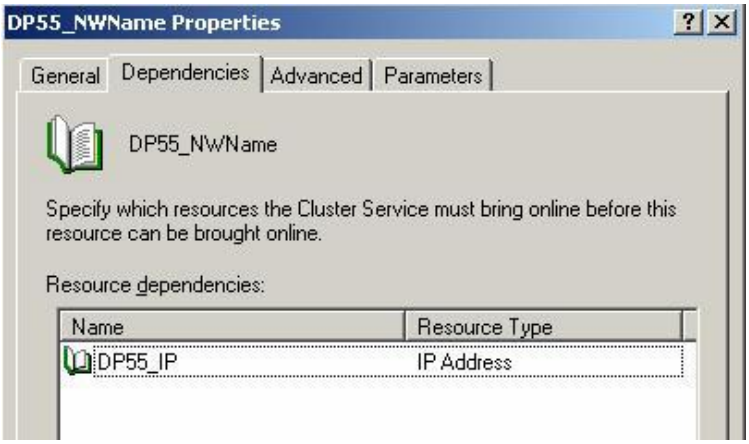



**Figure 20.** Dependencies of Network Name



## Tape Devices and Failover

Tape devices connected to cluster nodes and its loaded media require additional attention after failover.

**Note:** If a failover during backup activity occurs, the Data Protector may not be able to properly abort the session. Data may not be completely written which results in the corruption of the medium. It is highly recommended to restart the belonging backup session.

## Cluster Database Restore

Two major problems are known:

1. The restore session of the cluster database fails because the ASR process restarts the cluster services during the session.
   When DP starts the cluster database restore, it calls the belonging Windows API. The API stops the cluster services and with it DP session connections, before the restore session has finished.
2. The cluster database restore of a clustered Cell Manager may result in a failover.
   **Note:** Before starting the restore of a cluster database, you should stop the cluster service on all inactive nodes.

It is planned to fix this problems in the future. Please check the latest release notes and patches.

## ASR and Windows RSM

The Windows Removable Storage Manager (RSM) is activated during ASR.

RSM is a service used for managing removable media (such as tapes and discs) and storage devices (libraries). With RSM and SAN shared libraries, there are known issues.

RSM automatically scans system buses after reboot to determine if there are any removable storage devices available for Windows to manage. This can interrupt backup and restores by doing a poll of connected devices causing a SCSI reset on shared buses.

Additionally, there is a conflict of ownership for the removable storage devices. If the RSM service is running, it captures library devices and maps them to Windows. The devices will be no longer available for Data Protector.

**Note:** The RSM service should be manually disabled after the ASR process has finished (after the final reboot). A solution will be provided in the near future. Please check the latest AUTODR patch.

## ASR and Local Tape Devices

If the Data Protector Cell Manager together with local tape devices is installed cluster-aware, the ASR process cannot access the local tape devices by its virtual hostnames.

ASR enters the local restore mode, starts a device autoconfiguration and sets the tape device hostname temporarily to “machinename”, which does not match the name as described in the SRD-file “recovery.srd”. Change in the SRD-file the system name specified with “–mahost” file to “machinename” in order to avoid the local restore mode.

Please check in the *HP OpenView Storage Data Protector 5.5 Administrator’s Guide* chapter *Advanced Recovery Tasks* how to edit the SRD-file.

If the SRD-file is not changed, the autoconfiguration process will determine any available tape devices and offer it to the disaster recovery wizard. The devices and their hardware paths are displayed. You must insert a tape into the device and choose the correct path in the wizard. This can be quite complicated if the library is SAN-attached and drives are multiple displayed. In this case, the latest

hardware documentation is required to determine the correct path. If a wrong device is chosen, ASR will fail and the process must be repeated.

## ASR and Outdated SCSITAB

If you are using a locally attached device for ASR, test if it's supported. E.g., if the original DP 5.5 released SCSITAB-file was updated with information for the library used for the disaster recovery process, it must be copied to the first ASR disk.

Please check in the *HP OpenView Storage Data Protector 5.5 Administrator's Guide* chapter *Disaster Recovery / Automated System Recovery / Preparation*.

## ASR and Mismatch of Robotics and Tape Drivers

Due to historical issues of Data Protector, the OMNIDR utility ("omnidr.exe") utility always disables tape/robotics drivers, which are enabled per default by ASR. Example: Tape1:0:0:0 becomes scsi1:0:0:0. The same happens to the robotics devices. This is exactly what was necessary to be done in former Data Protector releases, because all devices were typically installed as "scsi#:#:#:#" and not "Tape#:#:#:#".

