Software Requirements Specification

for

Nextcloud

Version 1.0

Prepared by Theodoros Grammenos

Aristotle University of Thessaloniki

February 15, 2021

Contents

Revision History

Name	Date	Reason For Changes	Version
First Release	2021-02-15	-	1.0

1 Introduction

1.1 Purpose

This document aims to specify the software requirements for Nextcloud. This specification is intended for developers of the software, that can use it as a guide when developing the system, and people who are interested in deploying the software, who can use this specification to see if it fits their needs.

1.2 Product Scope

The software covered in this report is Nextcloud version 20. Nextcloud is an online collaboration suite that enables users to share files, send emails, manage their calendar and more. Nextcloud is a fully on-premises solution so it can be used by people or organizations who want full control over their data. The software can be extended with extra apps and plugins. This report focuses only on the functionality of a fresh Nextcloud install and on some officially supported plugins that are developed as part of the software.

1.3 Definitions, Acronyms and Abbreviations

1.3.1 cloud applications

applications that are run by companies and are provided as a service to individuals or other companies, the entity that is provided the software does not usually have control over the hardware or the environment the application is run in

1.3.2 configuation

a set of settings and customizations to the base software

1.3.3 deployer

the entity that installs the software

1.3.4 deployment

the process of installing and configuring the software

1.3.5 entity

an individual or a company

1.3.6 instance

a specific installation of the software, different instances can have different configuration

1.3.7 LDAP

Lightweight Directory Access Protocol, industry standard application protocol for accessing and maintaining distributed directory information services

1.3.8 SAML

Security Assertion Markup Language, an open standard for exchanging authentication and authorization data between parties

1.3.9 self-hosted applications

applications that can be fully controlled by the entity that installs them on their servers

1.3.10 TOTP

Time-based One-time Password, a number that is used alongside a password to verify a user's identiy and changes based on the current time

1.4 References

- https://nextcloud.com/
- https://docs.nextcloud.com/server/20/admin_manual/
- https://docs.nextcloud.com/server/20/user_manual/
- https://nextcloud.com/whitepapers/

2 Overall Description

2.1 Product Perspective

Nextcloud is a suite of client-server software for collaboration. It is based on OwnCloud, a similar product. The two projects differ mainly on their user interfaces and their licensing. Nextcloud is an alternative to many cloud based services such as Google Drive, Dropbox or Microsoft Office 365. Its key feature is that anyone can install and operate it on their own servers and hardware. The software has an extensible plugin system that lets each individual or company customise the functionality of their Nextcloud instance. For example, a home user might only want to use the file storage and sharing functionality, while an enterprise might want additional video conferecing or logging features. The officially supported plugins offer a wide range of functionality, covering the needs of most individals and enterprises.

Individuals may choose to use Nextcloud because they care about privacy and want to have full control over their data. Specifically, the software allows people to choose who can access their data, be protected of a cloud service permanently closing down, having an outage or losing part of their data.

Companies can use Nextcloud because of security requirements that disallow storing data in third-party services. This is especially important in sectors such as healthcare where data must remain confidential and there is strict regulation in place to enforce that. It can also integrate with other widely used enterprise software (like Microsoft SharePoint) allowing for quick deployment and fast adoption in the organization.

2.2 Product Functions

2.2.1 Administrative

- User management
- Integration with existing user management solutions
- User permission control
- User access control
- Sensitive action logging
- Integration with existing enterprise products

2.2.2 User

- File access
- File sharing between users and devices
- Audio/video conferencing
- Real-time document collaboration
- Calendar, contact, task and mailing management

2.2.3 Developer

- Easy development for the platform

2.3 Product Constraints

The nature of the product requires it to be accessible from many types of devices, like desktop computers or mobile phones. There should be an easy to access interface for circumstantial users, for instance a user outside the company that wants access to a specific document. For permanent users there should be more advanced tools that integrate into the environment of the user and allow them to perform frequent functions, like accessing or uploading files, with ease.

The product is targeted at comapnies or organizations that deal with sensitive and private data in sectors like healthcare, government or law. There are often regulations governing data access in such sectors. One key example is the HealthInsurance Portability and Accountability Act (HIPAA) in the United States. Nextcloud should ensure that it provides the necessary tools for enterprises and organizations that need to be compilant with such legistlations.

The product should be designed with scalability in mind. It must be able to handle deployments of tens of users and tens of thousands of users equally well. Depending on the environment the software is deployed in and the services it provides there are different hardware or network requirements that must be communicated to the deployers beforehand.

2.4 User Characteristics

2.4.1 Main Users

These are the users that interact with the software daily, either as part of their work or for personal use. Due to the frequency of their interaction with the software, these users can be expected to install additional software on their computers (e.g. file syncing software) that can make regular tasks easier. These users need to have a personal user account and will use most of the user-facing functionality of the system.

2.4.2 Occasional Users

These are users that do not have a personal account on the system and interact only with the public-facing functionality. For example, someone with permanent access to the system, inside a company, might want to share a document with a person outside the organization. Convenience and speed of interaction are very important. As an example, these users should not have to install any additional software to download a file that was shared to them.

2.4.3 Administrators

These are the users responsible for managing and configuring the system. In an enterprise environment they can be assumed to be IT professionals. In a home or small business environment they might be hobbyists, or people knowledgable about computers but inexperienced with server administration. For this reason, the default configuration should be usable ”out of the box”. At the same time, it must allow professionals and advanced administrators to customise the software to a deeper extent.

2.4.4 Plugin Developers

These are people that develop plugins and apps that extend or customise the functionality offered by the product. They do not necessarily interact with a specific instance of the software. It is important to make developing for the software easy, as this will ensure that the software can be adapted for use in many specifc scenarios.

2.5 Assumptions and Dependencies

It is assumed that the deployer runs the application on a suitable environment and appropriate hardware for the specific configuration. The software must, of course, aim to minimise resource usage as much as possible. This is important for requirements regarding system response time and availability.

While the software must be able to integrate with other applications, the correct installation and configuration of the other applications is left to the administrator. Additionally the administrator is responsible for installing and configuring any plugins that are not officially supported.

2.6 Documentation

There are three main manuals that are provided along with the program.

The administrator manual documents installation instructions for the software, as well as basic configuration and management instructions.

The user manual provides instructions on how to perform common tasks as a user of the system.

The developer manual documents how to create plugins that extend the basic functionality of the software.

