Realtime
publishers

Achieving Continous Data Protection with a Recycle Bin for File Servers

The Essentials Series

sponsored by

Condusiv
Technologies

Dan Sullivan

Copyright Statement

Continuous End User Data Protection

Businesses and other organizations often understand the need for continuous data protection for back office operations, such as databases and customer-facing applications, but may be less aware of the need for end user continuous data protection. If a bank loses data about a deposit or withdrawal, then balances will be off. A lost sales transaction can disrupt a customer's order. A lost change to a user authentication and authorization system could leave someone with excessive privileges to an application. These kinds of data losses are so potentially disruptive that large organizations take steps to provide continuous data protection. Should comparable measures be in place for end user data?

To answer the question about the need for continuous data protection for end user data, consider the following characteristics of end user data on file servers or network shares:

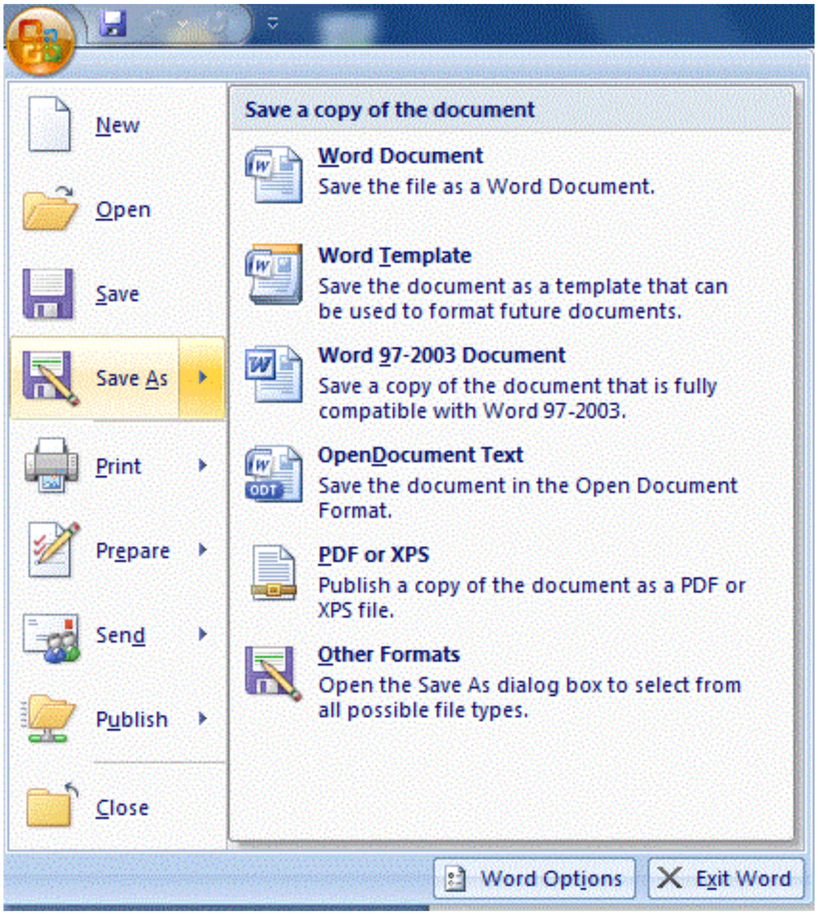
- Accidently deleting files
- Accidently overwriting files
- Maliciously deleting files
- Hardware failures and file corruption

Many of us have accidently deleted a file. Often it is not too much of a problem if we can recover the file from the Windows Recycle Bin. Unfortunately, there are a number of ways we can delete files in which they are not made recoverable by the Windows Recycle Bin.

> **Note**
>
> These recovery limitations are discussed in detail in the earlier article, "Limits of the Windows Recycle Bin: Improving File Recovery Options."

You can also delete multiple files, for example, by deleting a folder or using a wildcard in a delete command issued on the command line.

Accidents can happen within applications as well. Such is especially the case when you use "Save As" commands and accidently overwrite an existing file. For example, you might intend to save a document as one type, such as a .docx, but accidently select another type, such as .pdf, and overwrite the prior version of the file.



Save a copy of the document

Word Document
Save the file as a Word Document.

Word Template
Save the document as a template that can be used to format future documents.

Word 97-2003 Document
Save a copy of the document that is fully compatible with Word 97-2003.

