The BackupAssist File Replication Engine

Contents

Introduction

IT administrators often use third party command-line tools, such as Xcopy or Robocopy, to create a second copy of their important data for an extra layer of protection in addition to their primary backup. Such command-line tools often involve complex scripts that are difficult to manage and can produce unreliable results. To address the shortcomings of conventional file copy methods, we have developed the BackupAssist File Replication Engine.

BackupAssist's File Replication Engine is an integrated solution for administrators who want a powerful, yet simple solution out-of-the-box. File Replications backups can be configured in minutes, avoiding hassles like scheduling tasks and creating complex scripts. Used by itself or in conjunction with other backup engines, such as the Windows Imaging Engine, the File Replication Engine provides you with a powerful tool for data protection and recovery.

The following whitepaper outlines how the File Replication Engine works, as well as how to create and configure File Replication backup jobs in BackupAssist.

Single Instance Store

While BackupAssist's File Replication Engine is based on the simple concept of copying files from one location to another, it also includes backup history options and the power of Single Instance Store. Single Instance Store makes sure that only one unique copy of each file is stored on your backup device, allowing you to keep hundreds of days of backup history with minimal storage requirements. Single Instance Store is totally transparent, so you can restore your files without needing any proprietary software, to any machine. You can also search for files within your backups, just as you would with any normal file system. Refer to **Appendix I** for more information about Single Instance Store.

Advantages over traditional file copy methods

- **No scripting required:** easily setup basic mirroring of important files as well as comprehensive archival backups for hundreds of days of backup history to restore from.

- **Fully automated scheduling and monitoring:** backup jobs are automated with BackupAssist's one-click scheduler. You will receive HTML reports after each backup to inform you of the backup success or failure.

- **Backup redundancy and multiple restore points**: create a series of mirrors on your backup device, one for each day. Each backup looks exactly like a self-contained mirror of your data. To restore, simply copy the files back from the relevant folder, or, for more difficult tasks, use the BackupAssist Restore Console.

- **VSS support for open file and application backup and restore:** before each backup runs a VSS Snapshot is created so that any open files can be safely backed up. Microsoft applications such as Exchange Server, SQL Server, SharePoint and Hyper-V are all fully supported, as well as any other VSS-aware application that uses standard VSS restore methods. Simply choose the VSS application you want to back up from the list of detected applications. You can even drill down and choose individual components (databases, storage groups, etc). Application restore is also easy using the BackupAssist Restore Console.

- **System State backup and restore**: easily backup and restore system settings in the event of a disaster.

- **Exact File Copy:** NTFS security attributes and alternate data streams of directories and files are stored within File Replication backups, and both are restored when using the BackupAssist Restore Console.

- **Independent encryption and compression:** encryption and compression can be set on the backup destination without affecting the data source.

When to use the File Replication Engine

Please refer to our Usage Scenarios white paper for examples of when to use the File Replication Engine.

Modes of operation

The File Replication Engine offers two modes of operation: **mirror** and **backup with history**.

Mirror mode

The **Mirror** mode creates an exact replica of your selected files and folders to a specified backup destination. Every time a backup is created, the BackupAssist File Replication Engine will update modified files and add new files to the backup destination.

This type of backup is useful for situations where a primary drive or server needs to be replaced quickly.

Backup with history mode

The **Backup with history** mode creates a new set of mirrored data in a uniquely named folder each time a backup runs. Each backup looks like a self-contained mirror of your data.
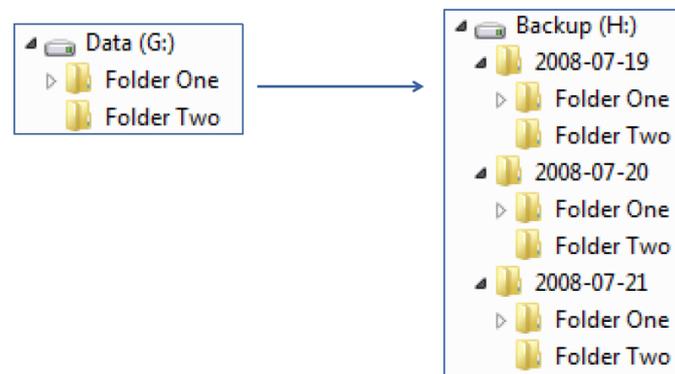
Backups created using this mode are useful for maintaining version history over a long period of time. For backup jobs to disk-based destinations, such as an external HDD, rdx QuikStor or REV drive, you can even configure backup storage options to make sure that disk space on the backup destination is properly utilized.

