Retrospect

Retrospect 8 for Windows

Reviewer's Guide

About this Reviewer's Guide

This document provides a concise guide to understanding Retrospect 8 for Windows. While it is not designed to replace the Retrospect User's Guide, it will provide the reader with…

- descriptions of Retrospect's technologies and terminology,
- knowledge on how Retrospect's components work together to provide reliable backup and recovery, and
- examples and methods for protecting laptops that come and go from the network, as well how to employ offsite (cloud) backups for added protection.

Understanding how Retrospect works

This section introduces certain terminology that is used by Retrospect. Such terms are highlighted with **bold** emphasis.

Retrospect is *file-based* backup software, as opposed to drive imaging software that copies blocks or sectors on a hard disk drive. While an image- or block-based tool can be very fast at recovering an entire disk partition or providing a point-in-time view into a partition's contents, a file-based backup provides several distinct advantages. For example, it's possible to quickly search multiple backup archives and recover multiple versions of a document, while still being able to provide a complete restore of an entire disk. It's also easy to restore files backed up from a Windows PC's NTFS volume to a Mac, because the volume format doesn't matter for file-based recovery.

Retrospect employs several technologies to ensure that it only and always backs up the minimum number of files necessary to restore whatever ***volume*** *it is protecting.*

That statement says a lot about Retrospect's design. Understanding this basic principle provides a good deal of insight into why Retrospect works the way it does and what we feel is the most important aspect of a backup system: reliability.

Retrospect's key components and terminology

The following components are the building blocks of every **backup**, **duplicate**, or **restore** operation in Retrospect:

- **Source** – a **volume** attached to the Retrospect server or a computer on the network running the Retrospect **Client** software that contains files and folders to be protected; can also be a network share
- **Destination** – the target for the files being copied or backed up; can be a **Backup Set** (see below) for backups or another volume for a duplicate operation
- **Selector** – a built-in or user-defined set of conditions used to filter what gets copied during an operation
- **Source Group** – a label applied to a source for the purpose of logical or physical grouping and abstraction; examples of Source Groups are: *Laptops*, *Accounting Dept.*, *2nd Floor*
- **Schedule** – the time or times during which Retrospect will run its operations
- **Script** – a saved procedure that defines the settings for an operation; scripts can be run manually or automated with one or more schedules

Two important components work together to store and track backed-up data:

- **Backup Set** – a logical container made up of one or more data storage mediums (including hard disks, network shares, digital tapes, USB thumb drives, etc.) that hold backed up files
- **Catalog** – a database that tracks all of the files stored in a Backup Set, as well as point-in-time information about each of the sources that have been backed up; each Backup Set has its own Catalog

The following example ties it all together: *A backup script runs nightly at 8:00 PM to protect all computers contained in the "Desktops" Source Group, copying any files that match the "Documents and Settings" selector to a destination Backup Set comprised of volumes on an iSCSI RAID.*

Smart Incremental backup technology

Retrospect doesn't use the traditional concepts of *full*, *incremental*, and *differential* backups. These are outdated modes of backup that have significant drawbacks with regard to performance, restore precision, or both. Traditional full backups are incredibly time consuming but offer precise restores. Incremental backups save time during the backup process, yet they restore unwanted files that were renamed, moved, or deleted since the last full backup.

Retrospect's Smart Incremental technology (sometimes called *Progressive Backup*) works by matching the files on a source volume with the files that are already stored on the destination Backup Set. By doing so, Retrospect only needs to back up those files that have changed or been newly created since files were last written to the destination. This provides the same performance advantage of a traditional incremental backup.

In addition to copying just the files not already present on the destination, the Smart Incremental process saves a complete listing of all the files and folders that were present on the source at the time of the backup. This provides a point-in-time **snapshot** of the exact state of a volume, which Retrospect can later use as a guide to select the proper files for a restore.

Instant Scan technology

In order to build the list of new and changed files for any particular volume being backed up, previous versions of Retrospect had to spend time scanning all the files present to determine what had changed since the last backup to that Backup Set. For a volume containing a million files, this scanning process could take 10-15 minutes—often far longer than the time needed to actually back up the new bits. When multiplied by 20 computers being backed up, that's several hours of time spent calculating what exactly to backup.

Retrospect now employs Instant Scan technology to significantly reduce the overall time spent determining what files need to be copied during a backup (and for certain types of restores). By using FSEvents on Mac OS HFS+ volumes and the USN change journal for Windows NTFS volumes, Retrospect and the Retrospect Client software are able to pre-scan disks and folders on Mac and Windows PCs, so that the list of new and changed files is ready to go when the backup starts. For a typical network environment where computers are backed up on a regular basis, *Instant Scan technology cuts overall backup times in half*.

Instant Scan technology is a major step forward in managing the ever increasing amount of data present on an organization's network and allows users to reduce costs and/or increase their level of protection:

- More computers (or data) can be protected during the backup window by each Retrospect host server.
- Critical data can be protected more often.

Data deduplication

Retrospect's Smart Incremental technology provides another benefit to users: data deduplication that saves time and storage space needed for backups.

Because Retrospect only backs up files that aren't already contained in the target Backup Set, it doesn't store multiple copies of files that are duplicated around the network. For example, if Retrospect encounters a PowerPoint presentation on Computer B that's exactly the same (in terms of name, size, creation and modification dates, etc.) as one it just backed up from Computer A, it doesn't need to copy that file again. Likewise, if Computer A and Computer B share most of the same 60 GB iTunes music library, Retrospect only needs to copy the matching files one time. The more data that is duplicated around a network, the more time and storage space Retrospect saves.

Using selectors to further refine backups and restores

Retrospect allows the user to create **selectors** that can be used to filter unimportant files, or to specifically select files that meet certain criteria. Several rules come pre-defined, such as the "All Files Except Cache Files" rule, which tells Retrospect to ignore temporary cache files like those created by Web browsers. Not backing up such files can save significant storage space, since it's typically unnecessary to restore them.

Selectors are flexible and powerful. They can be used to prevent operating system files from being backed up, or to restore all Microsoft Excel files larger than 2 MB, which were modified in the past 60 days, and contain the word "Forecast" in their names.

Smart Restores

Retrospect's modular design allows the Smart Incremental technology to be used in reverse during a restore operation. By using the snapshot saved with the backup as a guide, Retrospect ensures that only those files not already on the volume being restored need to be written, while (depending on the restore options selected) files that don't belong are deleted. This gives Retrospect the restore precision of a traditional full backup, only Retrospect doesn't have to unnecessarily re-copy matching files that are already present on the destination.

Retrospect offers three types of restores:

- Restore an entire volume to a previous point in time
- Browse and restore selected files and folders from a specific point in time
- Search for and restore one or more versions of one or more files from any backup

These options cover a multitude of cases and provide incredible restore flexibility.

Multiple backups improve reliability

We've learned that Retrospect only needs to copy a file once to be able to restore it to any destination. But what happens if a Backup Set is destroyed in a fire along with the computers for which it was storing backups? Not good!

To protect against data loss due to events such as theft, fire, and flood that can damage locally-stored backups just as easily as the original data, it's critical that more than one backup be created, and optimally, at least one copy be stored offsite for safe keeping.

By design, Retrospect's Smart Incremental backups select files to copy by comparing only against those already on the target destination. By simply targeting a different destination, it's possible to affect what files will be selected for backup. Targeting an empty Backup Set will result in all files being backed up, even if they've already been backed up to a different Backup Set.

Retrospect tracks each Backup Set independently.

The following table shows what files will be copied for each destination:

Backup Set Name	Last Written To	What Gets Copied
Backup A	Yesterday	Unique files changed or added since yesterday
Backup B	1 Week Ago	Unique files changed or added in the past week
Backup C	Never (empty)	All files

Unlike other backup software that chooses files based solely on dates or archive flags, Retrospect ensures that each destination is kept complete. By doing so, only one set is needed to perform a restore, and individual Backup Sets may be retired as archives without impacting other Backup Sets.

This is a great example of how Retrospect is designed to do the right thing. Give it an empty destination, and Retrospect will copy everything to it. Give it a set that already contains data, and Retrospect will copy just what's needed. The user doesn't have to change the type of backup to ensure that the right files get copied.

Data Verification

Retrospect's modular design and focus on reliability is readily apparent in how it verifies that backed up files can be restored successfully.

After Retrospect completes backing up a source volume, it reads back the files it copied and compares them to the originals. However, the way Retrospect does this is unique. To read back the files it copied, Retrospect actually uses its restore module. Then, instead of overwriting the original files with the backed-up copies, it simply compares them. This method has the benefit of testing the actual path that files will take when being restored, so in essence, file restorability is verified along with file integrity.

A note on performance testing: Retrospect defaults to thorough file verification, which can almost double the time that a backup operation takes. Retrospect's Media Verification option uses MD5 checksum digests generated during the backup and written to the media to quickly verify data integrity. This method doesn't test the entire restore path during a verification, but it is several times faster. Many other backup applications default to no verification, sacrificing reliability for performance.

Common Uses for Retrospect

This section provides guidance for using Retrospect in a couple of scenarios that illustrate how the software meets common usage needs. In addition to its focus on reliability, Retrospect is designed to be flexible for a variety of needs not touched on here.

