HP OpenView Storage Data Protector A.06.00

Disaster Recovery Enhancements

White Paper

Manufacturing Part Number: n/a

May 2007

Legal Notices

1 Disaster Recovery Enhancements

Overview

The release version of Data Protector A.06.00 supports Enhanced Automated Disaster Recovery (EADR) and One Button Disaster Recovery (OBDR) only on 32-bit Windows 2000 systems. The patch DPWIN_00270 adds support for additional platforms and replaces the existing disaster recovery module on Windows 2000.

For details on how to plan, prepare for, configure, and perform a disaster recovery, see the *HP OpenView Storage Data Protector Disaster Recovery Guide*.

Supported Platforms

EADR and OBDR are supported on the following Windows systems:

- Windows 2000
- Windows XP Professional SP2 (x86)
- Windows Server 2003 SP1, R2 (x86)

64-bit platforms are *not* supported in this release.

Prerequisites

See the *HP OpenView Storage Data Protector Disaster Recovery Guide* for general prerequisites for disaster recovery.

Installation and Upgrade

For details on how to install patches, see the patch documentation and the *HP OpenView Storage Data Protector Installation and Licensing Guide*.

When you install the patch, the following Data Protector components are replaced: CORE, CC, DA, and DR.

The following patches are required by DPWIN_00270:

- CORE packet patch: DPWIN_00265
- Disk Agent (DA) packet patch: DPWIN_00271
- Cell Console (CC) packet patch: DPWIN_00266

Windows 2000

IMPORTANT

Part of preparations for EADR and OBDR is a full client backup. A full client backup of a Windows 2000 system that will be used for creating a disaster recovery image and which is created before the disaster recovery patch DPWIN_00270 is installed, cannot be used to create a disaster recovery image on clients with the patch DPWIN_00270.

You must perform a full client backup after you install the patch. See the *HP OpenView Storage Data Protector Disaster Recovery Guide*.

Patch your cell sequentially:

1. Until you perform a *full backup of all clients in your cell*, keep at least one Windows 2000 client unpatched. This client can be used to create a disaster recovery image from old backups.
2. After you back up all patched clients, install the patch on the remaining client and perform a full backup of this client.

Windows XP and 2003

No additional steps are required for Windows XP Professional and Windows Server 2003.