File Replication jobs – setup and customization

Creating a File Replication job

1. Create a new job by going to **File > New backup job** and select **File Replication** as your backup type.

2. Proceed through the job creation wizard, selecting your backup destination and schedule.

3. During the **Setup Destination** step of the wizard, you can decide whether you want to user the Mirror mode or the Backup with history mode.
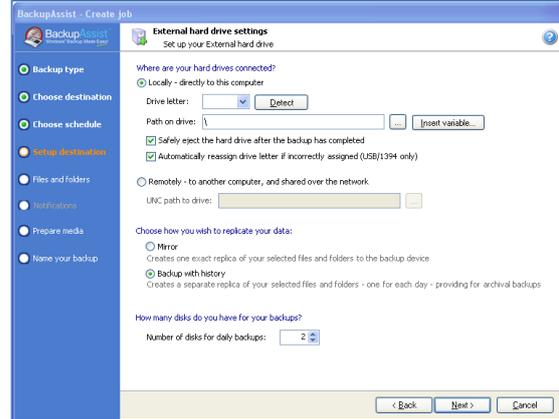
4. Continue with the rest of the wizard, specifying which files/folders, and applications to be back up, as well as whether to back up the System State. You will also be able to configure email notifications, prepare any portable media (if applicable), and name your backup job.

Customizing your File Replication job

Backups created with the **Backup with history** mode to disk-based destinations can be configured to use Single Instance Store, so that only one unique copy of each file is stored on the backup destination. Single instance store is enabled by default, but to modify this setting:

1. Click **Edit** from the top menu and select your job from the list.

2. Click **Destination** from the left menu and expand **Replication Mode** Options, and check the option to **Use the single instance store**.
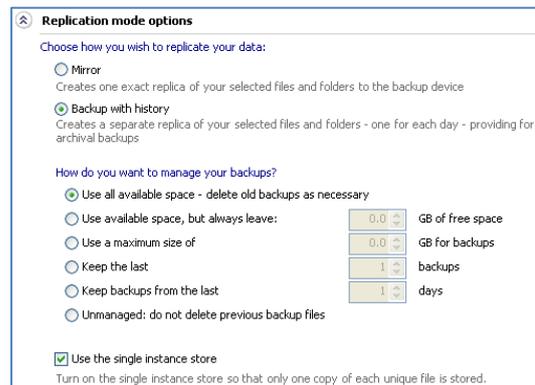
Preserving NTFS file attributes

The BackupAssist File Replication Engine is able to preserve certain NTFS file attributes set on the original source files. If you want to maintain NTFS file attributes we recommend you choose a backup destination formatted in NTFS. Preservation of NTFS attributes is enabled by default on destinations that support it.

File attributes at destination	Preserved?
Windows File Attributes	✔
Creation time	✔
Last modified time	✔
NTFS security (ACLs)	✔ *
NTFS alternate data streams (ADSs)	✔ *

* Excludes Linux or REV drive-based destinations.

How to preserve NTFS file attributes

1. Click **Edit** from the top menu and select your job from the list.

2. Click **Replication Options** from the left menu and check the option to **Copy NTFS security attributes and alternate data streams**.

You can also disable warnings that may appear in the backup report if the destination does not support NTFS attributes under the **File Attribute Warnings** heading.

Backing up VSS applications

BackupAssist will automatically detected locally running VSS applications and list them in the Files/Folders tab of a File Replication job for backup selection. You can even drill down to select individual components for each detected application.

How to back up VSS applications

1. Launch BackupAssist and edit your existing File Replication job by selecting **Edit** from the top menu and choosing the appropriate job.

