

Aufgabenstellung Ausgangslage	1
Projektmitglieder.....	2
Aufgabenbereiche	2
Baumstruktur.....	4
LDIF	4
Server Konfiguration.....	5
LDAP-Installation	5
Konfigurationsdatei slapd.....	5
Import des rfc2307bis Schemas	7
LDAP Commands	7
Access Control List.....	8
Erteilung von Berechtigungen	8
Client.....	10
Installation und Konfiguration	10
Backup	11
Skript.....	11
Ausführen des Backups	11
Restore.....	11
Graphische Oberfläche	12
Verbindung zum LDAP-Server herstellen.....	12
Integration von NextCloud	13
Installation des NextCloud Servers am “LDAP-Server“	13
Client-Integration.....	18

Aufgabenstellung | Ausgangslage

Im Unternehmen wird Ubuntu als Betriebssystem auf den Client-Rechnern eingesetzt. Um die Rechner zu verwalten, wird eine Benutzerverwaltung verwendet, welche folgende Gruppen unterscheidet: Administrator, Management, Office, Production. Mit Hilfe der Gruppen soll eine vernünftige Zugriffsregelung/Rechte implementiert werden.

Für das Speichern der Daten in der Cloud wurde vom Unternehmen NextCloud gewählt. Der Login Prozess und der Verwaltung der Rechte soll mit der zentralen Benutzerverwaltung gesteuert werden.

Projektmitglieder

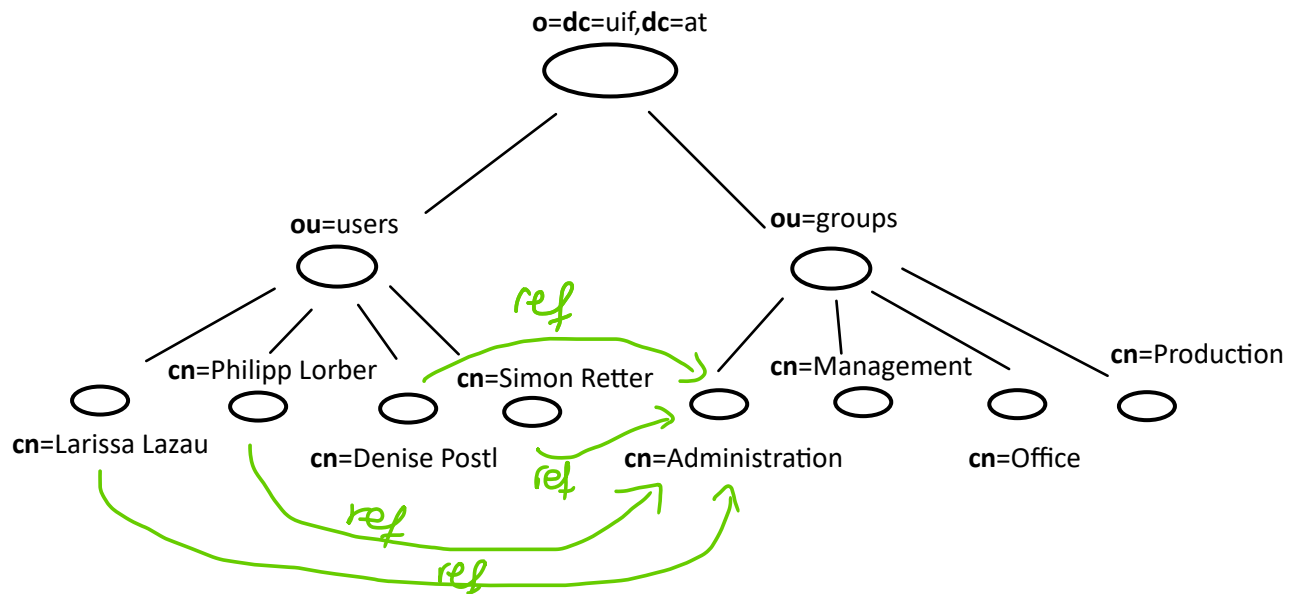
- Larissa Lazău
- Simon Retter
- Philipp Lorber
- Denise Postl

Aufgabenbereiche

Aufgabenbereich	Durchgeführt von
<ul style="list-style-type: none">• Aufsetzen des LDAP-Clients und Baumstruktur (10.01.2024)• ACLs, Baumstruktur fertig geplant und erstellt (17.01.2024)• Backup-Strategie Lösungsansätze versucht zu finden und ausprobiert (24.01.2024)• LDAP-Client (31.01.2024)• LDAP-Client, Mitgeholfen beim Server-NextCloud (07.02.2024)• LDAP-Client Integration (14.02.2024)• Dokumentation geschrieben (28.02.2024)	Larissa Lazău
<ul style="list-style-type: none">• Baumstruktur erstellen (10.01.2024)• Baumstruktur fertigstellen + ACL erstellen (16.01.2024)• Denise mit dem Aufsetzen des LDAP-Servers helfen (10.01.2024 - 24.01.2024)• Denise mit der Client implementation + Philipp mit NextCloud helfen (31.01.2024 - 16.02.2024)• Dokumentation (28.02.2024)	Simon Retter
<ul style="list-style-type: none">• Tutorial für Nextcloud Version 20.0.1 anfangen (10.01.2024)• Nextcloud Probleme mit Version 20.0.1 (17.01.2024 - 24.01.2024)• Nextcloud Version 20.0.1 funktioniert (31.01.2024)• Anfang von Installation Nextcloud Version 28.0.1 (31.01.2024)• Kleine Probleme mit nextcloud config (07.02.2024)• Nextcloud Version 28.0.1 komplett funktionsfähig (14.02.2024)	Philipp Lorber
<ul style="list-style-type: none">• Aufsetzen des LDAP-Servers (10.01.2023)	Denise Postl

