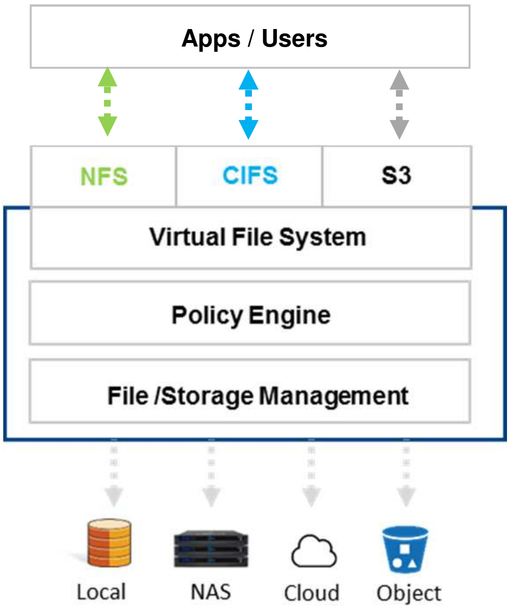
DATATRUST SOLUTIONS

Secure Archive Manager

Compliant Data Management and Archiving Software

Key Benefits

- > *Intelligent Archiving Software*
- > *WORM & Retention*
- > *Legal Hold & Disposition*
- > *Encryption and file obfuscation*
- > *Native CIFS, NFS and S3 Protocols*
- > *High Availability & Replication*
- > *Source Tiering to lower cost Target*



Software Architecture

Historically, vendors have provided an integrated solution for archiving fixed content. Storage software and storage hardware were integrated and delivered as an appliance. The challenges with this approach are:

- Most data outlives the storage system that hosts it
- Tight coupling of the file and the storage system make moving content without impacting the user difficult
- Limited size and scalability of storage systems
- High cost of upgrades
- Outages to transitioning data across disparate storage systems or technology generations

DTS developed Secure Archive Manager (SAM) software to solve data management problems for the life of the archived data. Storage hardware has been a limiting factor in archiving due to its proprietary nature, short lifespan, limited scalability and reliability factors. Our approach was to decouple the intelligent data management layer from the storage hardware. This enables storage vendor neutrality and gives the data the ability to transcend generations of storage technology.

Secure Archive Manager provides native file system interfaces for applications and users. SAM is available in NFS only, CIFS only and mixed protocol options. SAM presents users and applications with a Virtual Disk interface that is abstracted from the physical storage. The Virtual Disk interface does not use stubs, reparse points, DFS or other painful trickery. SAM is not subject to traditional limitations with file counts, directory depth, file name lengths or other challenges associated with file systems tightly coupled with an OS. This virtualization allows for the separation of the file system presentation and file management from the physical storage systems. Thus enabling SAM to present a static file system interface and allow transparent policy based movement of files across diverse storage technology, storage tiers and even across locations.

Storage Independence

Every customer has both common and unique needs so why shoe horn them into a particular storage system? SAM provides unprecedented storage options including: local storage, network attached storage, object storage, REST/cloud, and near-line options. An integrated storage manager provides support for a wide range of storage systems. It can transparently move data across devices to rebalance capacity or enable tiering or make replica copies for cloud or at other data centers.

Compliance

Secure Archive Manager was developed to help customers in regulated industries adhere to their retention, reporting and compliance requirements like SEC17a-4. The integrated Policy Engine enables administrative configuration options for WORM, Retention and non-WORM Archives. Legal hold and user activity logging further extend compliance features.

Encryption, Obfuscation

Security of archived content has been brought to the forefront with recent Ransomware attacks. SAM Archives can be configured to enable file encryption and versioning. Each file is independently encrypted with a unique key. With Versioning a copy of an archived file is kept even and can be recovered from even if it was maliciously encrypted. For additional security files can be obfuscated when written to any storage system by converting the file name and path to a Globally Unique ID (GUID).

High Availability / Replication

Access to data is paramount is the global 24x7 operations and SAM is available in multiple different configuration options to provide continuous access. SAM uses Storage Groups to make immediate 2nd copy on ingest. SAM also provides asynchronous replication options where the source and target can be different storage types. (e.g. local storage and cloud storage).

Tiering

SAM provides a tiering feature that allows files to be pulled into SAM and archived to a lower cost target. Files are copied from a high cost source to a lower cost target. Hashes are used to verify the copy and then the source is replaced with a symbolic link. Re-hydration is not required to read the file or to make changes to a file.

Filters

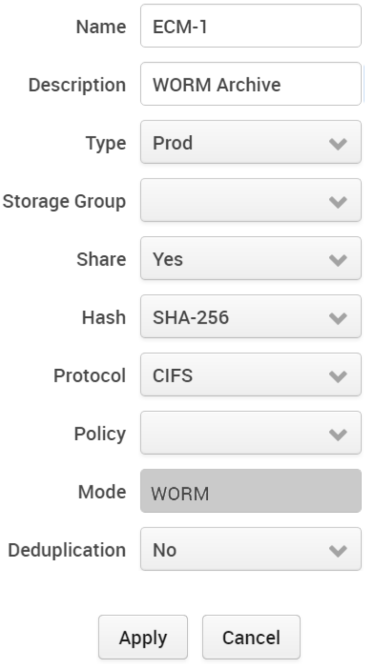
Not all data is equal and subject to the same requirements for retention and immutability. SAM uses Policy based filters for including or excluding files from WORM or Retention requirements. Filtering helps reduce capacity requirements and legal risk from keeping unneeded data.

S3 Front-End

Today most applications only support legacy file system interfaces like CIFS and NFS, thus they need a gateway to take advantage of cloud or object storage. However, in the future these applications may support the S3 interface. When this time comes SAM can update the application's pointers to use S3 and be removed from the environment or continue to operate as is.

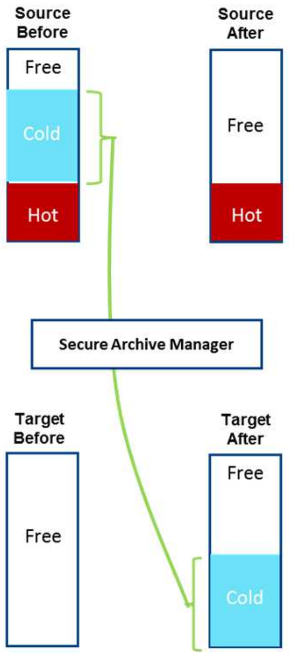
For more information please contact us at:
+1 720-502-1030
info@DataTrustSolutions.com.

Archive Policy Options



Name	ECM-1
Description	WORM Archive
Type	Prod
Storage Group	
Share	Yes
Hash	SHA-256
Protocol	CIFS
Policy	
Mode	WORM
Deduplication	No

Tiering



Requirements

SAM can operate in virtual or physical environments. OS requirements are protocol dependent. Windows Server 2016 is required for CIFS and Debian is used for NFS. CPU, RAM, Disk requirements are determined by archive scale. Minimum configurations are: 4 core hyper-threading CPU, 8GB RAM and 200GB local disk for Linux VM and twice the CPU and memory for Windows.