2. Select **Files and folder**s from the left menu:

Note: locally installed VSS applications will be automatically detected and listed for backup selection. In some cases only applications that are currently running will be detected. If an application is not listed in the Files and Folders tab, try re-starting it and then click the Refresh button in BackupAssist.
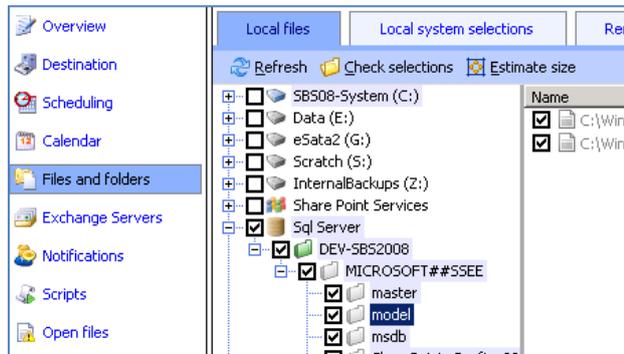
3. You can select either entire VSS applications to backup or drill down and choose individual components:
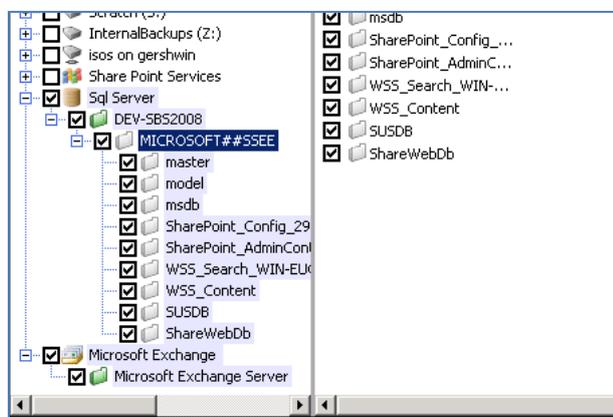
Note: *if you have selected VSS applications for backup we recommend disabling the **Enable VSS writers** option in the Open files tab.*
If the VSS writers option is enabled it will cause VSS to contact all applications before and after a backup, which can be slow and may cause the VSS application to register that a backup has been completed when it has not.
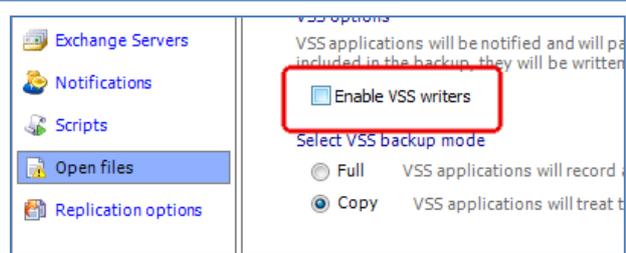
Backing up the System State

A System State backup includes a backup of any installed device drivers and related files, as well as most of the Windows directory. System State backups for Vista and Server 2008 are usually between 7GB and 15 GB when using compression via the BackupAssist Zip Engine. For XP and Server 2003, System State backups are generally much smaller: approximately 200MB to 300 MB.

Many files in the Windows directory have multiple hard links. If you are using the File Replication Engine only a single copy of each multiply linked file will be stored on your backup destination. This data does not need to be backed up on subsequent backup runs, which reduces backup times and saves storage space.

How to back up the local System State

1. Launch BackupAssist and edit an existing File Replication job by selecting **Edit** from the top menu and choosing the appropriate job.

2. Select **Files and folders** from the left menu, click the **Local system selections** tab, and then enable the **Backup local system state** option.
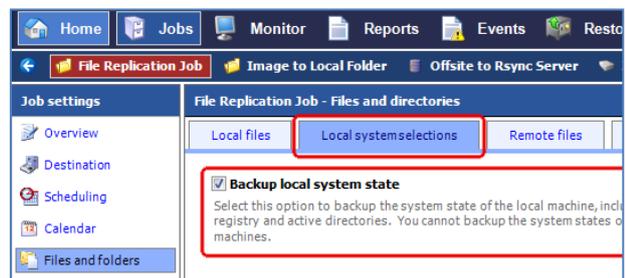
Restoring data from a File Replication backup

BackupAssist provides an inbuilt utility, the BackupAssist Restore Console, which can be used to restore files, VSS applications and the System State from a File Replication backup. The Restore Console can be accessed by clicking **Restore > BackupAssist Restore Console** from the main menu. For more information about how to use the Restore Console see our Restore Console Whitepaper.