- Definition & einspielen der .ldif Dateien (16.01.2023)
- Backup-Strategie - Baumstruktur als .ldif Datei exportieren und wieder einspielen (24.01.2023)
- Visuelle Version -> Installation von jxplorer und Herstellung der Verbindung zum LDAP-Server (31.01.2023)
- NextCloud Server aufgesetzt auf VM des LDAP-Servers -> Installation des php-ldap Moduls -> Verknüpfung mit LDAP-Server, Import der Kontakte/Gruppen (07.02.2023, 16.02.2023)
- Client Integration -> Installation der libnss-ldapd Bibliothek & Anpassung des Host Files der nslcd.conf, um den LDAP-Server zu definieren und zu erreichen (16.02.2023)
- Installation von NextCloud Desktop um anschließend die Integration der berechtigten Kontakte für NextCloud zu testen (16.02.2023)
- Dokumentation der Baumstruktur, LDIF, Server-Konfiguration, LDAP Commands, Access Control List, Client Integration, Backup, Visuellen Version (28.02.2023)

Baumstruktur



Dies wäre ein dynamischer Ansatz. Für ein größeres Unternehmen wäre dieser Ansatz auch der Bevorzugte. Benutzerinformationen werden auf Referenzen abgebildet und gesucht kann nach der ID werden. Beispielsweise soll ein Benutzer kurzzeitig administrative Tätigkeiten übernehmen. Somit erhält er eine Referenz auf die entsprechende Gruppe. Mittels der ACL (Access Control List) werden der Gruppe die notwendigen Berechtigungen gegeben. Um den Benutzer die administrativen Berechtigungen wieder zu entziehen, muss nur mehr die Referenz auf die Gruppe gelöscht werden:

member: uid=mmustermann,ou=office,dc=uif,dc=at.

member-uid: 20001

gid: 30000

Der Vorteil bei diesem Ansatz besteht darin, dass nicht kreuz und quer gemappt werden muss.

LDIF

LDIF steht für „LDAP Data Interchange Format“ (LDAP-Datenaustauschformat) und ist ein Textformat, das verwendet wird, um LDAP-Verzeichnisdienstinformationen zu repräsentieren. Es handelt sich im Wesentlichen um eine einfache Möglichkeit, Daten in einem bestimmten Format zu speichern, um sie zwischen verschiedenen LDAP-kompatiblen Systemen zu importieren oder zu exportieren. LDIF-Dateien können verwendet werden, um Verzeichniseinträge wie Benutzer, Gruppen, Organisationseinheiten und andere LDAP-Objekte zu erstellen, zu ändern oder zu löschen.

Schlüssel die verwendet werden können.

o	Organization.
ou	Organizational Unit.
cn	Common Name.
sn	Surname.
givenname	First Name.
uid	User ID.
mail	E-Mail des Benutzers.

Server Konfiguration

Im folgenden Abschnitt wird näher beschrieben, wie der LDAP-Server aufgesetzt wurde. Bei der Verwendung des Betriebssystems wurde sowohl beim Server als auch auf dem Client auf ubuntu gesetzt.

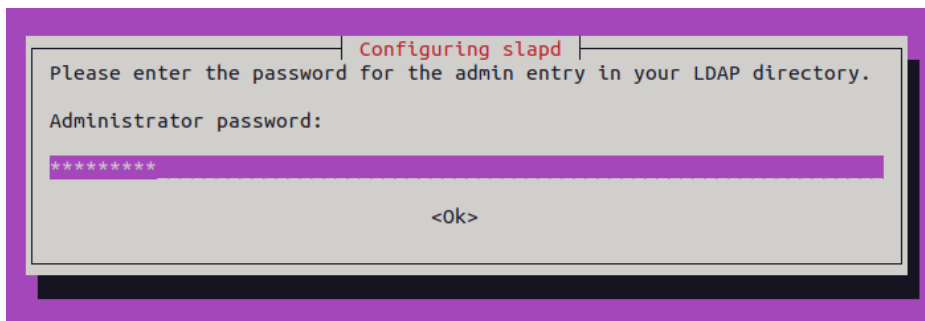
LDAP-Installation

Folgende Pakete sind erforderlich zu installieren:

```
sudo apt-get install ldap-utils slapd
```

- ldap-utils: beinhaltet die Command-Palette (ldap- /search/add/modify...).
- slapd: ist der daemon (service).