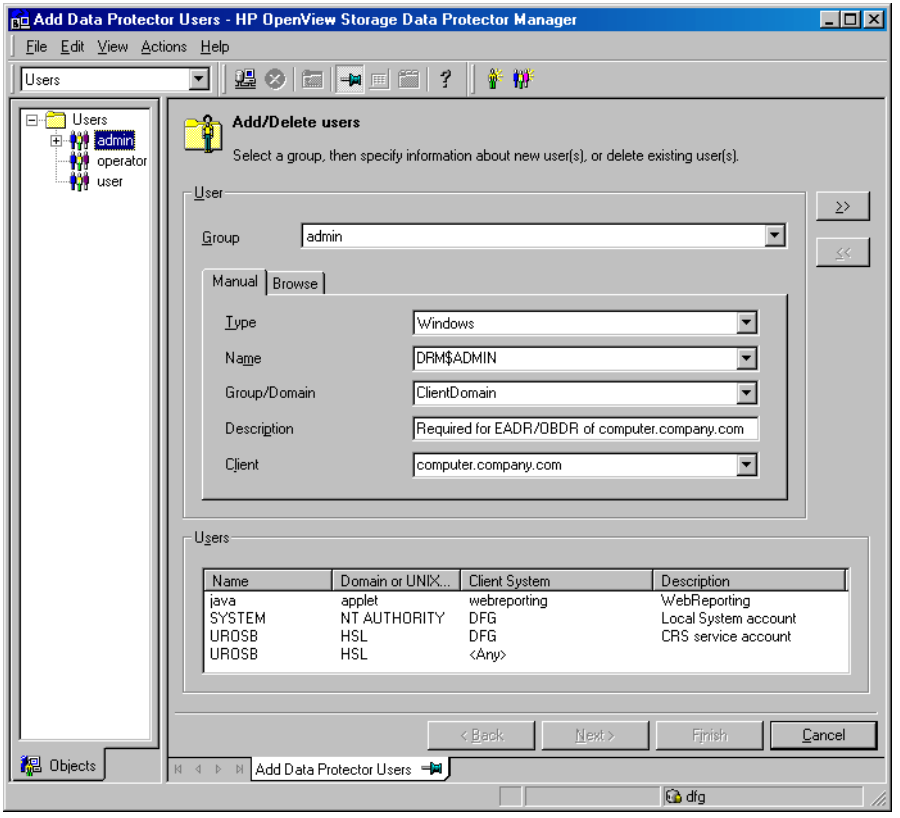
Compatibility and Interoperability

- Backups on Windows 2000 systems that were created before the disaster recovery patch was installed, cannot be used to create disaster recovery images on clients with the patch.
- The patched GUI is compatible with the old disaster recovery module and can be used to create disaster recovery images on Windows 2000 clients with the old disaster recovery module. For example, you can have a Windows 2000 system with the old disaster recovery module and patched GUI. In such a case, the GUI creates a disaster recovery image using a backup created with old disaster recovery module.
- For EADR and OBDR, you must add the `DRM$ADMIN` account to the Data Protector Admin user group instead of the client's local Administrator account (used in Data Protector 6.0 without the patch).

  See the "Recovery" subsections in the EADR and OBDR sections of the *HP OpenView Storage Data Protector Disaster Recovery Guide*.

The modified first step of the recovery procedure:

1. Unless you are performing an offline disaster recovery, add the `DRM$ADMIN` account to the Data Protector Admin user group on the Cell Manager. See the online Help index “adding Data Protector users”.



Encryption

IMPORTANT To perform disaster recovery using *encrypted* backups, export the encryption key (in the `OmniKeyStore` file) and store it in a safe location as part of disaster recovery preparations *before a disaster occurs*. The key is needed to decrypt the data during disaster recovery.

EADR/OBDR procedure when encryption is used:

1. Use the `omnikeytool -create` command to create the `OmniKeyStore` file in the `<Data_Protector_home>` directory.
2. Ensure that the `Encryption` option is selected in the backup specification.
3. Perform a full client backup when using EADR or an OBDR backup when using OBDR. For the OBDR backup, create the backup specification using the Data Protector One Button Disaster Recovery Wizard.
4. Copy the `OmniKeyStore` file to removable medium (floppy disk, CD, USB flash key) or to another system, and store the medium in a safe location.

IMPORTANT Each time you change or add additional keys to the client, update the copy of the `OmniKeyStore` file on the removable medium or other system.

5. If using EADR, create an EADR disaster recovery CD ISO image.

IMPORTANT Prepare a disaster recovery CD in advance for any critical systems that must be restored first (such as DNS servers, Cell Managers, Media Agent clients, file servers).

6. During disaster recovery, when the `omnidr` command is started, the following prompt is displayed:

   Do the following:

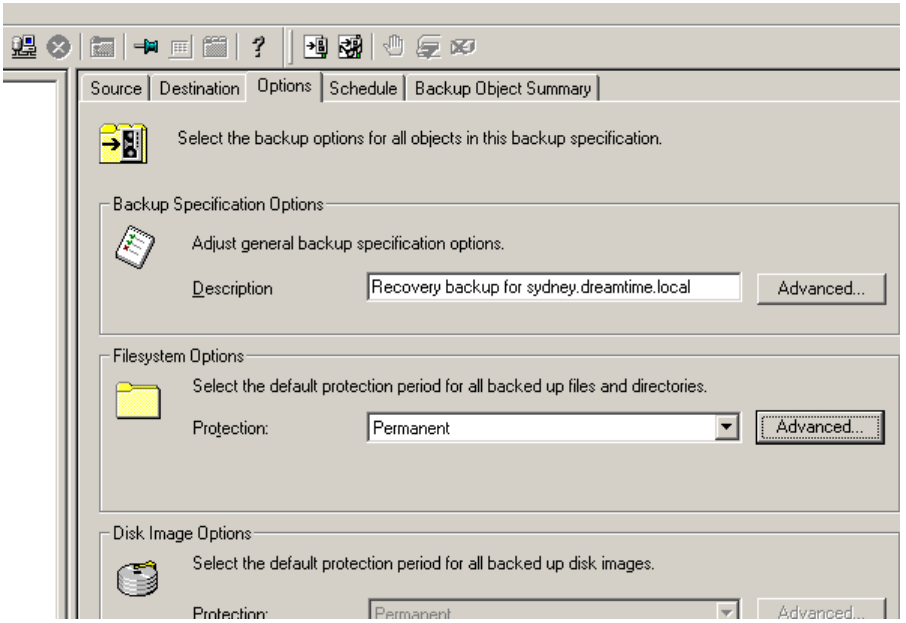
   - If encryption is not used, enter `n`. Disaster recovery continues without further interruption.
   - If encryption is used, enter `y`. Ensure that the `OmniKeyStore` file is available on the client (for example, by inserting a CD-ROM, floppy disk, or a USB flash key) and enter the full path to the `OmniKeyStore` file. The `OmniKeyStore` file is copied to the default location on the MiniOS and is used by the Disk Agents. Disaster recovery now continues without further interruption.

Creating OBDR Backup Specifications

When creating a OBDR backup specifications, encryption cannot be enabled. To enable encryption for a saved OBDR backup specification, proceed as follows:

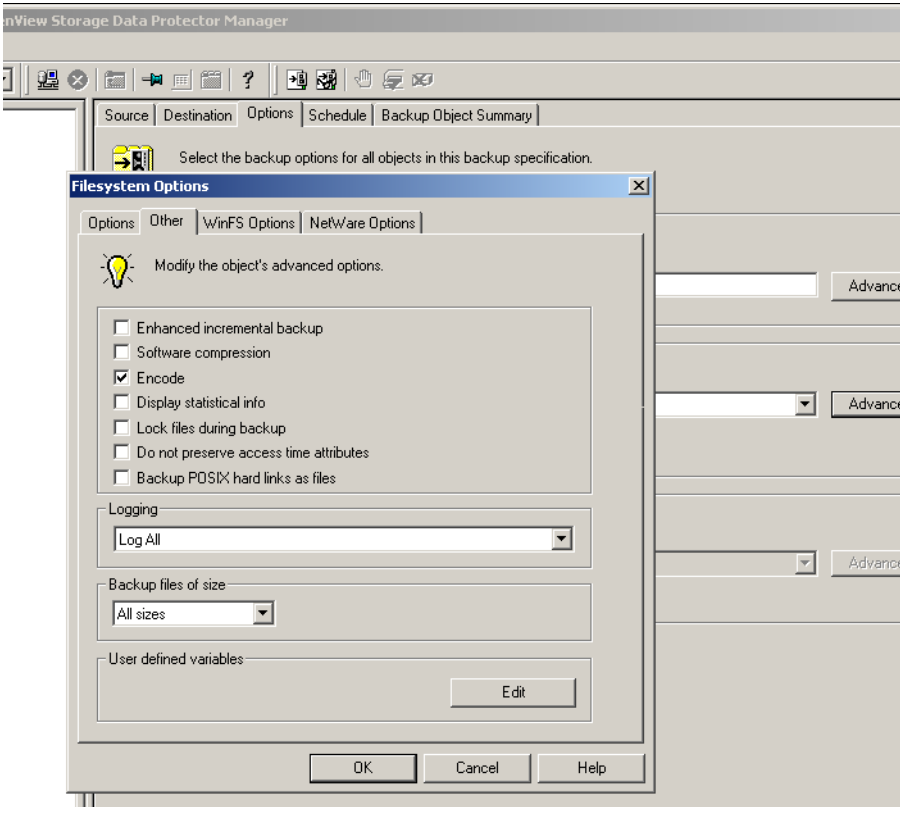
1. Create and save the OBDR backup specification without encryption.
2. Open the saved OBDR backup specification.When asked to treat the backup specification as an OBDR backup, click `No`.

