Nextcloud

Kronenstr. 22A
70173 Stuttgart
Germany

T: +49.711.89 66 56 - 0
F: +49.711.89 66 56 -10

Web: https://nextcloud.com/
E-Mail: sales@nextcloud.com

Nextcloud Solution Architecture

Bring data back under control of IT

Modern IT infrastructure is complicated, mixing new and legacy technologies with dumb and smart storage, private and public cloud services, logging and monitoring tools, authentication servers and more already deployed. New technologies should fit in the existing architecture rather than putting further demands on the IT department while protecting confidential information and preventing it from ending up in consumer grade applications. You need a solution which lets you leverage existing infrastructure without duplicating or moving data. A solution which puts you in control while bringing a modern, on-the-go and easy to use experience to your users.

Nextcloud provides a common file access layer through its Universal File Access, keeping data where it is and retaining the management and control mechanisms IT currently has in place to manage risk. By leveraging existing management, security and governance tools and processes, deployment is made easier and faster. Nextcloud brings data from cloud storage, Windows network drive and legacy data storage to users in a single, easy interface empowering them to access, sync and share files on any device, wherever they are, managed, secured and controlled by IT, see Figure 1. It complements this functionality with optional integrated communication and collaboration tools like online document editing, audio/video chat and more.

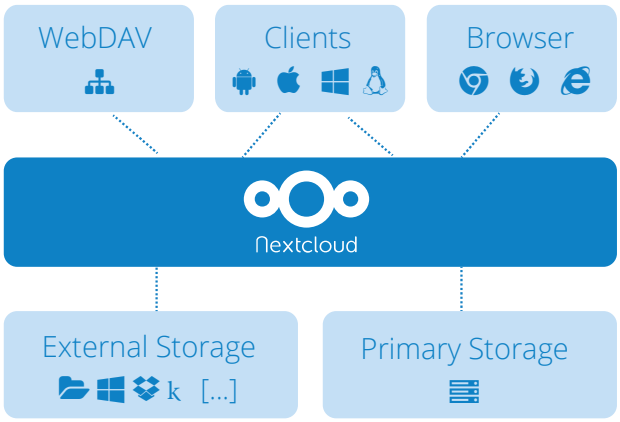


Figure 1: Nextcloud delivers users easy, unified access to files wherever they are stored

This white paper will detail the Nextcloud Architecture and provide a high level overview of typical deployment choices. Find a full feature list in Addendum 1.