Nach Abschluss der Installation sind einige Einstellungen vorzunehmen. Es wird nach dem Administrator Passwort gefragt:



Unter /etc/hosts kann der Host-Name geändert werden. Da später Clients ins Directory integriert werden sollen, wurde ein eigenes internes Netzwerk konfiguriert. Zu dieser IP-Adresse wurde dann ein definierter Domainname gemappt unter dieser der LDAP-Server erreichbar sein soll.

```
192.168.1.8          uif.at ldap.uif.at
```

Optional kann der Hostname geändert werden:

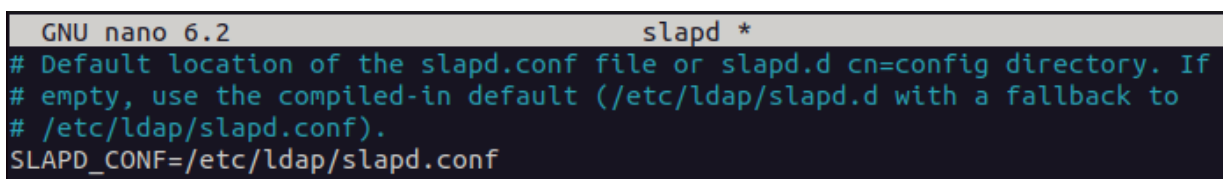
```
sudo hostnamectl set-hostname uif.at
bash
```

Konfigurationsdatei slapd

Bevor Konfigurationsänderungen vorgenommen werden, ist es wichtig, dass slapd nicht läuft – um zu vermeiden, dass etwas unabsichtlich überschrieben wird. Mittels `sudo systemctl stop slapd` wird das Service gestoppt.

Anschließend ist im `slapd` der Pfad für die `slapd.conf` anzugeben. Im `slapd.conf` befinden sich allgemeine Konfigurationseinstellungen wie zum Beispiel die Datenbank (auch Ablageort), Basis-Distinguished Name, Root-User, inkludierte Schema's, Access Control List,...

```
sudo vi /etc/default/slapd
```



Mit der Installation von ldap kommen dynamische DB's mit. Da diese nicht verwendet werden sind sie zu löschen:

```
root@uif:/var/lib/ldap# ls
data.mdb lock.mdb
root@uif:/var/lib/ldap# sudo rm *.mdb
```

Die slapd.conf ist die Konfigurationsdatei für den OpenLDAP-Server. Sie enthält Einstellungen wie Serverparameter, Sicherheitsrichtlinien und Verbindungsparameter. Zu Beginn werden die verwendeten Schema's definiert. Durch die Bearbeitung dieser Datei kann die Konfiguration des LDAP-Servers angepasst und gesteuert werden.

```
GNU nano 6.2      slapd.conf *
pidfile           /var/run/slapd/slapd.pid
argsfile          /var/run/slapd/slapd.args
modulepath        /usr/lib/ldap
moduleload        back_mdb
# Maximal 1000 Werte bei einer Suche zurück geben
sizelimit 1000
# Anzahl CPUs, die für das Indexing verwendet werden
tool-threads 2
#####
# Datenbank Nummer 1
database          mdb Datenbank
# Der Basis-DN Basis Distinguished Name
suffix            dc=uif,dc=at
# Root-User
rootdn            cn=admin,dc=uif,dc=at
rootpw            {SHA}PhXd/2trgnEtdoTixm1FtmFbR24=
# Ablageort der Datenbank
directory         "/var/lib/ldap"
```

Definition des Root-Users

Diese Reihenfolge ist erforderlich aufgrund der Baumstruktur. Es wird immer vom unteren „Knotenpunkt“ zum oberen gearbeitet. (cn – dc/o)

Ein Passwort kann folgendermaßen gehasht werden:

```
sudo slappasswd -h '{SSHA}' -s 'Kennwort1'
```

-s: Definiert String – Passwort

Für das hashen wird der SSHA-Algorithmus verwendet.

Im slapd.conf ist auch die Access Control List definiert. Diese kann auch ausgelagert werden, der Pfad zur ACL ist anzugeben. Eine detaillierte Beschreibung befindet sich im Abschnitt Access Control List.

```
# Access Control Lists
access to attrs=userPassword,shadowLastChange
    by dn="cn=admin,dc=uif,dc=at" write
    by anonymous auth
    by self write
    by * none
access to *
    by dn="cn=admin,dc=uif,dc=at" write
    by * read
access to dn.base=""
    by * read
```

Import des rfc2307bis Schemas

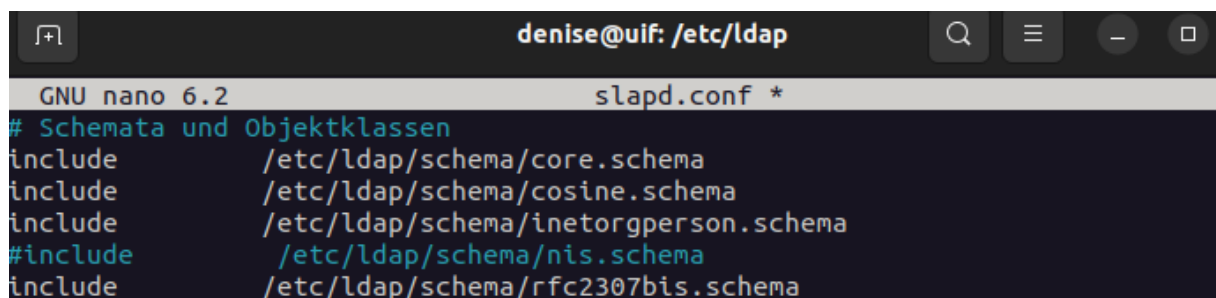
Um eine eindeutige Verbindung zwischen Benutzern und Gruppen herzustellen ist das member Attribut für eine Gruppe erforderlich. Damit dieses verwendet werden kann ist das rfc2307bis Schema zu importieren, da das member Attribut im Standard nis Schema nicht definiert ist. RFC steht für Request for Comments und diese sind eine Reihe technischer und organisatorischer Dokumente in denen Protokolle, Konzepte, Methoden und Programme des Internets behandelt, beschrieben und definiert werden.