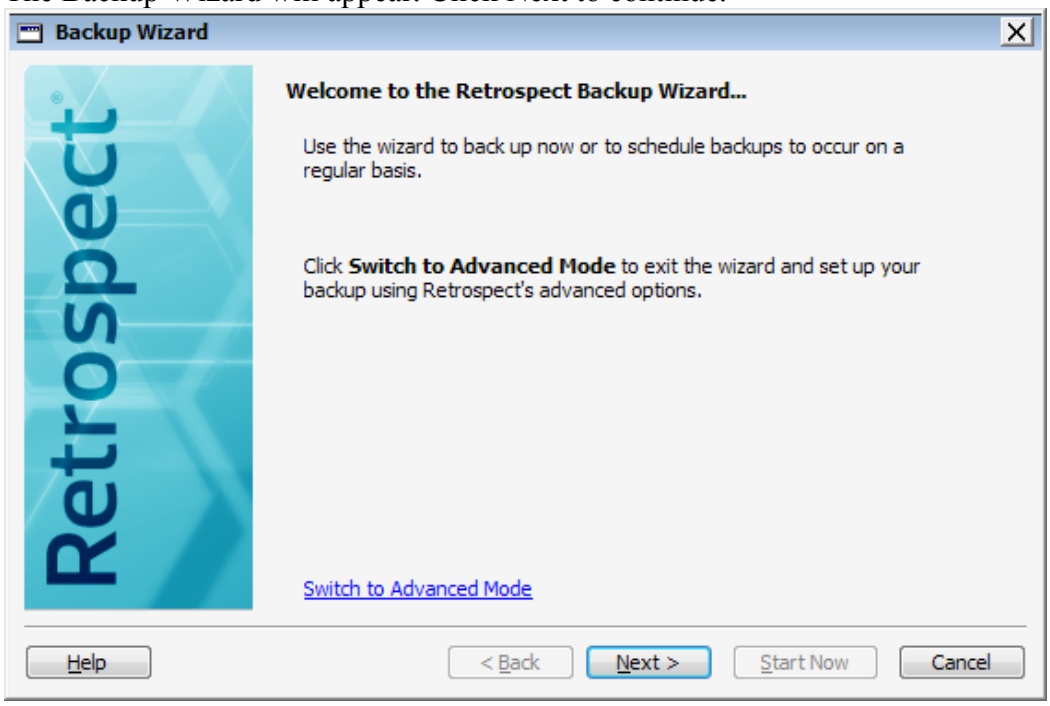
A note about scripts: A single Retrospect script can control the backups of an entire network of computers, with multiple sources, multiple destinations, and multiple schedules. However, each script's options, such as which selector to use, whether to use encryption, and on what schedule to run, will apply to all of that script's sources. If you want to back up desktops only at night and laptops 24 hours a day, you will need two scripts to do that. If you want to encrypt the backups for the accounting system and customer database, you will need to use a separate script than for non-encrypted backups of less sensitive data.

Nightly onsite backups with weekly offsite copies

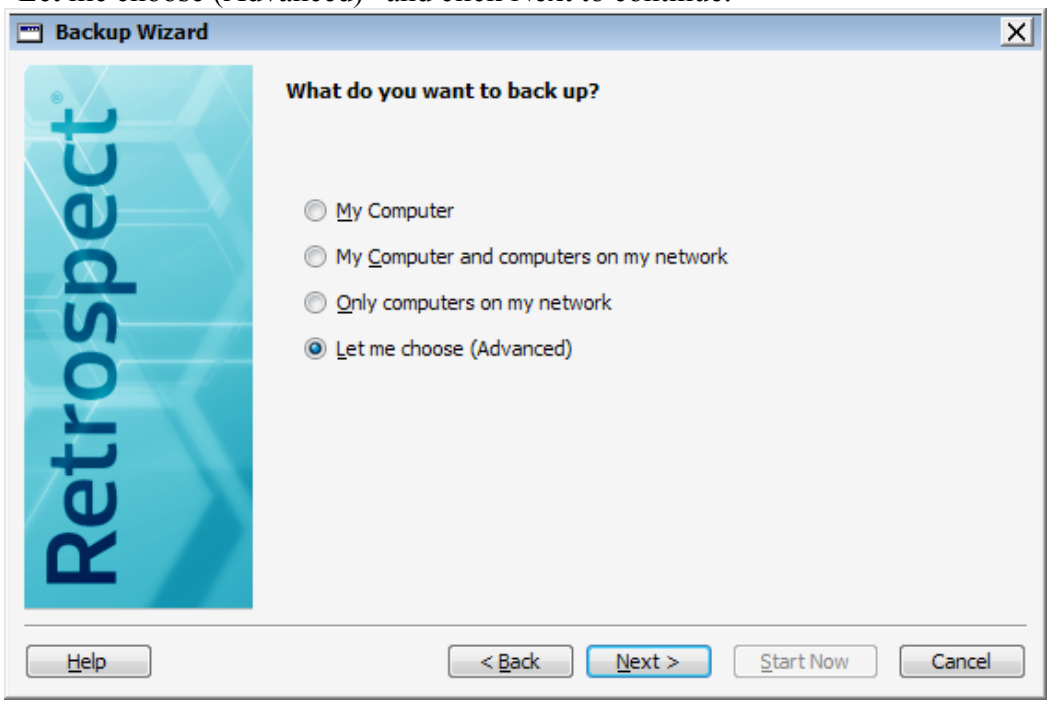
With just two scripts, Retrospect can protect an entire network of computers using both onsite and cloud-based storage. This exercise also provides a good example of how powerful Retrospect's rules can be.

Script #1 – Nightly backup to local disk or network share

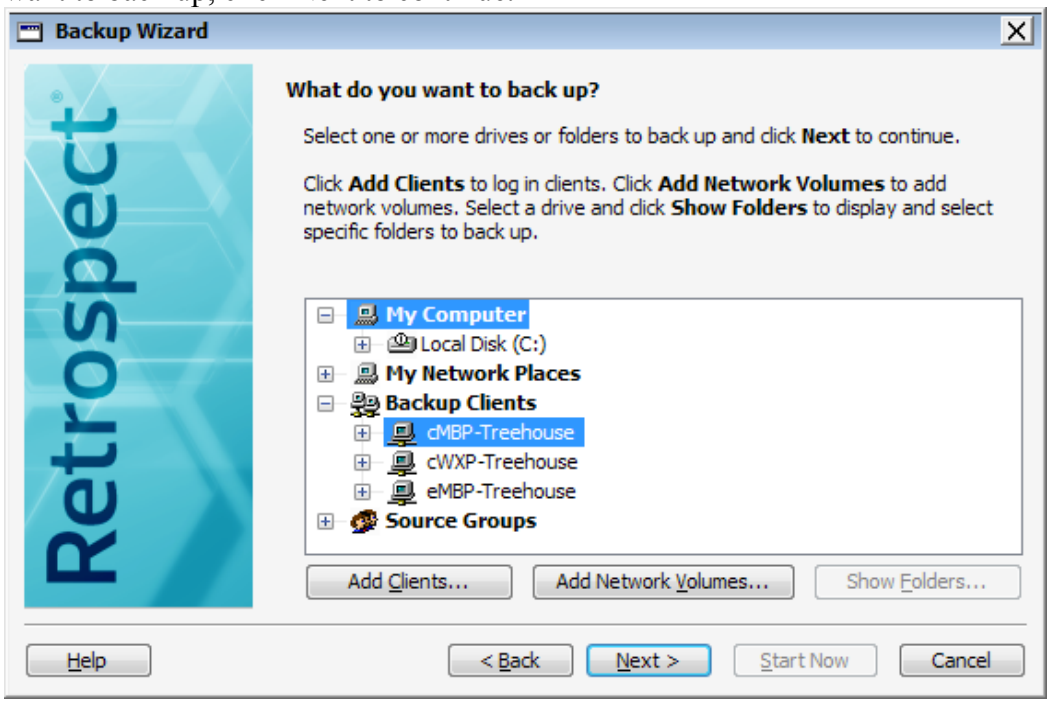
1. Create a Backup script by selecting Backup→Backup in the left navigation pane. The Backup Wizard will appear. Click Next to continue.



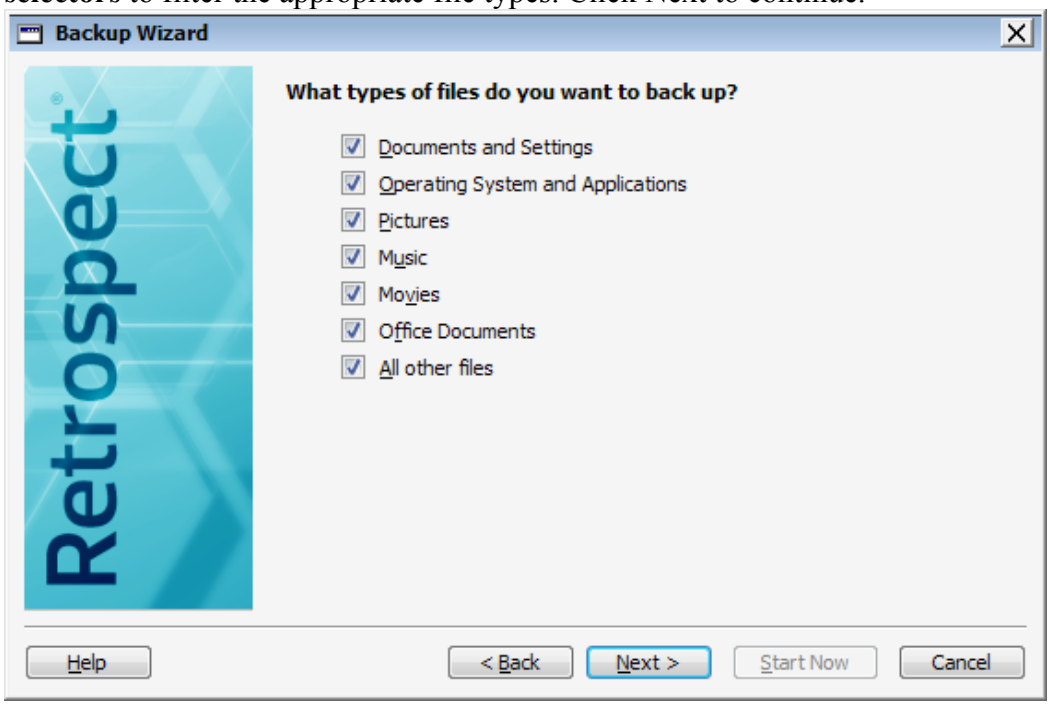
2. Choose a method to select the sources to be protected. For this example, select "Let me choose (Advanced)" and click Next to continue.



