
NextCloud bringt ihnen eine erweiterte Funktionalität der Bereitstellung und Synchronisierung ihrer Daten für Mitarbeiter. NextCloud biete über Erweiterungen und Plug-Ins die Möglichkeit auch in anderen Teilen ihres Unternehmens Verbesserungen der Zusammenarbeit zu schaffen. Prinzipiell ist NextCloud aber ihre Private Cloud - Sie wissen, wo die Daten liegen und Sie wissen wer darauf zugreifen kann und darf.

Vorbereitungen

NextCloud benötigt ergänzend zu dem evtl. massiven Speicherplatzbedarf auch noch eine funktionierend SQL-Datenbank. Hierfür wird der reine Open-Source mySQL Ableger MariaDB empfohlen.

Installation Datenbank mit Webmanagement und weiterer benötigter Komponenten

```
1 sudo apt install apache2 mariadb-server libapache2-mod-php php php-mysql php-xml php-gd php-curl php-zip php-mbstring php-intl php-bcmath php-gmp php-imagick php-redis redis-server php-ldap php-smbclient unzip phpmyadmin
```

Abfragen nach dem zu verwendenden Webserver: apache2

Konfiguriere phpmyadmin: Ja Datenbank Konfigurieren

Passwort setzen

Im Anschluss muss die Datenbank noch gesichert werden um etwaigen Missbrauch zu unterbinden und auch das Root-Passwort wird hier gesetzt

```
1 sudo mysql_secure_installation
```

1. Abfrage des aktuellen Passwortes NICHTS EINGEBEN NUR BESTÄTIGEN
2. Soll ein Root-Passwort gesetzt werden? Y
3. Passwort eingeben und wiederholen
4. Soll der Anonyme User entfernt werden? Y
5. Remote-Login für Root deaktivieren? Y
6. test-Datenbank entfernen? Y
7. Änderungen übernehmen? Y

Jetzt muss einmalig in die SQL-Datenbank der Login für root über das Webinterface aktiviert werden:

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

```
1 use mysql;
2 update user set plugin=''' where User='root';
3 flush privileges;
4 \q
```

Zugriff auf ihre Datebank per Webinterface:

<http://IP/phpmyadmin>

Legen Sie einen neuen Nutzer für NextCloud an und gewähren Sie dem Nutzer alle Rechte an seiner Datenbank „Nextcloud“.

NextCloud installieren

NextCloud bietet derzeit keine externe Paketquellen an. Deshalb muss Nextcloud als Zip-Archiv heruntergeladen werden und im Anschluss passend entpackt werden.

```
1 wget https://download.nextcloud.com/server/releases/latest.zip
2 unzip latest.zip
3 sudo cp -r nextcloud /var/www/
4 sudo chown -R www-data:www-data /var/www/nextcloud/
```

Jetzt legen wir noch ein Separates Datenverzeichnis an. Dies bringt den Vorteil, dass dieses sich auch auf einer separaten Partition befinden kann.

```
1 sudo mkdir /srv/cloud
2 sudo chown www-data:www-data -R /srv/cloud
```

erstellen `/etc/apache2/sites-available/nextcloud.conf` mit Inhalt:

```
1 <VirtualHost *:80>
2   DocumentRoot "/var/www/nextcloud"
3   ServerName nextcloud.hensel.dom
4   ErrorLog ${APACHE_LOG_DIR}/error.log
5   CustomLog ${APACHE_LOG_DIR}/access.log combined
6     <Directory /var/www/nextcloud/>
7       Options +FollowSymlinks
8       AllowOverride All
9         <IfModule mod_dav.c>
10           Dav off
11         </IfModule>
12         SetEnv HOME /var/www/nextcloud
13         SetEnv HTTP_HOME /var/www/nextcloud
14         Satisfy Any
15       </Directory>
16 </VirtualHost>
```

Speichern und aktivieren mit

```
1 sudo a2ensite nextcloud
2 sudo a2dissite 000-default.conf
```

Aktivieren der benötigten Apache2-Module

```
1 sudo a2enmod rewrite
2 sudo a2enmod headers
3 sudo a2enmod env
4 sudo a2enmod dir
5 sudo a2enmod mime
6 sudo a2enmod setenvif
7 sudo a2enmod ssl
8 sudo systemctl restart apache2
```

Nun können Sie per http auf den Webserver zugreifen <http://nextcloud.hensel.dom>

