Personen und Gruppen verwalten – manuell und mit LDAP Anbindung an paedML Windows

Inhaltsverzeichnis

1 Worum geht es?

In dieser Anleitung werden Ihnen Konzepte vermittelt, wie Sie Personen in einer Nextcloud hinzufügen und sie in Gruppen verwalten können. Sowohl Personen als auch Gruppen können manuell in der Nextcloud erstellt und verwaltet werden. Für kleine Schulen mit wenigen Personen mag dies eine Möglichkeit sein, eine überschaubare Anzahl an Accounts zu verwalten.

Wenn jedoch die Personenanzahl steigt, sollten Sie in Erwägung ziehen, diese mit Ihrem Schulserver zu synchronisieren. Die Vorteile dieses Vorgehens sind vielfältig:

- Personen müssen nur in der paedML angelegt werden. Danach stehen sie automatisch auch in der Nextcloud zur Verfügung.
- Es ist nur noch ein Account notwendig mit dem man sich im Schulnetz und in der Cloud anmelden kann

- In der paedML sind Lehrkräfte automatisch der Gruppe der Lehrkräfte zugeordnet – auch diese Gruppe und die Gruppenzugehörigkeit können in die Nextcloud übernommen werden.
- Ein großer Vorteil bietet sich, wenn weitere Gruppen benötigt werden. Beispiele hierfür gibt es viele im schulischen Umfeld:
  - Klassen- oder Jahrgangsteams,
  - Fachschaften,
  - Schulische Arbeitsgruppen z.B. die Steuergruppe.
- Die Zusammensetzung der vorher genannten Beispiele ändert sich immer wieder, besonders beim Schuljahreswechsel. Das manuelle Nachvollziehen dieser Änderungen bedeutet viel Arbeit. Daher sollten für diese Arbeiten andere Lehrkräfte hinzugezogen werden, ohne dass diese administrativen Zugang zur Nextcloud haben müssen. Dies kann über Projekte erfolgen, die in der Schulkonsole verwaltet werden können. So kann beispielsweise die leitende Person einer Fachschaft die Aufgabe erhalten, die Mitglieder der Fachschaft in der Schulkonsole über ein Projekt zu pflegen. Alle Mitglieder können dann automatisch auf einen Ordner mit Material der Fachschaft zugreifen.

Wichtig: Allerdings muss auf einen Nachteil hingewiesen werden: Ist der Schulserver nicht über das Internet erreichbar, ist eine Nutzung der Cloud nicht möglich. Zudem muss bei einer Neuinstallation des Schulservers darauf geachtet werden, dass die Benutzer wieder dieselben Anmeldenamen erhalten.

2 Voraussetzungen und Vorüberlegungen

Folgende Voraussetzungen müssen in der Nextcloud erfüllt sein:

- Die App *LDAP user and group backend* muss installiert sein.
- Der Schulserver muss für den LDAPS Anbindung konfiguriert sein. Hierzu gibt es Anleitungen vom LMZ, z. B. für die Anbindung von Moodle.