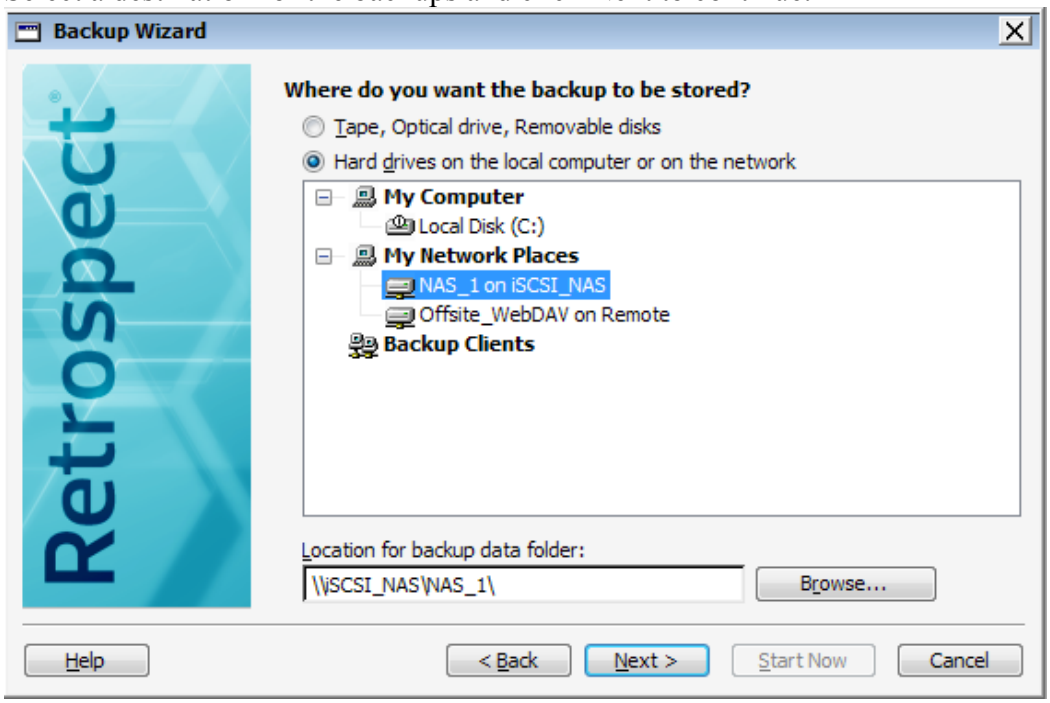
3. Click to select a source, or Ctrl-click to select multiple sources for the backup. This window also allows you to log in networked computers on which you've installed the Retrospect Client software. After you've selected the sources you want to back up, click Next to continue.



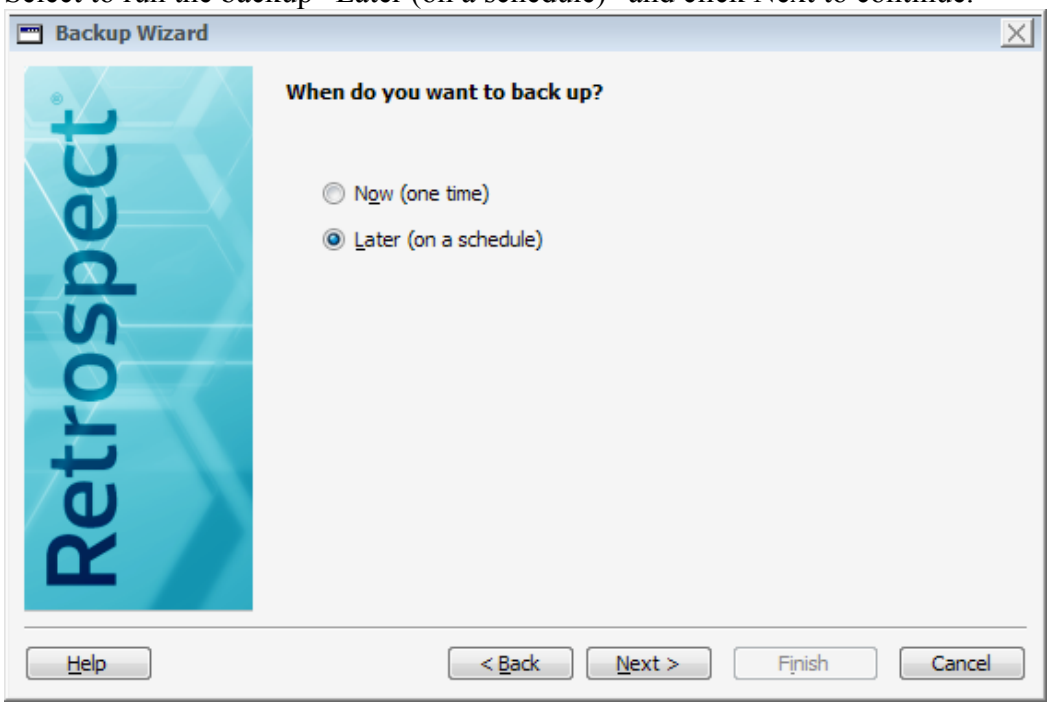
4. Tell Retrospect what types of files to copy during the backup by checking or unchecking the boxes for each type of file. Retrospect will employ its built-in **selectors** to filter the appropriate file types. Click Next to continue.



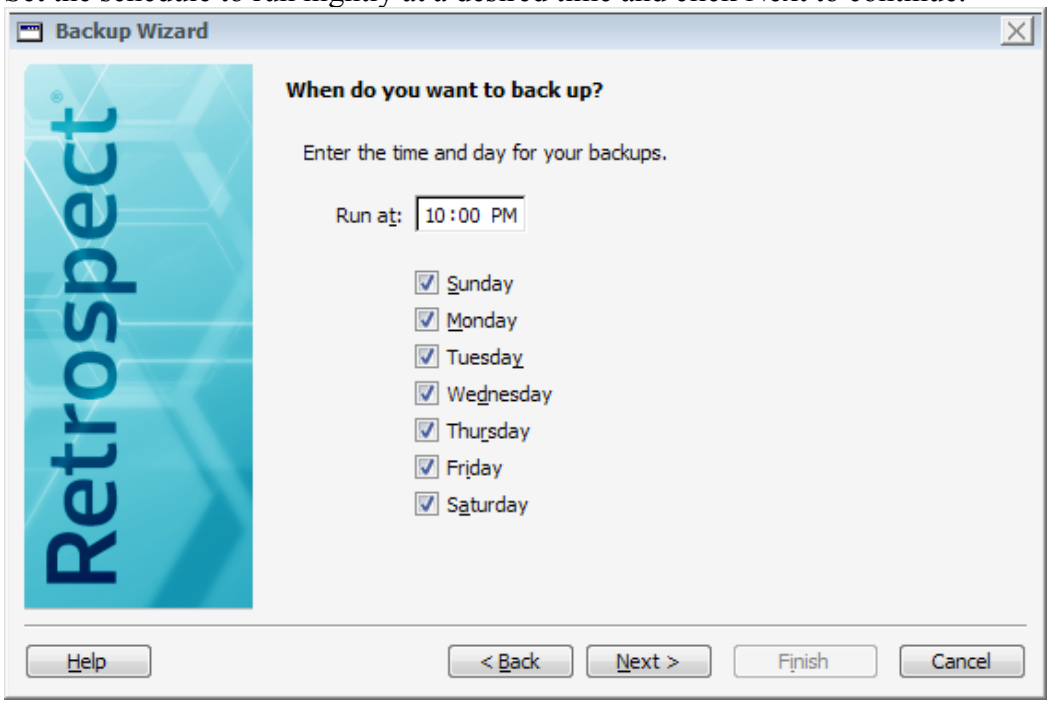
5. Select a destination for the backups and click Next to continue.



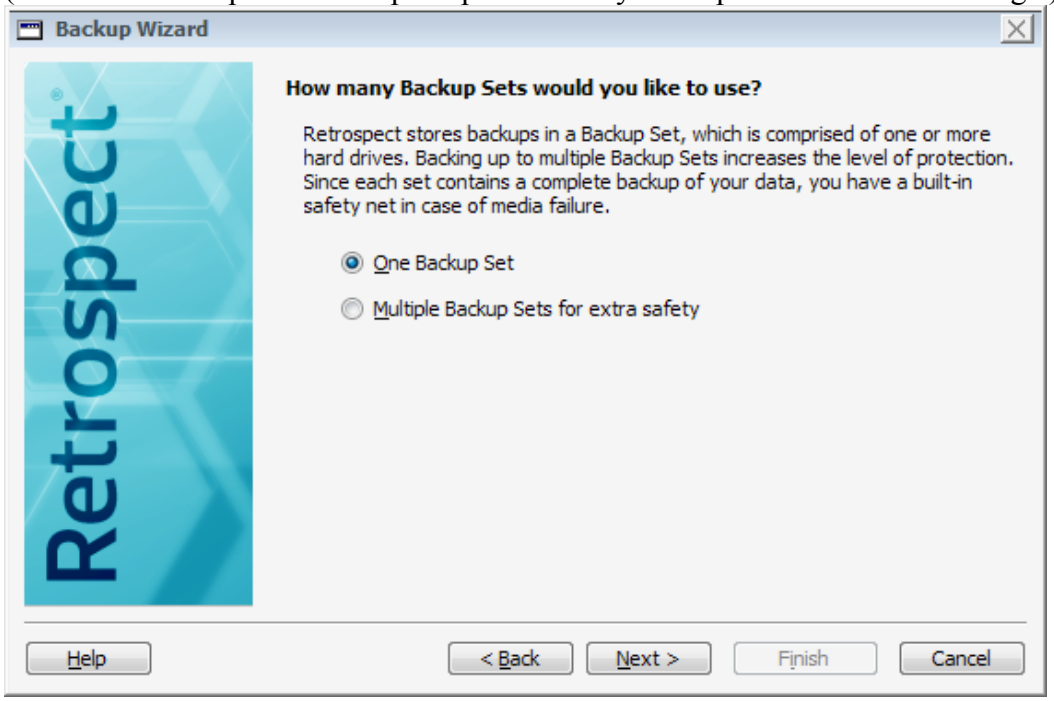
6. Select to run the backup “Later (on a schedule)” and click Next to continue.



