

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 the Archive storage service,** which provides scalable, redundant, dark storage within a single physical storage environment. A selling point of Oracle's Storage Cloud is their security, which Oracle states is their primary design consideration. Archive storage costs \$.001 / GB no matter the amount of storage, although there are costs for retrieval and data transfer.

Data Management

Data can be stored to Standard and Archive classes on Oracle's Storage Cloud to create a tiered storage environment. **The Archive provides deep storage for infrequently accessed content that requires long-term retention.** Geographical redundancy is available for an extra fee. The service is managed, monitored, and files 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. 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). **Oracle claims 11 9s (99.999999999%) data durability for Archive storage by maintaining multiple copies of each object on different devices.** Periodic data integrity checks with self healing are performed, although detailed information about these checks is not available. Stored data is never moved out of designated geographic regions (unless redundancy is selected as an option for added cost).

Accessibility

To access data stored in the Archive service, it must be "retrieved" from storage, which can take several hours. Once retrieved, it can be transferred out of the Storage Service. There is a base price per GB for data retrieval (\$.001 / GB), no matter the number of GB. For outbound transfers, the first GB per month is free. Thereafter, 1 GB to 9.99 TB is \$.12 / GB, 10 TB to 49 TB is \$.024 / GB, etc.).

Oracle Storage Cloud Services

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

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. Especially if stored in Archive storage service, which has significant cost implications associated with retrieval and data transfer, **it is extremely advantageous to plan far in advance in order to dramatically reduce costs in the instance of migration.**

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.