Disk-to-Disk-to-Offsite Backups for SMBs with Retrospect

Abstract

Retrospect® backup and recovery software provides a quick, reliable, easy-to-manage disk-to-disk-to-offsite backup solution for SMBs. Use Retrospect to stream backups to disk for fast backups and rapid restores, and then copy the backups to tape or external hard drive for secure offsite storage and archiving. Retrospect's efficient design also allows various third party tools to efficiently upload incremental backup data to the cloud storage of your choice.

www.retrospect.com

Overview

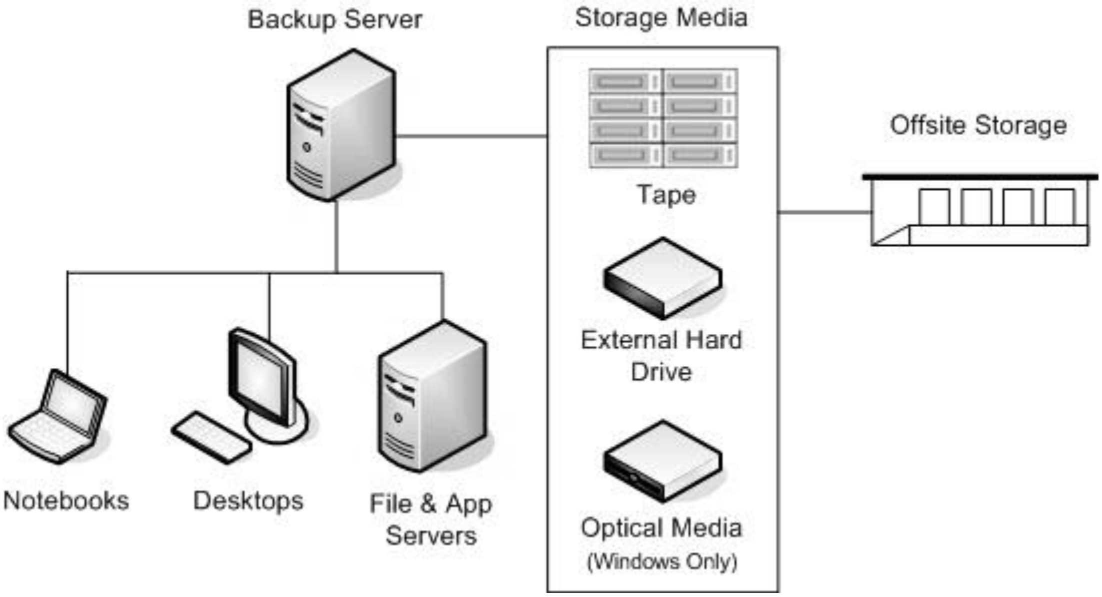
Small and medium businesses (SMBs) face unique challenges when selecting a backup and restore solution. The solution must protect all of your important data — not just servers, but desktops and notebooks as well. It must perform efficient backups so that both the time required for backups, and the amount of data being transferred over the network, is minimized. It must perform rapid restores. And it must enable you to easily create media for secure offsite storage to protect against data loss due to a disaster, such as a flood or fire.

Retrospect® is a reliable, easy-to-manage disk-to-disk-to-offsite backup and restore solution that meets all these requirements. The solution has been designed to be easy to set up and manage on an ongoing basis. Retrospect's patented technology automates many common backup tasks, performing backups and adjusting ongoing backup operations to react to changing network situations without the need for manual intervention.

The Solution

This data protection solution uses Retrospect 8.x for Windows Multi Server edition or Retrospect 10.x for Macintosh Multi Server edition backup and recovery software to create a local disk-based backup. Retrospect streams data from the computers that you are protecting to a dedicated backup server for local onsite storage. Devices attached to the backup server are used to copy the backups to additional sets of media for long-term offsite storage and archiving.

Figure 1 Network diagram of the Retrospect disk-to-disk-to-offsite solution



Backup Server

The backup server is typically a dedicated computer that hosts the Retrospect backup and recovery application. The disk is accessed from this server, as is the tape library, tape autoloader, external hard drives, or optical devices (Retrospect for Windows-only) used to create the offsite backup media. Installation of Retrospect is fast and easy. All valid backup devices are automatically recognized and configured without the need to install special device drivers.