7. Set the schedule to run nightly at a desired time and click Next to continue.

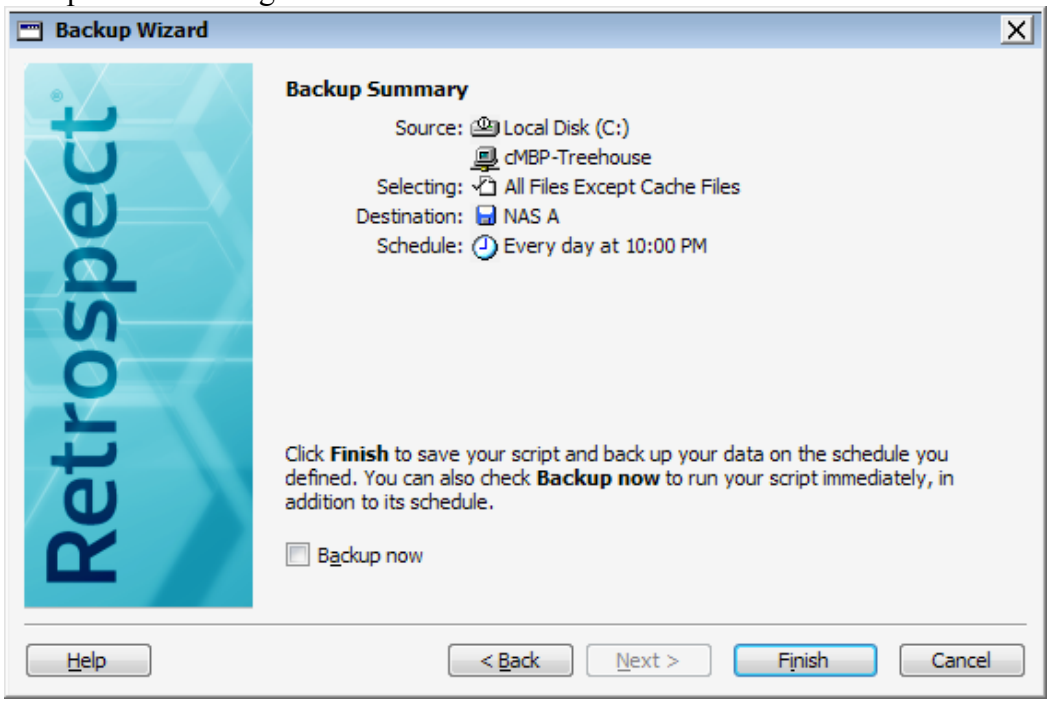


8. Choose to have Retrospect use only one Backup Set and click Next to continue. (We'll create a separate backup script for weekly backups to cloud-based storage.)



9. Give the Backup Set a descriptive name, then go through the next several screens of the Backup Wizard, selecting settings for compression, encryption, what to do when your disk fills up, and finally entering a descriptive name for the script.

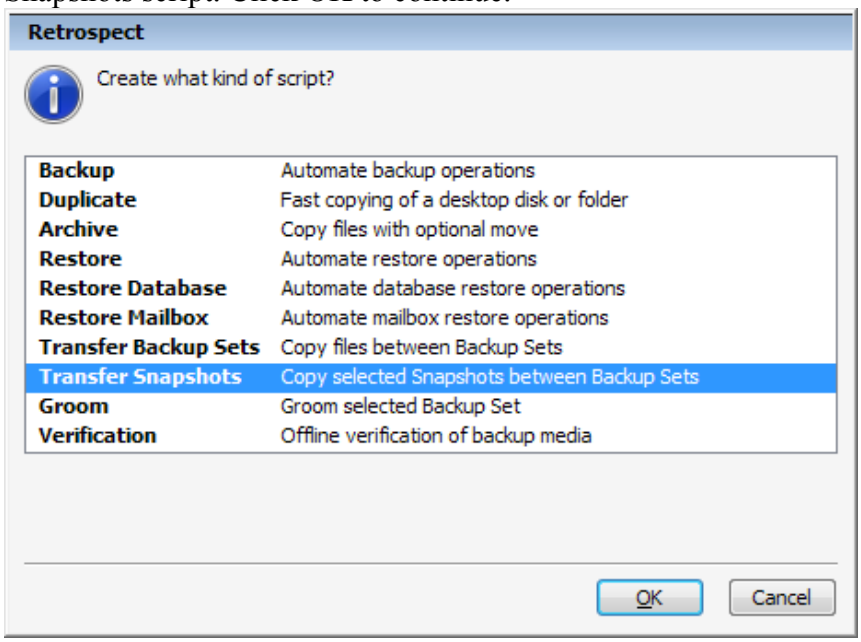
10. The final screen shows a summary of the script you've just created and gives you the option of running it now. Click Finish when done.



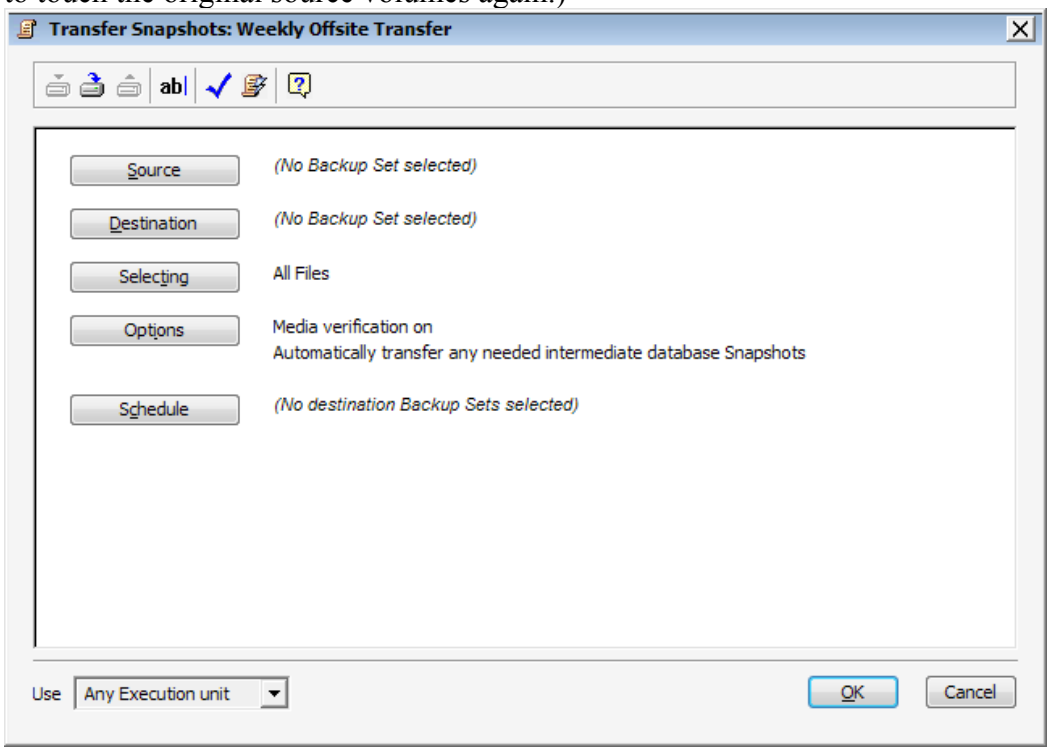
Script #2 – Weekly transfer to cloud-based (or offsite) storage

We'll handle the process of a weekly data transfer to cloud-based WebDAV storage with a Transfer Snapshots script. A Transfer Snapshots operation copies one or more snapshots (including the backed-up files they indicate) from one Backup Set to another. This allows Retrospect to copy the latest backup for each protected computer from the Nightly Backup set to a different one one stored at a remote location.