Alternatively, if you do not have BackupAssist installed and need to restore from a backup created using the File Replication Engine, you can simply browse to the location of your backup using Windows File Explorer and copy the required files back to their original location or an alternate location of your choosing.

Appendix I – how Single Instance Store works

With Single Instance Store enabled only one unique copy of each file is stored on your backup device. Single Instance Store backups are similar to incremental backups, because only new or modified files are actually copied to your backup device each time a backup runs. This saves both time and disk space.

The advantage of Single Instance Store is that the process is completely transparent. If no previous backup exists on the backup device, BackupAssist will perform a full backup of the selected files and folders. For subsequent backups, only new or modified files will be backed up, but a new and complete backup set will appear on your backup device. The 'complete' set of files takes no more space than just the modified and new files that were copied.

With each backup set looking like a complete full backup, restoration is easy and does not require any proprietary software. With Single Instance Store enabled you can potentially keep hundreds of days of backup history with minimal storage requirements; and because each backup only copies new or modified files, backups are extremely fast. Below is an illustrated example of how Single Instance Store works:
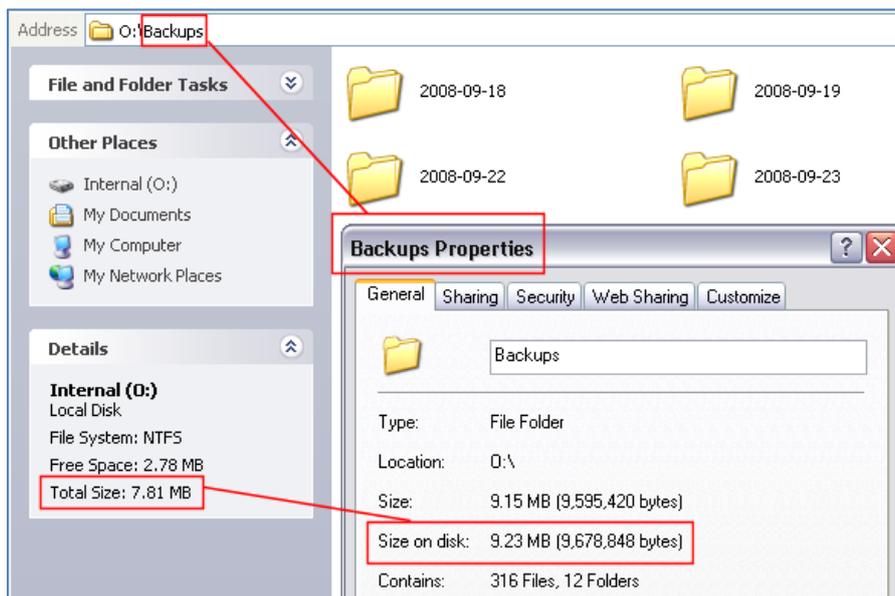
Note that the total size of the O: drive, where backups are being stored, is only 7.81 MB; and yet the combined size of the four backup sets stored in the Backups directory (2008-09-18, 2008-09-19, etc) is greater, at 9.23 MB. This is possible because Single Instance Store only allocates disk space once for each unique file copied to the backup drive. You can still navigate within each day's backup folder to see a list of files that can be restored:
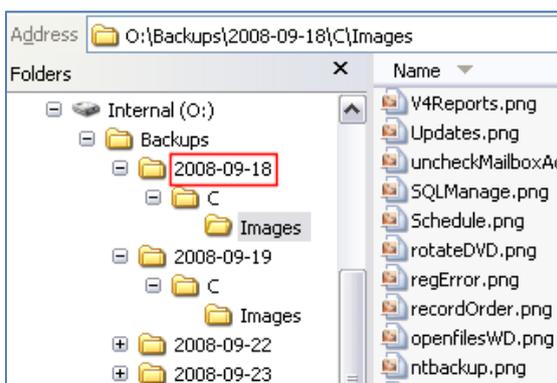
Backup set created on 18-September-2008
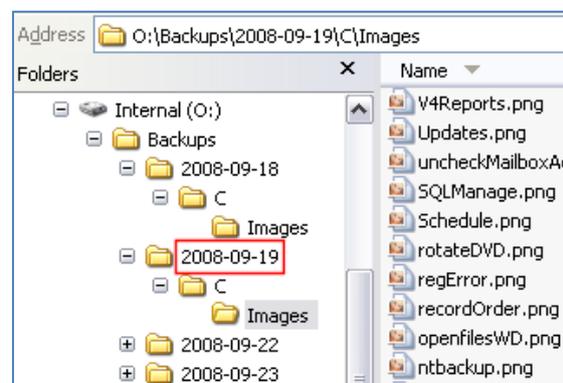
Backup set created on 19-September-2008