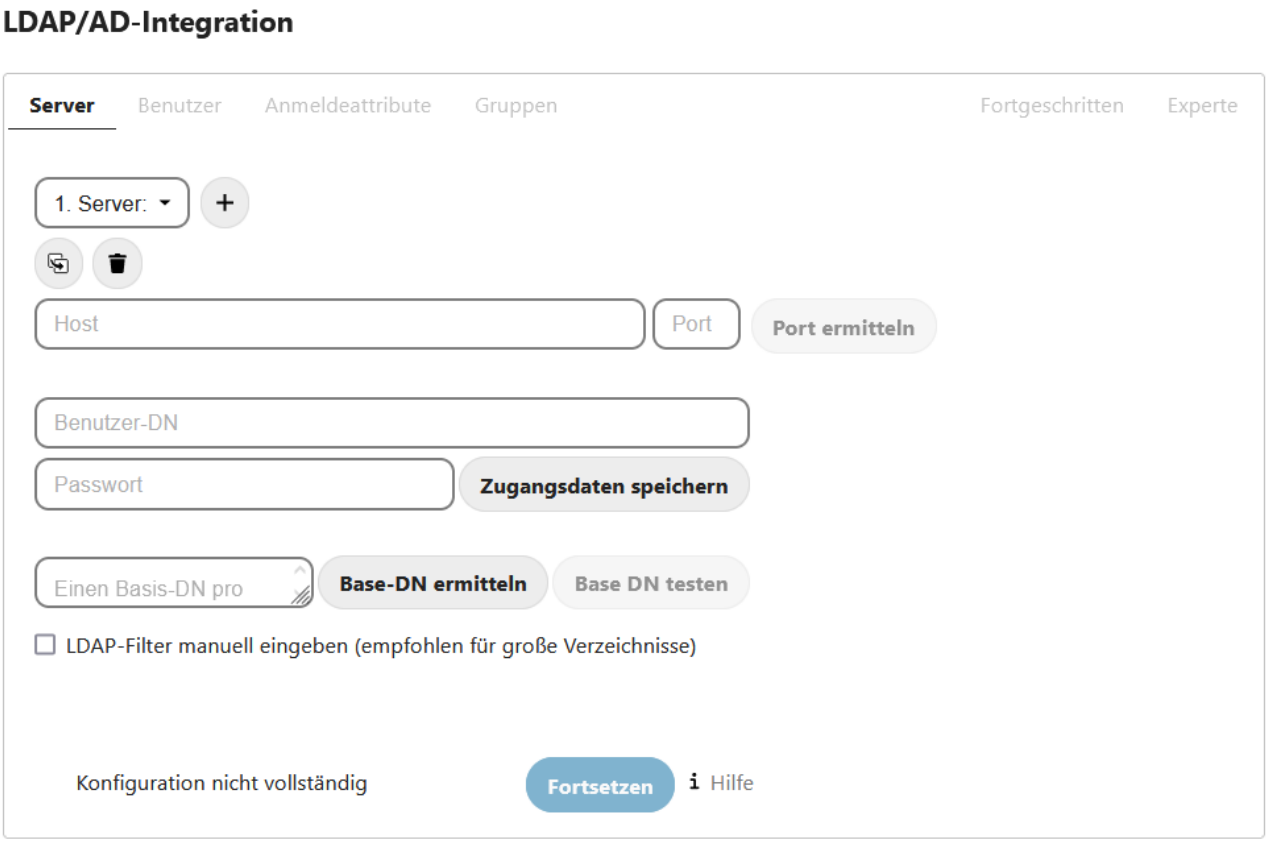
3 LDAPS Anbindung in der Nextcloud konfigurieren

In den folgenden Einrichtungsschritten wird davon ausgegangen, dass die paedML bereits gemäß der LMZ-Anleitung für die LDAP-Anbindung von Moodle konfiguriert ist. Hierbei ist zu beachten, dass der externe Zugriff auf die paedML normalerweise über den externen Namen der Octogate (z. B. abcdefgh.ozone.octogate.de) erfolgt.[1]

1 In einer Fortbildung in einem Fortbildungsraum ist dies nicht möglich, da der externe Name der Octogate bei allen Teilnehmenden der Fortbildung gleich wäre und somit die externe Erreichbarkeit nicht eindeutig wäre.

Die Einstellungen für die LDAP-Anbindungen finden Sie anschließend im Bereich *Administratoreinstellungen | LDAP/AD-Integration*.

Im Bild sehen die die erste Ansicht der Konfigurationseinstellungen.



Bildschirmfoto: Startseite Konfiguration LDAP von Nextcloud GmbH [CC BY-SA 4.0]

Zu erkennen ist, dass die Konfiguration die Bereiche *Server*, *Benutzer*, *Anmelde-Attribute* und *Gruppen* umfasst. Diese werden nun detailliert behandelt.