Back Up from a Windows Computer

To run your backups from a Windows computer, use a Retrospect for Windows 8.x edition, which (depending on your license) can protect an unlimited number of Windows Mac OS, and Linux servers, desktops, and notebooks. Retrospect for Windows also supports integration with VMware, enabling you to back up live virtual machines. The Retrospect backup server must be running one of the following operating systems:

- Windows Server 2012 Essentials or 2012
- Windows Server 2012, 2008 or 2003 (32-bit or 64-bit)
- Microsoft Small Business Server 2011, 2008 or 2003 (32-bit or 64-bit)
- Windows Storage Server 2008 or 2003 (32-bit or 64-bit)
- Windows 8.1/8/7/Vista/XP (32-bit or 64-bit)

Use a backup computer with acceptable CPU performance (greater than 2GHz is recommended, as well as multiple CPUs or cores), and with at least 2 GB of RAM; for larger environments, 4 GB of RAM or more is recommended.

Backing Up from a Macintosh Computer

To run your backups from a Macintosh computer, use a Retrospect for Macintosh 10.x edition, which (depending on your license) can protect an unlimited number of Windows, Mac OS, and Linux servers, desktops, and notebooks. The backup server must be running one of the following operating systems:

- Mac OS 10.6.8 or later
- Mac OS X Server 10.6.8 or later

Use a backup computer with any Intel processor. Select a computer with at least 2 GB of RAM; for larger environments, 4 GB of RAM or more is recommended.

You can administer Retrospect from one or more Macs by installing the Retrospect Console on those Macs. You can control one or more Retrospect backup servers from a single Console.

Networked Computers

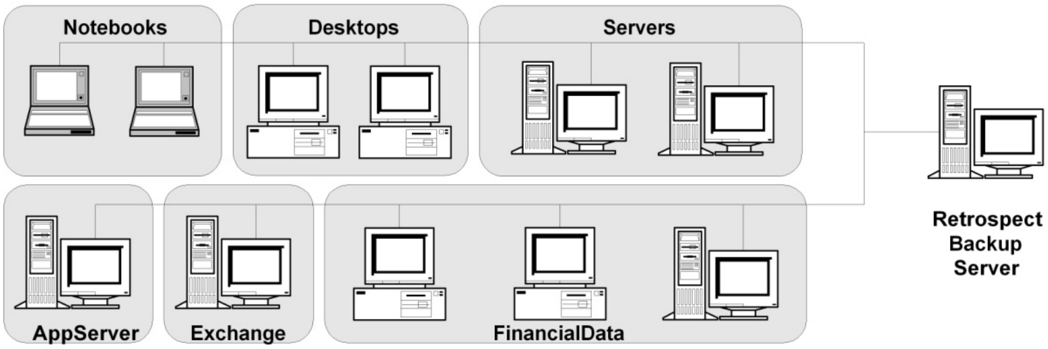
The lightweight Retrospect Client software is installed on each networked computer. It communicates with the backup server when a computer becomes available for backup, and manages the data transfer of files, folders, and system state information, which is required to recover a computer if needed. You can configure backups to run on a regular schedule. In addition, Retrospect's Proactive Backup technology recognizes computers when they connect to the network and prioritizes them for backup. This is particularly useful for backing up notebook and desktop computers. Notebooks are not always connected to the network at predictable times. Desktops might be turned off or located on a portion of the LAN that is temporarily inaccessible during the backup window, for example during off hours when backups are typically scheduled. If an unprotected desktop or notebook is discovered, Retrospect automatically begins a backup without manual intervention, keeping your data safe automatically.

This technology also avoids one of the most common challenges SMBs face when backing up desktops and notebooks: user error. Most SMBs rely on their employees to back up their own desktops and notebooks, but backup is a low priority for most employees. Even diligent employees can forget to back up when they are working on important projects under tight deadlines, which is precisely the time when backing up data is most important. By automating the backup process, Retrospect ensures that the data on your desktops and notebooks is always protected.

Source Groups

Client computers are typically placed into source groups so they can be protected as a group. For example, executive notebooks might be placed into one group and scheduled for immediate backup when they connect to the network. An application server might be placed in another group and backed up each evening. Financial data might be placed in yet another group to facilitate compliance with government regulatory guidelines regarding frequency of backups or data retention.

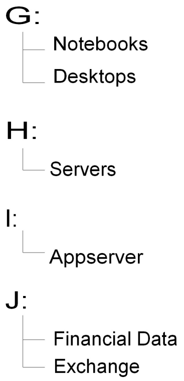
Figure 2 Organizing computers into groups



Each source group is backed up to a Disk Backup Set residing on disk, typically on the backup server. This allows Retrospect to back up as many as 16 source groups concurrently, each to its corresponding Disk Backup Set. In this example the Disk Backup Sets are distributed across the four volumes shown in **Figure 3**.

