Overview

Oracle's Cloud Services provide multiple cloud-based enterprise options built on Oracle cloud infrastructure. **Oracle Storage Cloud is comprised of two classes of storage: Standard (also referred to as "Object") and Archive. This profile focuses on Standard storage service**, which provides low latency, scalable, and redundant object-based storage in Oracle-managed and secured locations. A selling point of Oracle's Storage Cloud is their security, which Oracle states is their primary design consideration. For Standard storage, the first TB of storage costs $.24 / GB.

Oracle Storage Cloud Services

SERVICE PROVIDER: Oracle
WEBSITE: https://cloud.oracle.com/storage
PRODUCT RELEASED: Unknown
COMPLIANCE: HIPAA; FISMA; ISO/IEC 27001:2013
SERVICE: Production
INFRASTRUCTURE: Wholly owned
COST: Low

Data Management

Oracle's Storage Cloud Standard class provides low latency, geographically redundant (two locations) storage. The service is managed, monitored, and files can be uploaded and downloaded via several methods, including utilities on a user's command line interface (CLI), APIs, Oracle's web console, and a client-side Java application. Limited monitoring is available through a central Oracle Cloud Customer Portal (see below). Objects exceeding 5 GB cannot be uploaded to the Cloud Services without being segmented by users prior to upload. Objects are created within a container. A container is a user-created resource, which can hold an unlimited number of objects, unless a quota is specified for the container. Containers cannot be nested. The integrity of an upload can be checked against a user-created MD5 checksum through the CLI and API. Periodic data integrity checks with self healing are performed (although the frequency is unknown).

Reporting / Metadata

Storage monitoring can be performed via the methods listed above. Users and roles, and some storage metrics (e.g., incidents, up-time, and outages), can also be managed and monitored via the Oracle Cloud Customer Portal. **Some metadata about up-time, numbers, names, and sizes of containers and objects, and upload and download events is available; user-defined descriptive metadata can be assigned at the container and object levels.** User-defined metadata is submitted as key-value pairs. An MD5 checksum is maintained for all objects under 5 GB. For files larger than that, a single MD5 checksum is created that represents the concatenated file segments and their individual MD5 checksums.

Redundancy

Storage is replicated across nodes within a physical storage location (a minimum of three times). **Geographic distribution is built into the Standard storage—files are stored in two geographically distinct locations.** Periodic data integrity checks with self healing are performed, although detailed information about these checks is not available.

Accessibility

For outbound data transfer, the first GB per month is free. Thereafter, as the number of GB increases, the cost decreases. Bulk inbound transfer using physical storage is an option.

Security

Oracle does not automatically encrypt content on ingest. **If encryption is desired, customers can use the client-side encryption features of the software appliance and Java library to encrypt every**

object with a unique symmetric key before uploading and storing the object in the cloud service. Customers are responsible for maintaining the encryption key—if the key is lost, data cannot be retrieved. Additional optional encryption at the data center allows for increased security. Service administrators can restrict access to data by assigning read and write permissions to containers.

End of Service

Oracle's service agreement states that for a period of no less than 60 days after the termination of services, they will make a customer's content available for retrieval. At the end of 60 days, they will delete or otherwise make the content inaccessible. Planning in advance to reduce costs for migration is recommended.

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)**[1]	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 authorizations 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

[1] While this activity could not be confirmed, it is likely this is a part of general maintenance of the storage system.