3.1 Registerkarte Server

Auf der Registerkarte *Server* müssen Sie mindestens Eintragungen in den Feldern *Host*, *Port* *Benutzer-DN*, *Passwort* und *Basis-DN* vornehmen. Die Bedeutung der Felder wird nachfolgend erläutert:

- *Host*: Hier tragen Sie ein, unter welcher Adresse die Firewall von außen erreichbar ist. Die Adresse besteht aus zwei Teilen: *Protokoll + Adresse.* Das Protokoll lautet `ldaps` . Als Adresse trägt man den Namen, unter dem die Firewall Octogate von außen erreichbar ist. Für die Firewall Octogate, die bei den meisten paedML Windows Lösungen im

Stattdessen wird in der Fortbildung ein separater Domainname in der Form xxxx.zsl-server.de mit einem abweichenden Port verwendet, um die jeweilige Schulungsumgebung eindeutig von extern aus erreichbar zu machen. Die fortbildende Person wird Ihnen die notwendigen Serverdaten für den LDAP-Zugriff auf die eigene Schulungsumgebung mitteilen, damit Sie die nachfolgenden Konfigurationsschritte durchführen können.

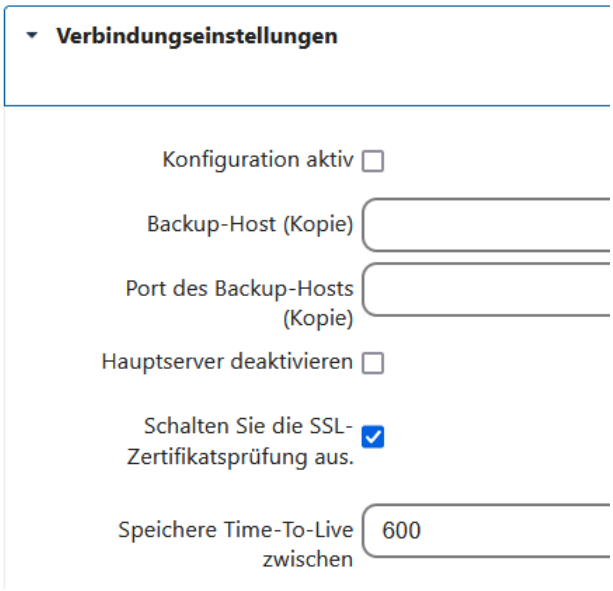
Einsatz ist, besteht diese Adresse aus dem Namen der Octogate Instanz und dem Suffix `ozone.octogate.de`. Lautet der Name der Octogate `abcdefgh` ergibt sich daraus die Adresse `abcdefgh.ozone.octogate.de`.[2] In diesem Fall ist unter Host einzutragen: `ldaps://abcdefgh.ozone.octogate.de`.

- *Port*: Für das Protokoll *ldaps* wird standardmäßig Port *636* verwendet. Sie können bei der Nextcloud von diesem Port abweichen und einen anderen Port verwenden, um die Sicherheit zu erhöhen. Ein abweichender Port muss in der Portweiterleitung der Firewall berücksichtigt werden.
- *Benutzer-DN*: Hier wird der Benutzer benötigt, unter dessen Account für die LDAP Anfrage ausgeführt wird. Hierfür richtet man einen speziellen Benutzer ein. Ein solcher Benutzer wird als *LDAP Bild User* bezeichnet. *DN* steht für *Distinguished Name*. Einfach gesagt ist das der Name des Benutzers und dessen Position im Active Directory – in einer ganz speziellen Schreibweise. Geben Sie ein: `CN=ldapbinduser,OU=_ServiceAccounts,DC=musterschule,DC=schule,DC=paedml`
- *Passwort*: Passwort des *LDAP Bild Users eingeben.*
- *Base-DN*: Dies ist die Position im Actice Directory, unterhalb der sich die Benutzenden im Active Directory befinden – wieder in einer speziellen Schreibweise. Setzen Sie einen Haken bei *LDAP-Filter manuell eingeben (empfohlen für große Verzeichnisse).* Geben Sie hier ein: `DC=musterschule,DC=schule,DC=paedml`.

Zum Test der Einstellungen klicken Sie (eigentlich) auf die Schaltfläche *Base DN testen*. Doch auch wenn alle Eingaben richtig vorgenommen wurden, erscheint unten im Fenster noch die Meldung „Konfiguration nicht korrekt“. Grund hierfür ist eine Zertifikatsproblematik, deren Erklärung den Rahmen dieser Anleitung sprengen würde. Zur Behebung des Problems, wählen Sie rechts oben im Fenster *Fortgeschritten*.