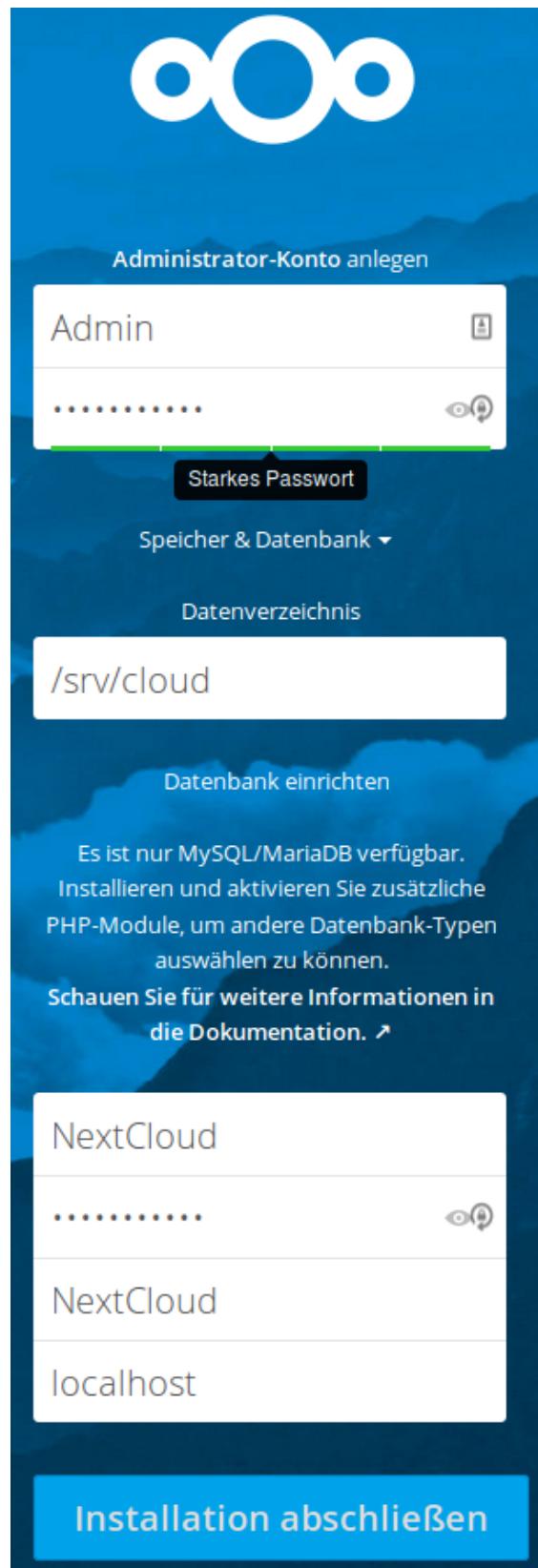


Figure 1: Erster Login, Eingabe der Admindaten

Hier legen Sie nun das Administrator-Konto ein, wobei natürlich Admin und ein schwaches Passwort hier Tabu sind.

Geben Sie als Datenverzeichnis das gerade angelegte Verzeichnis an und geben Sie die entsprechenden Daten die beim Anlagen der Datenbank gesetzt wurden ein.

Nach dem Klick auf Installation abschließen werden Sie auch schon ihr eigenes Datenverzeichnis befördert, wobei Ihnen erst noch ein Hinweis angezeigt wird wie Sie Desktop- und Mobile-Apps nutzen können.

Wechseln Sie als nächstes in der rechten oberen Ecke in das Administrator-Menü.

Im oberen Bereich begrüßen Sie dabei gleich einige Konfigurationsfehler:

Wir nutzen noch kein SSL und keinen Cache.

Kümmern wir uns erst einmal um den Cache, wobei wir den Redis-Server bereits installiert haben. Somit muss nur noch die Nextcloud-Configuration angepasst werden:

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

Fügen Sie eine weitere Zeile vor der schließenden Klammer ein: ...

```
1 'dbtype' => 'mysql',
2   'version' => '12.0.0.29',
3   'dbname' => 'NextCloud',
4   'dbhost' => 'localhost',
5   'dbport' => '',
6   'dbtableprefix' => 'oc_',
7   'dbuser' => 'NextCloud',
8   'dbpassword' => 'passw0rd#',
9   'logtimezone' => 'UTC',
10  'installed' => true,
11  'memcache.distributed' => '\OC\Memcache\Redis',
12  'memcache.local' => '\OC\Memcache\Redis',
13  'memcache.locking' => '\OC\Memcache\Redis',
14  'redis' => array(
15    'host' => 'localhost',
16    'port' => 6379,
17  ),
18 );
```

Laden Sie die Administrator-Seite neu – Der Fehler sollte weg sein.