The given documentation only covers the default configuration of the server. It is the responsibility of the administrators to properly document and inform all users of any changes they make that are instance specific and affect the functionality of the application, such as adding custom features or removing existing ones.

3 Requirements

3.1 External Interfaces

3.1.1 User interfaces

Main interface components

The main user interface of Nextcloud is web based. Nowadays, the internet is accessible from a wide range of devices that have many different screen sizes and input methods, so it is important that the web user interface changes depending on the user's device.

To access the main interface the user must first log in. The login screen can offer different login options depending on the configuration. For example in the next screenshot an option to log in with a device is offered.

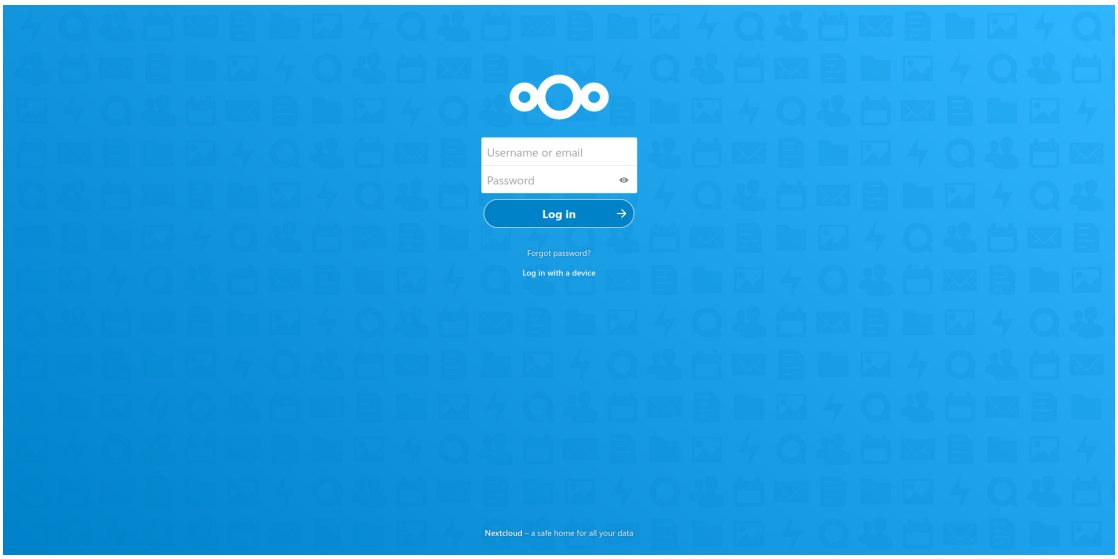

Figure 3.1: The login screen.

Once the user logs in they are faced with the main user interface of the application. The default page is the dashboard. The dashboard contains widgets which can be customized by each user. For example, a user might not use the file storage functionality and want only the calendar widget on their dashboard.

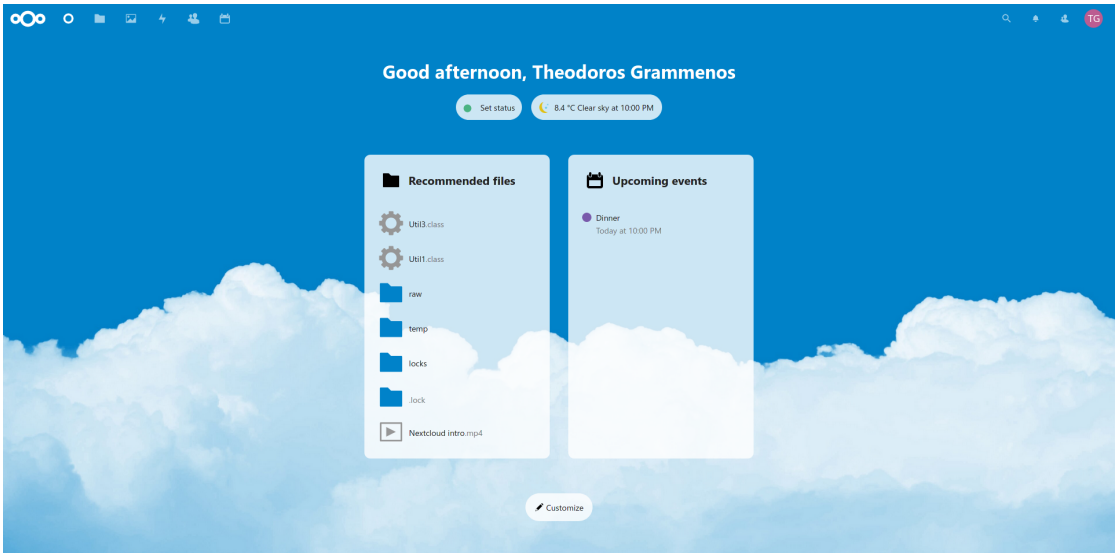

Figure 3.2: Dashboard

The main navigation mechanism is the navigation bar on top of the page. On the left side it displays all the apps offered by the software. On mobile devices the navigation bar hides the icons that do not fit and places them in a menu. On the right side the navigation bar offers quick access to commonly used functionality such as search, notifications and the user menu.

