LDAP-Information für Schulen

Liebe Schul-Admins,

wir freuen uns, dass ihr eure Schule per LDAP an die HPI Schul-Cloud oder Niedersächsische Bildungscloud anbinden wollt.

Damit die Userdaten sowie Rollen und Klassenzugehörigkeiten korrekt in die Cloud synchronisiert werden, muss euer LDAP bestimmte Informationen mitbringen. Die folgenden Punkte helfen Euch, das LDAP auf die Synchronisation mit der Cloud vorzubereiten.

Erklärvideo

Ablauf der Synchronisation

- Die Nutzer werden regelmäßig über den Sychronisierungsprozess angelegt bzw. aktualisiert
- Der Login erfolgt über den LDAP Server - Daher sind Passwortänderungen sofort aktiv

Voraussetzungen

1. Das LDAP muss verschlüsselt über ldaps:// erreichbar sein, der Standardport ist 10636 kann aber auch anders gewählt werden
2. In Firewall LDAP-Port (z.B. 10636) nach außen freigeben
3. Wenn die Firewall IPs filtert ist eine Freischaltung der IPs notwendig: 141.89.221.180 und abhängig von der Instanz:
    a. https://schul-cloud.org - 141.89.221.239
    b. https://niedersachsen.cloud - 78.46.103.254
4. Es muss ein Nutzer mit Passwort im LDAP angelegt werden, der Lese-Zugriff auf alle Nutzer und Gruppen hat (z.B. cn=schulcloud,ou=ldap, dc=ihreSchulDomain,dc=de). Dieser Nutzer sollte keinesfalls Schreibrechte haben.

LDAP-Struktur für Nutzer

LDAP-Verzeichnis, in dem alle Nutzer z.B. (ou=users) enthalten sind:

```
ou=users,dc=ihreSchulDomain,dc=de
```

Der Pfad zu einem Nutzer ist wie folgt definiert:

```
uid=max.mustermann,ou=users,dc=ihreSchulDomain,dc=de
```

Ein Nutzer benötigt folgende LDAP-Attribute (Tipp - ObjectClasses: person + inetOrgPerson + posixAccount):

- uid (eindeutige Login-ID, z.B. max.musterman)
- uidNumber (eindeutige *nicht änderbare* ID, uid kann sich z.B. bei Heirat verändern)
- mail (E-Mail-Adresse des Nutzers (darf nicht mehrfach vergeben sein))
- givenName (Vorname)
- sn (Nachname)
- userPassword (verschlüsseltes Passwort des Nutzers für den Login-Prozess, wird nicht von der SchulCloud sychronisiert)
- description (Gibt die Rolle des Nutzers an, siehe folgende Erklärung)
- objectClass (**Einer der Werte muss *person* sein**)

Folgende Rollen können als Attribut definiert werden, die Bennung ist variabel einstellbar:

- ROLE_STUDENT (Nutzer ist Schüler)
- ROLE_TEACHER (Nutzer ist Lehrer)
- ROLE_ADMIN (Nutzer ist Admin)
- ROLE_NO_SC (Nutzer möchte nicht an der Schul-Cloud teilnehmen)

LDAP-Struktur für Klassen

Optional lassen sich auch Klassenzugehörigkeiten in die Schul-Cloud synchronisieren. Benötigt wird ein LDAP-Verzeichnis Groups in dem nur Klassen (z.B. ou=classes) enthalten sind.

```
ou=classes,dc=ihreSchulDomain,dc=de
```

Der Pfad zu einer Klasse ist wie folgt definiert:

```
cn=klasse-1-c,ou=classes,dc=ihreSchulDomain,dc=de
```

Eine Klasse benötigt folgende Attribute (Tipp - ObjectClass: groupOfUniqueNames):

- description (Anzeigenamen) (nicht veränderbar und notwendig)
- uniqueMember (Einträge der User als LDAP-Pfade, die zur Klasse gehören)

Bei Rückfragen wende dich gerne an:

feedback@schul-cloud.org