The filesystem options are now enabled.



3. In the `Options` property page, under `Filesystem Options`, click `Advanced`.

4. In the `Filesystem Options` dialog window, in the `Other` property page, select `Encode`.
   Click `OK`.



5. Proceed with the OBDR backup.

Disk Delivery with AES Encryption

When performing a Disk Delivery Disaster Recovery you cannot provide the location of the `OmniKeyStore` file in the Disk Delivery wizard to enable an AES encrypted Disk Delivery.

To enable an AES encrypted Disk Delivery, proceed as follows:

1. On the client where Disk Delivery is being performed, rename the original `OmniKeyStore` file located in the *`<Data_Protector_home>`* directory to `OmniKeyStore.orig`.

2. Copy the `OmniKeyStore` file of the client you wish to recover to the *<Data_Protector_home>* directory on the client where disaster recovery is performed.

   The AES encrypted recovery will now find the `OmniKeyStore` file automatically and the recovery will continue.

3. After a successful recovery, remove the `OmniKeyStore` file from *<Data_Protector_home>* directory and rename `OmniKeyStore.orig` to `OmniKeyStore`.

GUI Changes

1. Before you install the patch DPWIN_00270, a disaster recovery image can be created only from a GUI started on Windows 2000 and Windows NT systems because a DRIM disaster recovery module is present only on these systems. After you install the patch DPWIN_00270, the GUI on any client can be used to create images for any client.

   If you try to create an image for a Windows 2000 client from GUI started on a Windows 2003 or XP and you want to use a backup created with the unpatched Data Protector client, the following error is displayed:

   ```
   Unsupported version of drecovery.ini file.

   The drecovery.ini file of your client is created with old
   version of Disaster Recovery Module and is not supported
   by the Disaster Recovery Module on this client. Go to the
   client that has the old version of Disaster Recovery
   Module and create ISO image for your client there.
   ```

Limitations

- Disaster recovery ISO images cannot be created on systems where Data Protector is installed on FAT/FAT32 partitions. You need at least one client in the cell where Data Protector is installed on an NTFS volume to be able to create disaster recovery images.

  However, OBDR ISO images are always created on the system that is backed up. OBDR is therefore supported only on systems where Data Protector is installed on an NTFS volume.

- The encryption key is *always restored to the default location* (`<Data Protector home>\omnikeystore`) and not to the location set by the `omnirc` variable `OB2ENCODE_KEYSTORE`.

  The variable `OB2ENCODE_KEYSTORE` is used to specify the location of the `omnikeystore` file so that it can be collected and included in a disaster recovery image. The variable is used only at the time of backup. When setting `OB2ENCODE_KEYSTORE`, note that the variable

must point to a location within the Data Protector directory tree (for example, if Data Protector is installed on drive `c:`, then only paths on drive `c:` are valid).

- Disk Delivery Disaster Recovery of a Windows client does not support AES encryption or decryption. Consequently, if a recovery of a system is performed with Disk Delivery using a backup encrypted with AES, the restored system will be unusable. To be able to recover a Windows client using Disk Delivery, a client has to be backed up without AES encryption.
- In a cluster environment, a cluster node can be successfully backed up if the bus address enumeration on each cluster node is the same. This means that you need:
  - — equal cluster node motherboard hardware
  - — the same OS version on both nodes (service packs and updates)
  - — the same number and type of bus controllers
  - — bus controllers must be inserted in the same PCI mother board slots.
- On Windows 2003 systems, the desktop can lock due to a long period of inactivity. To proceed with disaster recovery, unlock the screen. The password is `dr8$ad81n$pa55wd`
- Driver files that are locked exclusively (for example `sptd.sys` by Daemon Tools) cannot be backed up and will cause the backup to fail.
- A backup of all necessary data for disaster recovery may require a significant amount of free space. While normally 500 MB is enough, up to 1 GB may be required depending on the operating system.
- On some systems (depending on the disk controller and its configuration) a volume (without a drive letter assigned) associated with a mount point on a different volume may not be re-mounted properly during phase 1 of the disaster recovery. This may occur if the volume containing the mount point is recreated or reformatted (for example the System Volume with MiniOS), causing the operating system to boot in “Safe Mode” and to miss the detection of the file system present on the original mount point's target volume. Consequently, the disaster recovery module does not recognize this volume and reports it as `MISSING` in the `drecovery.ini` file. The contents of such a volume are intact, even if it is not recognized.