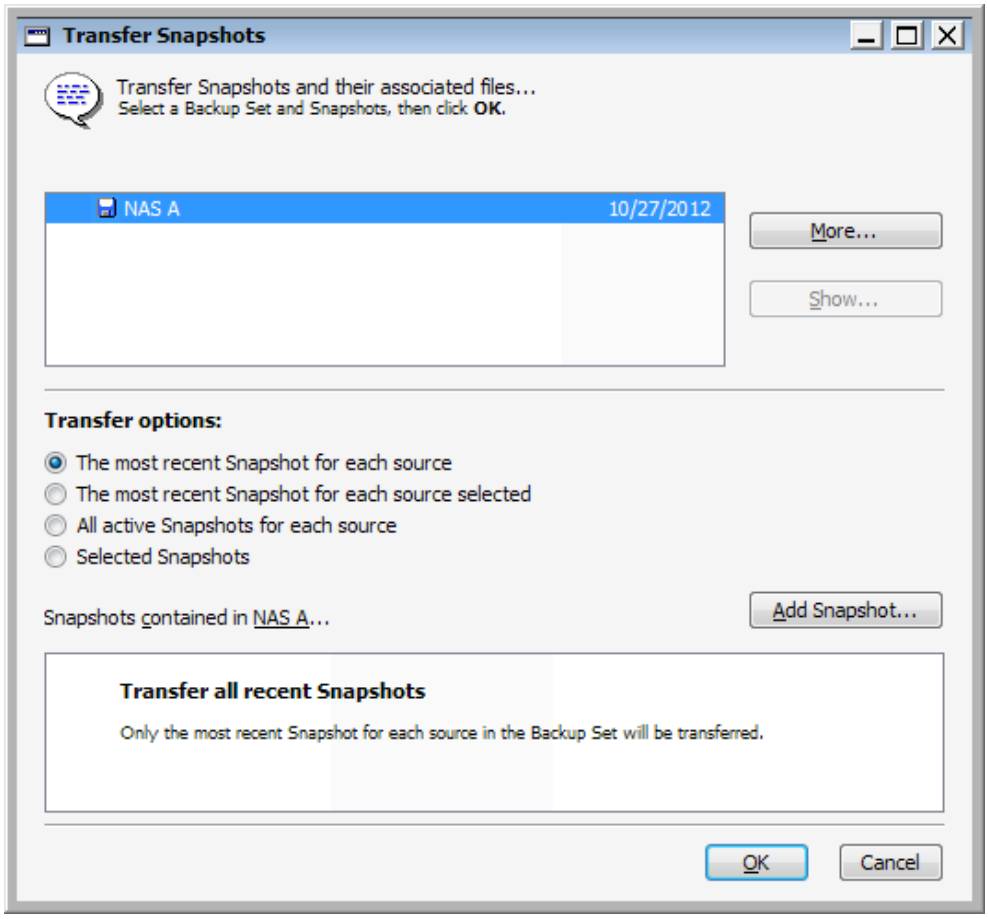
1. Click Automate→Manage Scripts in the left navigation pane. When the Scripts window appears, click New to select the type of script, and select a Transfer Snapshots script. Click OK to continue.



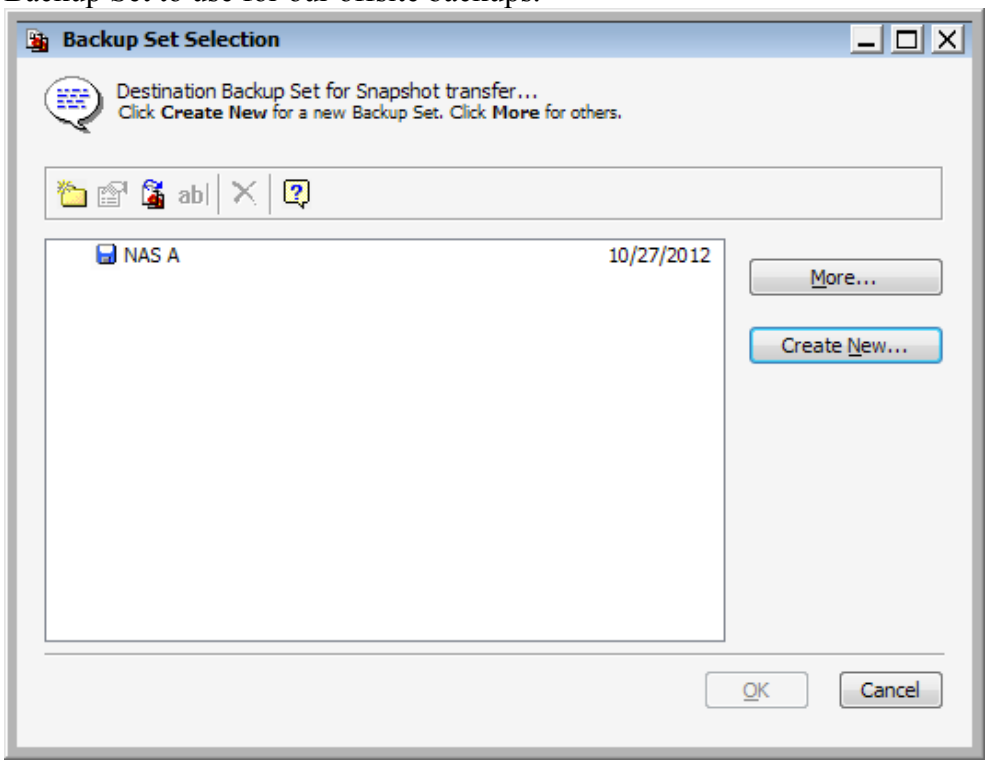
2. The advanced mode script editing window will appear. (A note about Transfer Snapshots scripts: The source for a Transfer Snapshots script is another Backup Set. This allows Retrospect to transfer data from one Backup Set to another, a useful method of copying files that have already been backed up without having to touch the original source volumes again.)



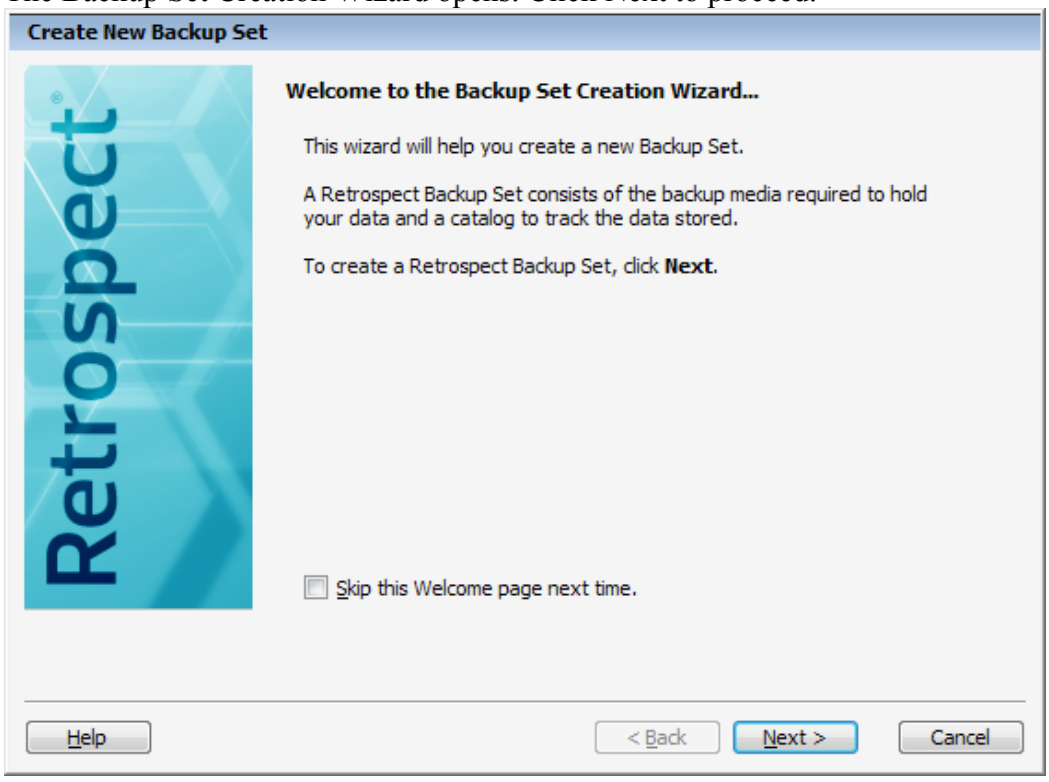
3. Click the Source button, then select the Backup Set that's used to store the nightly backups from Script #1. In the bottom half of the window, select "The most recent snapshot for each source." This tells Retrospect not to bother transferring files that may have been deleted from the source volumes earlier in the week. Click OK to continue.



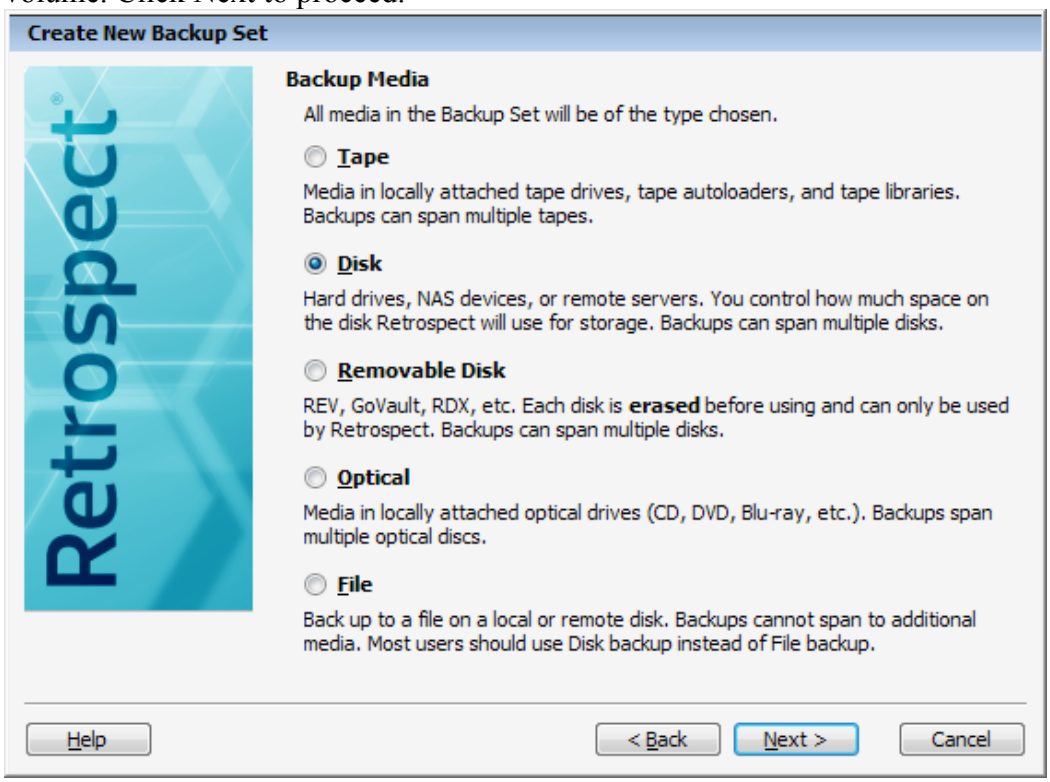
4. Click the Destination button, then click the Create New button to create a new Backup Set to use for our offsite backups.