Nextcloud

Kronenstr. 22A
70173 Stuttgart
Germany

T: +49.711.89 66 56 - 0
F: +49.711.89 66 56 -10

Web: https://nextcloud.com/
E-Mail: sales@nextcloud.com

Overview of the Nextcloud Architecture

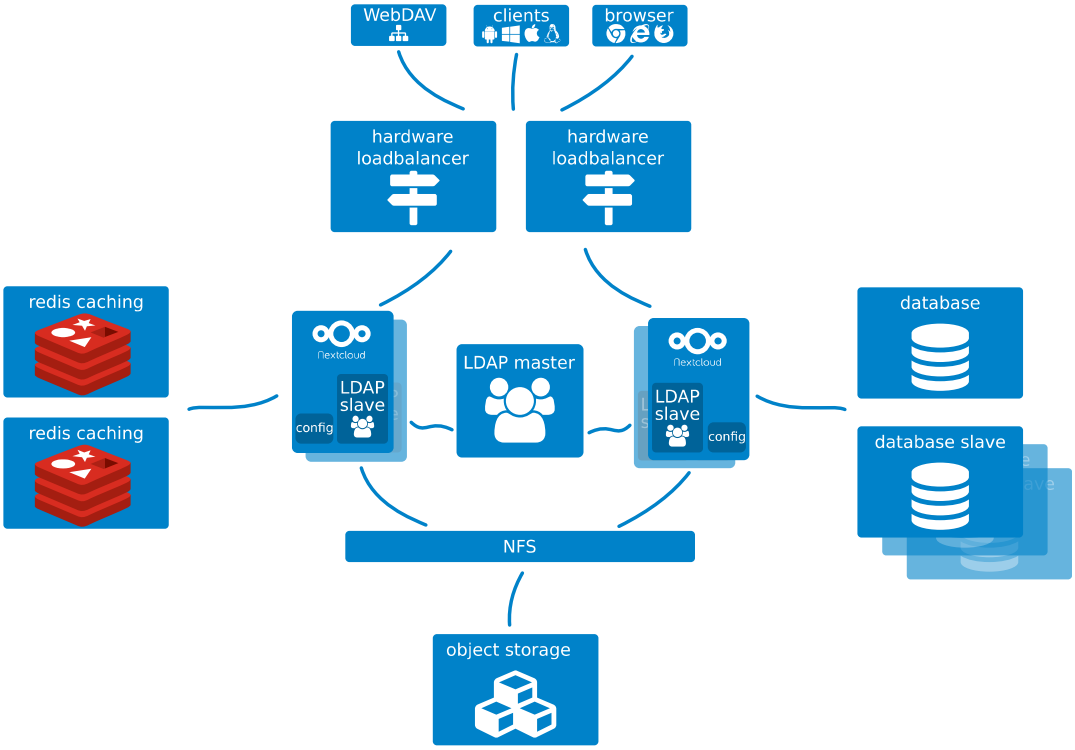
The Nextcloud Server is the center in the Nextcloud architecture, mediating file access and processing while monitoring and logging data access for auditing and analysis using SIEM tools like Splunk®. The Nextcloud server is configured through a secure web interface, enabling authorized users to control storage, set policies on file access or set up automated file processing, manage users, enable or disable functionality and more. Enterprise directory integration, WebDAV, custom provisioning and other API's enable integration with third party applications and platforms, monitoring tools like openNMS or Nagios and security key management systems.

Server Architecture

The Nextcloud Server is a PHP web application running on a Linux web server like Apache or NGINX. It stores file sharing information, user details, application data and configuration as well as file information in a database. Nextcloud has support for MySQL, MariaDB and PostegreSQL as databases. As a performance measure, a REDIS caching server can be used to speed up data access and lower the load on the database while the Nextcloud team also has extensive experience with clustering databases for large installations. Optional features like full text search, audio/video chat or collaborative, real time office document editing require additional services to be ran.

The storage layer can leverage any storage protocol that can be mounted on a server, like NFS, GFS_2, Windows Network Drive, CIFS, Red Hat Storage, IBM Elastic Storage and object stores compatible with SWIFT and S3. It is also possible to mount Windows home directories, (s)FTP, WebDAV and external cloud storage services like Google Drive and Dropbox in the user storage. The system can be configured to dynamically allocate storage based on user directory entries enabling data segregation and multi-tenant deployments.

See Figure 2 for an overview of a scalable Nextcloud setup with NFS as storage layer, an LDAP user directory, REDIS caching servers, multiple database servers and a load balancer. Find more details in the Deployment section below.



Accessing data

While Nextcloud provides a great deal of control over data access and sharing to administrators, users are presented with an easy to use and familiar interface through the web browser, Android and iOS apps and desktop sync applications. The intuitive interface makes it easy for users to access and share their data through on their desktop, tablet, phone or laptop with the Nextcloud apps. Alternatively they can access their files through a wide variety of their existing productivity tools thanks to Nextcloud's industry-standard WebDAV support. Nextcloud also offers a plugin for Microsoft Outlook which can automatically store attachments on Nextcloud to save storage space on the Outlook server and enable users to sent customers or partners a link where they can upload files.

Web interface features

The Nextcloud server provides a powerful web interface for configuring managing and monitoring Nextcloud systems for the admin. The admin can manage users, Nextcloud settings and configure, enable or disable features and set the access

control permissions or configure workflow features. A subset of capabilities and control can be delegated to designated power users who can be made admin over specified groups and given certain powers including adding or removing users from that group.

For end users, the web interface allows them to access their files and folders, initiate and control sharing, monitor who is doing what with their files, search for, comment on, edit, view and download files. Files can be deleted and brought back from the trash and users can view older versions of files and restore them if they wish. The Nextcloud web interface works on all major browsers on Windows, Mac OS and Linux operating systems. There is an optional, full text search feature.

