NUBE4 OBJECT STORAGE · DATA SHEET

NOS
Nube4 Object Storage

S3-compatible object storage, dedicated and managed by Nube4

A platform exclusive to each customer, on their own domain, with a web console in English and Spanish. It is installed on Nube4's infrastructure or in the customer's data center, and Nube4 operates it in both cases.

S3 API compatible with the tools you already use	**From 20 TB** of dedicated capacity, expandable	**175 of 175** automated compatibility tests passed	**1 customer** per platform: never shared

SERVICE MODEL

Service type	Amazon S3-compatible object storage, dedicated to a single customer and managed by Nube4.
Isolation	A platform exclusive to each customer: their own disks, storage engine, database and console. Never shared with other customers.
Where it runs	– On Nube4's infrastructure. – In the customer's data center, on their hardware and disks.
Management	Nube4 installs, updates, backs up and monitors the platform in both models. Updates are built and tested at Nube4 before being applied.
Capacity	From 20 TB of dedicated disks, with redundancy. Expanded by adding disks, without migrating data or changing buckets, keys or domain.
Domain	The customer's: the API at **s3.<domain>** and the console on the name they choose. Automatic TLS certificates (Let's Encrypt), renewed automatically.
Commercial model	By contracted capacity. No charge per request, outbound traffic, user, or number of buckets or keys.

S3-COMPATIBLE API

Protocol	Amazon S3 API over HTTPS, AWS Signature V4 signing. Path-style addressing: https://s3.<domain>/<bucket>/<object>.
Objects	Upload, download, query and delete; range reads (Range); copy, including onto itself to change metadata; multi-object delete; custom metadata; object and bucket tags. Supports keys with spaces, accents, ñ and emoji.
Listings	Paginated ListObjects v1 and v2, with delimiter (folders) and prefix. Version listing.
Multipart upload	Complete: initiate, upload parts, copy parts, list parts and uploads in progress, complete and abort. Tested with 5.2 GB objects, intact.
Presigned URLs	GET and PUT, including the parts of a multipart upload. Expired ones are rejected.
Integrity	Checksums from current SDKs (CRC32 and SHA-256), verified on write and on read.
Versioning	Per bucket: versions, delete markers, recovering previous versions and suspending versioning.

Object Lock	Date-based retention in GOVERNANCE or COMPLIANCE mode and legal hold (WORM). A locked object can't be deleted or overwritten until it expires.
Lifecycle	Rules by prefix: expiration of objects, noncurrent versions and incomplete multipart uploads. Does not include transitions to other storage classes.
Bucket policy	Private, public read (objects can be read, not listed or written) or a hand-written policy, with source IP conditions.
CORS	Per-bucket rules: origins, methods, headers and preflight cache time.
Quota	Optional space quota per bucket.
Tested tools	AWS CLI 2.37, rclone 1.75, restic 0.19 and the AWS SDKs for Java (v2) and Python (boto3), with no special tweaks. Applications that use Amazon S3 or MinIO today only change the endpoint and the keys.

IDENTITIES, KEYS AND PERMISSIONS

S3 identities	One identity per application or system (backups, document management, in-house application…), with no limit on identities.
Access keys	– Several per identity, with an optional description and expiration. – Enabled, disabled or revoked instantly. – The secret is shown only once and is never stored in the console. – Downloaded ready to use: .env, rclone.conf or AWS credentials.
Permissions	Read, write, read and write, or administration, on a whole bucket or a prefix (folder). The console shows the resulting policy.
Allowed IPs	Optional per identity: its keys only work from the specified IPs or CIDR ranges (IPv4 and IPv6), evaluated against the client's real IP.
Bucket prefix	All buckets carry the customer's prefix, set at installation. A key can't create buckets outside it.
Tested isolation	Automated suite of 43 tests: each key only sees and touches what is its own, doesn't create buckets outside the prefix, can't create other keys or change quotas, and stops working when revoked.

WEB CONSOLE

Access	Web browser, interface in English and Spanish, on the customer's domain.
Roles	– **Administrator:** everything, including users, identities and bucket configuration. – **Editor:** uses the explorer (upload, delete, folders, share, tags, restore versions) without configuring buckets. – **Read only:** views and downloads. – Editors and readers can be limited to certain buckets: they don't see the others, the identities or the platform's capacity.
Authentication	Username and password (at least 12 characters, stored with bcrypt) and optional TOTP two-step verification, compatible with any authenticator app. Temporary lockout after 5 failed attempts per user and IP (30 per IP) in 15 minutes. 8-hour sessions.
Corporate sign-in	Integration with the company's identity provider through Axeso, per project.
Buckets	Create (with the prefix), versioning, Object Lock, lifecycle, CORS, policy and quota. Deletion of non-empty buckets as a background task, with confirmation.

Object explorer	– Browse folders with filtering and sorting; upload files and whole folders by drag and drop. – Large uploads in parts (16 MiB, adjustable up to 9,000 parts) that resume after a network drop or a page reload. – Preview of images, PDF, text, audio and video. – Sharing links from 1 minute to 7 days. – Versions: show and recover deleted items, view a folder as it was on a date, and restore. – Retention and legal hold (administrators only). – Data travels directly between the browser and S3 over signed URLs; it doesn't go through the console's server.
Capacity and usage	Space used versus contracted, forecast of days until full, and daily charts per bucket (space, objects, requests and traffic), exportable to CSV.
Alerts	By email and in the console: capacity at 80, 90 and 95%, read-only volumes and low allocation space in the engine.
Audit	A record of every change and every shared link: who, what, when and from which IP, including the actions of Nube4's operator.
Reconciliation	Detects differences between the console and the engine (for example, buckets created directly through the API) and shows them; it never deletes anything on its own.

PLATFORM SECURITY

Exposure	Only ports 80 and 443. All other components live on an internal network and are never published.
Encryption in transit	HTTPS with automatic TLS certificates and security headers (HSTS, nosniff, framing protection).
Key management	Identity and key management isn't exposed to the Internet: only the console does it.
Client's real IP	The platform uses the connecting client's real IP for IP restrictions and for the audit log; forged headers are ignored.
Secrets	Key secrets aren't stored in the console or in the logs. Two-step verification seeds are stored encrypted (AES-GCM).

DATA PROTECTION AND BACKUPS

Redundancy	Data disks have redundancy at the storage layer: mirror or RAIDZ2 with ZFS, or the customer's RAID. A disk failure loses no data.
Immutability	Versioning and Object Lock for backups that can't be deleted or encrypted, not even with the application's credentials.
Platform backup	Daily: the console's database, the storage index (which object is on which disk, identities and policies) and encrypted configuration. Kept for 14 days, and the platform is restored from them.
Write durability	Restarting each engine component with writes in progress lost no confirmed writes.
Second copy	Replicating the data to another site is planned with the customer, as a separate service.

Specifications current as of October 2026; they may change with new versions. Capacities and prices are quoted per project.