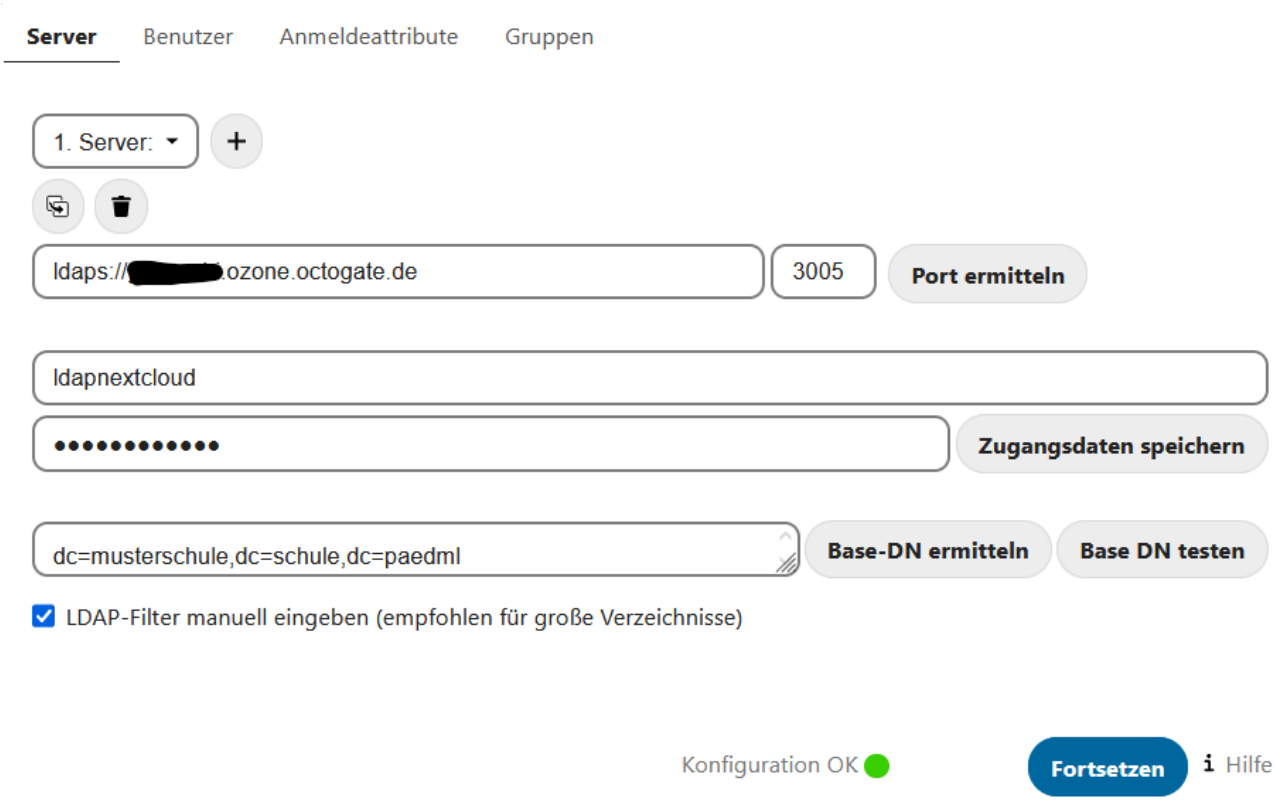
Unter Verbindungseinstellungen setzen Sie einen Haken bei „Schalten Sie die SSL Zertifikatsprüfung aus“.

2 Die tatsächliche Überprüfung der Anmeldeinformationen erfolgt nicht durch die Firewall, sondern durch den Server, auf dem das Active Directory läuft. Dies ist bei einer paedML Windows der Server DC01. Durch eine Portweiterleitung in der Firewall wird die LDAPS Anfrage an den Server DC01 weitergeleitet.