Communication and document editing

Nextcloud features optional integrated audio/video chat using WebRTC browser technology. Its ability to connect users in heavily firewalled networks is greatly enhanced by the installation of a STUN/TURN server setup.

Optional real time, collaborative office document editing is available, enabling users to work individually or collectively on common office documents like XLSX, DOCX or PPTX as well as OpenDocument files. Collaborative document editing requires an additional service running, either using a docker container or native Linux packages for a variety of enterprise platforms.

File handling and storage

Nextcloud abstracts away file system and storage differences for the end users. It stores user files in standard file system formats, supporting most enterprise file storage systems. This enables Nextcloud to work seamlessly with existing tools and workflows used to secure, monitor back up and audit storage in the IT department.

Storage can either be mounted on the server Nextcloud runs on or through the Nextcloud interface which also supports Swift and S3 object stores or compliant systems, FTP, NFS and others.

To add an additional layer of protection, Nextcloud can encrypt files on storage through the Encryption app. This also has support for third party key management systems.

The optional full text search feature requires an Apache Solr Java servlet running on the application server or a separate, dedicated (virtual) server, indexing the storage

systems providing instant-search in office documents and (through optional OCR) images for the users. It fully supports all Nextcloud storage systems as well as encryption.

Authentication and Provisioning

Nextcloud integrates in existing account handling infrastructure. Active Directory and LDAP support provides account provisioning, integration and quota management. SAML 2.0 is supported for token-based authentication and the Nextcloud plugin infrastructure enables easy integration in other authentication systems through a REST API or internal API's.

User group memberships, storage paths, quotas and other settings can be centrally managed, with even the posibility to use both SAML and LDAP/AD at the same time, using SAML for authentication and LDAP/AD for group management.

Nextcloud also supports Kerberos authentication and other authentication mechanisms mediated by Apache modules.

Additional security is provided through the Two Factor Authentication support which works with TOTP and YubiKey and can easily be extended to other 2FA schemes.

A REST API is provided for external user provisioning, often the preferred method on medium to large installations (between 10.000 and millions of users).

File Access Control and Processing

Through File Access Control and automatic file tagging, Nextcloud gives administrators control over data access by enabling them to define strict rules requests need to adhere to. If users in certain groups or geographic regions should not be given access to certain file types or if data with a specific tag should not be shared outside the company, administrators can make sure their Nextcloud instance enforces these rules.

The Workflow engine expands these capabilities, enabling administrators to start any kind of actions based on these triggers, for example converting document file types to PDF upon upload by members of a specified group.

File retention and deletion can also be controlled based on tags set manually or automatically, ensuring legal or practical requirements for the longevity of data lifespans can be enforced.

Kronenstr. 22A
70173 Stuttgart
Germany

T: +49.711.89 66 56 - 0
F: +49.711.89 66 56 -10

Web: https://nextcloud.com/
E-Mail: sales@nextcloud.com

Security

Security is a prime concern for Nextcloud customers. Nextcloud aligns with industry standards such as Clause 14 of ISO/IEC27001-2013 and related standards, guidance and security principles. We provide security training to our developers, review designs for security implications, use advanced threat modeling / attack surface analysis and a mandatory code review process during development. Our product undergoes regular static and dynamic security scans and follow industry standard disclosure and CVE identifier processes. We run a successful Security Bug Bounty Program where thousands of international security experts are invited to find and responsibly report security issues in Nextcloud. Rewards of up to $5000 make Nextcloud security bug bounties among the highest in the open source industry.

We employ third-party review and verification of our security tools and processes. The NCC group has validated our development processes and ISO 27001 alignment; We worked with the Linux Foundation's CoreInfraStructure initiative to validate our development. We use Veracode vulnerability scanning as well as several other tools to ensure our code is checked for common security issues.

The Nextcloud server is architectured to be highly secure with both passive as well as active security measures. Passively, Nextcloud employs a wide variety of security hardening capabilities, including:

- Content Security Policy
- Same-Site Cookies
- Brute force protection

Data transfer is protected using industry standard TLS encryption, using the facilities provided by the web server on the server side and openSSL on the clients. With third party apps, client side encryption can be implemented.

