Overview

Rackspace is a cloud computing and storage vendor that emphasizes open source solutions, providing multiple cloud-based services built on the open-source OpenStack cloud infrastructure. Cloud Files, the service highlighted in this profile, provides scalable object storage optimized for low-latency, high bandwidth distribution. It utilizes Akamai's content delivery network to provide high availability access to files in storage. **It is best utilized for access scenarios and should not be considered for long-term preservation of digital materials.** Other services offered by Rackspace support long-term, backup or disaster recovery use cases, and will be evaluated in a future profile.

Cloud Files

SERVICE PROVIDER: Rackspace

WEBSITE: www.rackspace.com

PRODUCT RELEASED: 2008

COMPLIANCE: SSAE16, ISO 27001

SERVICE: Production, streaming

INFRASTRUCTURE: Wholly owned

COST: Medium

Data Management

Rackspace's web interface allows customers to manage, monitor, and upload files to the cloud. **Files exceeding 5GB cannot be added to the storage through the web portal** and will require segmenting by users prior to upload to the web portal. Users may also use the Rackspace APIs or FTP applications (such as FireUploader or CyberDuck) to upload and manage objects. Rackspace's API allows users to provide an MD5 checksum in a submission manifest together with the objects size. The checksum and object size are verified on ingest, with the system indicating success or failure via the API response. Other submission mechanisms do not support checksum validation and the available documentation does not reference ongoing data integrity monitoring. Files are stored in user-defined containers: top-level compartments that store up to about one million objects before encountering performance issues. Rackspace does not compress or encrypt files in its data centers.

Reporting / Metadata

Service and storage monitoring via the web-based control panel is not robust, but metadata that is helpful in this regard may be retrieved using the Cloud Files API. Retrievable **metadata includes item-level metadata submitted as key-value pairs, container metadata—file manifests, container size, and number of files—and logs containing records of access requests for data in storage.**

Redundancy

Three redundant copies of all data uploaded to Cloud Files are stored in one of Rackspace's six international zones selected by the user. Rackspace claims its infrastructure is designed to withstand any disruption in the data centers within a zone and guarantees 100% network uptime.

Accessibility

Cloud Files utilizes Akamai's content delivery network (CDN) for high-speed delivery of files from Rackspace data centers to end-users. The monthly cost of this service is based on the scale of your bandwidth needs, which decreases as use increases. **Akamai's CDN does not support transmission of files larger than 10GB.**

Security

ACloud Files does not currently support encryption and decryption of files stored in its service. Clients may upload encrypted data, but must manage its own keys for client-side decryption. All traffic between the client and Cloud Files utilize Secure Sockets Layer (SSL) protocols to help ensure data is not intercepted during transfers. User permissions cannot be configured through the web interface and will require technical expertise to manage properly. Role-based permissions are managed through an API and specify the authorized activities of users, including create, read, update, and/or delete.

End of Service

Service Agreements for Cloud Files and General Terms for Rackspace services do not specify an exit path or retention period in cases where Rackspace or the user terminates the service. According to Rackspace representatives, data is removed from Rackspace upon termination of an agreement between users and the service provider. Data may be retrieved prior to termination by developing custom processes with the Rackspace API.

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 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**

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