Figure 3

Sample directory structure for Disk Backup Sets and their associated Catalog Files.



Retrospect allows one concurrent backup to each Backup Set. By creating multiple Disk Backup Sets, as many as 16 simultaneous backups can be supported. For faster backups, configure the backup server with multiple volumes, and distribute the Disk Backup Sets across them. When Retrospect is utilizing Disk Backup Sets in parallel the overall I/O performance will be higher because the write operations will be distributed across separate volumes.

Each Backup Set also has an associated catalog file, which Retrospect uses to track the content of the Backup Set. The catalog file contains a list of all files that are contained in its corresponding Backup Set. Retrospect also uses the catalog file to record the directory structure of each backed-up volume for future restores. If Retrospect detects an identical file residing in multiple locations on the networked computers, it uses a process known as file-level deduplication to copy only one instance of the file to the Backup Set, saving considerable time during the backup and reducing the storage space required for the Backup Set.

Proactive Backup

Each group of computers will be backed up into its corresponding Disk Backup Set with a Proactive Backup. Proactive Backups have significant advantages over fixed schedule backups because they minimize the manual efforts required to keep backup operations running smoothly.

Fixed scheduled backups run at a specific time. If a computer is unavailable, an error is logged. In the case of notebook computers, trying to catch them for backup when they are available on the network can be especially frustrating. A manual effort is required to read the backup logs each day and create custom backups to protect computers that are not available during regular scheduled backups. This is a tedious, time consuming, and difficult task.

In contrast, Proactive Backups adjust themselves to keep backup operations running smoothly without the need for manual intervention. A backup window is established for the Proactive Backup to identify when the first backup can begin, and when the last backup must be stopped. Computers are automatically recognized when they appear on the network because the Retrospect Client that is installed on them communicates to the Retrospect backup server so they can be prioritized for backup. Computers that have not been backed up recently are raised to a higher priority than others in the same group to ensure they are not starved from being backed up. If all backups for the group cannot be completed during the backup window, they will be captured during the next window. If a computer is only partially backed up, its backup will resume from where it left off when backups are again possible.

Easy Ongoing Maintenance of Backups

Maintaining the ongoing backup operations is easy. If computers do not get backed up during a particular backup session because they were inaccessible or there was not sufficient time, Retrospect's patented Proactive Backup technology automatically adjusts the backup operations to ensure the computers are protected during subsequent backup sessions. As more computers are added to your network, simply assign them to the appropriate group as described in *Source Groups* earlier in this document. They will be protected along with the other computers in the group according to the same policy.

Retrospect also greatly simplifies rotation of Backup Sets between onsite and offsite locations each week. In the recommended backup strategy two sets of media are used, A and B. Transfers of data from local disk to offsite media take place each week. The first week offsite Backup Set A is used, then for the following week offsite Backup Set B is used. Move the tape or disk that is not being used for a particular week and store it offsite. This protects against catastrophic loss of critical data due to disk failure, fire, or theft. Tape backup media should be moved offsite to long-term storage at the end of each quarter, and new media should be introduced.

Disk Grooming — No Weekly Full Backups

The first backup into a Disk Backup Set is a full backup of everything from the computers in the source group. Thereafter only new or changed files, folders, and system state information needs to be added to the Disk Backup Set during each backup session. This is referred to as an incremental backup. The amount of backup data gradually increases over time until it fills the disk space allotted for backups. This is why a data grooming capability is built in to Retrospect.

Retrospect's automated data grooming feature can delete older, unnecessary files and folders from the backup disk to ensure that there is always plenty of available disk space for newer backups to be stored. Because disk space never has to be adjusted or reallocated on the backup server, incremental backups can be performed forever without manual intervention. In this way, a Disk Backup Set is self-maintaining. Regardless of the disk configuration, after the maximum size has been established for a Disk Backup Set, Retrospect can be set up to groom out older backups automatically.

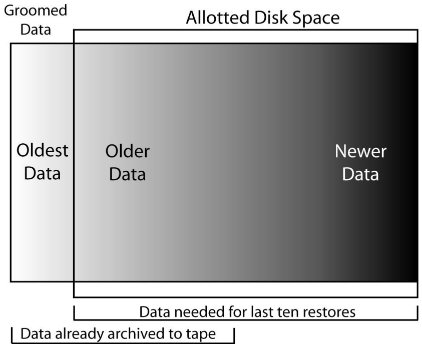
Retrospect can be configured to perform data grooming in three ways:

- Grooming can be triggered automatically when the allotted disk space is full.
- Grooming can be set to occur according to a predetermined schedule.
- Grooming can be initiated manually.

