

Advanced backup explained



Overview

net-runna ReStor is a powerful, configurable data backup and restore solution that provides the user with a simple user interface to achieve advanced backup and data recovery tasks. On installation, default backup sets are already set up and a wizard and quick start guide takes the user through a simple setup process. The default settings can be easily edited later in the intuitive *ReStor* console which contains comprehensive help files.

Backup sets

- **Full system:** By default this backs up the following files and folders: Documents and Settings, Program Files, Windows, the Registry and the system files in the root of C.
- **Data files:** By default this backs up the logged on user's Documents and Settings folders.
- **Registry:** This performs a full Registry (Windows settings) backup.
- **User set:** This allows the user to browse to specific files and folders and group them into a single backup set. Multiple user sets can be created.
- **File filters:** This is a global setting and allows specified file types to be excluded from all backups.
- **Specific backup exclusions:** the Windows hibernation file (Hiberfil.sys) and the Windows swap file are excluded from all types of backups. The maximum file size *ReStor* can backup is 2GB; this limit does not apply to folders, just single files.

Backup in the live environment

The *ReStor* application is designed to run in System Idle time so that the impact on the user is minimised. Traditional backup applications require the user to give the backup application exclusive use of the machine during a backup to ensure the backup completes successfully. *ReStor* allows the user to continue working on the machine while the backup is running. Special file handling algorithms have been implemented to allow for access to locked files. A backup will contain a snapshot of the files as they were at the time of the backup so any open document file will contain the data that had been committed to disk at the time of backup.

ReStor is designed to minimize its in memory footprint at all times, as such it will successfully execute in 16 Megabytes of system RAM, although if more memory is available, performance will be enhanced.

Fast, frequent backup

Due to the speed of a backup that is performed by *ReStor* and the unique repository implementation, it is possible to schedule backups of important data to be performed at 5 minute intervals, or even shorter if required. This would mean that the user would always have a current backup to recover from should something go wrong.

All data that is backed up is tied to a specific machine account and can only be accessed by the account holder. This ensures that any data residing in the repository is unreadable and therefore useless to an outside party. Even though the remote repository can be shared among multiple users, one user can not retrieve or review the data of another user.

Registry backup

The user has the option to backup and restore the registry files as part of any backup process. The content of the registry is constantly changing with numerous processes that update it. *ReStor* needs to gain exclusive access to the registry files to conduct a backup of the registry. As a security precaution during a registry backup the machine will be locked out to the user for approximately a minute (dependant on the registry size), this is to ensure accurate and safe backup of the registry.

Scheduler

The user can automate backups by scheduling them to run at set intervals. Multiple schedules can be created and each backup type can have its own schedule. The backups can be set to repeat every few hours or minutes or to run at a specific time each day, week or selection of days.

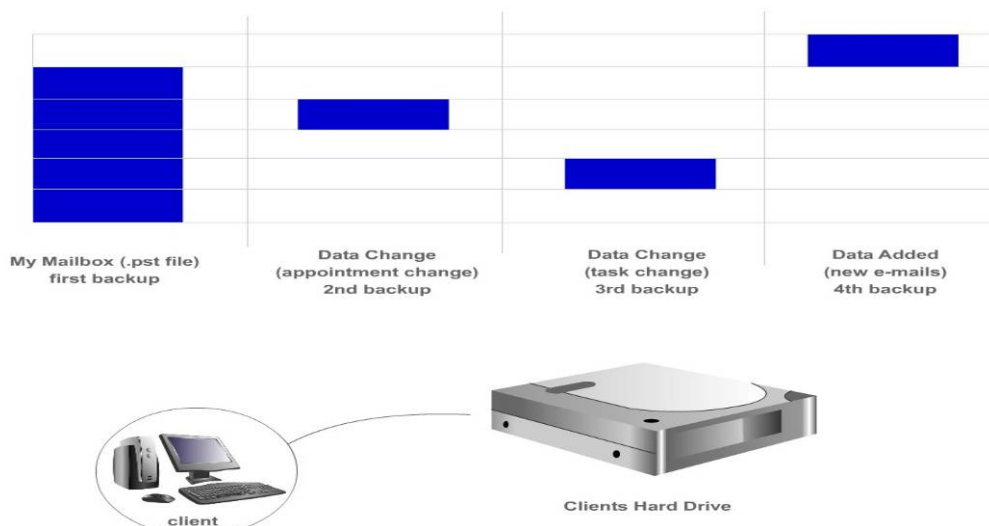
Block level single instance storage

Traditional backup solutions perform a complete backup each time - *ReStor* is different. Initially it will backup all target data; however for each backup thereafter it will only backup altered files. This is achieved by utilising intelligent single instance storage data repositories in which data is never duplicated. Files are only backed up once to the repository and where there are multiple instances of a particular file, the file is only stored once. The benefit of this is that the size of the backup repository is dramatically reduced, and, backing up only new and altered data means subsequent backups can be performed much faster than ever before. A standard 128 bit encryption algorithm is used and all backed up data is compressed.