Bildschirmfoto: SSL Zertifikatsprüfung ausschalten von Nextcloud GmbH [CC BY-SA 4.0]

Kehren Sie zurück zur Registerkarte Server und klicken Sie erneut auf die Schaltfläche *Base DN testen*. Nun sollte die Verbindung hergestellt werden können. Sie erkennen es unten im Fenster an der Meldung „Konfiguration OK“.



Bildschirmfoto: Erfolgreiche Verbindungseinstellungen von Nextcloud GmbH [CC BY-SA 4.0]

Beachten Sie beim Testen, dass es immer wieder zu falschen Fehlermeldungen kommt. Probieren Sie es mehrfach. Klicken Sie auf *Fortsetzen*, um zur Registerkarte Benutzer zu kommen.

3.1.1 Optionale Anpassung der Base-DN

Bisher ist als Base-DN eigetragen: `DC=musterschule,DC=schule,DC=paedml.`

Dies bewirkt, dass das gesamte Active Directory durchsucht wird. Optional können Sie nur die Orte angeben, in denen tatsächlich die Benutzenden und die Gruppen gefunden werden.

Der LDAP Bind User befindet sich hier:

`ou=_serviceaccounts,dc=musterschule,dc=schule,dc=paedml`

Alle Lehrkräfte:

`ou=lehrer,ou=benutzer,dc=musterschule,dc=schule,dc=paedml`

Alle Schülerinnen und Schüler:

`ou=schueler,ou=benutzer,dc=musterschule,dc=schule,dc=paedml`

Alle Gruppen wie Projektgruppen, Lehrkräfte einer Schulart, Schülerinnen und Schüler einer Schulart oder einer Klasse:

`ou=fileshare,ou=sicherheitsgruppen,dc=musterschule,dc=schule,dc=paedml`

Die Gruppen aller Lehrkräfte G_Lehrer und die aller Schülerinnen und Schüler G_Schueler:

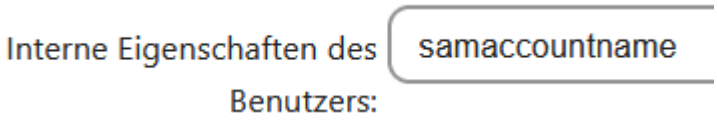
`ou=Active Directory,ou=sicherheitsgruppen,dc=musterschule,dc=schule,dc=paedml`

Tragen Sie im Feld Base-DN nur die Zeilen ein, die tatsächlich benötigt werden.

3.2 Registerkarte Benutzer

Bevor nun Benutzende mit der Nextcloud synchronisiert werden, stellen wir ein, dass für die Synchronisation der Kontos der *Anmeldenamen* verwendet wird. Tut man dies nicht, werden Benutzende mit einer kryptischen UUID angelegt. Dass statt der UUID der Anmeldename verwendet wird, ist besonders wichtig, wenn Sie irgendwann den Schulserver neu installieren und die Benutzerkonten erneut erstellen müssen. Dann ändert sich nämlich die UUID und die Benutzenden können nicht mehr auf ihr Nextcloudkonto zugreifen. Mit dem Anmeldenamen gelingt dies. Die Bezeichnung des Benutzernamens in LDAP lautet *samaccountname*.

Klicken Sie im Fenster rechts oben auf *Experte* und tragen Sie im Feld *Interne Eigenschaften des Benutzers* den Text `samaccountname` ein.