Appendix II – sample reports

Backups run using the BackupAssist File Replication Engine will generate reports that are very similar to those created from other backup engines in BackupAssist. Some sections, however, are unique to the File Replication Engine and are explained in greater detail below.

Exchange database consistency check

When backing up Exchange databases using the VSS writers option, a section within the backup report will outline whether BackupAssist was able to backup Exchange databases consistently. Any errors that relate to the Exchange database integrity check will be listed in this section of the report.

Exchange Database Consistency Check Report

The **Exchange Database Consistency Check** task has status: **Successful**

Exchange Database Integrity Check	
Healthy database files:	✓ C:\Program Files\Microsoft\Exchange Server\Mailbox\First Storage Group\E00*.log ✓ C:\Program Files\Microsoft\Exchange Server\Mailbox\First Storage Group\Mailbox Database.edb ✓ C:\Program Files\Microsoft\Exchange Server\Mailbox\Second Storage Group\E01*.log ✓ C:\Program Files\Microsoft\Exchange Server\Mailbox\Second Storage Group\Public Folder Database.edb
Corrupted or damaged database files	(none)

File Replication Report

The File Replication report section outlines how much data was backed up, how many files were backed up, and also includes details about Single Instance Store (if enabled).

File Replication Report

The File Replication task has status: **Successful**

```
File Copy Log

Total file count: 5
Files copied: 5
Files where no copy required: 0
Total size: 70.09 MB
Size of files copied: 70.09 MB
Size of files where no copy required: 0.00 B
```

The details outlined in this section are as follows:

- **Total file count**: the total number of files that were selected for backup.
- **Files copied**: the actual number of files copied during the backup. If no files have been modified or no new files have been added since the last backup, BackupAssist will not copy them to your backup destination.
- **Files where no copy required**: if Single Instance Store is enabled, files that have not been changed since the last successful backup do not need to be copied to your backup destination.

- **Total size**: the total size of a full backup (i.e. all files selected for backup).
- **Size of files copied**: the amount of data that actually needed to be copied for this backup (i.e. new or modified data not already present on the backup destination).
- **Size of files where no copy required**: the total size of the files that did not need to be backed up due to Single Instance Store.

Media usage report

The important thing to notice about the media usage section is the list of File Replication backups stored on the backup destination. This list helps you to determine the number of backups stored on your device that you can restore from, as well as monitor the amount of free space available to accommodate future backups:

Data usage for **Directory - C:\Test Backups**

This Backup	Previous Backups	Other Data	Free Space
69.99 MB	13.55 MB	50.74 GB	182.06 GB

Total Capacity 232.88 GB↓

Data Used 50.82 GB (21.8%)

0%   20%   40%   60%   80%   100%

Backup files residing on **Directory - C:\Test Backups**

| 2009-09-04 | 69.99 MB / 69.99 MB† | |
| 2008-08 | 13.55 MB / 13.55 MB† | |

Key
Data Backed Up
Size on Medium†