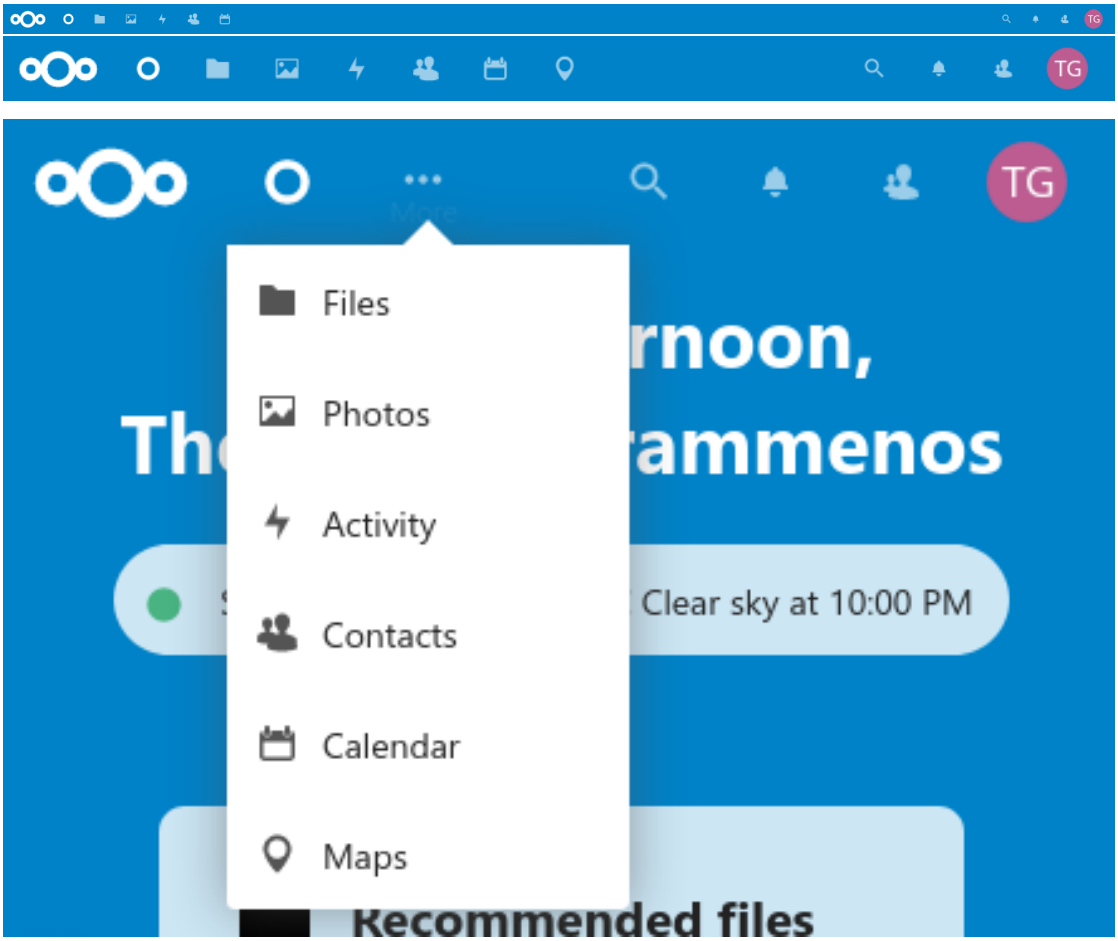

Figure 3.3: Navigation bars.

The user menu can have different options depending on the group of the user.

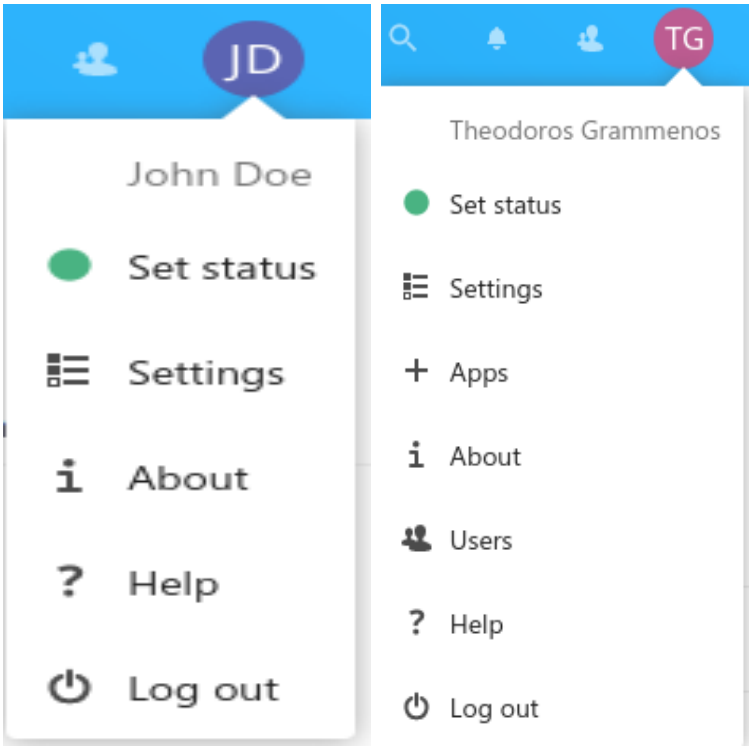

Figure 3.4: The user menu.

Files

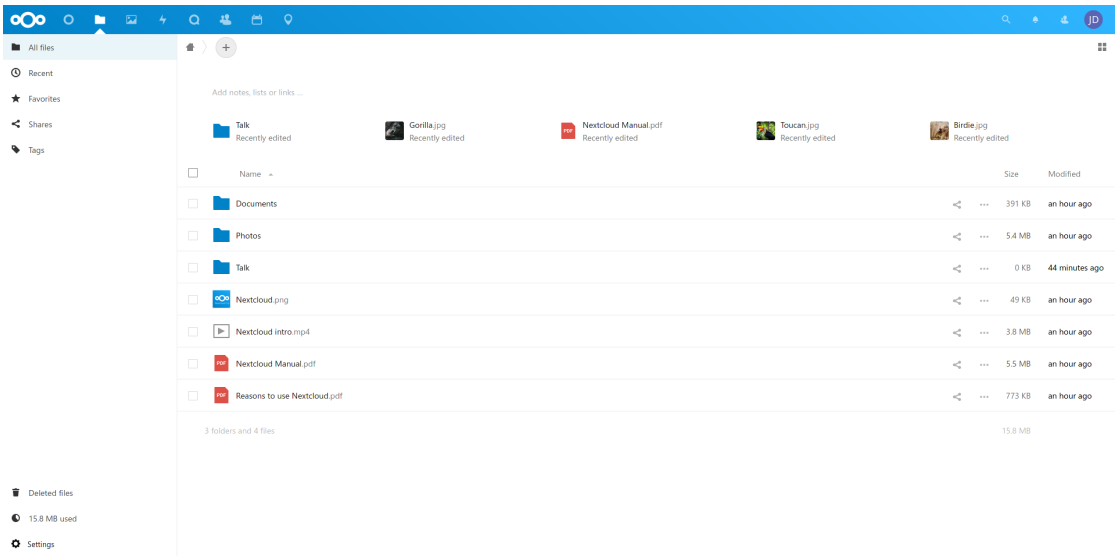

Figure 3.5: Files app.

The Files app allows the user to perform basic file management operations such as:

- Browsing existing files and folders.
- Uploading files through the browser.
- Downloading files through the browser.
- Creating new folders.
- Moving files between folders.
- Sharing files with other users.

