

As the central component of business, data is growing by leaps and bounds and the management of ever-expanding amounts of data over time is now becoming a major challenge. A slew of regulations involving the financial industry, healthcare providers and public companies have increased the requirements for data retention, and many companies have stepped forward to create requirements that align with audit and risk management policies.

In meeting needs to retain critical data, users must also consider how to efficiently and cost-effectively use their storage capacity. Information Lifecycle Management (ILM) and tiered storage strategies have been created to address these needs, allowing companies to categorize business data according to factors including type, importance and need for retention. These strategies also require that business critical information must be stored to allow rapid access for business continuance, and that lower level data – such as e-mail and other less accessed data – can be archived for compliance and/or auditing purposes. ILM allows companies to optimize the use of storage data, moving archival data to lower cost secondary storage while keeping business critical data on primary storage. These strategies, as well as data protection and movement of archival copies to remote locations, make for a robust ILM implementation.

Select robust, enterprise class storage for primary use

As we explore implementation of an overall solution to address ILM and tiered storage requirements, we must consider the types of data that will reside in primary and secondary storage pools. Primary storage, used for daily business operation, should typically be stored on a highly available solution. In our ILM solution, we recommend RAID's Magellan storage system for primary storage use. The Magellan is an intelligent, self-contained storage system that delivers storage scalability, redundancy and data services.

Use SATA-2 for secondary storage

For the secondary storage pool, we have chosen to use RAID's SATA-2 expansion enclosures, which brings administrators a modular approach to deploying tiered storage solutions for applications that require storage with varying performance, availability and cost characteristics.

Add intelligent ILM software to manage data

To enable ILM functionality in this application, we have chosen CaminoSoft's Managed Server HSM software to provide the policy-based data movement DLM component for the solution. Managed Server HSM allows organizations to establish comprehensive administrative policies that allow companies to reclaim storage resources, dramatically reduce backup and recovery time, control file retention, and achieve regulatory compliance. CaminoSoft's server-based solution allows administrators to configure usage and policies of the virtualized storage without user interruption. Users continue to read and write files to the same servers, volumes and folders as they always have. In the background, Managed Server HSM, based on policies set by its administrators, monitors volume watermarks and dynamically compares against real-time storage utilization to make decisions about migrating files that are infrequently accessed. With this implementation, companies can automate file migration and retrieval from primary to secondary storage, gain immediate and seamless access to migrated files, and achieve full administrative control over migration activity via comprehensive policy maintenance.

Benefits

- Enables the creation of highly affordable infrastructures that deliver policy-based applications that manage and safeguard valuable data throughout its productive lifespan.
- Support ILM requirements to achieve maximum information availability and data protection, moving production files via policy to the most effective storage - regardless of location and without distance limitations.
- Allows administrators the opportunity to automate the movement of data that has not been accessed over time, to lower cost storage.
- Affordable infrastructure with policy based applications that manage and safeguard data throughout its lifecycle.