Das Schema ist in einem eigenen File zu speichern und ist unter folgendem GitHub-Repository zu finden:

<https://github.com/jtyr/rfc2307bis>

```
denise@uif:/etc/ldap/schema$ sudo nano rfc2307bis.schema
```

Im slapd.conf ist das Schema zu inkludieren, das nis Schema wird nun nicht mehr benötigt und kann auskommentiert werden.



```
denise@uif: /etc/ldap
GNU nano 6.2      slapd.conf *
# Schemata und Objektklassen
include           /etc/ldap/schema/core.schema
include           /etc/ldap/schema/cosine.schema
include           /etc/ldap/schema/inetorgperson.schema
#include          /etc/ldap/schema/nis.schema
include           /etc/ldap/schema/rfc2307bis.schema
```

Nach der Übernahme der Konfigurationen ist das slapd Service wieder zu starten. Um zu überprüfen, ob slapd richtig läuft kann der Status abgerufen werden. Kommt eine Fehlermeldung ist die Konfiguration im slapd.conf fehlerhaft.

```
sudo systemctl start slapd
```

```
denise@denise:~$ sudo systemctl status slapd
● slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access>
   Loaded: loaded (/etc/init.d/slapd; generated)
   Drop-In: /usr/lib/systemd/system/slapd.service.d
            └─slapd-remain-after-exit.conf
   Active: active (running) since Wed 2024-01-10 11:43:29 CET; 40s ago
```

LDAP Commands

Mithilfe von LDAP-Commands kann die aufgebaute Baumstruktur ergänzt, manipuliert, gelöscht oder abgerufen werden.

Add

Wird verwendet um eine neue .ldif Datei einzuspielen.

```
sudo ldapadd -x -D "cn=admin,dc=uif,dc=at" -w Kennwort1 -f users.ldif
```

Modify

Wird verwendet, um einen bestehenden Eintrag mit angepassten Informationen zu modifizieren.

```
sudo ldapmodify -x -D "cn=admin,dc=uif,dc=at" -w Kennwort1 -f modify_users.ldif
```

Search

Wird verwendet, um bestehende Einträge im Verzeichnis anzuzeigen.

```
sudo ldapsearch: sudo ldapsearch -x -D "cn=admin,dc=uif,dc=at" -b "dc=uif,dc=at" -H "ldap://ldap.uif.at" -w Kennwort1
```

Delete

Wird verwendet, um bestehende Einträge aus dem Verzeichnis zu löschen.

```
sudo ldapdelete "cn=office,ou=groups,dc=uif,dc=at"
```

- x Einfache Authentifizierung – die Authentifizierung mit Klartextpasswort aktivieren.
- D Gibt den Distinguished Name an, unter dem die Bindung oder Authentifizierung erfolgen soll.
- b Legt den Basis-DN für Suchoperationen fest, d.h., den Startpunkt der Suche im LDAP-Verzeichnisbaum.
- f Das File, das verwendet werden soll.
- w Passwort direkt als String angeben.
- H Spezifiziert die URL des LDAP-Servers, einschließlich Protokoll, Hostname und Portnummer.

Access Control List

Access Control Lists dienen der Rechteverwaltung. Mithilfe von Access Control Lists kann gesteuert werden, welche Benutzer bzw. welche Gruppen welche Berechtigungen erhalten.

Bei der Rechteverwaltung wird im Allgemeinen zwischen folgenden Konfigurationseinstellungen unterschieden:

- base / exact: Es wird auf genau diesen Knoten zugegriffen.
- one: Es wird auf den Knoten eine Hierarchie tiefer zugegriffen.
- children: Es wird nur auf die Knoten tiefer zugegriffen.
- subtree: Es wird auf den Zugriffsknoten und alle darunterliegenden Knoten zugegriffen.

Erteilung von Berechtigungen

Bei der Definition der Access Control List müssen zunächst Überlegungen angestrebt werden was bzw. worauf eingeschränkt werden soll und für wen diese Regelung gilt.

Die Regelung kann bestimmte Attribute wie zum Beispiel die Änderung des Passworts, der E-Mail, der Telefonnummer, ... betreffen,

```
access to attrs=userPassword,shadowLastChange
```

oder bestimmte Knoten wie zum Beispiel base/exact, one, children, subtree.

```
access to dn.subtree="ou=office,dc=uif,dc=at"
```

(Hier würde die Berechtigung auf den Zugriffsknoten inkl. alle darunterliegenden Knoten unter der organizational Unit *office* bezogen sein.)

Damit bestimmte Benutzer oder Gruppen durch die Regelung auch eingeschränkt werden, sind bestimmte Benutzer oder Gruppen anzugeben, durch folgende Angaben:

Einzuschränkender Benutzer	Entität
*	Alle, einschließlich anonymer und authentifizierter Benutzer.
anonymous	Anonyme (nicht authentifizierte) Benutzer.
users	Authentifizierte Benutzer.
self	Benutzer, der mit dem Ziel-Eintrag verbunden ist.
dn[.<basic-stype>]=<regex>	Benutzer, die mit einem regulären Ausdruck übereinstimmen.
dn.<scope-stype>=<DN>	Benutzer innerhalb des Bereichs einer DN.