A file or folder can be shared with another user inside or outside the Nextcloud instance. When a file is shared with another user in the same instance, it will show up in the user's files app with the original user's icon next to the file name. It can be viewed and modified as a normal folder in the user's files, depending on the sharing permissions. The user that received the file has the option to unshare it.

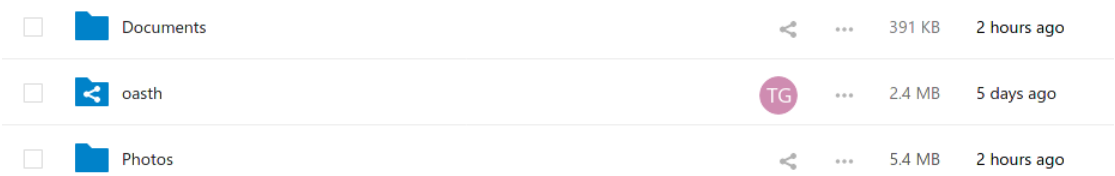

Figure 3.6: An internally shared folder.

When a file is shared with someone outside this instance the user is given a link they can give to anyone who needs access to the file. The person who received the file then accesses the link and is given access to the files without having to log in to the instance.

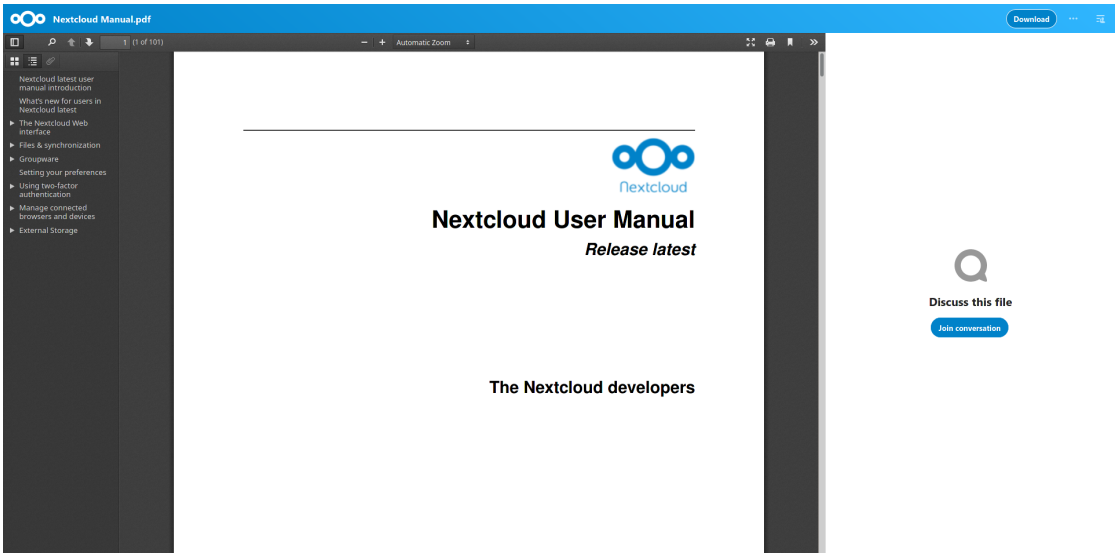

Figure 3.7: A publicly shared file.

In both cases the user who shares the file can adjust the level of access they give, if the file can be edited, deleted or viewed, and can set an expiration time so that the file gets unshared after a specific amount of time. Public links can additionally be protected with a password, something helpful when sharing sensitive files. A public link for a folder can be marked as drop-only, meaning anyone with the link can upload files to the folder but not view the existing files.

Each logged-in person that has access to a file can make comments on it and see the comments others have made.

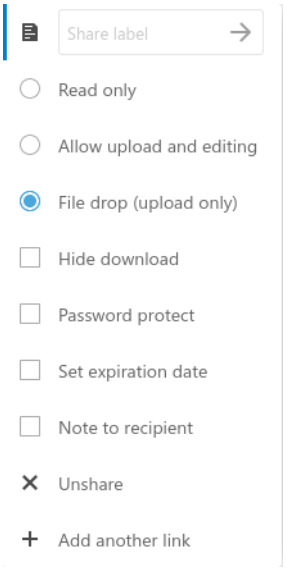

Figure 3.8: File sharing options

If the person that receives a public link for a file is a user of another Nextcloud instance they have the ability to add it directly to their files, where it is displayed as if it was shared internally.

User settings interface

The user settings interface allows the user to modify their information and select who can access it. They can choose if they receive e-mail alerts and can see a privacy report.

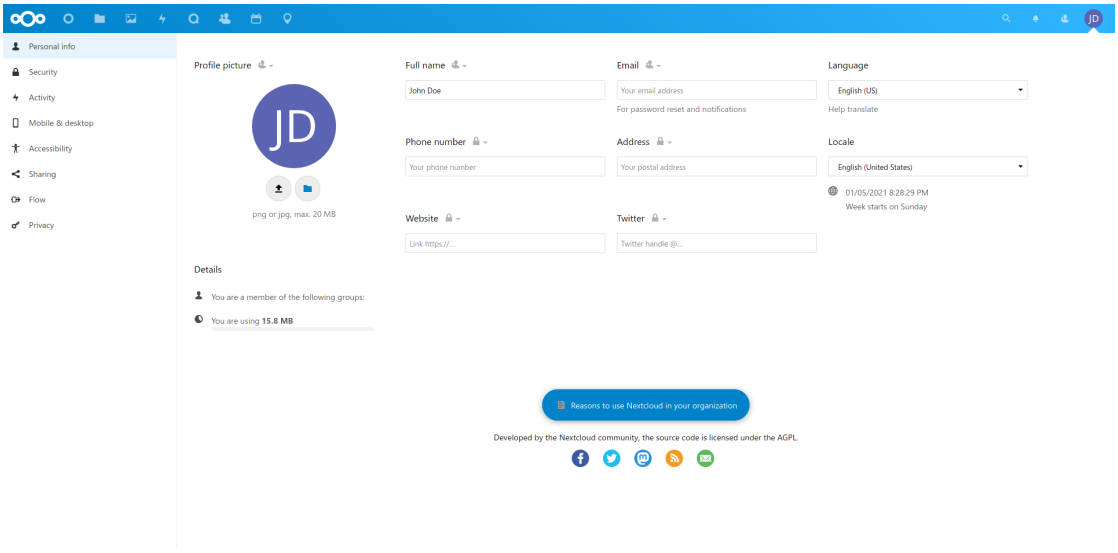

Figure 3.9: User settings.

