

Data Protection for the Standard 3HD (XP) DAW

Norton Ghost 2003 and NovaStor NovaBackup

DEFINITION: A “Standard 3HD DAW” is a music-computer with three Hard-Drives, representing what I believe to be the current standard for a complete single-computer system.

My goal is to provide convincing analysis and guidelines for the protection and availability of computer music files. As a DAW composer and technical consultant, with a long history in mainstream IT, I believe there is a need for such information at this point in DAW development. As important as our digital music is, what does the DAW community currently use for backup? Imaging utilities are popular because of their ability to reliably “clone” drives for Disaster Recovery, but this only affords a partial solution. Other data is often simply copied to external hard-drive or burned to cd/dvd. Generally there is no master catalog used to organize backup/restore, nor comprehensive strategy applied to the full range of protection needs. As the size of DAW data increases, so does the complexity and necessity of its total protection. Fortunately, there are now numerous affordable backup applications along with massive data storage options from supersized SATA hard-drives to Blu-Ray DVD. All considered, now is a great time to move up to a more complete data protection plan.

In this guide I will explain the protection concepts and strategies I’ve developed, as specifically applied to the Windows XP operating system. Using “Norton Ghost 2003” for imaging and “NovaStor NovaBackup” as traditional backup software (along with a few hardware tools), I will show how you can setup and support a comprehensive, high-speed, low-maintenance, backup/restore solution.

Think of all the time you spend in the process of creating computer-music. You sweat and toil, revising and updating, until your artistic vision is realized. As you work in a digital medium, all of this labor is saved in complex patterns of zeros and ones to computer files stored on hard-drive. These files can be easily retrieved; updated, relocated... it’s a happy digital world until that hard-drive fails. This failure is not a distant possibility, but an inevitability. All hard drives, no matter how expensive and well designed, will fail. Your personal user files and the installed programs and data that help create them, can be gone in an instant, without warning. As traumatic as this scenario sounds, it is one you must contemplate in order to build a solid strategy of data protection and disaster recovery.

How important are your user-files? How much time and trouble will it take to re-install your computer programs and data? For DAW users, these questions have special significance. Today’s standard DAW holds at least 300gb of storage. To effectively manage programs, audio recording, and streaming Virtual Instruments, a single-computer DAW needs three hard-drives, each requiring a special approach to data protection and (DR) Disaster Recovery.

- **OS&Programs “C:”** – where Operating System and programs reside.
- **Streaming-Data “D:”** - where Virtual Instrument and other “static” data reside.
- **User-Files “E:”** - where personal files and recorded “dynamic” data reside.

Essential Data Protection Ideas

1. Organize your DAW so that each hard-drive has a specialized function. Each drive should have its own backup priority based on the value and replaceability of its files. I would rank standard DAW drives in the following priority (high-to-low): User-Files, OS&Programs, and Streaming-Data.
2. Maintain duplicate backup data, on different devices or media, for each DAW drive. Relying exclusively on a single backup drive is, in itself, insecure. My approach places moderate and high priority data on at least two different media, with the level of duplication reflecting the priority of content. For your User-Files drive (highest priority), I suggest three levels of duplication: session, standard, and off-site. (These specific levels will be detailed later in this guide).
3. Notate all software backup/restore to a hardcopy “Backup Log”, indicating date, media type, and unique label. Documenting to a visible log acts as both reference and reminder. Place this on a clipboard in your studio, within plain view.

Fundamental Data Protection Terms

1. Disaster Recovery (DR): for our purposes, the ability to completely recover all files for a given hard-drive after that drive has failed and been replaced.
2. Full, Differential, Incremental - the three basic types of backup offered by a traditional backup software application.
 - Full: backup of all selected files (often targeting an entire drive).
 - Differential: backup of all selected files that have been modified or newly added since the last Full.
 - Incremental: backup of all selected files that have been modified or newly added since the last Full or Incremental.

Necessary Tools (comprehensive protection for as little as a few hundred dollars).