Bsp.: by dn="cn=office,dc=uif,dc=at"

(Hier würde die Regelung für Mitglieder der Gruppe office gelten.)

Abschließend ist noch der Zugriff, der gewährt werden soll zu definieren. Hierbei bestehen folgende Möglichkeiten:

Level	Privilegien	Beschreibung
none	=0	Kein Zugriff.
disclose	=d	Erforderlich für Informationsfreigabe bei Fehlern.
auth	=dx	Erforderlich für Authentifizierung.
compare	=cdx	Erforderlich zum Vergleichen.
search	=scdx	Erforderlich zum Anwenden von Suchfiltern.
read	=rscdx	Erforderlich zum Lesen von Suchergebnissen.
write	=wrscdx	Erforderlich zum Ändern/Umbenennen.
manage	=mwrscdx	Erforderlich für die Verwaltung.

Bsp.: by dn="cn=office,dc=uif,dc=at" **write**

(Hier würde das Schreiben gewährleistet werden.)

Regelungen, die in der Access Control List weiter oben stehen werden, zuerst beachtet.

Die ACL befindet sich im slapd.conf und kann auch ausgelagert werden. In der slapd.conf ist der Pfad zur ACL zu inkludieren.

```
# Access Control Lists
include /etc/ldap/ac1.conf
```

Client

Installation und Konfiguration

Für die Konfiguration des ldap-clients ist die `libnss-ldapd` Bibliothek erforderlich. Diese Bibliothek ermöglicht den Zugriff auf LDAP für das Network Security Service (NSS) und unterstützt die Integration von LDAP für die Authentifizierung und Identitätsverwaltung.

```
sudo apt install libnss-ldapd
```

Nach Installation dieser Pakete wird nach dem LDAP-Server URI gefragt. Hier ist der entsprechende Server anzugeben.

LDAP server URI:

```
ldap://192.168.1.8/
```

Anschließend ist der Basis Distinguished Name zu definieren.

LDAP server search base:

```
dc=uif,dc=at
```

Diese Informationen werden im Host-File unter `/etc/hosts` am Server verwaltet.

Nachfolgend sind die Services auszuwählen, die verwendet werden sollen.

Name services to configure:

```
* passwd
* group
* shadow
```

Die `nsld.conf` muss entsprechend angepasst werden, um die Konfigurationseinstellungen für den `nsld-Daemon` festzulegen, einschließlich Informationen über den LDAP-Server, um eine Integration von LDAP als Namensdienst auf Unix-Systemen zu ermöglichen.

```
sudo nano /etc/nsld.conf
```

```
uri ldap://192.168.1.8/
```

```
sudo pam-auth-update
```

```
* Create home directory on login
```

```
sudo service nsld restart
```

Anmelden

Anschließend kann man sich nun entweder über das Terminal:

```
su -l mmustermann
```

anmelden oder über die graphische Benutzeroberfläche.

Backup

Ziel des Backup's ist es die lokale Baumstruktur zu sichern.

Skript

```
#!/bin/sh
LDAPBK=ldap-$( date +%y%m%d-%H%M ).ldif
BACKUPDIR=/home/backups
<pre>/usr/sbin/slapcat -v -b "dc=uif,dc=at" -l $BACKUPDIR/$LDAPBK
gzip -9 $BACKUPDIR/$LDAPBK
```

- **LDAPBK=ldap-\$(date +%y%m%d-%H%M).ldif** Erstellt einen Dateinamen für das Backup, der das aktuelle Datum und die Uhrzeit enthält.
- **BACKUPDIR=/home/backups** Legt das Verzeichnis fest, in dem das Backup gespeichert wird.
- **/usr/sbin/slapcat -v -b "dc=uif,dc=at" -l \$BACKUPDIR/\$LDAPBK** Führt den Befehl slapcat aus, um das LDAP-Verzeichnis zu sichern. Dabei werden die Optionen -v für den verbose-Modus (ausführliche Ausgabe) und -b "dc=uif,dc=at" für die Basis-DN (Distinguished Name) des zu sichernden Verzeichnisses verwendet. Die Ausgabe wird in die zuvor definierte Datei gespeichert.
- **gzip -9 \$BACKUPDIR/\$LDAPBK** Komprimiert das erstellte Backup mit dem gzip-Algorithmus und verwendet die höchste Kompressionsstufe (9).

Ausführen des Backups

Das Backup kann wie folgt ausgeführt werden.

```
sudo /usr/sbin/slapcat -v -l /home/backup/ldap.diff
```

Restore

Das Backup kann folgendermaßen eingespielt werden.