Administrative User Interface

The Administrative User Interface is the part of the user interface intended to be used by the administrators for configuration of the software instance. The main administration options are visible in the normal user settings interface. Privileged users have access to a new administration section, where they can adjust global settings for this instance.

The app management screen is another component of the administrative UI. It allows installing, enabling and disabling apps. It displays the apps available at the Nextcloud App Store (https://apps.nextcloud.com/). The app store offers both officially tested and untested apps. Untested apps are clearly marked.

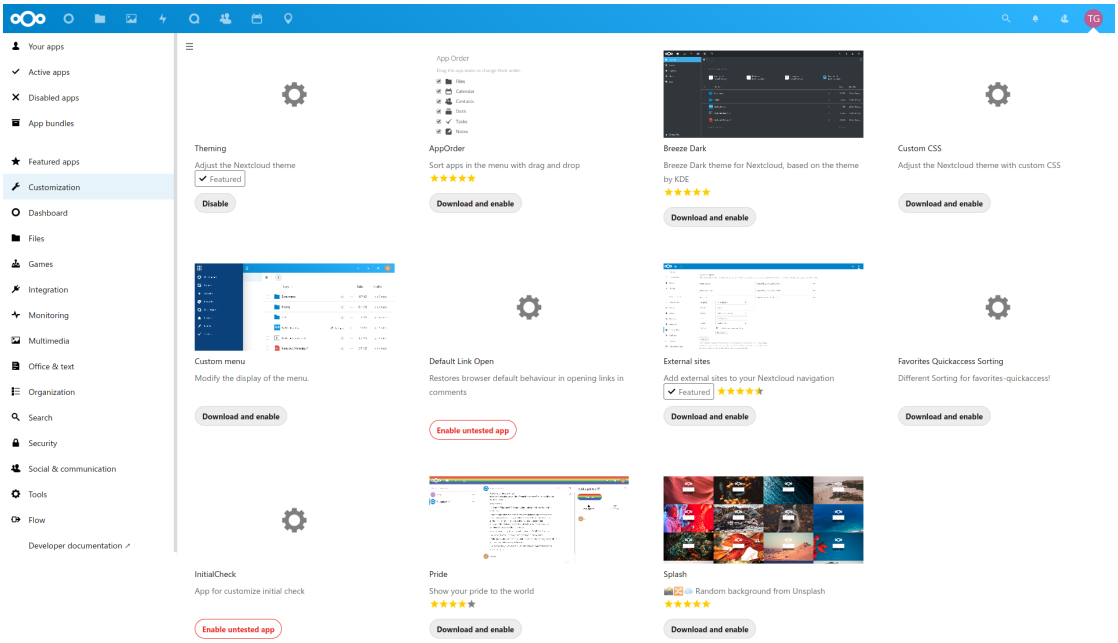

Figure 3.10: App installation.

The integrated user management interface allows creating new users and groups and modifying existing ones. It provides the option to set storage quotas and see storage usgae information. This UI should not be used when using an external user authentication solution (such as LDAP).

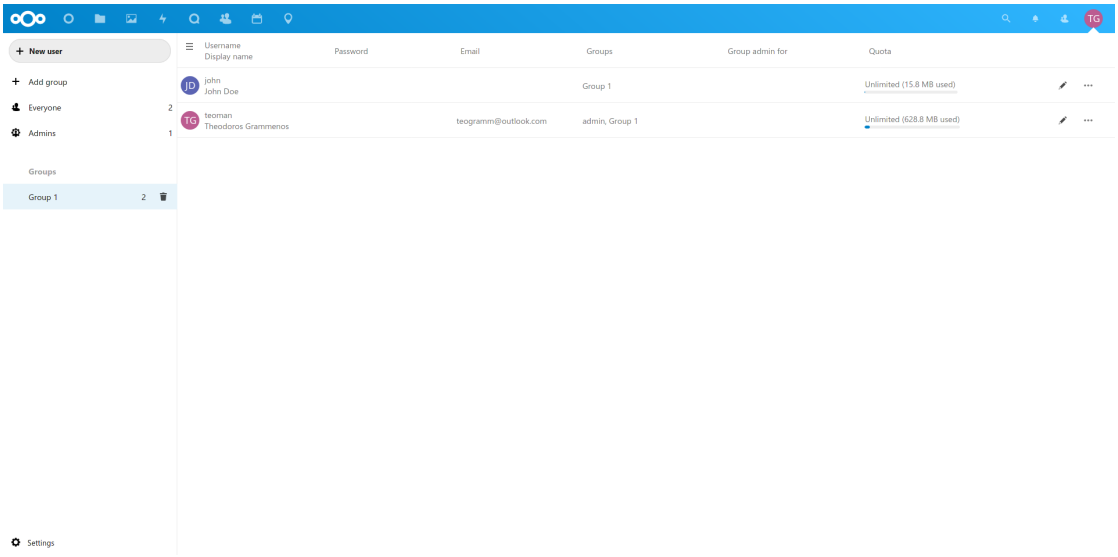

Figure 3.11: User administration interface

The administrative user interface also checks for common misconfigurations or security issues, as can be seen on the screenshot below.

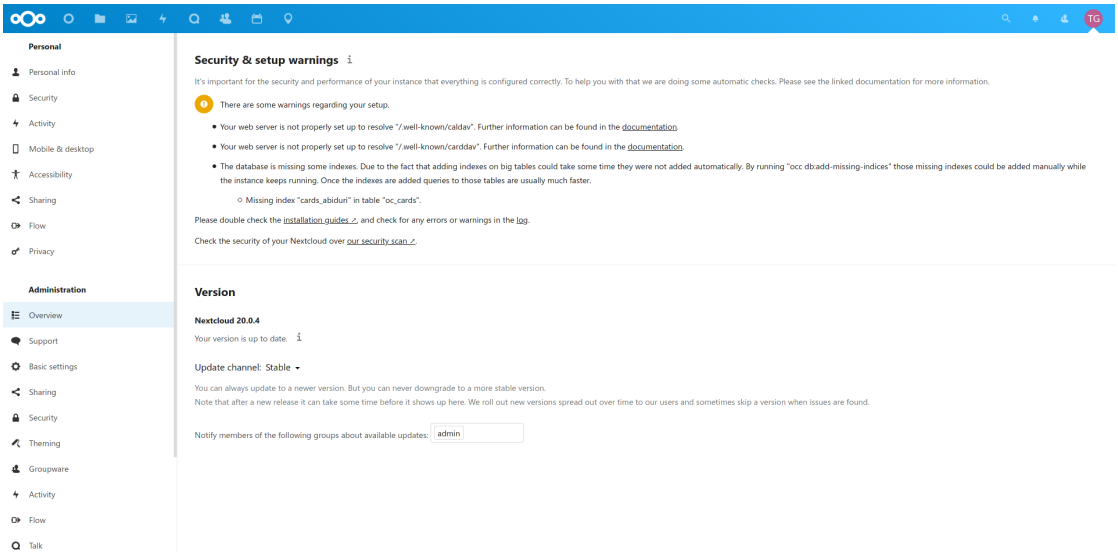

Figure 3.12: Administration overview

The occ command line tool is used for administration of the software as complement to the administrative graphical user interface. It can perform many common server operations and can be used when the web interface is unavailable, e.g.