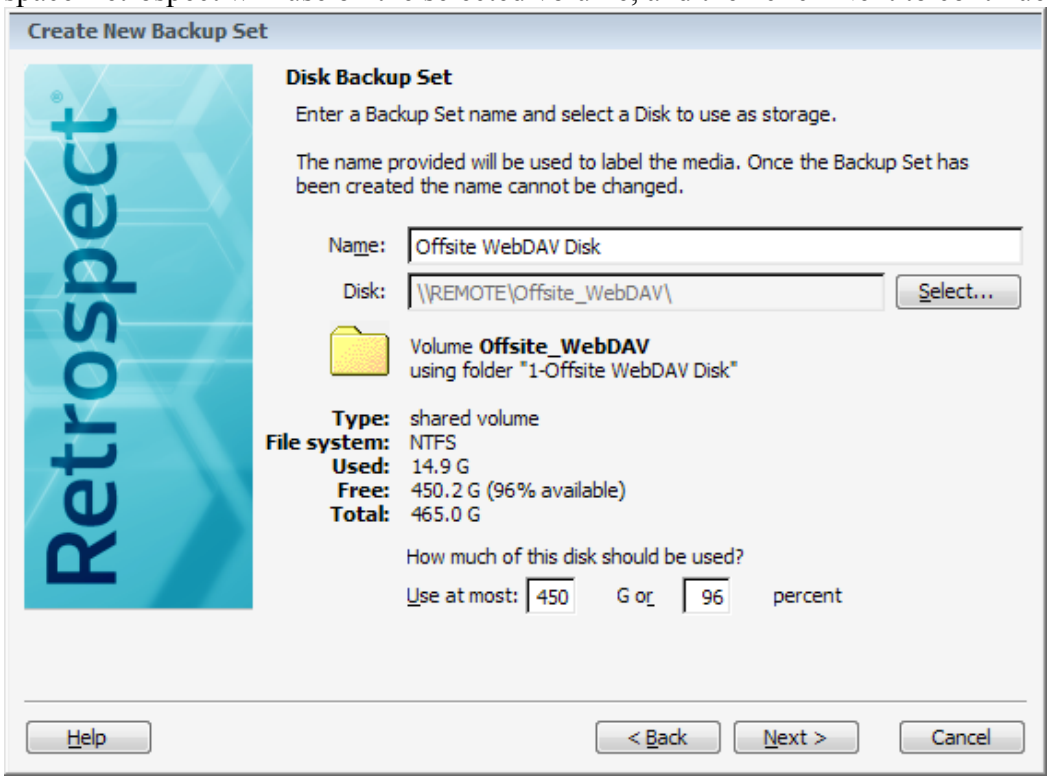
5. The Backup Set Creation Wizard opens. Click Next to proceed.



6. Select Disk for the type of media that will be used for the Backup Set. Disk can be direct- or network-attached media, including a network share or remote WebDAV volume. Click Next to proceed.

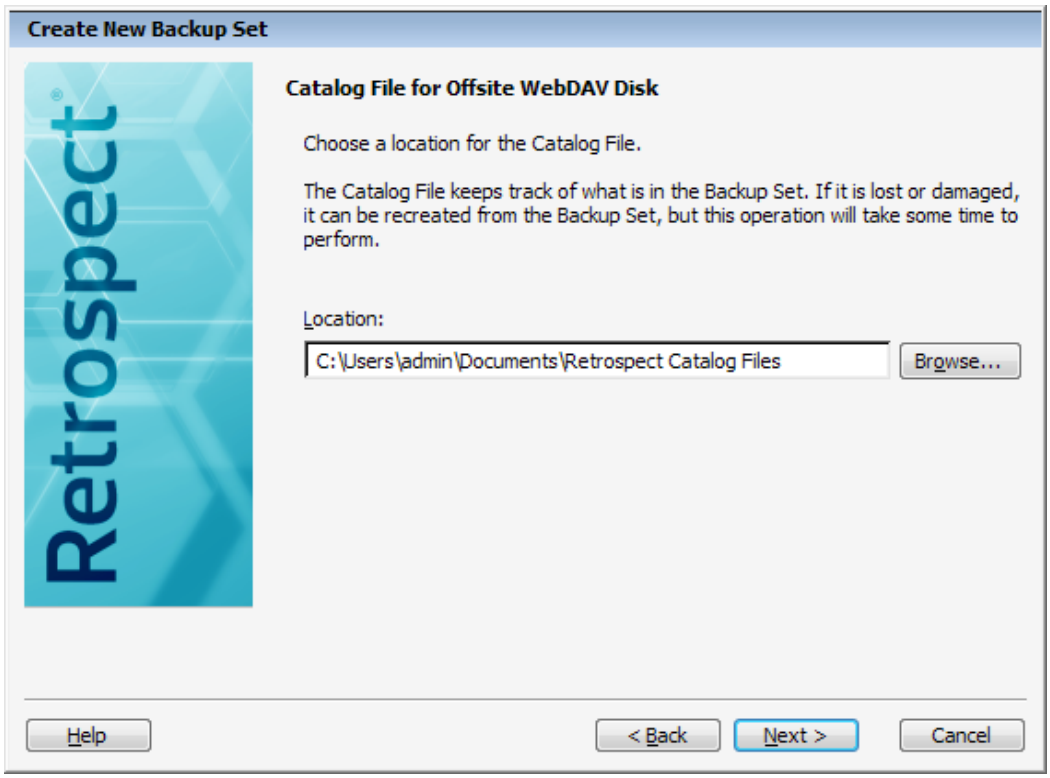


7. Give the Backup Set a descriptive name and click the Select button to choose location for the Backup Set. If necessary, set a quota to cap the amount of storage space Retrospect will use on the selected volume, and then click Next to continue



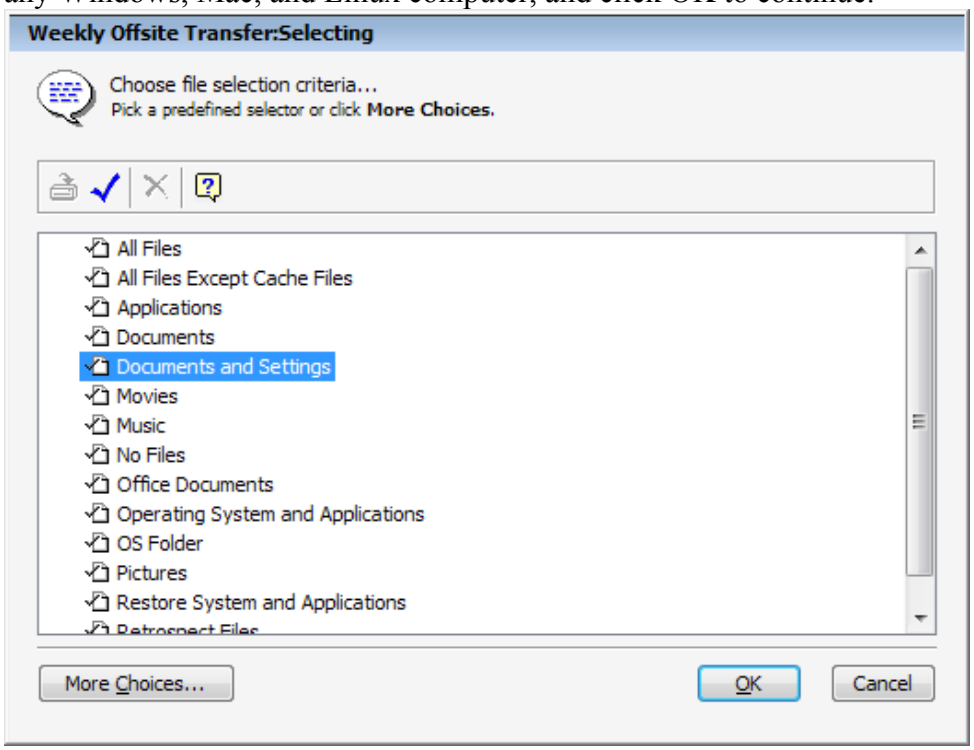
8. Go through the next few screens to configure security settings and what Retrospect should do if it runs out of space on the destination media.

9. Retrospect will ask you to select a location for the Catalog File—the database that tracks everything that gets written to this particular Backup Set. Select a location and click Next to continue.



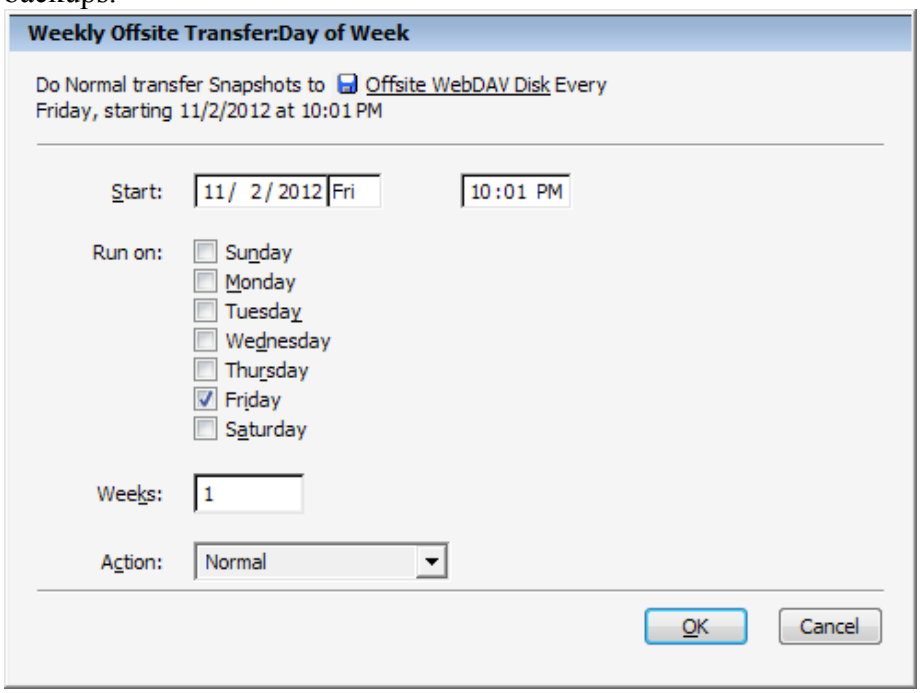
10. Once you are satisfied with your selections, the Create New Backup Set Wizard is complete. Click Finish, ensure that the Backup Set you just created is highlighted in the Backup Set Selection window and click OK to return to configuring the Transfer Snapshots script.