SSL-Zertifikat

Für die https / SSL Übertragung benötigen wir noch ein selbst-signiertes Zertifikat welches dem Browser übergeben werden kann.

```
1 sudo -s
2 openssl req -new -x509 -days 365 -nodes -out /etc/ssl/certs/NextCloud.pem -keyout /etc/ssl/private/NextCloud.key
```

Konfiguration Apache für das SSL-Zertifikat

Konfiguration der Benötigten Module:

Bearbeiten der Datei `/etc/apache2/sites-available/nextcloud.conf`

```
1 <VirtualHost *:80>
2     Redirect permanent / https://nextcloud.hensel.dom
3 </VirtualHost>
4
5 <IfModule mod_ssl.c>
6     <VirtualHost *:443>
7         SSLEngine on
8         SSLCertificateFile      /etc/ssl/certs/NextCloud.pem
9         SSLCertificateKeyFile /etc/ssl/private/NextCloud.key
10
11    <IfModule mod_headers.c>
12        Header always set Strict-Transport-Security "max-age
13            =31536000; includeSubDomains; preload"
14    </IfModule>
15
16    DocumentRoot "/var/www/nextcloud"
17    ServerName nextcloud.hensel.dom
18    ServerAlias www.nextcloud.hensel.dom
19
20    ErrorLog ${APACHE_LOG_DIR}/error.log
21    CustomLog ${APACHE_LOG_DIR}/access.log combined
22
23    <Directory /var/www/nextcloud/>
24        Options +FollowSymlinks
25        AllowOverride All
26        <IfModule mod_dav.c>
27            Dav off
28        </IfModule>
29        SetEnv HOME /var/www/nextcloud
30        SetEnv HTTP_HOME /var/www/nextcloud
31        Satisfy Any
32    </Directory>
33 </VirtualHost>
34 </IfModule>
```

Aktivieren:

```
1 sudo a2ensite default-ssl.conf
2 sudo systemctl restart apache2
```

Apache Neustarten und Fertig

CronJob für regelmäßige Aktualisierung der Datenbank

NextCloud aktualisiert bei jedem Zugriff auf das Webinterface die Datenbank, allerdings kostet dies wertvolle Sekunden bei einem „Wohlfühl-Interface“ daher aktivieren wir einen CronJob

Die Aktion soll vom User www-data ausgeführt werden

```
1 sudo crontab -u www-data -e
```

nun können wir einen neuen Job einfügen:

```
1 */15 * * * * php -f /var/www/nextcloud/cron.php
```

Wählen Sie nun im Administrations-Bereich von NextCloud bei Cron entsprechend auch cron aus.

Im Anschluss am besten einmal reboot

LDAP

Konfiguration smb.conf bei einem Samba AD-DC

```
1 [global]
2 ldap server require strong auth = no
```

```
1 sudo systemctl restart samba-ad-dc
```

Im Anschluss daran suchen wir in den NextCloud-Apps nach dem LDAP user and group backend:

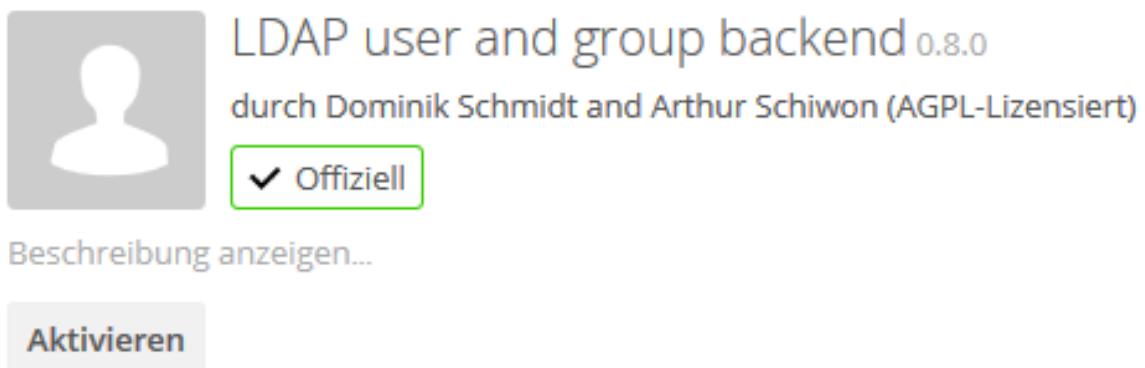


Figure 2: Auswahl LDAP-APP

Aktivieren Sie die App und wechseln Sie wieder in den Administrationsbereich. Dort finden Sie einen neuen Bereich LDAP.

LDAP

Figure 3: Einrichtungstab Server

Die benötigten Informationen finden Sie in ihrer Serverkonfiguration. In diesem Beispiel:

- FQDN + Port des AD

- Nutzer, Gruppe, Domäne Dieser Account muss keine Admin-Rechte haben sollte aber eigener Account sein.
- Passwort
- Der Ort in der Domäne an der die User zu suchen sind

LDAP

Den ownCloud-Zugriff auf Benutzer, die den folgenden Kriterien entsprechen, beschränken:

Nur diese Objektklassen: **person**

Die häufigsten Objektklassen für Benutzer sind `organizationalPerson`, `person`, `user` und `inetOrgPerson`. Wenn Sie nicht sicher, welche Objektklasse Sie wählen sollen, fragen Sie bitte Ihren Verzeichnis-Admin.