when an upgrade has left the system in a bad state. Furthermore, it can perform more advanced openrations that are not available via the GUI such as migration between different database systems. This enables extensive customization for administrators who desire it.

3.1.2 Hardware interfaces

The software can run on any x86 computer and does not require any special hardware to run.

Optionally, users can activate passwordless authentication. This requires the user to possess a special hardware authentication device that follows the FIDO2 standard.

3.1.3 Software interfaces

A database server is needed to store data regarding the instance. The supported database server software are: PostgreSQL 9.4+, MariaDB 10.1+, MySQL 5.6+ and Oracle 11, 12. The software asks for credentials to connect to a database during the intial setup. Installation and proper configuration of the database server is not part of Nextcloud, but an obligation of the administrators.

The software can utilise an external caching software in order to improve performance notbaly in deployments with a large amount of users. Memory caching allows the applciation to store frequently requested objects in memory for faster retrieval. An example of memory cahcing software is Redis which supports both local and distributed (across multiple servers) caching something critical for larger deploymens, where a single server is inadequate for sustaining the load. It is vital to note that said software would not make a notable difference in the performance of smaller instances, so it should remain optional.

Nextcloud is able to connect to widely used enterprise applications, like Microsoft SharePoint. This allows users to use all the features of Nextcloud with existing files stored in in Microsoft SharePoint which could prove useful for enterprises with existing installations of SharePoint that are considering switching to Nextcloud as employees can test the new system alongside the existing one and state their preferences.

Enterprises often have existing user and group management infrastructure in place with software like LDAP and Microsoft Active Directory. Having to manage a new system and keeping it in sync with the preexisting one would be a complicated and error-prone task. Nextcloud can use the the existing system for authentication so the existing user management software can continue to be used. The integrated user system can be kept as an option for smaller deployments where it is sufficient.

The application offers support for the WebDAV protocol. WebDAV is an extension of HTTP and is supported in all major operating systems. With the protocol, users are able to access their files on Nextcloud natively via their operating system's

file manager without installing any additional software. An extension CalDAV is used for synchronising calendar events and contacts and is supported, too.

3.2 Functional

The following section contains the functional requirements for the software. Each requirement is assigned a priority which should be considered when deciding the develpoment timeline. The features are split by the intended category of users.

3.2.1 Administrative

3.2.1.1 User Management

The software allows the administrator to create and delete users. Multiple users can be added and removed from groups. The adminstrator can see each group's members, can create new ones and delete existing ones and can change the information of existing users. Users can be imported and exported from and into files for backup purposes or in case of migration to/from another user management system.
Priority: **High** This is an essential feature of the program.

3.2.1.2 Integration with existing user management solutions

The software must allow administrators to use the LDAP protocol instead of the built-in user management. The LDAP protocol is used by many enterprise user management solutions. Specifically, when the administrator configures a connection to an LDAP server the integrated user management is disabled and the new backend is used to validate credentials instead. It is important to note that changing the backend does not change the authentication method, it simply checks the credentials given by the users against an external database.
Priority:**Medium**

3.2.1.3 Integration with existing authentication solutions

The software must allow the administrator to configure authentication with an external source based on the SAML protocol. When the administrator configures SAML the new authentication backend is either added as an option or replaces the other backends. Registering a new authentication backend does not affect the user management backend. The user backend receives the authentication result and some information about the user (e.g. username, email, unique id) and determines if the user exists in the user database or creates a new user entry. Authentication is critical to the security of the application so the software must have secure defaults. As an example, if the authentication provider is down, access to a file should be

denied by default.
Priority: **Medium**

3.2.1.4 User access control

The administrators must be able to restrict features of the software to certain users or groups. They must be able to restrict sharing options to outside users and to groups inside the instance or completely disable sharing.
Priority: **Medium**

3.2.1.5 Audit logs

Nextcloud must have the option to keep detailed logs of the users' actions in the instance. This information must include the username, IP address, date and time. Actions that must be able to be logged include:

- user session (login, logout, user agent)
- file handling (download, upload, modify, (un)delete, tag, comment, restore old version)
- user management (creating/deleting/changing user, setting a password)
- sharing (creating, deleting, changing permissions, updating a password, setting expiration date, creating link)

Priority: **Medium**

3.2.2 User

3.2.2.1 File access

The sofware must offer a way for users to store, retreive and delete their files without being forced to install additional software on their devices.
Priority: **High**

3.2.2.2 File sharing

The software must allow users to share files with other users or groups in the same instance or with other people outside this instance. When sharing with users or groups inside this instance the users must be able to select each person or group that has access to a file and assign unique permissions for each. Permissions for files are: view only, delete or modify. Permissions for folders are: create new files, delete files, view files in folder or delete folder.

When sharing with users outside this instance the users must get a unique URL to the file or folder they are sharing with the selected permissions. When sharing files or folders through links user must have the ability to:

- allow editing
- set a password to access the file
- set an expiration date after which the link becomes invalid

When sharing a folder users must be able to additionally turn it into an upload only folder and anyone with a link can upload files to the folder and cannot view or modify existing files. Users must be able to create multiple links for the same folder or file that have different permissions.