Workarounds:

— Mount the volume with a drive letter and verify it with the `chkdsk /v /f` command or wait until the system is completely restored and then recreate the original mount point.

— Manually reboot the system directly to MiniOS (do not reboot from the recovery CD). The previously unmounted volume will be automatically mounted to a drive letter.

- The disaster recovery MiniOS is currently incompatible with NVIDIA ActiveArmor firewall (integrated on network adapters that come with certain Hewlett Packard's workstations, for example XW9300). You must either remove or disable the firewall before performing a disaster recovery backup to establish the proper network environment for the recovery phase. The same might be necessary for on-board firewalls of other vendors.
- If the operating system was not activated at the time of the backup and the activation period expires, disaster recovery fails.
- To properly restore an ADS server, the person responsible for its' restore has to know the password for the ADS repair mode (which is not necessarily the same as the password used for the domain administrator login). To ensure that the correct password is indeed known to the administrator, he/she should - prior to performing a disaster recovery backup - reboot the server into the ADS repair mode to determine that the password used during the recovery will be recognized by the system. If you cannot log in to the system during this test procedure, the same will happen during the restore. In such cases measures should be taken to properly configure ADS repair mode login credentials (for example by using the `ntdsutil` tool).

Uninstalling

Uninstalling on a Client

Use the Windows `Add/Remove Programs` tool to remove the Automated Disaster Recovery module from the client:

1. Open `Start` > `Settings` > `Control Panel` > `Add/Remove Programs`.
2. From the list of installed software, select `HP OpenView Storage Data Protector A.06.00` and click `Change`. Click `Next`.
3. In the Program Maintenance window, select `Modify` and click `Next`.
4. In the Component Selection window, deselect `Automatic Disaster Recovery`.
5. Click `Next` and then `Install` to uninstall the disaster recovery module from the client.

This procedure will uninstall any disaster recovery component from the client.

Restoring the old Disaster Recovery Module

On Windows 2000 clients, to restore the disaster recovery functionality as it was before the patch DPWIN_00270 was installed, uninstall the patch from the Installation Server and reinstall the (old) Disaster Recovery module from the Installation Server to the client.

Uninstalling on an Installation Server or Cell Manager

Go to the directory with the Data Protector utilities:

`cd <Data_Protector_home>\bin\utilns`

`remove_patch DR <path to the original product depot>`

For example, if the product DVD is mounted on drive E:

```
remove_patch DR E:\WINDOWS_OTHER
```

Third-party Software Included in this Release

Parts of this product contain third party software licensed under the following licenses:

1. **Boost**

   Revised $Date: 2005/12/05 04:16:19 $ Copyright Beman Dawes, David Abrahams, 1998-2003. Copyright Rene Rivera 2004-2005. Distributed under the Boost Software License, Version 1.0. (See accompanying file `LICENSE_1_0.txt` or copy at http://www.boost.org/ LICENSE_1_0.txt):

   Boost Software License - Version 1.0 - August 17th, 2003

   Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

   The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

   THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

2. **MKIsofs**

   Copyright (C) 1999, 2000, 2001 Joerg Schilling

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.

3. **ZLIB**

   The zlib/libpng License

   Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler

   This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

   a. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

   b. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

   c. This notice may not be removed or altered from any source distribution.