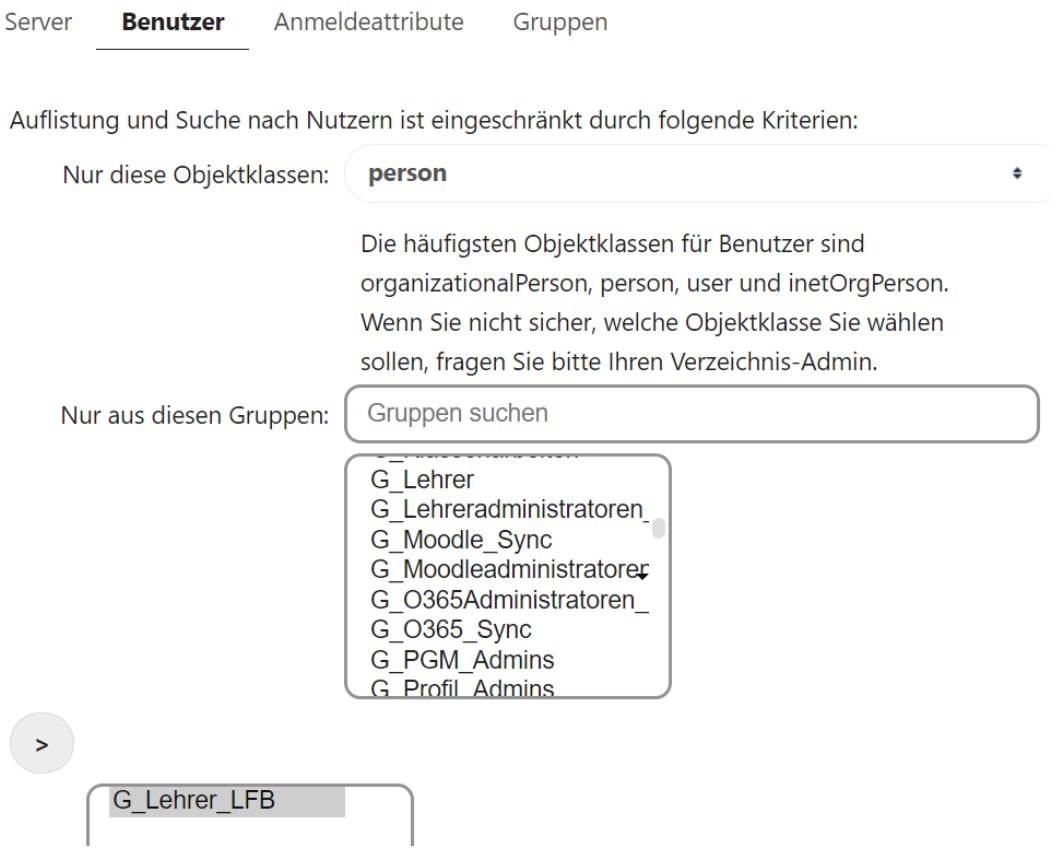


Bildschirmfoto: Benutzernamen für Anmeldung festlegen von Nextcloud GmbH [CC BY-SA 4.0]

In der Registerkarte *Benutzer* suchen Sie nun die Gruppen aus dem Active Directory aus, deren Mitglieder Zugang zur Nextcloud haben sollen.

Klicken Sie auf *LDAP-Abfrage bearbeiten*. Bestätigen Sie die nachfolgende Meldung, dass der Modus umgeschaltet wird, mit Ja. Sie erhalten diese Ansicht:

Im oberen Auswahlfenster sehen Sie alle Gruppen, die unterhalb der Base DN gefunden werden. Mittels des Pfeils verschiebt man diese Gruppe ins untere Feld.