OpenDocument Text
Save the document in the Open Document Format.

PDF or XPS
Publish a copy of the document as a PDF or XPS file.

Other Formats
Open the Save As dialog box to select from all possible file types.

Figure 1: The Save As command can lead to accidently overwriting existing files.

Not all file loss is accidental. Malicious attackers, from disgruntled employees to any number of targeted viruses, may delete files that appear important, randomly select files, or methodically attempt to delete all accessible files. Security measures are important to mitigate the risk of such attacks. In spite of best efforts, though, organizations can still suffer malicious attacks that lead to data loss. In such cases, it is important to have an incident response plan in place to respond to the attack. Responses should include measures to contain the damage, assess the means by which the attack was carried out, and restore operations to their pre-attack state. Continuous data protection can help mitigate the impacts of malicious attacks.

In addition to accidentally deleting files, overwriting existing files, and malicious attacks, there is the risk of hardware and software failures. Disk drives fail. Bugs in applications can corrupt data. Laptops can be dropped and broken. It is difficult to anticipate the specifics of these kinds of failures, but it is prudent to plan for them.

Limits of Backups and Snapshots

Backups and snapshots are useful for data protection but they are typically not a comprehensive solution for continuous data protection of end user files. For example, backups do not recover changes made since the last backup. Work performed between the time of the last backup and the time of file loss is not protected by the backup.

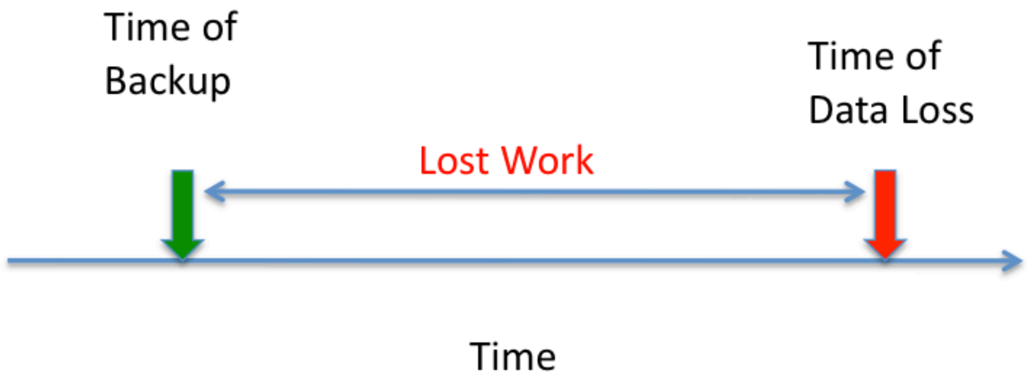


Figure 2: The work performed between the time of the last backup and the time of data loss is not protected by backups.

Snapshots can improve data protection between backups. With snapshots, copies of data on persistent storage devices are made at intervals between backups. This setup improves the RPO but does not meet the ultimate goal of continuous data protection. Further more, snapshots entail significant storage overhead. Managing snapshots and ensuring the right balance of space utilization and data protection can add to systems administrators' workloads.

State of the Art End User Continuous Data Protection

The state of the art in end user continuous data protection is based on file recovery applications that provide many key features:

- Allowing for self-service recovery of files deleted from a file server or network share. End users do not have to solicit the help of systems administrators for simple recovery operations. This setup reduces the workload on administrators and can help speed the time to recovery for end users.
- Offering the ability to capture versions of files as they are saved rather than just the last version of a file.
- Compensating for the limitations of the Windows Recycle Bin by protecting files deleted at the command line or in applications while also protecting files deleted from network file shares.
- Preserving file system security controls in the file recovery applications. Users should not have access to files in the recovery repository if they do not have access to that file in the file system.

This combination of features is a benefit to both end user and IT support staff. The former have better control over the time it takes to recover deleted files while the latter are left with more time for higher-priority issues.

Summary

It is possible to offer end users continuous data protection. At the same time, those users can gain greater control over the recovery process with the use of self-service recovery features for all local and network files. IT administrators can still maintain control over file security while reducing their overall workload when it comes to restoring files. Continuous data protection provides for better RPOs and reduces the risk of losing substantial amounts of work. The Windows Recycle Bin has worked well for some cases of deleted files but not all, especially in large environments that normally use centralized storage. Third-party tools are now available to fill those gaps.