Overview

EVault's Long-Term Storage Service (LTS2) is positioned as long-term bit-preservation storage leveraging disk-based storage architecture to provide immediate access capabilities, eliminating the wait time of similar services like Amazon Glacier. **LTS2 is built on the open-source OpenStack Swift storage system, helping to mitigate concerns regarding vendor lock-in.** EVault storage can be integrated with existing applications via OpenStack Swift and Amazon S3 APIs. EVault emphasizes a focus on preservation functionality and storage, providing regular fixity checking, actively managed hardware replacement and migration, transparent logging of data management events, and robust auditable logging of metadata.

Long-Term Storage Service (LTS2)

SERVICE PROVIDER: EVault

WEBSITE: lts2.evault.com

PRODUCT RELEASED: 2013

COMPLIANCE: HIPAA-HITECH; SSAE 16; SOC1

SERVICE: Deep storage, Production

INFRASTRUCTURE: Wholly owned

COST: Low

Data Management

Assets may be delivered to EVault via a web-based UI, client-side applications, or web services using EVault's API. A bulk ingest service is also available at additional cost; requiring shipment of LTFS formatted LTO tapes to EVault. The EVault storage system runs ongoing fixity checks on data object chunks, validating MD5 checksums monthly. Clients may also provide checksums upon ingest, which are validated on the same schedule. Fixity check failures are automatically restored from one of the two redundant stores at EVault's data center.

Reporting / Metadata

EVault offers auditable tracking of events in CSV the data center, including data integrity checks, self-healing, and access occurrences via the service's web portal. Metadata management capabilities are referred to in EVault literature, but details on these features were not available at the time of drafting this profile.

Redundancy

EVault currently supports one data center outside Salt Lake City and does not offer geographic dispersal in its service. While they do replicate data three times within the data center to ensure redundancy in case of technology failure, materials are at risk in disaster scenarios. **True locational redundancy at a minimum of two locations was reported to be on the product's roadmap at the time of this writing.**

Accessibility

EVault estimates a **first byte latency of less than 5 seconds and allows retrieval of 5% of average data store for free per month.** Two web-based clients are available for administrative—user account management and organization of data containers and files—and object-level management within the EVault storage system. The service also supports multiple methods of interaction and access via third-party client tools (Cloudberry Explorer, Cyberduck, and ExPanDrive), cloud computing gateways, or command line interfaces via the OpenStack Swift and Amazon S3 APIs. Create, read, update, and delete functions can be implemented and integrated through any of these integration points. EVault allows 50 read/copy API requests per GB of data stored each month at no additional cost.

Security

EVault uses HTTPS and encrypted streams for transfer of data in and out of the service. **Clients may enforce their own encryption methods for security prior to submission**, but it is the responsibility of the client to manage the decryption process. LTS2 uses Access Control Lists (ACLs) to manage user access to data, which specify read and write capabilities permissible to users. The user authentication process acts as a security layer, confirming user identification prior to submitting commands to the EVault data center.

End of Service

EVault provides a 60-day window for retrieval of data following the end of service or termination of the service agreement. **A premium "data survivorship" service is available for an additional $.002/GB per month ensuring ongoing services for up to six months or the completion of a bulk export in the event of service termination.** Clients may elect a bulk export via tape or transfer over WAN or direct connection at additional cost. **The service charges an early removal fee of $.03/GB for any object removed or deleted within 90 days of upload to the data center.**

Levels of Preservation

	Level 1 (Protect)	Level 2 (Know)	Level 3 (Monitor)	Level 4 (Repair)
Storage	• **Two complete copies that are not collocated**	• **At least three complete copies** • At least one copy in a different geographic location	• At least one copy in a geographic location with a different disaster threat • **Obsolescence monitoring for storage system(s)**	• At least three copies in geographic locations with different disaster threats
Data Integrity	• **Check file fixity on ingest if it has been provided with content** • **Create fixity info if it wasn't provided with the content**	• **Check fixity on all ingests** • Virus-check high risk content	• **Check fixity of content at fixed intervals** • **Maintain logs of fixity info; supply audit on demand** • **Ability to detect corrupt data** • Virus-check all content	• **Check fixity of all content in response to specific events or activities** • **Ability to replace/ repair corrupted data** • **Ensure no one person has write access to all copies**
Security	• **Identify who has read, write, move, and delete authorization to individual files** • **Restrict who has those authorization to individual files**	• **Document access restrictions for contents**	• **Maintain logs of who performed what actions on files, including deletions and preservation actions**	• **Perform audit of logs**

Have more questions? We can help.
Contact AVPreserve at info@avpreserve.com