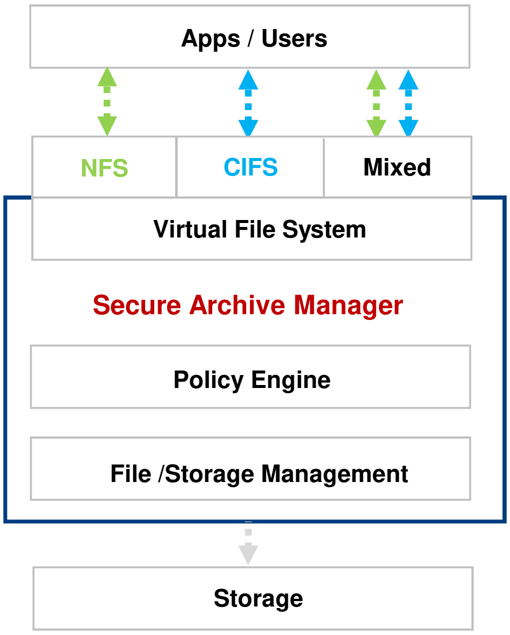
Secure and Compliant File System Archiving

Secure Archive Manager

Key Benefits

- *Intelligent Archiving Software*
- *WORM & Retention*
- *Legal Hold & User Audit Logs*
- *Encryption and file obfuscation*
- *Native NFS, CIFS and Mixed Mode*
- *High Availability & Replication*
- *Read and Write Verification*
- *Integrated data movers*



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 a 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. Thus 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, near-line and off-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. 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 encryption thus preventing access to file contents. Each file is independently encrypted with a unique key. 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). Additionally SAM is locked down and will only run a limited command set.

Trust

SAM provides optional write verification to ensure the content was committed to the archive was identical to the content it received. The read verification option uses hashes to verify that each requested file return the same hash value stored with the original file. This eliminates the possibility of bit rot or backend file contamination.

High Availability / Replication

Access to data is paramount is the global 24x7 operations and SAM is available in Active-Active, Active-Passive and cluster configurations . SAM offers replication options and does not require homogeneous hardware at primary or DR sites.

Filters

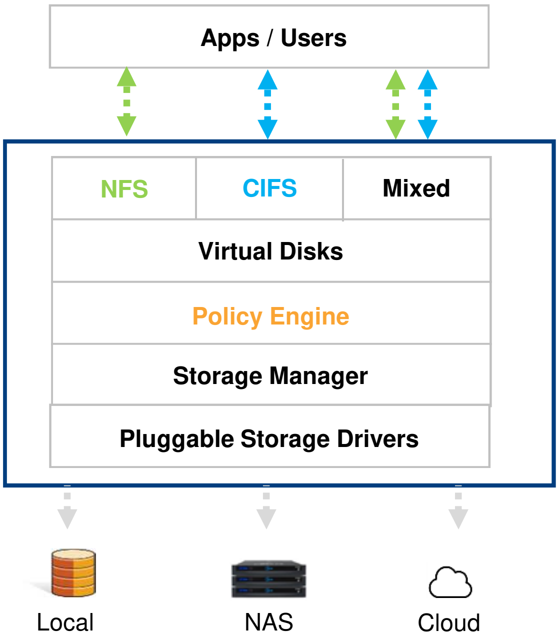
Not all data is equal and subject to the same requirements for retention and immutability. SAM uses Policy based filters for including or excluding files from WORM or Retention requirements. Filtering helps reduce capacity requirements and legal risk from keeping unneeded data.

Data Mover

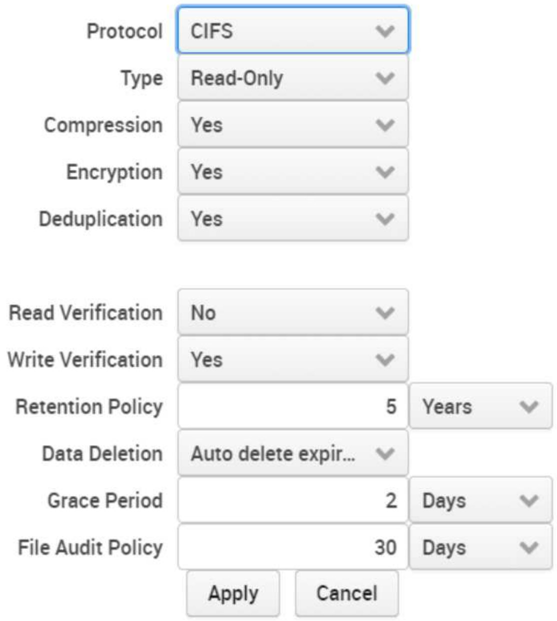
Need to move data from your legacy archive into SAM? SAM includes an integrated data mover from our ShadowFS file migration software. Files can be inventoried, filtered, copied and verified. Chain-of-Custody Reports are generated to prove the content copied to SAM is identical to the original source content. Need to move SAM content from one backend storage system to another, no problem with the integrated data mover technology.

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

Secure Archive Manager



Archive Policy Options



Protocol	CIFS	
Type	Read-Only	
Compression	Yes	
Encryption	Yes	
Deduplication	Yes	
Read Verification	No	
Write Verification	Yes	
Retention Policy	5	Years
Data Deletion	Auto delete expir...	
Grace Period	2	Days
File Audit Policy	30	Days

Requirements

SAM can operate in virtual (KVM or VM) or physical environments. OS requirements are protocol dependent. Windows Server 2012 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.