Active security measures system administrators can enable includes two-factor authentication with device specific passwords. This feature offers a list of connected browsers and devices on the users' personal page. Active sessions can be invalidated through the list, by removing the user in the admin settings or by changing passwords.

We provide an extensive hardening guide in our documentation and support our customers actively in securing their installation.

Server side encryption

Usage of Amazon S3 or a compatible object storage can be secured through server side encryption on the Nextcloud server, making the object store (or any other external storage) act as a blind storage server, negating the need to trust the cloud storage provider.

Nextcloud supports built in or external key management. The built in key management supports all Nextcloud's features including sharing and collaboration and offers the option to generate a recovery key and allows administrators to encrypt or decrypt all files from the command line.

Inherent to the concept of server side encryption, encryption keys will be present in memory of the Nextcloud server during the time a user is logged in and could be retrieved by a determined attacker. We take care to ensure keys are not stored unencrypted on permanent storage and at rest keys are encrypted using a strong cypher.

If you face a regulatory or compliance need to encrypt data on the server but do not need to actually secure this data, encrypting the data using our built in key management may satisfy compliance requirements.

Find more information, documentation and white papers on security on nextcloud.com/secure

Federation

A unique capability of Nextcloud is Federation. This feature enables transparent file sharing between users on different servers. For this, users can use a 'Federated Sharing ID', a unique identifier consisting of the user name and server address of a Nextcloud server. When a file is shared between two Nextcloud servers, the server can optionally exchange address books, enabling auto-completion of user names on the other server. The system administrator can enable or disable this functionality and manually add or remove trusted servers. Communication between Nextcloud servers takes place through a REST API, standardized in the Open Cloud Mesh initiative and also implemented by some other cloud vendors. File exchange is based on WebDAV and uses standard TLS based security.

Files remain on the server they were shared from, ensuring the user who owns the file and the admin of their server remain in full control of the data.

Nextcloud
Kronenstr. 22A
70173 Stuttgart
Germany
T: +49.711.89 66 56 - 0
F: +49.711.89 66 56 -10
Web: https://nextcloud.com/
E-Mail: sales@nextcloud.com

Extending capabilities of Nextcloud

Nextcloud has a modular architecture, enabling administrators to add or disable functionality like the picture gallery, virus scanner, file versioning, logging, or sharing. Optional features available for installation also include Calendar and Contact applications and more.

Thanks to extensive developer documentation and easy API's, Nextcloud customers have integrated functionality like video streaming, custom authentication mechanisms and a variety of storage systems in Nextcloud.

Refer to the features table in addendum 1 for a more complete overview of Nextcloud's capabilities.

Deployment on site

Nextcloud has developed extensive documentation on best practices around deployment and maintenance of Nextcloud servers. While, as a PHP application, Nextcloud can be deployed in a wide variety of circumstances, a typical deployment uses the standard 'LAMP' stack, with Linux, Apache, MySQL or MariaDB and PHP.

A fully redundant system servicing up to about 1000 users with a storage of around 200TB could require 2-4 application servers, 2 database servers, a Haproxy load balancer and NFS storage. We will detail the choices made and how to integrate in existing infrastructure.

Overview

Nextcloud can be deployed on physical, virtual or private cloud servers using native binaries or virtual appliances. Load balancers enable not only better performance but also provide a fail-over in case of hard or software issues. The web servers host the Nextcloud PHP code, and communicate with the databases, frequently clustered MySQL. While the database stores user and group metadata, a file cache and Nextcloud App data, a clustered file system accessible over NFS is the most frequently used file storage system. Scaling up can be done with further web servers and load balancers while REDIS caching can provide a performance boost on installations going from tens of thousands to hundreds of thousands of users. Beyond this point, customers often employ Federation to enable further scaling into the many millions of users.

Kronenstr. 22A
70173 Stuttgart
Germany

T: +49.711.89 66 56 - 0
F: +49.711.89 66 56 -10

Web: https://nextcloud.com/
E-Mail: sales@nextcloud.com

Database and performance

Most used is a MySQL/MariaDB Galera cluster with master-master replication, though we often recommend customers to use what they are familiar with.