The mismatch driver problem could be fixed in the SRD-File by replacing all "Changer" and "Tape" entries ("-devioctl" and "-devaddr") with the appropriate SCSI-paths:

1. After the DR wizard starts, please open at least one CMD-window as described in step 16 of chapter Process Flow.
2. Execute the OMNIDR utility: "omnidr.exe –srd recovery.srd". This will disable all tape/robotics drivers (must run before "devbra.exe" is executed).
3. If it fails, determine the appropriate SCSI-paths by executing "devbra.exe -dev" in the CMD-window.
4. Modify the SRD-File as described above.
5. Restart the OMNIDR utility: "omnidr.exe –srd recovery.srd".

## ASR and Shared Disks

This chapter covers the EVA only. Other disk arrays might have different procedures.

**Note:** Before executing ASR, it's highly recommended to start with **clean and unpartitioned** virtual disks. If not, the ASR process could skip the discs due to a function that avoids overwriting existing data. The virtual discs would have to be manually created and recovered afterwards.

If the problem with the mass storage controller, as described in chapter Automated System Recovery (ASR), cannot be fixed and shared disks are not correctly recognized, a workaround with manual disk partitioning and formatting could be executed. In this case, execute steps 1 – 16 as described in chapter Process Flow. Then, follow this procedure:

1. Select wizard option "Install Only".
2. Follow the directions on the screen and insert all ASR floppy disks (which are copied to "\WINDOWS\system32\OB2DR\bin").
3. Determine the cluster disk numbers (Disk #) in the diskinfo section of the SRD-File.
   First, search for the appropriate drive letter in the parameter "-letter" and the belonging signature in "-volume":
   "*-volume 1141165761* -number 2 *-letter Q* …"
   Then, search with the just determined signature in "-layout" for the belonging disk number in the disk section:
   "*-disk 2* -addr 0 -sizelow 0 -sizehigh 0 -descr "Compaq Secure Path Disk" -geo 12 -cyl 261 -tpc

255 -spt 63 -bps 512 *-layout 1141165761* -partcount 4"
In this example, disk 2 would be the searched disk.

4. In the CMD-window, execute:
   "\WINDOWS\system32\bin\diskpart.exe".
   - List all disks, e.g.:
   "DISKPART> list disk"
   - Select the correct disk with the determined disk number, e.g.:
   "DISKPART> select disk 1"
   - Create a partition, e.g.:
   "DISKPART> create partition primary".
   - Assign a drive letter, e.g.:
   "assign letter=Q"
   - Repeat the steps for all remaining cluster disks - create partitions and assign drive letters.
   - Finish diskpart.
5. Format all partitioned disks of step 5 from the CMD-window, e.g.
   " C:\WINDOWS\system32> format Q: /fs:ntfs"
6. In the CMD-window, execute
   "\WINDOWS\system32\bin\omnidr.exe –srd recovery.srd".
   This will start multiple restore sessions for Windows file protection catalog, critical data including IDB, and Windows configuration.
7. After successful restore, select the Abort button. This will finish the Install Only mode.
8. ASR reboots automatically.
9. Install Microsoft Resource Kit Tools.
10. Execute ClusterRecovery and replace all bad disk resources.
11. Start second cluster node.
12. Delete all bad disk resources.

**Note:** The DR wizard option WinDisk, which would start the disk manager, cannot be used during ASR.

# Tools

## Microsoft Windows Server 2003 Resource Kit Tools

The resource kit contains tools, which allows fixing cluster problems. E.g., ClusterRecovery helps to re-create shared disks and resource checkpoints. Please check the Microsoft documentation for use cases and appropriate tools.

Microsoft Windows Server 2003 Resource Kit Tools
http://www.microsoft.com/windowsserver2003/downloads/tools

# Summary

This white paper describes the Microsoft Windows Server 2003 Cluster Server integration issues of HP OpenView Storage Data Protector 5.5. Installation, software maintenance (patches), configuration and cluster recovery issues are covered with examples. Additionally, known issues are documented for avoiding common problem cases.

The described limitations and notes should be very well considered.

# For more information

HP OpenView Storage Data Protector
http://www.hp.com/go/dataprotector

HP OpenView Storage Data Protector 5.5 Guides
http://ovweb.external.hp.com/lpe/doc_serv

HP OpenView Storage Data Protector v5.5 Support Matrices
http://www.openview.hp.com/products/datapro/spec_0001.html

Windows Server 2003
http://www.microsoft.com/windowsserver2003

Microsoft TechNet
http://www.microsoft.com/technet

Guide to Creating and Configuring a Server Cluster under Windows Server 2003
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/clustering

Products Designed for Microsoft Windows – Windows Catalog and HCL
http://www.microsoft.com/whdc/hcl

Microsoft Windows Server 2003 Resource Kit Tools
http://www.microsoft.com/windowsserver2003/downloads/tools

Microsoft Windows Server 2003 Cluster Documentation
http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/win_cluster.asp



4AA0-7013ENW, 07/2003

invent