

Service certificate

STACKIT

Object Storage

Version and start of validity

Version 1.2	Valid from 2026-03-26
-------------	-----------------------

Service certificate | STACKIT Object Storage

Service name

STACKIT Object Storage

High level service description

The STACKIT Object Storage Service (“Object Storage”) provides customers with a means of object-based data storage using an S3-compatible protocol. Object Storage supports scalable data storage for various use cases such as websites, mobile applications, backup and recovery, archiving, and IoT. Object Storage is provided to customers in the form of storage units (buckets). These buckets can be deployed, used, scaled, and deleted separately from each other. Data are stored redundantly across multiple Availability Zones.

Key features

- Easy and secure access: Access control for buckets as well as access via encrypted HTTPS connection
- Scalable object-based data storage to support multiple use cases
- Demand-based creation of new buckets for storing data
- Flexible storage and deletion of files in the storage environment
- High availability through redundancy: Data storage across multiple Availability Zones
- Optionally available Object Lock (Compliance Mode) for immutability of data for a period defined by the customer (limited to a maximum period defined by STACKIT)

Service plans

-

Metrics

Billing per hour or part thereof per gigabyte or part thereof.

SLA specifics

- Availability is defined as the percentage of time the system remains operational and data in the system can be accessed. This does not include customer configurations or other customer-related properties for unavailability.
 - The Availability of the Object Storage is 99.9% on a calendar month average.
- Durability is defined as the ability of the Object Storage to ensure that stored data remains intact and protected against unintended, system-induced data corruption over time, while strictly adhering to data integrity standards. Durability is calculated based on the probability of data loss, i. e. an error event in the system that can lead to data corruption or permanent loss of data access.
 - The durability of the Object Storage is 99.999999999% (11 Nines) on a calendar month average.

Backup

Backup and restoring of the Object Storage are the responsibility of the customer and are not included in the service.

Additional terms

- The creation and recovery of backups are the responsibility of the customer.
- The customer is responsible for the settings on their bucket (especially the setting and granting of access rights).

Additional terms Object Lock (= Compliance Mode)

- An Object Lock set by the customer (compliance mode) is not elastic or scalable; the data stored in the Object Storage concerned cannot be changed. During the period selected by the customer when configuring the Object Lock ("**Object Lock Period**"), the Object Lock applies until the Object Lock period expires:
 - Content in STACKIT Object Storage for which the Object Lock has been activated cannot be deleted for the duration of the Object Lock Period, even if the subscription is terminated - for whatever reason. The agreement on the deletion of Customer Data pursuant to Section 7 of the

STACKIT Cloud Terms of Use shall apply with the proviso that the deletion of the Customer Data affected by the Object Lock within the Object Storage shall take place at the earliest at the end of the Object Lock period, unless a later date is agreed with the Customer. **The Customer is expressly informed and accepts that for technical reasons it is not possible for STACKIT to delete the Object Storage affected by the Object Lock before the Object Lock period expires**

- The Object Lock cannot be deactivated or removed during the Object Lock period
- The minimum contract term of the underlying STACKIT Object Storage is automatically extended to the duration of the associated Object Lock period selected by the Customer, i.e. ordinary termination of the subscribed Object Storage, which has been provided with an Object Lock by the Customer, is possible at the earliest at the end of the longest Object Lock period relating to the respective Object Storage, contrary to Sections 5.2 and 5.3 of the STACKIT Cloud Terms of Use.
- In the event of a premature termination of the respective subscription before the end of the Object Lock period (in particular by effective extraordinary termination of the contract), the Customer agrees that the data will continue to be stored until at least the end of the Object Lock period and will be deleted by STACKIT no later than 30 days after the end of the Object Lock period. Access by the customer to the data affected by the object lock is possible for a maximum of 30 further days from the time of termination of the subscription.

Annex | Exportability

(Online Register)

Data Type	Description	Exportable (Yes/No)	Format	Additional notes
Customer data	Data stored by the customer on the STACKIT Object Storage (incl. Metadata)	Yes	various, depending on the customer data	Customer data can be stored on or exported from the STACKIT Object Storage via the S3 protocol. This usually requires an S3-compatible client.
User Accounts & Permissions	Useraccounts (Access- und Secretkey)	Yes	JSON / Text	The credentials can be accessed via API or STACKIT portal.
	Permissions (within the Object Storage, e.g. Bucket Policies)	Yes	JSON / Text	The bucket policies can be saved and exported using the S3 protocol. This usually requires an S3-compatible client.
	Access to STACKIT project	Yes	JSON / Text	General access to the STACKIT project can be seen in the "IAM and Management" section in the STACKIT Portal.
System Metrics (Instances / Resources in Use)	Sizes and Capacities, e.g. the used Object Storage space	Yes	JSON / Text	The current Object Storage space usage can be read out via the S3 protocol. Limits are published in the STACKIT documentation. This usually requires an S3-compatible client.

System properties (Instances / Resources in use)	Versions and information necessary to check compatibility	Yes	JSON / Text	Functionality can be validated via S3 protocol. In addition, compatibilities are stored in the STACKIT documentation. This usually requires an S3-compatible client.
Product / service-related data (product properties)	Configuration data and source code	No. Company confidential STACKIT.	-	-
	Log Data (non personalized and personalized) <i>System-status, technical events, etc.</i>	No. Company confidential STACKIT.		-
	Log Data (non personalized and personalized) of the STACKIT Object Storage Management API <i>Login/Logout of User, User activities</i>	Yes	JSON / Text	All API-Calls to STACKIT Object Storage Management API via STACKIT Audit Log.
	Log Data (non personalized and personalized) of the STACKIT Object Storage API <i>Login/Logout of User, User activities</i>	No. Company confidential STACKIT.	-	-