



PRIVATE CLOUD COLLABORATION

Nebulas Managed Nextcloud

Your Nextcloud workspace. Professionally managed. Built on AWS enterprise cloud infrastructure.

Data control and collaboration without adding another platform for your team to operate.

Collaboration needs control. Operations need an owner.

Nextcloud can bring files, sharing, calendars, contacts and collaboration into one private environment. The value appears when the architecture, identities, updates, backups and daily operations work as one service.

Nebulas designs, migrates and operates that complete environment. Your team keeps visibility and decision-making power while a named provider manages the work that keeps the platform secure, observable and recoverable.

A managed service is more than hosted software: it makes responsibility visible before an incident.

What a server alone leaves with your team

- Sizing compute, database, storage, cache and network
- Hardening the operating system and application stack
- Managing identities, permissions and administrative access
- Planning updates without disrupting critical workflows
- Protecting coherent copies and proving recovery procedures
- Monitoring capacity, certificates, jobs and service health

Nextcloud

+

Nebulas managed operations

+

AWS cloud security & resilience

Three layers. One accountable service.

Nebulas Managed Nextcloud combines the data-control and collaboration capabilities of Nextcloud with Nebulas managed security and operations on AWS enterprise cloud infrastructure.

CLOUD PROVIDER	Amazon Web Services	Security of the cloud: physical datacentres, hardware, core networking, virtualisation and the infrastructure controls within applicable AWS certification programmes.
MANAGED SERVICE PROVIDER	BETA Technologies S.r.l. / Nebulas Software	Security and operation in the cloud: system and Nextcloud configuration, identity, network rules, encryption settings, updates, monitoring, backups and customer-specific controls.
APPLICATION PLATFORM	Nextcloud	The collaboration layer for files, controlled sharing, calendars, contacts, teamwork and supported apps and integrations.

AWS protects the underlying cloud. Nebulas secures and operates the managed service in the cloud.

AWS Shared Responsibility Model

The operational work is part of the service.

The exact scope is agreed for each architecture. It can cover the complete service or complement an internal IT team in clearly defined areas.

01

Architecture and isolation

Compute, database, storage, cache, network and access designed around volume, risk, location and availability needs.

02

Migration and adoption

Data and permissions inventoried, rehearsals and cutover planned, integrity reconciled and users prepared for the new environment.

03

Identity and access

Administrative paths, roles, MFA or SSO options, least privilege and customer-specific access rules configured and reviewed.

04

Security and updates

Operating system, application and supported apps maintained through controlled change with hardening and firewall rules.

05

Backup and continuity

Protected copies, retention and recovery objectives defined in the agreement, with recovery checks for the complete service.

06

Monitoring and improvement

Application and infrastructure signals, capacity, certificates, backup jobs and operational risks monitored and reviewed.

Enterprise cloud infrastructure powered by AWS.

Nebulas Managed Nextcloud is hosted on Amazon Web Services and leverages AWS cloud services covered, where applicable, by internationally recognised security and compliance programmes.

AWS

AWS Security & Compliance

ISO/IEC 27001
Information Security Management

ISO/IEC 27017
Cloud Security

ISO/IEC 27018
Protection of personal information in public clouds

ISO/IEC 27701
Privacy Information Management

ISO 22301
Business Continuity Management

ISO/IEC 20000-1
IT Service Management

ISO 9001
Quality Management

CERTIFICATION SCOPE

Certifications refer to Amazon Web Services and the AWS services included within their respective certification scope. BETA Technologies S.r.l., Nebulas Software and Nebulas Managed Nextcloud are not independently certified under these standards unless explicitly stated otherwise.

Place data, identities and integrations inside a defined architecture.

The design records where data resides, who can administer each layer, how information is protected and which external services are involved. European data hosting options can be selected where they fit the agreed customer architecture.

Data location

AWS region, storage, replicas and backup destinations are selected and documented for the specific service.

Access control

Users, administrators, service identities and integration permissions follow agreed roles and least-privilege rules.

Encryption

Connections, storage and backups use encryption controls appropriate to the architecture, with key custody and boundaries made explicit.

Connected work

Supported apps and APIs link Nextcloud to identity, ERP, CRM and business workflows without fragile core changes.

Continuity is designed as a system

01

Protect

Data, database, configuration, apps and keys form one coherent backup set.



02

Observe

Infrastructure and application signals show whether the service and protection jobs are healthy.



03

Recover

Recovery procedures and objectives are agreed and checked against the complete environment.

Make the operating model clear before launch.

Architecture and commercial scope are translated into decisions that IT, procurement and governance teams can inspect.



Questions the proposal should answer

- Which AWS region and services are in scope?
- Who administers application, system and cloud layers?
- Which encryption controls apply, and who holds the keys?
- What is backed up, retained and included in recovery checks?
- Which apps, integrations and external processors are involved?

No product or hosting provider makes an organisation compliant on its own. We document the controls we operate and the responsibilities that remain with the customer.

NEXT STEP

Bring collaboration under professional operation.

Start with the data, users, integrations and responsibilities. We will turn them into an architecture and a managed-service scope your team can review.

Design the architecture

Define location, access, security, capacity and continuity around your requirements.

Plan the migration

Inventory content and permissions, rehearse the move and set clear acceptance criteria.

Talk to Nebulas

Discuss your current platform, constraints and the work your team wants to hand over.

Talk to us

nebulas-software.com/en/contact

info@nebulas-software.com · +39 079 097 6894



nebulas-software.com/en/managed-nextcloud

Certifications refer to Amazon Web Services and the AWS services included within their respective certification scope. BETA Technologies S.r.l., Nebulas Software and Nebulas Managed Nextcloud are not independently certified under these standards unless explicitly stated otherwise.

Nextcloud is a registered trademark of Nextcloud GmbH. Amazon Web Services and AWS are trademarks of Amazon.com, Inc. or its affiliates. Nebulas Software provides an independent managed service.

Nebulas Software is a brand of BETA Technologies S.r.l. · EU VAT IT02412440907