- Novastor Novabackup v7.5x (full-featured, traditional backup software for XP).
- Norton Ghost 2003 (Imaging utility for Windows).
- USB-2 External SATA/IDE drive enclosure with high capacity hard-drive (ideally twice the size or greater than your Streaming-Data drive). This device should be reserved exclusively for use with your backup software application and will be referred to in this guide as your “USB-BU-HD”. Create a single large Partition and Format the drive NTFS. Make two folders at root: “D-backup” and “E-backup”.
- DVD recordable device and “burn” software (4gb capacity minimum).
- Replacement hard-drives, same capacity or greater, for all three DAW drives. Place your “User-Files” SATA replacement drive in its own USB-2 drive enclosure (see Addendum).

Why use both Imaging and Traditional Backup Software?

Image backup is sector-by-sector, effectively enabling an exact “clone” of your hard-drive. Norton Ghost 2003 boots from prepared diskette or CD via its own OS. It images the target hard-drive while that drive’s OS is at rest, enabling an ultra-clean clone. While Ghost provides the most reliable means of cloning or restoring an OS drive it does have the limitation of insisting that the restore target boot under similar hardware, especially motherboard/chipset. It is also unaware of the file “archive” bit which is essential to traditional backup software applications

Traditional backup is file-by-file, utilizing the “archive” bit and other file-based info to check each file’s backup status. The OS&Programs drive requires both imaging and traditional backup strategies to insure its complete data protection. The first provides a sector-by-sector base while the second adds the ability to include modified files to insure the latest DAW customizations and backup catalog are restored atop the clone. Other DAW drives can be protected using traditional backup software alone.

NovaBackup Configuration

NovaBackup (v7.5x) is a well-designed and affordable traditional backup software. Though not created specifically for DAW use, it can be optimized effectively for our needs with a few simple tweaks after its installation.

Firstly you will want to clean up its default-installed automatic services.

- Run MSConfig <Startup> and de-select load of "NBKCtrl.exe" at boot. <OK>.
- At reboot, select not to show the Config utility warning screen by selecting, “Don’t show this message...”. <OK>.
- Set the two services that are components of NovaBackup to “Manual” Startup Type : "NMSAccess.exe" and "NSEngine.exe" (via XP Administrative Tools/Services).

Now, only when you invoke Novabackup will "NBKCtrl.exe" be called and its two corresponding services loaded. This is a clean approach for DAW users who should backup only as needed, without scheduling, and reboot immediately after any backup/restore session.

Note: The properties of the “NsEngine” service should be set to login, via “This Account”, to an Administrator level account. This will insure complete administrative access to the system.

Secondly, configure Backup and Restore settings for optimal DAW use. Invoke *NovaBackup* to view its main “Welcome” screen. Select “Global Settings” from the Shortcuts menu and configure as follows to modify defaults.

<**Backup**> de-select the following.

- Compress backup files. (not useful for DAW files).
- Enable Open File backup. (not needed for DAW data drives).

<**Restore**> select the following.

- Overwrite existing files if they are older. <OK> to save new defaults.

<**Notification**> select the following.

- Log Creation options = Summary.
- Log Notification options = Only if operation had messages/errors....

Backup Jobs: seven (*.nbk files) total, created via NovaBackup Wizard as detailed below

Note: using Windows Explorer, create folder “\C-backup” at *Streaming-Data*, drive “D:”.

1) Backup C-Full specific.

Full backup of: “C:\Program Files” and “C:\Documents and Settings”, including all of their sub-folders and files (and backup catalog, “Program Database”), to “D:\C-backup”. After Wizard creation, File/Open again and right-click on root-folder, select “Apply Filter” to setup rules to condition backup.
√ Exclude wildcard: *.exe, *.dll, *.dat, *.disk.vol. Filter Attributes: √ Archive, √ Normal (only).

2) Backup C-Diff specific.

Differential backup of: “C:\Program Files” and “C:\Documents and Settings”, including all of their sub-folders and files (and backup catalog, “Program Database”), to “D:\C-backup”. After creation via Wizard, File/Open again. Right-Click on root-drive folder, select “Apply Filter”.
√ Exclude wildcard: *.exe, *.dll, *.dat, *.disk.vol. Filter Attribute: √ Archive (only).

3) Backup D-Full all.

Full backup of drive “D:” (Streaming-Data) all folders and files, to USB-BU-HD “\D-backup”.

4) Backup D-Diff all.

Differential backup of drive “D:”, all folders and files, to USB-BU-HD “\D-backup”.

5) Backup E-Full all.