Use HAProxy running on a dedicated server in front of the application servers. Sticky session needs to be used because of local session management on the application servers. The SSL termination is best done in the HAProxy load balancer. A standard SSL certificate is needed, installed according to the HAProxy documentation.

Storage

For storage, we recommend an off-the-shelf NFS solution, such as IBM Elastic Storage or RedHat Ceph. Storage using REST API's can be used to either replace or augment the storage, with Swift and S3 as examples of HTTP based storage backends. Once a primary storage is configured, Nextcloud will generate a directory for each user with versions, folders and files stored in it. Object Storage flattens the file path in the database, otherwise acting the same. In our experience, object storage' performance characteristics make it most suitable for archival or streaming of large files. To optimize object storage performance, Nextcloud will assign a single bucket to each user.

User information from LDAP or Active Directory can be used to dynamically assign a storage path to each user, enabling the admin to match storage solutions to users based on group membership or other properties.

Once LDAP/AD is connected, the storage path attribute can be inherited and it is possible to direct users to multiple storage paths.

Besides primary storage, multiple additional storage systems can be mounted and added through the configuration panel for the system administrator, differentiating for specific groups or users. This way, a sub group can be given access to a CIFS or FTP system, while other users are allowed to configure access to their private dropbox. All the same, the system administrator can use File Access Control to prevent access to sensitive data or enforce full encryption of all files before they are sent to external storage. These capabilities combine to enable IT to manage storage systems, mixing and matching local, cloud and hybrid storage to use case, security requirements and costs.

Authentication

Authentication is usually managed with several LDAP or Active Directory Servers. For optimal scalability, read-only slaves should be deployed on the Nextcloud application

servers. Settings for users can be managed centrally and new users should, on larger installations, be provisioned via the provisioning API.

Upon first login, Nextcloud will provision users according to the settings in the user directory. Custom attributes like display names and avatars can be configured, either by the admin or the users themselves. Nextcloud enforces admin policies and will log out users when their accounts are locked or removed or the password is changed.

The Nextcloud API's have been used to integrate with Data Loss Prevention tools, antivirus mechanisms and Mobile Device Management tools.

Third party integration

Nextcloud comes with a number of server API's which enable integration in other systems. Included are:

- Activity Feed – An overview of all activities associated with a user. These include new shares, updated or removed files, calendar events and more. Nextcloud applications can provide additional information for the Activity feed. The Activity feed can be accessed externally through an RSS feed.
- Sharing – external applications including our own mobile and desktop applications can share files through this REST API.
- Capabilities – Nextcloud servers can be queried for information about their version and features by Nextcloud and third party applications.
- Provisioning – Nextcloud features an API to add and remove users remotely and query for storage usage and quota.
- Monitoring – Nextcloud offers a monitoring API endpoint, enabling easy monitoring of activity on Nextcloud servers with tools like Nagios. Available is information on the number of active users, shares in various categories, storage statistics, server settings and more.
- Application API – Nextcloud functionality can be extended through Nextcloud apps, offering a powerful API for integrating with existing infrastructure and offering additional capabilities like custom authentication backends, streaming applications and more.

As a typical n-Tier web application, standard tools like Intrusion Detection Systems, firewalls, network management and monitoring tools can be leveraged. Backup can be done either online or offline as with any web application.

Kronenstr. 22A
70173 Stuttgart
Germany

T: +49.711.89 66 56 - 0
F: +49.711.89 66 56 -10

Web: https://nextcloud.com/
E-Mail: sales@nextcloud.com

Conclusion

The open-by-design nature of Nextcloud provides IT with an unprecedented flexibility while integrating natively in existing, legacy infrastructure. This results in a cost-effective solution which gives IT full control over corporate data while end users benefit from the pleasing, productive interface they demand.

More information

Visit www.nextcloud.com for more information about Nextcloud products, services and support.