Sharing a file or a link must be reversable. Users may unshare files they previously shared with other users. Links must be able to be revoked. After revoking a link it must not provide access to the file or folder.
Priority: High

3.2.2.3 Real-time document collaboration

The software hast to include an edditor for text documents, spreadsheets and presentations. The editor must have the ability to be used completely in the web browser if the user is using a desktop or laptop computer and may require smartphone users download an app. The editor must be able to handle multiple people working on a file at same time. Users must be able to see changes others make in real time.
Priority: Low

3.2.2.4 Real-time communication

The software must offer the ability for users in the same insatnce to communicate with each other in real time by text messages or by audio and video. The app must integrate with other features of the system allowing users, for example, to share files directly through messages.
Priority: Low

3.2.2.5 Calendar and contact management and synchronisation

The software must offer basic calendar, contact and task management features.

The calendar allows user to organise their schedule. For each event the user must be able to set a description, a starting and an ending time, a location and categories. Additionally they may invite other users to the event. Users in this instance can be notified by the built-in notification system. Users outside the instance can be sent an email to reply to the invitation and add the event to their personal calendar software.

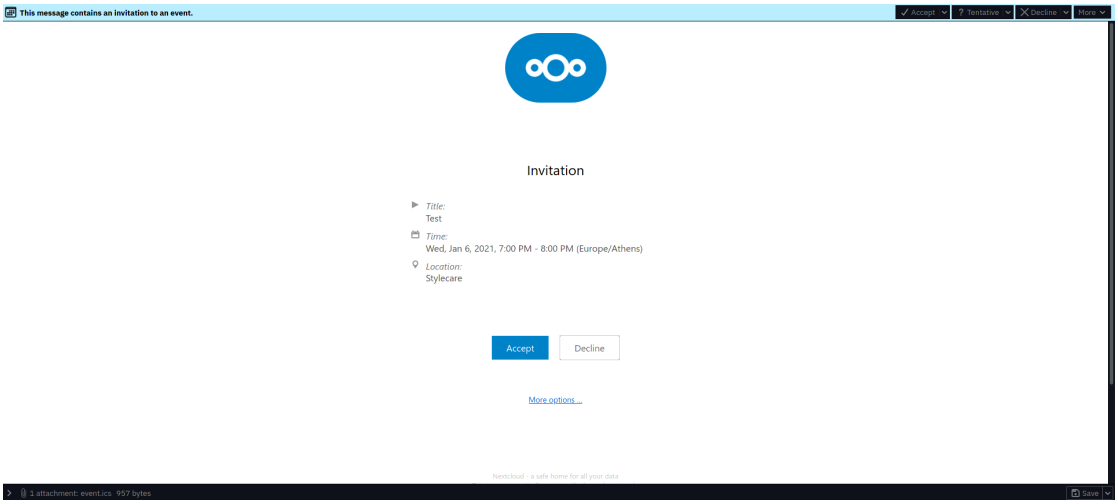

Figure 3.13: Invitation sent to an outside user

Users must be able to add, remove and edit contacts. Information stored for each contact includes: full name, multiple phone numbers, multiple emails, multiple addresses.

The application must allow synchronisation of contacts and calendars with local devices using the CalDAV and CardDAV protocols.
Priority: Medium

3.2.3 Developer

3.2.3.1 Easy development for the platform

The application must expose the necessary APIs and mechanisms that allow any developer to extend the functionality of Nextcloud by creating their own apps. These apps must be able to be installed and removed without having to reinstall the software or even reatarting the server. It is essential that documentation and app examples are provided online on the software's website in order to assist potential developers for the platform.
Priority: High

3.3 Quality of Service

3.3.1 Performance

The developers of the software must publish recommended system requirements depending on the amount of users.

Performance is important for the real-time features of the software:

- When multiple users are editing a document at the same time they should be able to see changes made by others with a 5 second delay at most.
- On live video and audio chats the server must add as little overhead as possible in order to minimise the delay.

3.3.2 Security

Security is of utmost importance as the software may be used to store sensitive or confidential files. Care should be taken that users can only access files that have explicitly been shared with them. Limited information about the configuration of the instance should be exposed to the internet in order to give as little information as possible to potential attackers. Protection agaist relativly simple to detect attacks, like brute force attacks, should be integrated into the product. TOTP based two factor authentication must be provided as an option for users to enable. Administrators should be able to configure password requirements for users.

The security of the software should be adjustable by the administrators. For instance in a corporate environment administrators might want to mandate two factor authentication for all users or set password expiration policies, something required by regulation.

Security against common attacks such as cross site scripting or SQL injection attacks must be guranteed.

The software must have an option to encrypt the data on the physical storage of the server. The encryption keys must be different for each user and managed by the server. Additionally, an option for client-side encryption could be present where the user can encrypt files with their own keys and upload them to the server.

3.3.3 Reliability

The software must ensure that it processes users' data correctly and no corruption occurs due to failure of the software. The software must inform the user about any errors that occured as not doing so can lead to data loss. For instance, a user might incorrectly think a file was uploaded successfully to the server and delete it from their local storage.

3.4 Compliance

As mentioned before, the software must offer the necessary tools for organizations to be compilant with general privacy regulation. The GDPR (General Data Protection Regulation) makes organizations liable for any violations of user privacy and deviations from a high data security standard. Legislation like the CCPA (California Consumer Privacy Act of 2018) brings similar regulation to other countries. Additional regulation exists on many sectors requiring logs tracing data changes

and file access.The software must provide logging features that are sufficient for such regulation and can be used for legal purposes. Moreover, it must provide tools that allow the administrators to act on data processing and deletion requests.