Full backup of drive “E:” (User-Files) all folders and files, to USB-BU-HD “\E-backup”.

6) Backup E-Inc all 1.

Incremental backup 1 of 2, of drive “E:”, all folders and files, to USB-BU-HD “\E-backup”.

7) Backup E-Inc all 2.

Incremental backup 2 of 2, of drive “E:”, all folders and files, to USB-BU-HD “\E-backup”.

To create a **Backup job**, select Backup from the *NovaBackup* main menu “Welcome” scene. This will display a 5-step Wizard to assist you. Proceed as follows to create and submit a job.

1) Let me select items manually <Next>.

- √ Select desired folders/files from “Select Items to Backup”.
- √ Select “Program Database” from lower-left pane to backup the Catalog. <Next>.

2) - Backup Name: (rename given default to target job name).

- (i.e. “Backup C-Diff specific”).
- Click <Backup to> and select target destination. (i.e. “D:\C-backup”).
- Set “Backup Type” accordingly. <Next>.

3) Options will list the new defaults you have set, to modify if needed. <Next>

4) Review all the backup settings you have requested for this job. <Next>.

5) Save and Backup Later. (Accept default <One Time> Schedule Type, and Start Date/Time).

- Show Progress. Overwrite Backups. <Finish>.

When finished creating your backup jobs, use *NovaBackup View/Schedule* to delete all scheduled items. Backups should be manually run, on demand only. To facilitate this I recommend creating a script for each backup job (optional as backups can be run within *Novabackup* if desired). Scripting requires a command-line *.BAT file to be called by a corresponding Windows Shortcut. Place the *.BAT files in the “C:\Program Files\NovaStor\NovaBackup” folder. Per example below, you need only change the (underlined) job name.

```
@echo off
cls
echo PREPARING BACKUP...
NbkCmd "backup" "C:\Program Files\NovaStor\NovaBackup\Scripts\Backup\Backup E-Diff all.nbk"
```

The corresponding Windows Shortcut, used to launch the above backup, would have properties stating:
“C:\Program Files\NovaStor\NovaBackup\ Backup E-Diff all.bat”

Place all seven corresponding backup Shortcuts in the *NovaStor Start/Programs* folder.

To **Restore** a previously run backup job, select *Restore* from the *NovaBackup* main menu "Welcome" screen. This will display a 4-step Wizard to assist you. Proceed as follows to restore a previously run backup.

- 1) Select Source device containing your target backup set.
(click the "+" prefix to display that devices list of backups). <Next>.
- 2) Select the items that you wish to include in the restore. <Next>.
- 3) Destination default is to restore files to their original locations. <Next>.
- 4) Review, then launch the restore by selecting. <Finish>.

Drive-by-Drive Strategy

OS&Programs – This drive requires both imaging and traditional backup strategies to insure its complete protection. The numbered routine below should be run in sequence, after optional DVD burn of existing Ghost image files at "D:\C-backup".

- 1) Using *NovaBackup*, run the "Backup C-Full specific" job to do a full backup of specific folders on the OS&Programs drive.
(This is only required for updating the archive info, its corresponding backup data at "D:" is not needed. Additionally, all records of C: backups may now be deleted within NovaBackup View/Restore).
- 2) Delete all files at "D:\C-backup". This clears the folder, ready to re-populate with fresh data.
- 3) Using *Ghost*, image the entire OS&Programs drive ("C:") to your Streaming-Data drive ("D:"), in its folder "\C-backup", as per details below.

Boot via Ghost and select from within its program interface:

- Local/Disk/to Image.
(will ghost the entire disk-drive. Select <drive 1> as local source to image *OS&Programs*).
- "Look in" = (select drive 2, *Streaming-Data*).
- (Select "\C-backup". Display will show reverse arrow [to parent]).
- Enter the filename for your image <Save>. (Initial filename is ????????.GHO).
(As a DOS-based utility, Ghost will render the image as a set of linked files each no larger than 2gb).
(Subsequent files start ??????001.GHS, with number suffix incrementing as needed).
- Compress Image <No>, Proceed <Yes>.