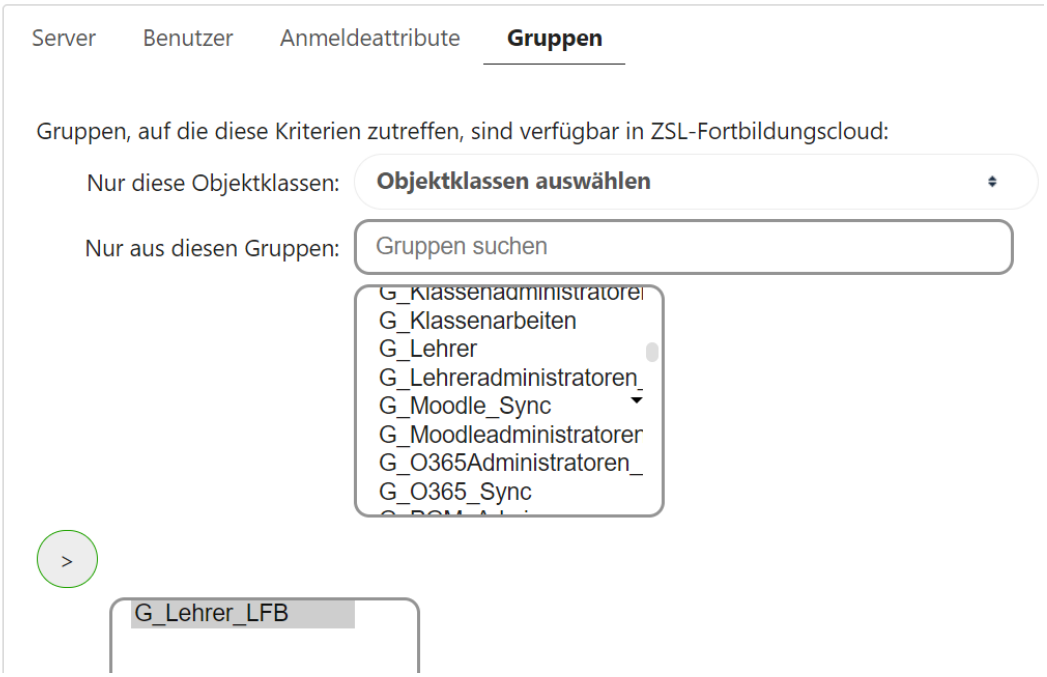
Bildschirmfoto: Gruppe G_Lehrer ausgewählt von Nextcloud GmbH [CC BY-SA 4.0]

In unserem Beispiel soll die Gruppe aller Lehrkräfte der Schulart LFB hinzugefügt werden. Dies ist die Gruppe *G_Lehrer_LFB*. Markieren Sie im oberen Feld die Gruppe *G_Lehrer_LFB* und bewegen Sie diese über die Schaltfläche > ins untere Feld.

Klicken Sie dann auf *Fortsetzen* um auf die Registerkarte *Anmeldeattribute* zu gelangen. Hier klicken Sie auf *Fortsetzen*, da dort keine Änderungen vorgenommen werden müssen.

3.3 Registerkarte Gruppen

In der Registerkarte *Gruppen* legen Sie fest, welche Gruppen in die Nextcloud übertragen werden sollen. Diese Gruppen stehen dann in der Nextcloud zur Verfügung, um z.B. Berechtigungen für Gruppenordner zu erteilen oder Ressourcen wie einen Kalender mit der Gruppe zu teilen. Wählen Sie erneut den Gruppennamen *G_Lehrer_LFB* aus. Beachten Sie dabei, dass hier nicht die einzelnen Personen der Gruppe, sondern nur die eigentliche Gruppe ausgewählt wird. Diese Registerkarte wird zu einem späteren Zeitpunkt relevant, wenn in der paedML Windows Projektgruppen erstellt werden.



Bildschirmfoto: Gruppe G_Lehrer ausgewählt von Nextcloud GmbH [CC BY-SA 4.0]

Anschließend ist die LDAP-Konfiguration abgeschlossen und nach kurzer Zeit können sich alle Mitglieder der synchronisierten Gruppen mit denselben Daten in der Nextcloud anmelden wie im Schulnetz.

4 Gruppen verwalten durch Projekte in der paedML Windows

Werden in der Nextcloud nun zusätzliche Gruppen benötigt, kann dies durch Projektgruppen umgesetzt werden, die in der paedML Windows erzeugt und gepflegt werden. Diese Vorgehensweise hat den Vorteil, dass Projektgruppen von Lehrkräften verwaltet werden können und nicht alle Änderungen von den Administrierenden der Nextcloud durchgeführt werden müssen.

Projekte werden in der paedML Windows von Lehrkräften erstellt. In Projekten gibt es zwei Rollen: *Projektleiter* und *Projektmitglieder*. Projektleiter können im Wesentlichen andere

Projektleiter und Projektmitglieder hinzufügen und entfernen. *Wichtig* ist, dass alle Personen, die in der Nextcloud einer Gruppe angehören sollen, in der paedML *Projektmitglieder* sind. Projektleiter sind nicht automatisch Projektmitglieder, sondern müssen auch zu den Projektmitgliedern hinzugefügt werden. Näheres zur Verwaltung von Projekten entnehmen Sie dem Handbuch für Lehrkräfte zur paedML Windows.