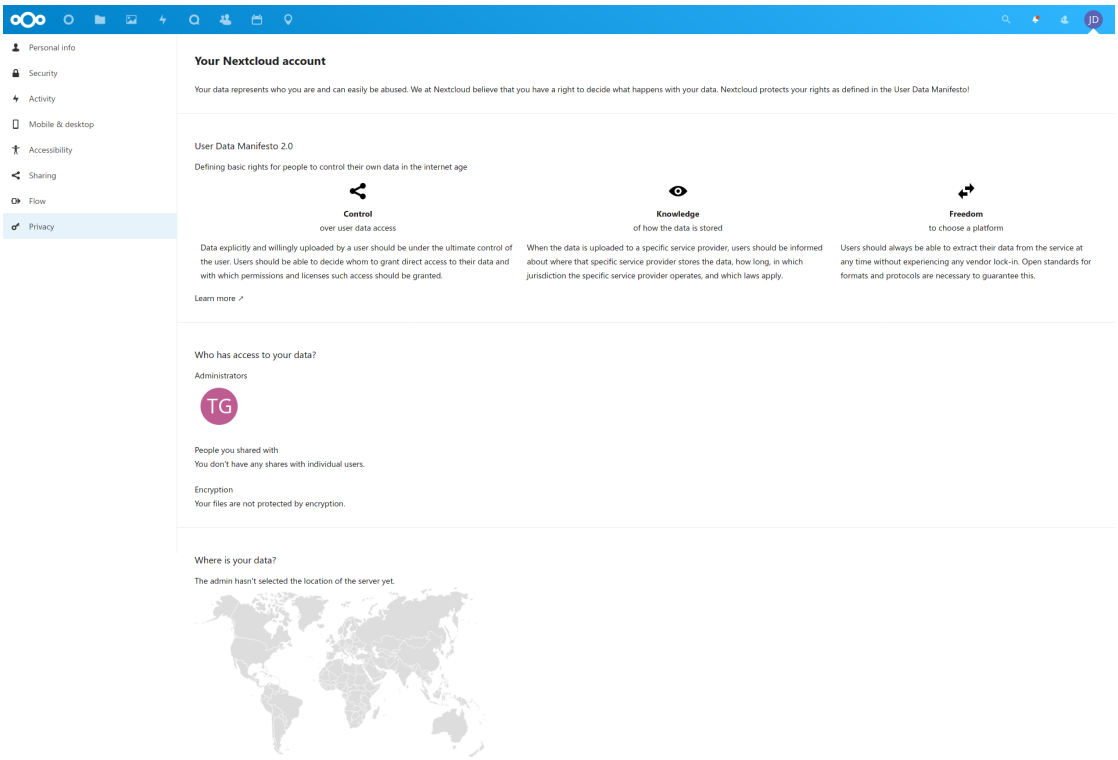

Figure 3.14: Privacy information about stored data

4 Verification

This chapter presents verification guidelines for the requirements of the previous chapter.

4.1 External Requirements

4.1.1 User interfaces

The functionality of the user interface can be tested at first by the developers and the testers of the product who should ensure the interface performs the required functions. In addition, the user interface elements that list objects, such as the file list, should be tested against extreme scenarios, like folders with hundreds of files, and ensure that the user interface remains functional. Afterwards, the interface can be presented to users who can give their feedback to the developers of the software.

4.1.2 Hardware interfaces

The shoftware should be tested on a wide range of machines to ensure that any hardware incompatibilities are found. As an example, different memory configurations should be tested to determine the minimum amount of memory required for the product. Any features that depend on specific hardware should be tested with hardware made by different manufacturers.

4.1.3 Software interfaces

The software must be confirmed to function with the database systems in the requirements section, as the database is a critical component of the application. Any features that require third party software must be tested against multiple versions of the software to eliminate any version incompatibilities. In case any incompatibilities are found they may be fixed or the specific version can be documented as incompatible. Features that have received inadequate testing should have a warning attached to them.

4.2 Functional

Each functional requirement is assigned an importance between 1 and 9. This can be used as a guideline when testing the software.

4.2.1 Administrative

4.2.1.1 User management

The integrated user management system must be tested using non-trivial datasets with multiple users and groups. An existing user dataset could be imported to verify the correct operation of the system.
Importance: 9

4.2.1.2 Integration with existing user management solutions

LDAP is a standardized protocol, so the implementation must comply with the standards. To verify the functionality the system should be tested against a widely used LDAP server, like Microsoft Active Directory or Red Hat Directory Server. It is of high importance that user information is correctly retrieved from the LDAP server
Importance: 7

4.2.1.3 User access control

Access control can be verified by setting permissions and trying them out. Care should be taken to try ways users might bypass any action control. Some examples include:

- restricting access to a certain app must completely lock the user out of it, not only hide the icon, as the user might try to access the app by its URL.
- a user that has no permission to change their password must not be able to do so by using the ”Forgot password?” button.

Importance: 9

4.2.1.4 Integration with existing authentication solutions

SAML is a standardized protocol, so the implementation must comply with the standards. Verification can be done by setting up the configuration and checking whether authentication is working correctly and the correct information is being passed to the server from the authentication provider.
Importance: 8

4.2.1.5 Audit logs

Verifying the functionality of the audit logs involves monitoring the log and asserting that performing an action creates a matching entry in the logs. The contents of the logs must contain correct information.
Importance: 7

4.2.2 User

4.2.2.1 File access

All basic file operations should be tested and ensure they are producing the expected results. File access is performed via a web browser, so the functions must be tested using many web browsers on both desktop and mobile phone operating systems.
Importance: 9

4.2.2.2 File sharing

When sharing between users in the same instance it should be ensured that sharing a file does indeed make it appear in the user's file list and that the correct permissions apply. When sharing with links, it should be ensured that the links generated are valid and can be accessed from the internet from someone without a user account at this instance. It should be certified that users can't assign wrong combinations of permissions. For example a file that can't be viewed but can be modified, or a folder which files can't be viewed but can be deleted.
Importance: 6

4.2.2.3 Real-time document collaboration

This feature involves real-time synchronisation between multiple users. The document must not be left in an undefined state. Testing the features should involve checking whether the synchronisation features work properly. For example what happens if a user tries to delete a file that others are working on, what happens if two users try to change the same word at the same time etc.
Importance: 4

4.2.2.4 Real-time communication

It should be verified that communication works reliably on both computers and smartphones.
Importance: 4

4.2.2.5 Calendar and contact management

It should be verified that invitations for events are correctly sent out to both internal and external users, that event creation and saving works and that contact information is stored correctly.
Importance: 6

4.2.3 Developer

4.2.3.1 Easy development for the platform

As some of the default features of the software come as apps the developers of the plugins who are Nextcloud developers can determine whether the available development platform is adequate or changes are needed. In addition feedback can be received from in-house developers at companies that need to extend the software in to satisfy their specific needs.
Importance: 7

4.3 Quality of service

In general, quality of service requirements are harder to verify than functional requirements.

4.3.1 Performance

To ensure the recommended system requirements are correct they should be tested at full capacity and ensure they continue functioning properly without crashing or rejecting any requests. Response time must be at most 10 seconds. This can be a realistic scenario, for instance, in a company when many employees save their documents and files as their shifts end.

4.3.2 Security

Security can be verified by a third-party organization performing an audit of the software codebase. In addition, proper code review processes during development can help identify and remove potentially dangerous code.

4.3.3 Reliability

Reliability cannot be completely verified as there is always the possibility of bugs. Reliability can be verified only by testing the software's functions at various loads and ensuring that user requests are correctly processed.