Active Directory / LDAP in Nextcloud

Integrating existing user management

Authentication and group management

Lightweight Directory Access Protocol (LDAP) servers like for example Active Directory (AD) or OpenLDAP are commonly used in large organizations to provision, authorize and manage users. Keeping user accounts in a central place simplifies user management and makes it easier for IT to keep full overview of access rights. Nextcloud supports authenticating users through the LDAP protocol and will handle properties like group membership, user details and more for one or multiple LDAP server connections in addition to local accounts.

Technical specifications

On Nextcloud side:

- Nextcloud requires the PHP LDAP module.
- The LDAP Backend must be enabled in the apps overview.

On LDAP side:

- A system user needs to be able to read the portion of the LDAP server they need.
- Password hashing must be done and ensured on the server side to enable password reset.

Benefits

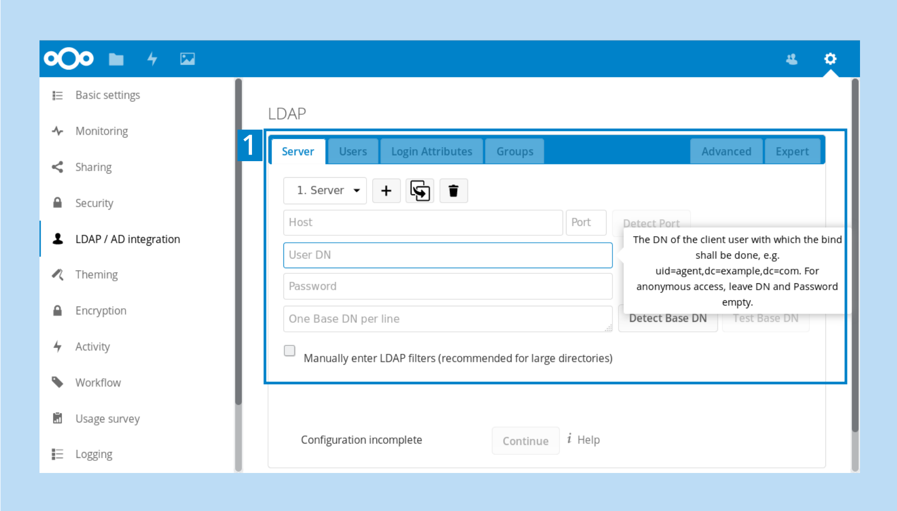
- Integrate with existing processes for provisioning and managing users
- Control access rights, sharing policies and applications in one place
- Users log in with their known company credentials, all authentication and password policies apply

How does it work?

Administrators can set up LDAP server connections from the Nextcloud Administrator Interface. Nextcloud imports users and optionally groups, enabling administrators to configure file access rights, sharing capabilities, application usage, and other Nextcloud features (1).

The configuration wizard helps with setting up filters applied to user login and listings, automatically detects some attributes, and offers to specify more fine-grained options like specialized attributes and policies (2).

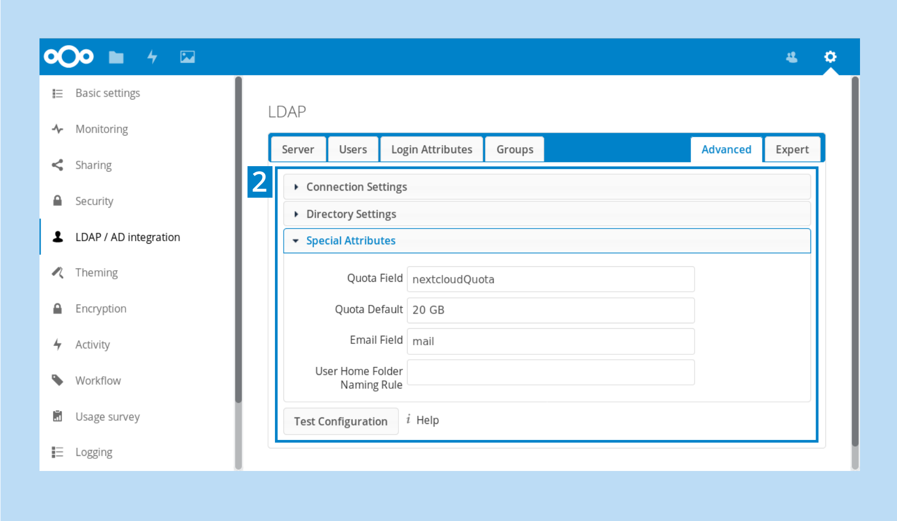
A short-lived cache helps to keep the communication to the LDAP server down while having live data. New users, group changes but also user removals have almost immediate effect.



The DN of the client user with which the bind shall be done, e.g. uid=agent,dc=example,dc=com. For anonymous access, leave DN and Password empty.

□ Manually enter LDAP filters (recommended for large directories)

Configuration incomplete



Quota Field: nextcloudQuota
Quota Default: 20 GB
Email Field: mail
User Home Folder Naming Rule:

Capabilities

- Support for multiple LDAP server connections in parallel. Other backends (like local accounts) can also be supported next to the LDAP backend.
- Server agnostic, support for OpenLDAP and Active Directory
- LDAP group support enabling file sharing with Nextcloud users/groups with support for primary groups. POSIX-like user accounts are also supported with Nextcloud 12.
- Auto-detection of LDAP attributes such as base DN, avatar, email, and others, enabling usage by the Nextcloud instance.
- Only read-only access needed, Nextcloud does not write to LDAP (except opt-in password reset which implies writing to LDAP)
- LDAP provider enables reuse of the connection for other Nextcloud apps
- (opt-in) password reset and LDAP password policy (ppolicy) support with OpenLDAP
- Detects Member-Of support on the server for better performance
- Detects users deleted from LDAP, local data is kept until admin decides to remove the remnants

Capabilities (continued)

- Dedicated bases for users and groups
- Configuration Wizards that composes the LDAP filters, unless the admin prefers to do it manually
- Each connection supports a replica (backup) server
- Search attributes for users and groups can be specified
- Support for dynamic groups
- API for managing (creating, modifying, deleting) LDAP server connections

Contact our sales team for more information:

Andreas Rode
Head of Sales

Email: sales@nextcloud.com
Phone: +49 711 896656-77

nextcoud.com