Bevor das Backup eingespielt wird, ist der slapd-Daemon zu stoppen.

```
sudo systemctl stop slapd
```

Wird das LDAP-Backup auf dem Server neu eingespielt kann die alte Datenbank folgendermaßen gelöscht werden. Dabei ist darauf zu achten, dass man im richtigen Directory ist.

```
cd /var/lib/ldap
rm -rf *
```

Anschließend kann die Datenbank mittels des backup.ldif Files wieder hergestellt werden.

```
/usr/sbin/slapadd -l backup.ldif
```

Abschließend ist der slapd Dienst wieder zu starten.

```
sudo systemctl start slapd
```

Graphische Oberfläche

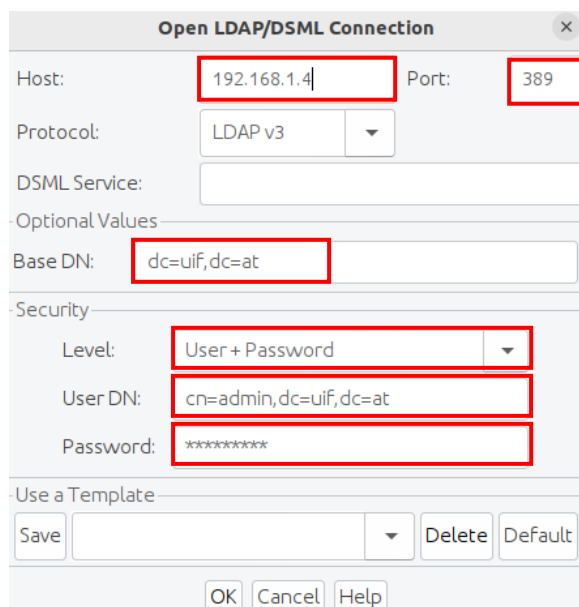
Die LDAP-Struktur kann auch mit einer graphischen Oberfläche erweitert, manipuliert, gelöscht bzw. angezeigt werden. Eine Möglichkeit besteht darin, den `jxplorer` zu verwenden.

```
sudo apt-get update
```

```
sudo apt-get install jxplorer
```

Verbindung zum LDAP-Server herstellen

Nach der Installation des `jxplorer`'s ist eine Verbindung zum LDAP-Server herzustellen. Dafür sind folgende Einstellungen unter der Registerkarte *File >> Connect* erforderlich:

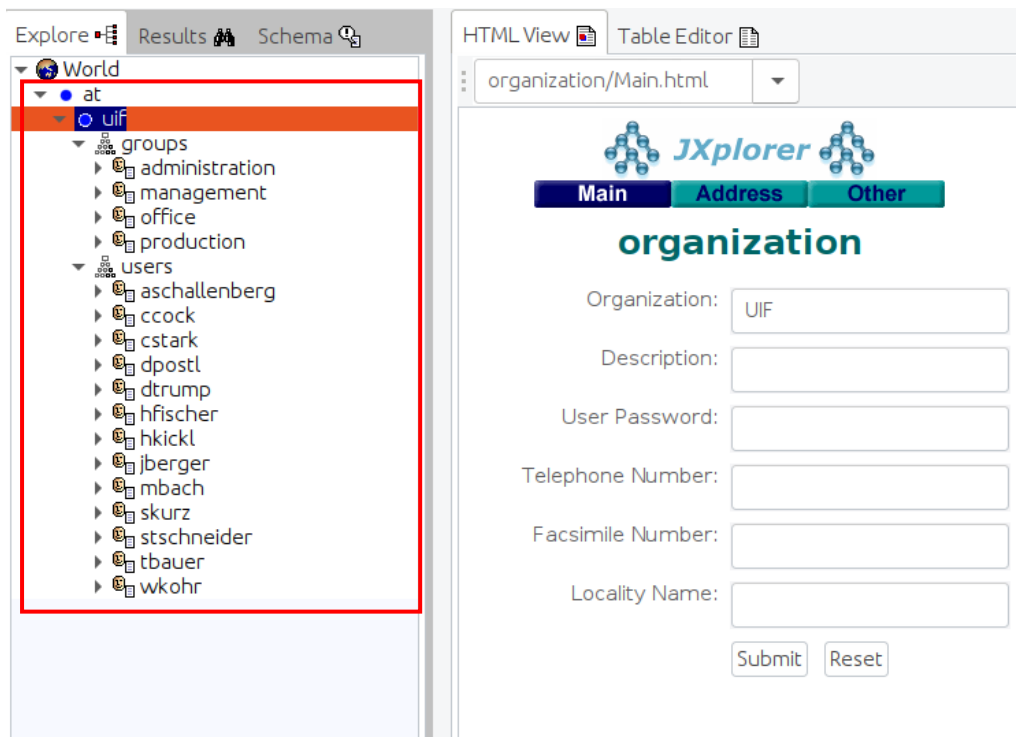


Definition des Hosts & des Ports. LDAP verwendet standardmäßig den Port 389. Im `etc/hosts` wurde dem Host die entsprechende IP zugewiesen.

Definition des Basis Distinguished Name. Der DN ist sozusagen der Ausgangspunkt bzw. stellt das Wurzelement in der Hierarchie des LDAP-Verzeichnisses dar. Unter dem Basis DN befinden sich die einzelnen `ou`'s. Sprich es wird der darunterliegende Baum ab diesem Ausgangspunkt angezeigt.

Authentifizierung. Auswahl des Levels. Wird `User + Password` ausgewählt kann sich ein berechtigter Benutzer mit seinem Passwort einloggen. Dabei ist darauf zu achten, dass der gesamte Pfad angegeben wird und nicht nur der `common-name`.

Nachfolgend wird die Baumstruktur angezeigt. Per Kontextmenü auf groups bzw. users können neue Gruppen bzw. Benutzer hinzugefügt werden. Und durch die Auswahl der einzelnen Elemente können diese auch bearbeitet oder gelöscht werden.