11. Next, click the Selecting button to choose a Selector to filter out unwanted files from the backup. The Nightly Backups script backs up all files, but for this exercise, we don't want to bother copying operating systems, applications, and things like registry data to our offsite storage, because those files eat up a lot of bandwidth. Choose Documents and Settings, which will preserve user data from any Windows, Mac, and Linux computer, and click OK to continue.



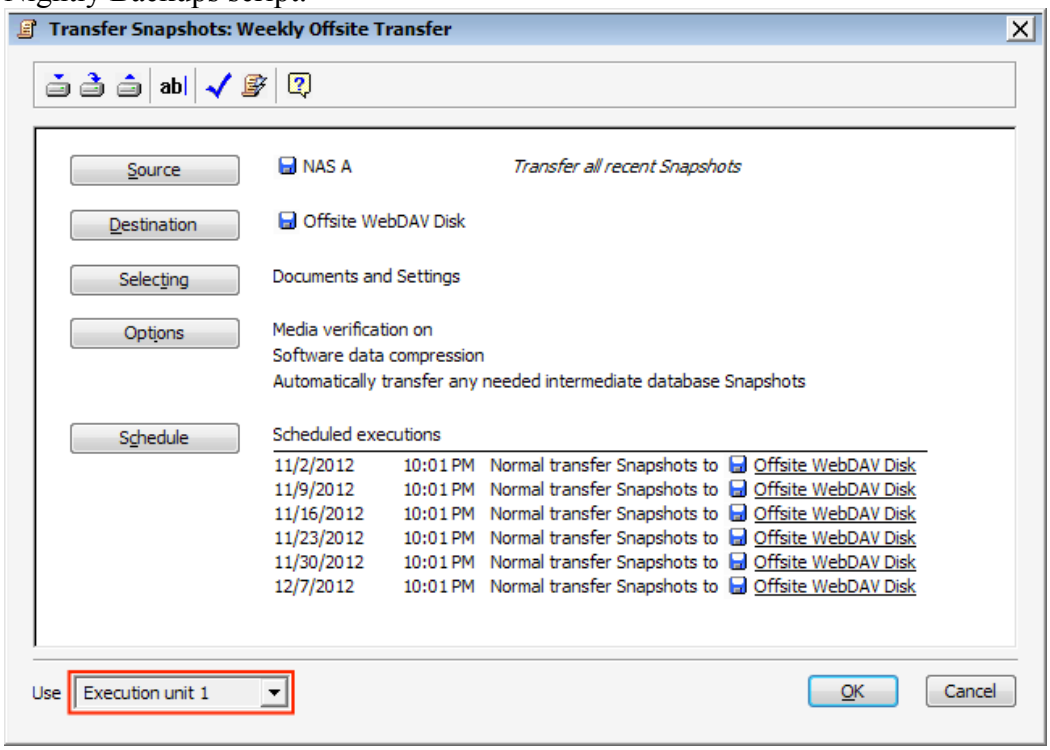
12. Click the Options button and turn on Data Compression. This will save time when Retrospect transfers data to the cloud storage. Click OK.

13. A single Retrospect script can have multiple schedules, but we only need one for this weekly transfer. Click the Schedule button and click Add. Choose a Day of Week, and configure the schedule to run on Friday nights, starting one or more minutes after our Nightly Backups script is set to run (so 10:01 PM for this example). This will allow the Weekly Offsite Transfer script to follow the nightly backups.



14. Click OK once you have the schedule to your liking, and click OK again to return to the advanced script editing window. You will see a summary of the Transfer Snapshots script settings.

15. Choose Execution unit 1 from the “Use” pop-up menu at the bottom of the window. We’re going to do the same for our Nightly Backups script in the next step, which will ensure that Weekly Offsite Transfer gets in line behind the Nightly Backups script.



16. Click OK to close the Weekly Offsite Transfer script, then double-click the Nightly Backups script in the Scripts window. Retrospect will show the advanced editing window. All we need to do here is change the Nightly Backups script to also use Execution unit 1. After you’ve done that, click OK to save.

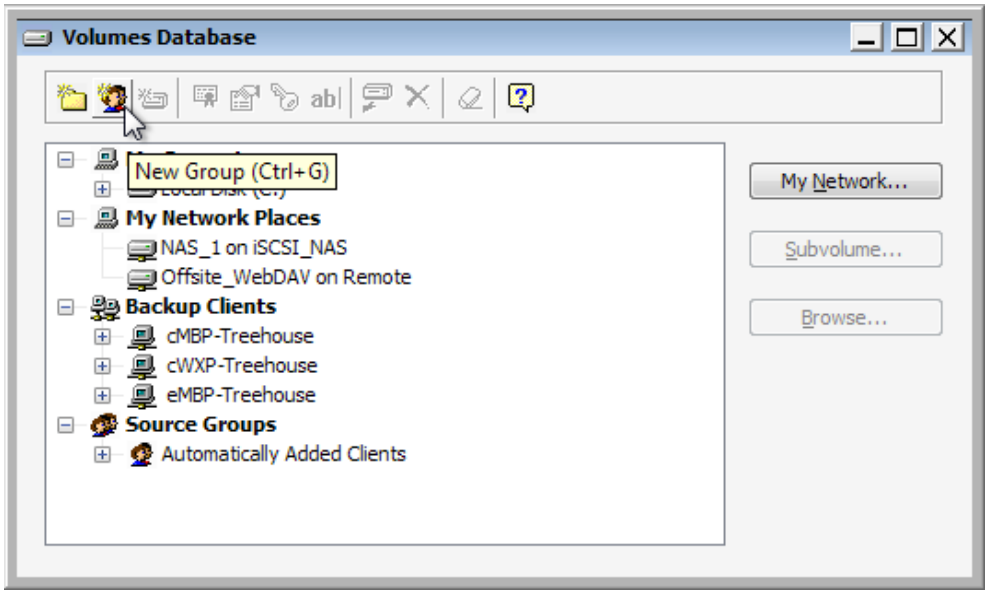
Good job! Retrospect will now back up nightly to local storage. Then on Friday, as soon as the nightly backups are done, Retrospect will transfer the latest backups to offsite storage. In this exercise, we experienced Retrospect’s wizards and advanced configuration modes. Even though the advanced modes provide an incredible amount of control, they’re easy to step through.

Using Proactive Backup to protect laptops

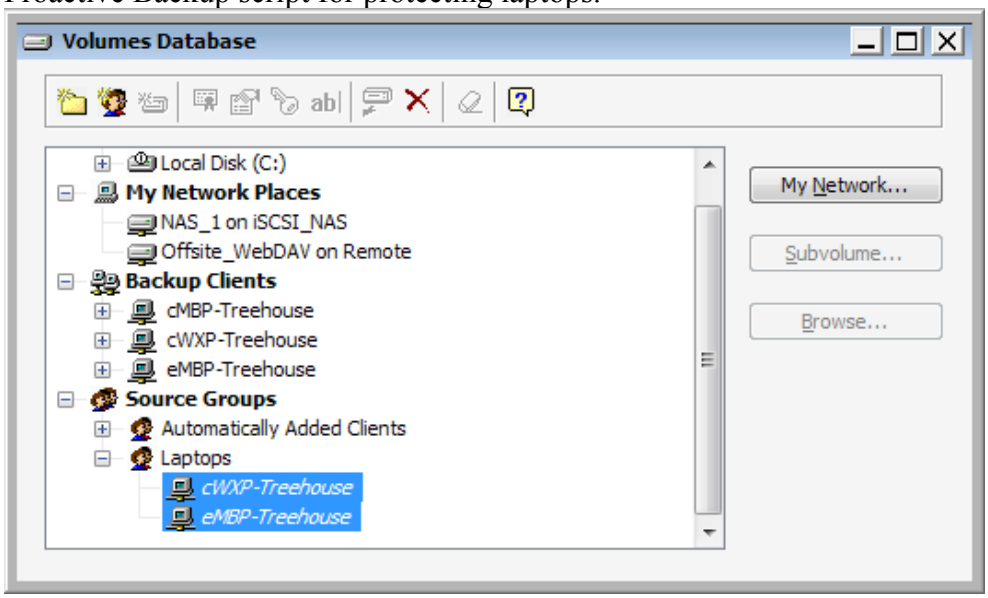
Laptops represent a particular challenge to backup administrators. They often come and go from the network, which makes it difficult to protect them on a predictable schedule. Retrospect’s answer to this problem is the **Proactive Backup** script, which uses dynamic prioritization, scheduling, and resource management to ensure that systems are effectively protected when they become available.