Because data grooming deletes older files, a reliable offsite archiving policy utilizing tapes or remote disk is essential to prevent the loss of potentially valuable older data. Onsite disk provides fast operational recovery of time-sensitive data, while offsite archiving prevents the permanent loss of data that has been groomed from the onsite disk. **Figure 4** shows the advantage of overlapping offsite backups with onsite disk backups that employ data grooming.

Figure 4

Combining data grooming and archived backups.


Groomed Data
Allotted Disk Space
Oldest Data
Older Data
Newer Data
Data needed for last ten restores
Data already archived to tape

The recommended strategy is to back up to a Disk Backup Set, which is set to retain only the last 30 days for each source. Snapshot Transfers are performed to tapes each week to ensure that data is safely stored for long term archives well before it is groomed out of the Disk Backup Set to make room for newer backups. Snapshot Transfers are discussed in the next section.

Secure Offsite Storage

For archiving and disaster recovery purposes, data that is stored on local disk needs to be copied to offsite media (tape, external hard drives, or optical media) and stored in a secure offsite location for long-term storage in case the data ever needs to be restored. Use Snapshot Transfers to automatically schedule the copying of data from disk to media for offsite storage.

Create Offsite Backup Sets

Estimate the amounts of data that will be backed up and procure the appropriate number of tapes, external hard drives, or optical media. Your offsite storage media should have enough capacity to hold all of the data that is stored on your local disk. If you use tape as your offsite media, consider using a tape library. At least two separate Backup Sets are recommended to store backups. With two sets, you will always have a working backup set, even if a tape, hard drive or optical media fails in one of the sets.

Transfer Snapshots from Disk to Offsite Media

Retrospect uses the term Snapshot to describe a list of all files, folders, and settings on a computer at a point in time when a backup occurred. Each time a backup is performed, a current Snapshot is added to the Backup Set as an available restore point. Using Snapshot Transfer, you can very easily copy selected data from the Disk Backup Set to a new offsite media set or add to an existing one.

After the first Snapshot Transfer to an offsite media Backup Set, the offsite media contains the selected Snapshots (restore points) for each protected source computer. The data is copied from the Disk Backup Set without having to repeat the backup of the original source computers or clog the network infrastructure.

Subsequent Snapshot Transfers to an existing offsite media Backup Set adds corresponding restore points onto the offsite media for each source. However, the Snapshot Transfer operations need to copy only the files and folders that are new or changed compared to those already stored in the Backup Set. The result is a collection of restore points that make extremely efficient use of your offsite media.

Sync to Cloud Storage of Your Choice

Each Retrospect Backup Set consists of multiple Retrospect RDB files. During backup or snapshot transfer, Retrospect packages new or changed data as additional RDB files to the Backup Set, without modifying the existing RDB files. Therefore, you can easily use various third party tools to efficiently synchronize or mirror RDB files in a Retrospect Backup Set, along with its much smaller catalog file, to the cloud storage of your choice. Each RDB file is transferred once and not modified again. This provides a practical solution to selectively store smaller and more important offsite Backup Sets on the cloud, while much larger offsite media Backup Sets for all your data go to your physical offsite location.

Offsite Storage and Encryption

Store the Backup Sets offsite in a secure location when they are not being used. Retrospect supports AES-256 encryption with password on Backup Sets to prevent access to the data if the offsite media is lost or stolen. Passwords should be stored in an encrypted or physically secured location with access by a few trusted employees to ensure continued password availability, despite employee turnover. Creating a password management process is critical because if you lose or forget the password, encrypted data will not be restorable.

NOTE: AES-256 encryption is recommended for off-site backups when possible. However, encryption will slow throughput to offsite media. If speed outweighs your encryption needs, password protection is recommend for a basic level of offsite security.

Conclusion

Retrospect’s backup-to-disk features protect the maximum amount of data in the shortest amount of time by utilizing the speed and efficiency of disk. Backups can be stored internally on hard disk within the backup server or externally on a disk storage device. Disk provides an easy-to-use, cost-effective destination for backups. Rapid restores are achieved by storing the most recent data, for example files and folders that are less than 30 days old, on disk.

For archival and disaster recovery purposes, Retrospect uses patented, automated technology to simplify the process of transferring backups from the backup disks to other media for offsite.