Integration von NextCloud

Installation des NextCloud Servers am "LDAP-Server"

Für die Installation des NextCloud Server sind folgende Pakete für apache, mysql und php erforderlich:

```
sudo apt install unzip apache2 php php-mysql mysql-client mysql-server php-zip
php-xml php-mbstring php-gd php-simplexml php-curl php-intl php-imagick php-gmp
php-bcmath php-memcache libmagickcore-6.q16-6-extra
```

Unter <https://nextcloud.com/install/> ist das Server Image zu downloaden:

```
>> Menu >> Get Nextcloud -> Nextcloud Server: Community Projects -> Get Zip file
```

Anschließend ist das Zip file zu entpacken:

```
sudo unzip /home/username/Downloads/latest.zip -d /var/www/html/
```

Nachfolgend sind die Permissions für den Webserver zu setzen:

```
sudo chown -R www-data:www-data /var/www/html/nextcloud
```

Folgende Einstellungen sind im `php.ini` File zu übernehmen:

```
sudo nano /etc/php/8.1/apache2/php.ini
```

- Das Comment entfernen (semicolon ;) bei: `max_input_vars`
- Größe von `max_input_vars` zu mind. 5000 erhöhen
- `memory_limit = 512M` erhöhen
- `upload_max_filesize = 1GB` ändern
- `max_file_uploads = 50` ändern
- `post_max_size = 0` ändern
- `max_execution_time = 300` erhöhen

Anschließend kann der Webserver gestartet werden:

```
sudo service apache2 start
```

Folgendes Datenbank Setup ist erforderlich:

Service starten:

```
sudo service mysql start
```

Einloggen:

```
sudo mysql -u root -p
```

Datenbank erstellen

```
CREATE DATABASE nextcloud_db;
```

Datenbank Benutzer erstellen:

```
CREATE USER 'nextclouduser'@'localhost' IDENTIFIED BY 'Password123!!';
```

Benutzer Permissions für die Datenbank geben:

```
GRANT ALL PRIVILEGES ON nextcloud_db.* TO 'nextclouduser'@'localhost';
```

Cache cleanen

```
FLUSH PRIVILEGES;
```

mysql verlassen

```
quit;
```

Anschließend kann zu `http://localhost/nextcloud/index.php` navigiert werden.

Admin Account erstellen:

Username: admin

Password: Kennwort1

Speicher & Datenbank:

Data folder: `/var/www/html/nextcloud/data`

Database user: nextclouduser

Database password: Password123!!

Database name: nextcloud_db


Database host: localhost:5432

LDAP Integration

Damit das erforderliche ldap Service aktiviert werden kann ist das php-ldap Paket zu installieren.

```
sudo apt-get install php-ldap
```


Anschließend kann das LDAP user and group-backend aktiviert werden.



 LDAP user and group backend	1.19.0	<input checked="" type="checkbox"/> Vorgestellt	Deaktivieren
---	--------	---	--------------

Nachfolgend ist der LDAP-Host zu definieren.

LDAP/AD-Integration

Server Benutzer Anmelde-Attribute Gruppen

1. Server: 

192.168.1.8

LDAP-Server IP

389

LDAP Port

Port ermitteln

Basis DN

dc=uiif,dc=at


Zugangsdaten speichern


dc=uiif,dc=at

Base DN ermitteln

Base DN testen

☐ LDAP-Filter manuell eingeben (empfohlen für große Verzeichnisse)

Konfiguration OK 

Fortsetzen  Hilfe

Wenn die Integration erfolgreich ist, sollten die entsprechenden Benutzer gefunden werden

Einstellungen überprüfen und Benutzer zählen 16 Benutzer gefunden

Die Benutzer, die sich in NextCloud einloggen können sollen, können anschließend definiert bzw. eingeschränkt werden. Mithilfe von Anmelde-Attributen kann festgelegt werden, wie sich Benutzer anmelden dürfen z.B. Benutzername, E-Mail.

LDAP/AD-Integration

Server **Benutzer** Anmelde-Attribute Gruppen

Auflistung und Suche nach Nutzern ist eingeschränkt durch folgende Kriterien:

Nur diese Objektklassen:

Die häufigsten Objektklassen für Benutzer sind organizationalPerson, person, user und inetOrgPerson. Wenn du nicht sicher bist, welche Objektklasse du wählen sollst, frage bitte deinen Verzeichnis-Administrator.

Nur aus diesen Gruppen:

>

<

[↓ LDAP-Abfrage bearbeiten](#)

LDAP-Filter: `((objectclass=inetOrgPerson)(objectclass=posixAccount)(objectclass=shadowAccount)(objectclass=top))`

LDAP/AD-Integration

Server Benutzer **Anmelde-Attribute** Gruppen

Beim Anmelden wird Nextcloud den Benutzer basierend auf folgenden Attributen finden:

LDAP-/AD-Benutzername: ☒

LDAP-/AD E-Mail-Adresse: ☐

Andere Attribute:

[↓ LDAP-Abfrage bearbeiten](#)

LDAP-Filter: `(&(((objectclass=inetOrgPerson)(objectclass=posixAccount)(objectclass=shadowAccount)(objectclass=top)))(dc=%uid))`

Konfiguration OK ● [i Hilfe](#)

LDAP/AD-Integration

Server

Benutzer

Anmelde-Attribute

Gruppen

Gruppen, auf die diese Kriterien zutreffen, sind verfügbar in Nextcloud:

Nur diese Objektklassen:

groupOfNames, posixGroup, top

Nur aus diesen Gruppen:

administration, management, office , production

>

<

[LDAP-Abfrage bearbeiten](#)

LDAP-Filter: (&((objectclass=groupOfNames)(objectclass=posixGroup)(objectclass=top))((cn=administration)(cn=management)(cn=office)(cn=production)))

Einstellungen überprüfen und die Gruppen zählen

Konfiguration OK Zurück

Hilfe

Einstellungen überprüfen und die Gruppen zählen

4 Gruppen gefunden

Konfiguration OK Zurück

Damit sich Clients tatsächlich anmelden können ist es wichtig zu kontrollieren das NextCloud nicht unter dem localhost abrufbar ist, sondern über die IP-Adresse des Servers. Hierfür wurde die IP-Adresse des Servers zu den trusted_domains hinzugefügt und die URL unter die der NextCloud Server erreichbar sein soll entsprechend auf die Server-IP geändert.

```
sudo nano /var/www/html/nextcloud/config.php
```

```
$CONFIG = array (
    'instanceid' => 'ocfjb5g6aint',
    'passwordsalt' => 'xTZ9r2cT8lbaIuF/zRgSh4DNAn5+jH',
    'secret' => 'EHfoJVCsxWA1Xl8J6k8Svy8fN3/360pbF9S3ceQ14NHgplBU',
    'trusted_domains' =>
    array (
        0 => 'localhost',
        1 => '192.168.1.8',
    ),
    'datadirectory' => '/var/www/html/nextcloud/data',
    'dbtype' => 'mysql',
    'version' => '28.0.2.5',
    'overwrite.cli.url' => 'http://192.168.1.8/nextcloud',
    'dbname' => 'nextcloud_db',
    'dbhost' => 'localhost:5432',
```

Client-Integration

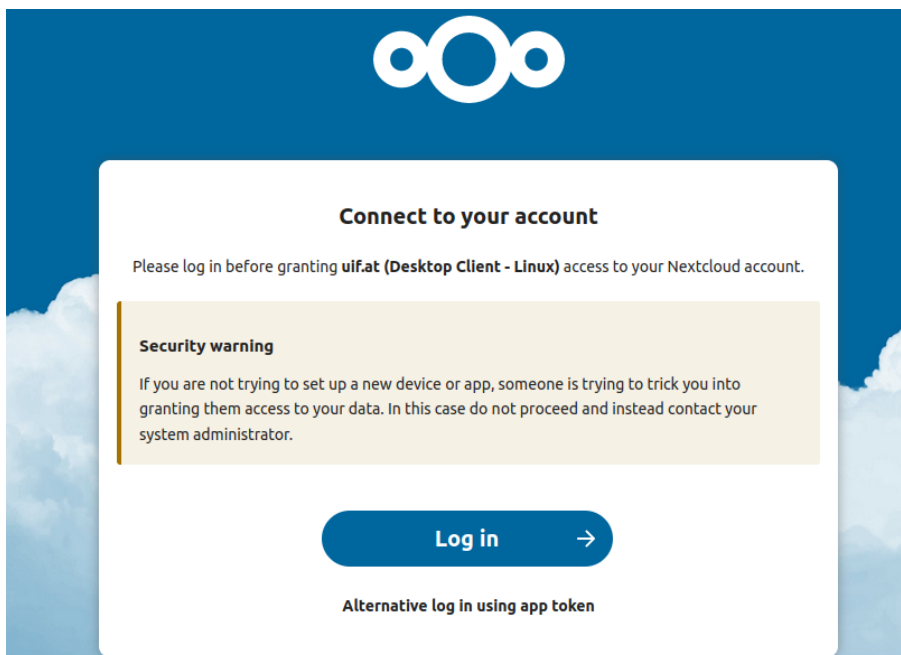
Am Client kann die Nextcloud-Desktop Applikation installiert werden.

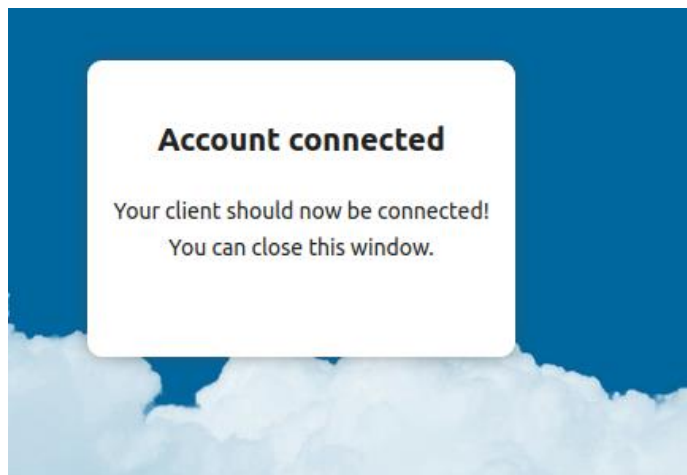
```
sudo apt-get install nextcloud desktop
```

Anschließend kann man sich unter der URL des Nextcloud Servers, welche im config.php definiert ist anmelden.



Es erfolgt eine automatische Weiterleitung zur nextcloud login page, wo anschließend die Zugangsdaten eingetragen werden können.





Bei einer erfolgreichen Anmeldung werden die Daten nun synchronisiert.

