



El Fresko's MagnaStor™: Magnetic WORM File System and Regulatory Compliance

By Jeff Ellestad, Director, Product Management

Many corporations and government departments are increasingly subject to stringent regulations that specify how information is managed, retained, and protected from unauthorized tampering, use or access. Files must be readily producible for audit or e-Discovery, and files that have been stored beyond their retention period must be deleted, including all backup images of the same file. There must be a verifiable audit trail of all changes to each file, and in some cases, the details of each access to a file. Data must be easily classified to protect unauthorized disclosure of sensitive material.

In the past, these demands were addressed using optical-based WORM (write-once read-many) storage systems in conjunction with a document or records management system. But optical WORM is expensive to support, optical vendors and media suppliers are dwindling, and there are serious limitations in capacity, performance, and retention options that make it less attractive for large-scale archives. Magnetic storage offers much higher performance and storage densities with lower costs, but these attributes must be offset with controls and mechanisms that deal with the much shorter lifetimes of magnetic drives, higher error rates, and the media's inherent erasability.

Meeting Regulatory Compliance with El Fresko's MagnaStor™ File System

MagnaStor™ is a new and unique file system that is engineered to provide a robust, trusted archiving and compliance storage system on low-cost magnetic disk technology. To achieve these goals, MagnaStor™ implements multiple, policy controlled data management layers that control all aspects of file system operations, data flow, validation, auditing, and health monitoring. Each layer refers to its associated policy to determine if a file system request is permissible before processing and passing the request to a lower layer.

Embedded File System Policy

MagnaStor™ allows the user to define the rules or policy by which the file system will govern all file system operations and data that moves to and from the file system. The MagnaStor™ policy is defined at the time the file system is created, and thereafter is permanently embedded within the file system's management layers.

The policy system also provides several tunable settings and control mechanisms, which simplify integration with existing applications that would otherwise have difficulty interacting with a strictly write-once file system. These settings control

only how the upper file system level interacts with MagnaStor™, but do not have any influence on data written to the physical media, which always obeys write-once rules. Thus if the policy permits a time period during which the file may be re-opened, modified, or deleted, MagnaStor™ will transparently record each change in its internal, perpetual metadata journal, and retain all prior records of data associated with the file. For transparency with existing applications, MagnaStor™ defaults to presenting the user or application with the most recent view of the file by reconstructing the chain of entries in the metadata journal.

Data Protection

MagnaStor™ provides the fundamental assurance of WORM operation on magnetic media, which is required to protect all file system contents from potential alteration, removal, or renaming. Storage space that is allocated to file system metadata and user data at the media level is never overwritten or deleted in MagnaStor™. Instead, each permitted operation incrementally extends the internal file system metadata journal, which serves as both an authenticated, immutable audit trail for the file system, and also as the authoritative source for constructing the view of any file or directory object at any given time.

Data Retention

MagnaStor™'s data retention policies further protect data by ensuring that files are preserved in their original state for the duration of the retention period. Files that have reached their retention period can be marked for deletion and have their associated data erased, but active contents of the file system and user data may never otherwise be altered.

Data retention policies are defined when the MagnaStor™ file system is created, and then become permanently embedded within the file system itself. If present, a global policy cannot be relaxed, overridden, or circumvented by a local policy. For example, if a global retention policy requires all files to be retained for a minimum of seven years, then a local policy defined at the directory or file level may only extend this period, never shorten it. If the corporate retention policy varies depending on the type of file being archived, then a directory level policy can be defined to address specific requirements, subject to the restrictions of the global policy. For example, if email records are to be retained for one year, and legal documents for seven years, the file system could be created with a short global retention policy (for example six months), and top level directories could then be created that specify the longer periods of one year and seven years.

Data Preservation

MagnaStor™ ensures write-once behaviour at the media level and preserves every incremental change to every file for the lifetime of the entire file system. Regardless of policy settings or file operations, all file and directory operations are permanently recorded as incremental changes at the media level. The exact state of the file system and any directory or file at any point in time can be presented for

audit, recovery, or review purposes. Each permitted file operation always results in new storage being allocated at the media level, including a new event being added to the file-system metadata journal, and new file-data blocks for each file-write operation.

MagnaStor™ includes data backup and migration tools to preserve all file system history across file system backup and restore operations, and across migrations to new storage devices. Release 2.0 will include automatic replication of MagnaStor™ file system contents to another MagnaStor repository at local or remote locations.

File Authentication and Chain of Custody

The basic foundation of compliance requires WORM semantics to be strictly obeyed and the authenticity of the file system contents to be complete and verifiable. Competitive file systems often attempt to provide WORM-like behaviour by injecting a filter driver or file system extension over top of an existing file system, such as Ntfs. While convenient and simple, such approaches result in a file system with complex structures that are subject to overwrites, and often with external dependencies for journaling or logging. In such implementations it is therefore very difficult to prove the authenticity and completeness of a file.

On the other hand, MagnaStor™ was written from an audit and compliance perspective, intended to support discovery and litigation processes with clear, provable audit trails of the entire chain of custody for each file system object. MagnaStor™'s metadata journal is not simply an add-on – it is intrinsic to the file system core. And because it is simple, chronological, and verifiable, non-IT experts can produce an easily understood audit report that can be used to quickly validate the entire lifecycle of chain of custody of any file.

File System Data Management Layers

At the media layer, strict WORM semantics are enforced that prevent the upper layers of the file system from any attempt to overwrite, change, or erase previously written media sectors. The only permitted exception is the destruction of file data that has exceeded its retention period. File system policy at the media layer is inaccessible to all higher layers and cannot be altered.

Intermediate layers are responsible for managing and authorizing the serialization of all changes and additions to the file system as it responds to user and application requests. These layers also maintain current and historical views of each file system object, as represented by the sum of the serialized metadata events associated with each object.

At the upper file system interface layer, the associated policies allow the behaviour of the MagnaStor™ file system interface to be tuned for specific user or application environments. This layer allows existing applications to operate transparently with MagnaStor™, even though the underlying (rigid) WORM semantics remain fully in force. Each file system operation permitted by the policy in effect results in an

incremental addition of an event to the file system's metadata journal. These events are assigned validation information and fingerprints, and then gathered and further encapsulated for presentation to lower file system layers.

When a file is opened for reading, the intermediate layers perform validation and authentication checks on all associated file system metadata and all user data presented to the upper layers. If a validation check fails due to an error in the underlying storage system or unauthorized tampering, the file system will report the error and determine if self-healing is enabled and possible. If so, self-healing is initiated and the file system is repaired automatically.

#

ABOUT EL FRESKO TECHNOLOGIES:

El Fresko provides proven, scalable and cost-effective data archiving solutions to protect businesses and preserve their critical data. MagnaStor™, the company's patent-pending software solution, offers certainty of data preservation and guaranteed proof of authenticity while leveraging the high performance of magnetic disk. Providing trusted solutions for more than 20 years, El Fresko's software suite includes a range of fast, simple and reliable storage archiving solutions for magnetic and optical media. Learn more at www.elfresko.com.

MEDIA CONTACT:

Christine Payne or Adam Bello
Primoris Group
+1 (416) 489-0092
media@primorisgroup.com

SALES, PRICING AND RESELLER INQUIRIES:

Kimberly Ballendine
El Fresko Technologies
+1 (403) 265-5727
kimberly@elfresko.com