On a weekly basis, run the "Backup C-Diff specific" job to backup files that have been modified or newly added since the last (step 1) Full. Each run will overwrite the existing destination (*.nb7) backup set, as you will only need your latest differential for restore. This job should be extremely fast, taking only a few minutes to run at the end of a day's session. This will insure that DAW application customization settings and the backup software catalog are saved on a regular basis, so as not to necessitate frequent re-image. You will then only need to re-image after any significant hardware or software changes to your DAW, such as the installation or removal of a hardware device or software application. Please note that Imaging should be done as part of the 3-step routine detailed above. The image and differential file-sets at "D:\C-backup" will also be recorded by your traditional backup software's Full and Differential backup of the Streaming-Data drive, so you will have a second level of data protection on separate media.

Restore should only be required in a drive-failure (DR) scenario. When this occurs, replace the failed drive. Use *Ghost* to restore the image set from your Streaming-Data drive to the new drive (details below). Re-boot and complete with *NovaBackup* "Import" then restore of the Differential "Backup C-Diff specific.nb7" file from the same Streaming-Data location.

To Image Restore, select from within the Ghost program:

- Local/Disk/from Image.
- (select image filename from drive2, *Streaming-Data*: "\C-backup").
- Local Destination = drive 1 (empty replacement drive).
- <OK> <Yes> proceed with disk image restore.

Hardware: Streaming-Data internal drive.

Software: Ghost and NovaBackup.

Frequency: 1) Re-image after any significant software or hardware changes to DAW.
2) Run "Backup C-Diff specific" job weekly, depending on your work activity.

In a DR scenario, without a specific backup/restore strategy for the OS&Programs drive, you would need to manually re-install your Operating System, re-do its customizations, then re-install all your application programs. This task could be multi-day. With an image backup strategy your complete restore to the replacement drive should take little more than an hour.

Streaming-Data - use *NovaBackup's* drive-to-drive capability, accessing your USB-BU-HD. First run the "Backup D-Full all" job, to save all of the drive's files. Then run the "Backup D-Diff all" job, monthly or as needed, to save files that have been modified or added since the last Full. Each job will overwriting its existing destination (*.nb7) backup set by design, as you will only need your latest backup for restore. Restore should only be required in a drive-failure (DR) scenario. When this occurs, replace the failed Streaming-Data drive, partition and format accordingly, then Restore from your USB-BU-HD using your NovaBackup application. You should restore your full backup first, then differential as referenced by NovaBackup's (View/Restore) catalog.

Hardware: USB-BU-HD external USB drive.

Software: Novabackup.

Frequency: Run "Backup D-Diff all" job as needed, or monthly.

In a DR scenario without specific backup/restore strategy, you would need to manually re-install all VI applications that do not allow for separate breakout of data-sets, then re-copy data-sets from cd/dvd supplied by the applications that do. This task could take a full day or more. With a drive-to-drive backup strategy your complete restore to the replacement drive should take no more than a couple of hours.

User-Files – You will want your heaviest backup duplication for this drive as its files are irreplaceable. Level-1 (session) duplication should occur at the end of each day's session, where you would duplicate to another device all files created or modified. The easiest way to achieve this is to simply copy newly created or modified files from their original locations on the User-Files drive to a single designated folder on your Streaming-Data drive (such as "\E-session BU"). When this folder is near DVD capacity, burn the folder's files, then clear its contents to repeat the process with new data. This process is facilitated by naming your created files with a version# suffix, a good general practice that helps to insure more uniquely-meaningful filenames.

Level-2 (standard) duplication will utilize your NovaBackup software and external USB-BU-HD. Do one Full backup of all files on the User-Files drive (job= Backup E-Full all). Follow with your two monthly incremental backups ((jobs= Backup E-Inc all 1 & 2). This will create a three-month backup data "history" (full/Inc1/Inc2) as a resource to examine/restore prior versions of your user files before their (*.nb7) backup data-sets are overwritten in cycle. If you need a longer history, create additional incremental jobs as needed. Keep in mind though that every incremental job you create will be required, one-after-the-next, in a restore scenario.

