Handy Backup

Preserving Native Data Format when Keeping Backups

The **native backup format** means preserving source formats for all data backed up to somewhere, up to preserving individual file attributes such as date and time of last modification. This approach allows many tricks and workflow optimizations, especially in conjunction with some actions improving stability.

Handy Backup keeps native data formats for backups by default, and has a set of tools to make these data into a consistent backup file or multiple files. This means possibility of using Handy Backup for both native and non-native backup saving. Let us talk about the approaches.

➲ Some Alternative Interpretations of the Term "Native Backup Format"

Not all types of data provide a possibility for backing up these data simply as folders containing a file structure. For example, the native format for databases can look like a set of SQL queries creating a copy of the existed database content from scratch. This is a *native* format, too.

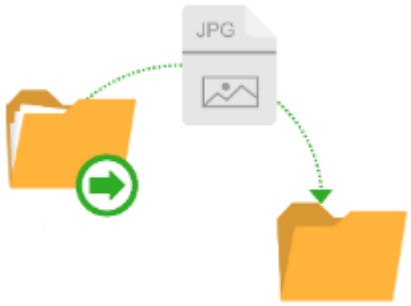
Advantages of Backing up Data Natively

This is a short list of obvious advantages of the native backup format and different techniques using this approach as a basis:

- ✓ A possibility to clone, replicate and copy the dataset instead of merely backup;
- ✓ Working with parts of backup content as with common files and folders of these types;
- ✓ Moving, copying and restoring components of backup dataset, instead of full restoration;
- ✓ Automating processing files and folders in backups with the same procedures as for a source;
- ✓ Changing or repairing the "bad" backup content manually before restoring it.

The backup dataset saved by Handy Backup without special preparations is often a folder containing a copy of a source dataset "as is", including file and subfolder attributes. The name for this backup dataset can contain a *time stamp*, the specially formatted folder name with a date and a time of backup.

➲ Manipulating with Native Backups



A user can open any backup folder created by Handy Backup, to view, copy or even modify any part of its file structure. For example, a user can open the subfolder containing JPEG images, then copy some of these images to another place, or even open and modify one with a photo editor tool.

➲ Partial and Manual Restoration

If the native backup set contains a bunch of files and folders, and a user needs only one or a few of it, this is completely possible to copy the “native” backup data to a source location manually, using the file manager or a batch file to select data. It removes the obligate need to restore all the bulk of files.

➲ Sorting and Processing Backup Data

Some script (batch) files or dedicated tools can use a folder containing native backup data to process the information stored in it with some automated routines. For example, if your batch must select only files modified from a particular period, it can easily work with your folders containing native backups.

➲ Modifying Special Data Types in Native Format

Even if your data is not just a copy of some folders, you can take advantages from the native backup principle! For instance, a SQL database dump kept in the native format is merely a set of SQL queries stored in text files. You can open and modify such file manually without a single problem!

Improving Stability when Keeping Backups in Native Data Formats

Theoretically, these are no significant problems, except that uncompressed files of some types (e.g. text files) tend to occupy much more space than actually needed when packing these files properly. Therefore, some problems of native backup format are the consequences of its advantages!

➲ Inconsistent Backups

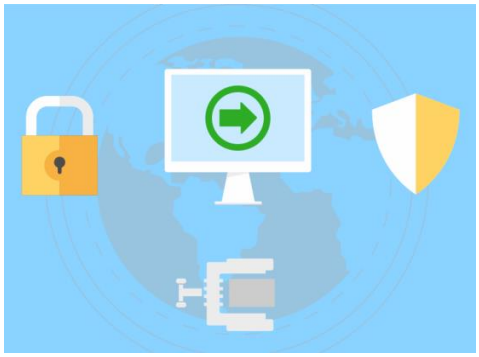
If a user modifies some dataset in a backup copy, and then restore it to an original place, this is not the "restoration" itself but replacing some old data with a newer information instead. This can be a result a user want, or may cause an accident of, say, losing some data by replacing it with a newer version.

➲ Viruses and Mishaps

The information stored in backups in the native format is prone to virus attacks, worms, Trojans and other perils specific to the data types present in a particular backup dataset. Therefore, after the restoration or cloning this information, a peril can attack data on the target computer.

Note: Handy Backup allows checking data for consistency as well as virus removal. To do it, please use the pre- and post-actions on a Step 7 where you create a new task. You can start a program or a batch containing such software as antiviruses, garbage cleaners, checksum control utilities and so on.

Using Native and Non-Native Format by Circumstances



As mentioned before, Handy Backup has a default option of saving all backups when preserving the native data format. All advantages of this technique described here are fully applicable for any copy of any dataset made by Handy Backup.

In addition, Handy Backup allows a user to compress all backup set into a single file, or zip each file in the set separately, to make the resulting backup smaller and less prone to attacks. It can also encrypt any backup, requiring the restoration procedure for returning data from backups to an original place.

Note: Handy Backup does not contain a classical "non-native backup format", which means a proprietary format with many tricks and operations possible for proprietary software only. It just provide a stability and a consistency for all data backed up.

Use Cases: When Take a Native Format and When Compress and Encrypt Your Data?

This is not a simple question. Consider all circumstances of your backup activity, including the backup purpose, the type of a dataset, the frequency of backups and the planned situations when you can need your backup data. Then use a native or a non-native backup.

- ✓ For **small daily backups** of typical user-level data, such as files, projects and folders, we are recommending backing up in native format.
- ✓ The native format is also good to **clone or share your backups** with other users and/or machines, e.g. for backing up data into common folders on some commercial cloud service.
- ✓ For **cloning or replicating databases**, especially for tests or new projects, we are strongly recommending native backups, allowing changing any parameters simply and quickly.
- ✓ The regular **total backup of your computer** content, such as libraries, server-level data or even a system image, often requires a non-native backup format and a regulated restoring procedure.
- ✓ Always use non-native format, at least **with encrypting your backup dataset**, for critical data, to protect these data from unsanctioned access or from a viral threat.

Please remember that, for Handy Backup, the difference between taking data snapshots in a native and a non-native backup format is just a few clicks. For using the resulting dataset, the difference is much bigger. Therefore, you can always select an optimal strategy for each of your backup tasks.

Download the latest version of Handy Backup http://handybackup.net/download

Learn more about the Backup Solution - http://handybackup.net/handybackup-smallserver

Contacts

To learn more about any of these methods please write us a mail at sales@handybackup.net

More contacts:

Web: handybackup.net

Tel: +1 (707) 703-1315