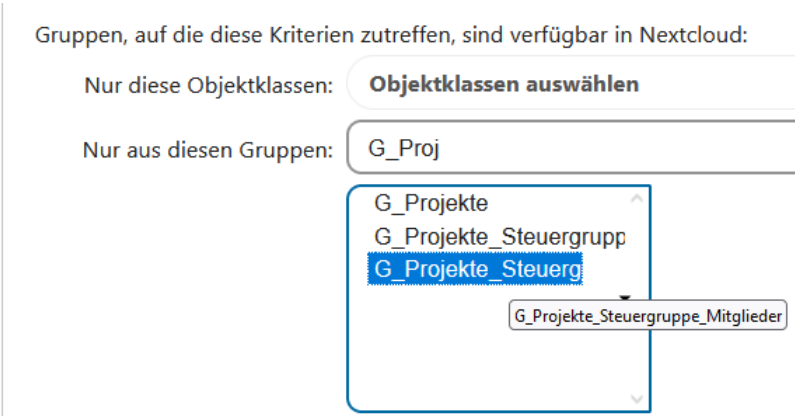
Das Vorgehen der Verwaltung von Gruppen durch Projektgruppen in der paedML wird am Beispiel einer Steuergruppe demonstriert.

4.1 Projektgruppe in paedML erzeugen

In der paedML Windows ist es nur Lehrkräften möglich, Projekte zu erstellen. Daher sind die nachfolgenden Konfigurationen von einer Lehrkraft durchzuführen. Erstellen Sie als Lehrkraft über die Schulkonsole ein Projekt namens *Steuergruppe* und fügen Sie alle Mitglieder der Steuergruppe hinzu. Beachten Sie, dass Projektleiter NICHT automatisch in der Gruppe der Projektmitglieder enthalten sind. Daher muss sich die Projektleitung auch selbst als Mitglied hinzufügen.

4.2 Projektgruppe in LDAP-Integration einbinden

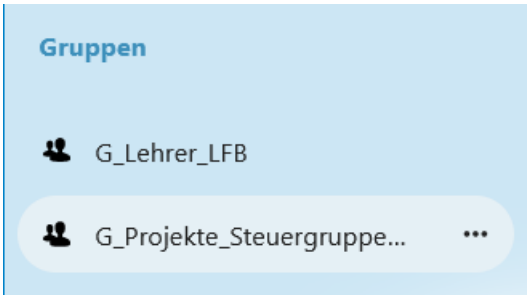
Nun soll die vorher erzeugte Projektgruppe in die Nextcloud eingebunden werden. Verschieben Sie hierzu in der Registerkarte „Gruppen“ der *LDAP/AD-Integration* die Gruppe *G_Projekte_Steuergruppe_Mitglieder* in das untere Feld. Diese Aufgabe wird dadurch erschwert, dass der Name der Gruppe zu lang für das Feld ist und so nicht erkennbar ist, welches die Gruppe mit der Leitung ist und welche die Mitglieder enthält. Abhilfe schafft es, mit der Maus über die Gruppe zu fahren, dann erscheint der gesamte Gruppenname.



Bildschirmfoto: Anzeige des gesamten Gruppennamens durch Mouseover von Nextcloud GmbH [CC BY-SA 4.0]

Verschieben Sie die Gruppe ins untere Feld, um die Gruppe in der Nextcloud verwenden zu können.

Wechselt man nun im Administratormenü zu den Benutzern, sieht man unter den Gruppen die Gruppe *G_Projekte_Steuergruppe_Mitglieder*



Bildschirmfoto: Erfolgreich hinzugefügte Steuergruppe von Nextcloud GmbH [CC BY-SA 4.0]

Berücksichtigen Sie, dass die Pflege der Gruppe ausschließlich über die Schulkonsole in der paedML Windows erfolgt. Die Gruppe ist dynamisch. Das heißt, Änderungen an den Mitgliedern in der Schulkonsole werden automatisch auch in der Nextcloud übernommen. Nachdem die Struktur einmal erstellt wurde, können die Mitglieder der verschiedenen Gruppen einfach über die Schulkonsole aktualisiert werden.