Nextcloud

Kronenstr. 22A
70173 Stuttgart
Germany

T: +49.711.89 66 56 - 0
F: +49.711.89 66 56 -10

Web: https://nextcloud.com/
E-Mail: sales@nextcloud.com

Addendum 1

Feature overview

Feature list

File handling

- Tags
- Favorites
- Search (tags, filenames)
- Full text search (optional)
- Comments
- File versions

File manipulation

- Text editor
- PDF viewer
- Image gallery
- Video player
- Online office with collaborative editing (optional)

File syncing

- Win/Lin/Mac clients
  - Sync all or per folder
  - Can skip syncing any sub folder
  - File manager integration
- Android/iOS clients
  - Sync 'favorite' files or folders
  - Auto-image/video upload
  - Full sharing integration

Kronenstr. 22A
70173 Stuttgart
Germany

T: +49.711.89 66 56 - 0
F: +49.711.89 66 56 -10

Web: https://nextcloud.com/
E-Mail: sales@nextcloud.com

Sharing

- Groups or users
- Public link with expiration, password
- Optionally allow uploading/changing files
- Optionally hide already uploaded files (creating upload folder or 'file drop')
- Share between different Nextcloud/ownCloud/Pydio servers (Federation)
- Auto-complete user names between connected instances

Activity tracking and announcements

- Notifications/activities tracked and visible for users:
  - Files created, updated, shared, un-shared and deleted by user or others
  - Shared file downloaded (optional)
  - Comments on files
  - Calendar/todo changes
  - Admin announcements
- Admin can sent notifications to all users, specific users or groups

Storage

- The following storage systems are supported:
  - local storage
  - Object Storage (Swift/S3)
  - SMB/CIFS
  - Dropbox
  - Google Drive
  - (s)FTP
  - Windows Network Drive
  - WebDAV
  - And anything which can be locally mounted on the server
- Users can be given ability to mount any external storage type

Kronenstr. 22A
70173 Stuttgart
Germany
T: +49.711.89 66 56 - 0
F: +49.711.89 66 56 -10
Web: https://nextcloud.com/
E-Mail: sales@nextcloud.com

Authentication methods

- LDAP
- Active Directory
- SAML 2.0
- OneLogin
- Shibboleth
- Active Directory Federation Services (ADFS)
- Authentication via environment variable
- Kerberos (Apache mod_auth_kerb)
- Any other or custom provider that authenticates using the environment variable

monitoring and auditing

- Built in monitoring app showing basic server health properties like CPU/memory load, # of active users or shares, storage, system configuration etc
- Monitoring API for external tools like Splunk, openNMS, Nagios
- Optionally logging full audit trail to log file

Security

- File Access Control blocks access requests based on rules like IP, user/group, file type, ...
  - Positive security model compatible with mod_security compliant WaF solutions.
- Anti-Virus app (ICAP support coming)
- Server side encryption
  - Using built-in or external key management
  - Built in has optional master password for recovery, encrypt/decrypt all feature, sharing
  - Encryption can be enabled/disabled on local storage and per external storage connection
- Brute force protection

- Additional password check
- Two-factor authentication
  - Time-based One-Time Password (TOTP)
  - Universal 2nd Factor (U2F)
- Define password policies (NIST compliant)
- Full control over connections between clouds (Federation)
- Web interface protection includes:
  - Content Security Policy CSP 3.0 protection
  - Same-site cookies

Third party integration

- Outlook Add-in providing Calendar/Contacts syncing
- Outlook Add-in for replacing attachments with Nextcloud links, supporting:
  - Custom link insert text/html
  - Password policy
  - Default expiration date
- Integration with DAVDroid providing Calendar/Contact sync on Android
- CalDAV/CardDAV compatible with iOS

Workflow

- Automatic tagging based on properties like IP of uploader, time/date, user/group, file type, ...
- Retention based on tags
- Automatic execution of scripts at time of file upload based on automatic tagging

Calendar and Contacts

- Built in Calendar and Contacts app

API

- All data is accessible through WebDAV, CalDAV, CardDAV
- OCS Sharing API (REST style) enables sharing files
- Provisioning API enables creating/listing/changing users

Audio/video chat

- Audio/video communication with users and groups on Nextcloud
- Users without account can be invited to calls via a public link
- Scaling to 5-8 users per call (depending on network quality)
- STUN server, TURN server optional (highly recommended)
- SIP gateway optional

Other

- Easy theming
- Modify email templates (used for notifications to users, invites to shared links etc)
- Easily add external websites as 'Nextcloud app' in a iframe