Nur aus diesen Gruppen: **OwnCloud**

LDAP-Abfrage bearbeiten

LDAP-Filter: `(&(&(|(objectclass=person))(|(|(memberof=CN=OwnCloud,CN=Users,DC=hef,DC=dom)(primaryGroupID=1108))))(|(uid=%uid)(|(sAMAccountName=%uid))))`

Figure 4: Einrichtungstab Benutzer

Welcher Typ soll abgefragt werden? Hier empfiehlt sich eine Separate Gruppe für Nutzer anzulegen welche NextCloud nutzen sollen. Klicken Sie am unteren Rand auf „Einstellungen prüfen und Benutzer zählen“ um ihre Konfiguration zu überprüfen.

LDAP

Beim Anmelden wird ownCloud den Nutzer basierend auf folgenden Attributen finden:

LDAP-/AD-Benutzername:

LDAP-/AD-E-Mail-Adresse:

Andere Attribute: **sAMAccountName**

LDAP-Abfrage bearbeiten

LDAP-Filter: `(&(&(|(objectclass=person))(|(|(memberof=CN=OwnCloud,CN=Users,DC=hef,DC=dom)(primaryGroupID=1108))))(|(uid=%uid)(|(sAMAccountName=%uid))))`

Figure 5: Einrichtungstab Anmeldeattribute

Hier definieren Sie mit welchen Möglichkeiten sich der Nutzer Authentifizieren kann. Wählen Sie die sAMAccountName aus, um dem Nutzer zu ermöglichen Sich direkt mit seinem Windows-Login anzumelden.

LDAP

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

Nur diese Objektklassen: **group**

Nur aus diesen Gruppen: **OwnCloud**

[LDAP-Abfrage bearbeiten](#)

LDAP-Filter: `(&(|(objectclass=group))(|(cn=OwnCloud)))`

Figure 6: Einrichtungstab Gruppen

Hier definieren Sie welche Gruppen ihres Servers in NextCloud übernommen werden sollen um ihre Nutzer auch in NextCloud passend sortieren zu können und auch Gruppenspezifische Externe Laufwerke einzubinden.

LDAP

Standardmäßig wird der interne Benutzername mittels des UUID-Attributes erzeugt. Dies stellt sicher, dass der Benutzername einzigartig ist und keinerlei Zeichen konvertiert werden müssen. Der interne Benutzername unterliegt Beschränkungen, die nur die nachfolgenden Zeichen erlauben: [a-zA-Z0-9_@]. Andere Zeichen werden mittels ihrer korrespondierenden Zeichen ersetzt oder einfach ausgelassen. Bei Kollisionen wird ein Zähler hinzugefügt bzw. der Zähler um einen Wert erhöht. Der interne Benutzername wird benutzt, um einen Benutzer intern zu identifizieren. Es ist ebenso der standardmäßig vorausgewählte Name des Heimatverzeichnisses. Es ist auch ein Teil der Remote-URLs - zum Beispiel für alle *DAV-Dienste. Mit dieser Einstellung kann das Standardverhalten überschrieben werden. Um ein ähnliches Verhalten wie vor ownCloud 5 zu erzielen, fügen Sie das anzugehende Attribut des Benutzernamens in das nachfolgende Feld ein. Lassen Sie dies hingegen für das Standardverhalten leer. Die Änderungen werden sich nur auf neu gemappte (hinzugefügte) LDAP-Benutzer auswirken.

Interne Eigenschaften des sAMAccountName Benutzers:

Standardmäßig wird die UUID-Eigenschaft automatisch erkannt. Die UUID-Eigenschaft wird genutzt, um einen LDAP-Benutzer und Gruppen einwandfrei zu identifizieren. Außerdem wird der interne Benutzername erzeugt, der auf Eigenschaften der UUID basiert, wenn es oben nicht anders angegeben wurde. Sie müssen allerdings sicherstellen, dass Ihre gewählten Eigenschaften zur Identifikation der Benutzer und Gruppen eindeutig sind und zugeordnet werden können. Lassen Sie es frei, um es beim Standardverhalten zu belassen. Änderungen wirken sich nur auf neu gemappte (hinzugefügte) LDAP-Benutzer und -Gruppen aus.

UUID-Attribute für Benutzer:

UUID-Attribute für Gruppen:

Lösche LDAP-Benutzernamenuordnung

Lösche LDAP-Gruppennamenuordnung

Testkonfiguration i Hilfe

Figure 7: Einrichtungstab Expert

In der Benutzerübersicht sollen alle Nutzer mit ihrem Benutzernamen und nicht mit der UUID angezeigt werden. Somit ist es auch für die Nutzer einfacher, sich gegenseitig zu finden.

[PDF herunterladen](#)