Level-3 (off-site) duplication is intended for emergency security. Its data set should be kept away from your studio at a friend's house or even a safe-deposit box. If local fire, etc, wipes out your studio's DAW and data - this is your ace to rebuild. Attach your *replacement* User-Files drive, in its USB enclosure, and copy all files from your current User-Files internal drive. There is no reason why you should not put your replacement-in-waiting drive to immediate use as a valuable duplicate. Place the entire enclosure in a sealed moisture-barrier/electronics bag along with a de-moisture pack such as "silica gel". This sealed, enclosed, drive should be then kept off-site. Periodically bring it in to your studio, clear its file contents, then copy over the latest *complete* set of files from the User-Files drive. Make sure to mark your Backup Log accordingly.

Restore will be needed to replace missing or corrupt files as well as in response to drive-failure. In DR scenario, replace the failed drive, partition and format accordingly. Restore the Full backup-set from your USB-BU-HD using NovaBackup then restore each Incremental, starting with the oldest to the latest. Lastly, you might need to copy files from your "end of session" DVD archive or from its designated duplication folder ("E-session BU") on your Streaming-Data drive.

Hardware: USB-BU-HD external USB drive, DVD, replacement "User-Files" drive (see Addendum).

Software: NovaBackup, DVD burner application, Windows Explorer copy function.

- Frequency:**
- 1) Session copy, daily.
 - 2) "Backup E-Full" job every 3 months or longer, depending on Incremental cycle.
 - 3) "Backup E-Inc all (n)" jobs monthly.
 - 4) Copy to replacement "User-Files" usb-drive, as needed.

Without specific backup/restore strategy your personal user-files are in serious jeopardy of being irretrievably lost. The cost for drive data-recovery (from a professional service with "clean room") is in the thousands of dollars and there is no guaranty of success! With a drive-to-drive backup strategy your complete restore to the replacement drive should take no more than a few hours.

Addendum: modern large-capacity hard drives are designed primarily to store data while spinning, though If used in periodic backup rotation they can provide many years of service via USB enclosure, etc. Drive backup to SSD is preferred, especially as off-sight media, because of superior data retention "life span". **Backup Task-Table** is below.

Frequency	Description	Run Time	Destination Media
Daily	End of session backup	1 – 5 min	"D:\E-session BU"
Weekly	"Backup C-Diff specific"	2 – 5 min	"D:\C-backup"
Monthly	"Backup E-(*) all (n)"	10 – 30 min	USB-BU-HD "E-backup"
Periodic/Monthly	"Backup D-Diff all"	5 – 20 min	USB-BU-HD "D-backup"
Periodic	Re-Image (Ghost)	15 – 30 min	"D:\C-backup"
Periodic	"Backup C-Full specific"	15 – 30 min	"D:\C-backup"
Periodic	"Backup D-Full all"	30 – 90 min	USB-BU-HD "D-backup"

Software Restore and Copy Protection

Copy protection mechanisms should only pose potential problems for "OS&Programs" DR Restore.

BEST: USB Master-dongle, such as used by Steinberg or VSL. This one (Syncrosoft) USB dongle can authorize all compliant manufacturers software products. When invoked, these applications will look to the USB dongle for access authorization. In the event of OS&Programs drive failure, an image of this drive can be restored to a new drive and all the residing master-dongle apps should function perfectly without need for software re-installation.

ACCEPTABLE: Challenge/Response variant of "signature" based copy protection, such as deployed by Spectrasonics. With this method the "Response" code is the signature authorizer, based on the Challenge code issued during software install. This approach allows for cloned applications to function perfectly on their newly imaged drive, as long as the Challenge/Response procedure alone is redone.

WORST: Hard-drive "signature" (as used by "brand X"). This creates a unique reference from low-level hard-drive info concatenated with application serial# to create an authorization reference for each application. The purpose of this approach is to prevent software piracy. Unfortunately, it severely cripples cloning/imaging as a legitimate means of data protection for fully licensed users. In the event of OS&Programs drive failure, an image of this drive when restored to a new drive will disallow access to any "signature" based application. The user will be forced to uninstall and re-install such applications. A more humane, "lite", version of this copy protection is used by NI, where application serial# is combined with hardware component info, such as motherboard, to provide a unique reference. Simple drive replacement should not be a problem here, as only major changes to low-level hardware require full re-authorization.

John O'Mahoney, DAW-solo.com © 2008, v1.1.5 (11/30/08)

Disclaimer: I offer this guide as a free service to the DAW community. Use it at your own risk. I make no guarantee or warranty about its results, though I have made every effort to carefully research its subject material.