Part 1 – Defining the laptops

1. Click on Configure→Volumes and click the New Group button on the Volumes Database window toolbar.



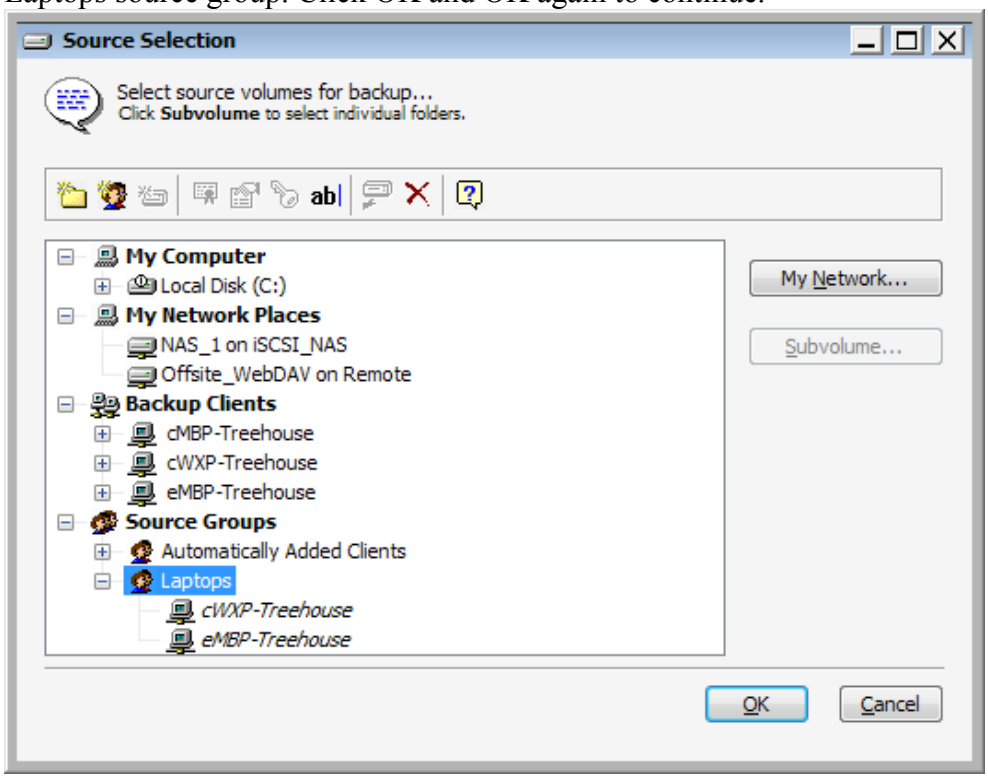
2. Name the group "Laptops" and click OK to continue.
3. Highlight one or more laptop clients that you have logged in and drag them to the Laptops group. (If you don't have any Retrospect Client systems to test with, you may define any source volume as a laptop for this exercise.) Later, any additional systems that you add to the Laptops group will be automatically added to your Proactive Backup script for protecting laptops.



4. Close the Volumes Database window.

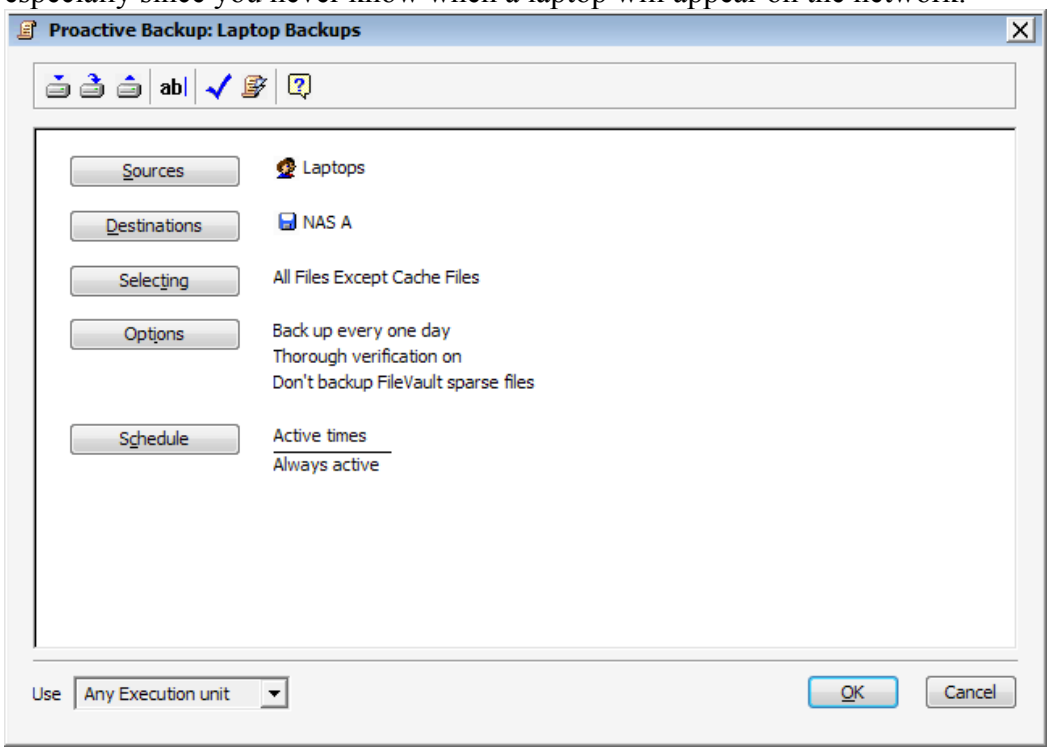
Part 2 – Create the Proactive Backup script

1. Create a Proactive Backup script by clicking Automate→Proactive Backup, clicking New, and giving the script a descriptive name (like Laptop Backup). Click OK to continue.
2. In the advanced script editing window, click the Sources button and highlight the Laptops source group. Click OK and OK again to continue.

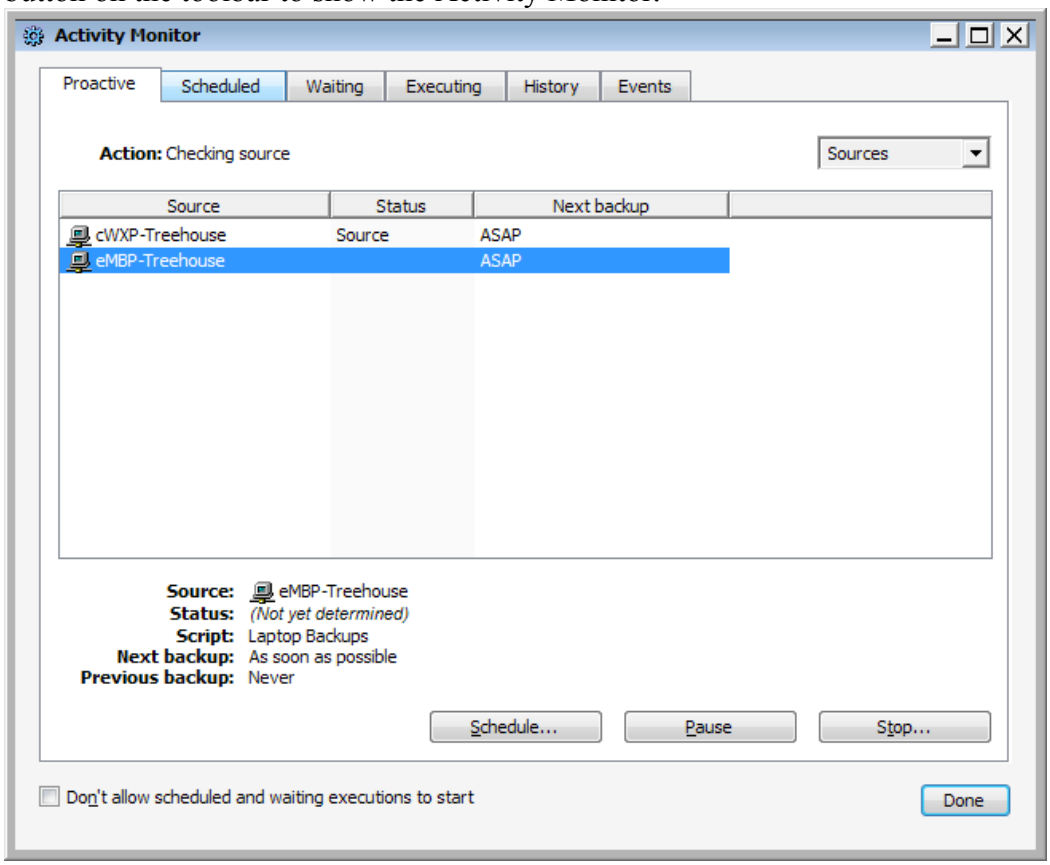


3. Click the Destinations button and select the same Backup Set that you're using for the Nightly Backups script. This will ensure that the data from the laptops also gets transferred offsite once a week, and Retrospect's file-level deduplication will only copy the files that aren't already in the Backup Set. Click OK and OK to continue.
4. Click Selecting, and select the All Files Except Cache Files rule. This is a great way to save time and storage space by not backing up files that you won't ever need to restore.

5. The default options are to back up each laptop source once a day and a schedule that looks for laptops 24 hours a day, seven days a week. That's a solid practice, especially since you never know when a laptop will appear on the network.



6. That's all there is to setting up a Proactive Backup script. When you click OK, Proactive Backup will start running automatically, which you can monitor from the Proactive tab of the Activity Monitor. Click the gear-shaped Activity Monitor button on the toolbar to show the Activity Monitor.



If multiple destinations are selected in step 3, Proactive Backup will automatically alternate between them. If one's not available, it will keep running to the available Backup Set(s). This provides flexibility to swap out the Backup Sets (e.g., to take one offsite for safekeeping and protection from fire, flood, theft) without needing to adhere to a rigid schedule.

Where to go for additional information

The Retrospect User's Guide and Retrospect User's Guide Addendum contain useful information for beginners and Retrospect veterans alike. The first two chapters of the Retrospect User's Guide cover how Retrospect works in more detail, while the Retrospect User's Guide Addendum covers the features new to version 8.

Additional resources, including user forums, a searchable knowledgebase, and support contact information, are available online at www.retrospect.com.