To determine whether a file has been changed, traditional backup solutions query the archive area of a file. *ReStor* conducts a far more robust check by querying the file date time stamps (file creation, last write and last access) and comparing these to the backup history database. Should any date stamp differ, a hashing algorithm (MD5) is performed on the contents of the file in conjunction with a CRC32 algorithm to determine whether the content of the file has been altered. If this is the case, then the file is backed up.

Block level

Data backups are split into small blocks, the advantage of this is that when large files are repetitively backed up only the section of the file that has changed (a block) is backed up again. The size of the blocks can be set within the *ReStor* console. This approach is perfect for files like the email PST (Outlook Personal Folder) file which is usually a large file that constantly changes. Regularly backing up this file would rapidly increase the size of the repository if the whole file was backed up again every time it changed. Block level backup only backs up the block that has changed; this would typically save hundreds of megabytes of space on every backup.



Data repositories

The backup repository location can be to any mapped drive residing locally or remotely, e.g. a second partition, second physical drive, removable drive or network share. When using a single repository it is recommended that a network share or removable device is used to avoid data loss in the event of computer theft, hard disk failure or hard disk format. To illustrate this here are some typical scenarios:

1. Local repository – data backups are stored on the local hard disk.

This is very convenient for backing up and archiving your files and requires little intervention however in the event of computer theft, hard disk failure or hard disk format backed up data will be lost.

2. Data backups stored on a second partition of the local hard disk

Similar to 1 but a hard disk format of only partition 1 would preserve the data backup.

3. Data backups stored on a removable disk

Using a removable disk bay, USB hard disk or a USB memory stick, will mean that your data will generally be safe as long as you store your removable device in a different physical location to your source data computer.

4. Data backups stored on a network share or file server

In this situation your data will generally be safe as it will be on a network storage device or file server.

5. A unique ReStor feature: Dual data repositories

This offers the best of both worlds with a data repository that is set up on a local disk and a second remote backup repository on a network share. This allows the mobile user to run backups, archive and restore data even if they are not connected to a network with the safety of having a duplicate copy of their data backups stored on the network. When working away from the network backups are saved to the local repository. Then when reconnecting to the network the user can synchronise the repositories. When backing up whilst connected to the network a ReStor backup automatically copies the data to both locations simultaneously.

Shared data repository

The network data repository can be shared by multiple users; this takes maximum advantage of the single instance storage facility as when multiple users back up the same file it will only be copied into the repository once.

The benefits of incremental backup and the block level single instance storage are:

- Less data needs to be sent over the network which reduces network bandwidth utilisation
- Data backup storage requirements are lower and the data repositories grow more slowly

Restoring data

- **Restore files from backup:** Each backup creates a restore point; the user is presented with a list of all the backups listed by time, date and description, and can rollback to any point by restoring the entire backup.
- **Find file:** Allows you to search for a specific file by file name and extension. All the restore points for the different versions of the file are shown. If an existing file (the current version) is overwritten during a restore, it will be moved to the 'Keep' folder inside the backup repository so that the user may still access the original file.
- **Backup browser:** An explorer style file browser interface is presented in which the user can easily select a backup to explore and then select the specific files or folders they would like to restore.
- **Registry:** The complete registry can be restored from the last backup.

Fast data restore

Unlike most backup tools when the user selects a Restore of files in a backup set, only those files that have been altered or deleted are restored. This method is extremely fast because there is no need to restore files that are already correct and in existence. Existing files are not wiped out but are optionally merely moved to a folder labelled KEEP on the hard drive.

Reports

Detailed text file reports are created for each backup and restore operation. The reports are listed by time, date and backup description. Any error conditions or faults encountered are logged in the report files.

Compatibility

The *ReStor* application is compatible with Microsoft Windows 2000 and Microsoft Windows XP (Home/Professional). The current version of *ReStor* is not recommended for server backup as it is assumed that a server would be running some form of database application such as SQL, Exchange or Oracle etc. The file handling algorithms implemented by *ReStor* to bypass file locking do not support the large files of these applications. Please note *ReStor* is not a full system recovery tool and cannot recover a computer from a non-bootable state, however this is a feature of our *net-runna Enterprise* preboot recovery product.

Licensing

The *ReStor* application includes extremely strong copy protection which requires licensing and activation once the 30 day trial expires.

www.net-runna.com

Advanced Network Technologies, 6 Amber Business Village, Amber Close, Tamworth, Staffordshire, B77 4RP, UK
T: +44 (0) 1827 311 811 F: +44 (0) 1827 313 888 E: sales@net-runna.com