IServ über LDAP an Moodle anbinden

Die ursprüngliche Version stammt von Matthias Grünwald aus dem IServ-Supportforum. Sie können diese

hier

herunterladen.

Moodle ermöglicht die Authentifizierung per LDAP, also die Überprüfung der Zugangsdaten beim Login über die Schnittstelle. Bei jedem Login in Moodle wird also bei IServ angefragt, ob die Benutzerdaten korrekt sind. Außerdem kann man recht einfach sämtliche IServ-Gruppen in Moodle hochladen. Das ist jedoch mit etwas Arbeit verbunden, so dass immer zu prüfen ist, ob nicht Schüler:innen sich auch eigenverantwortlich in Kurse einschreiben können sollten.

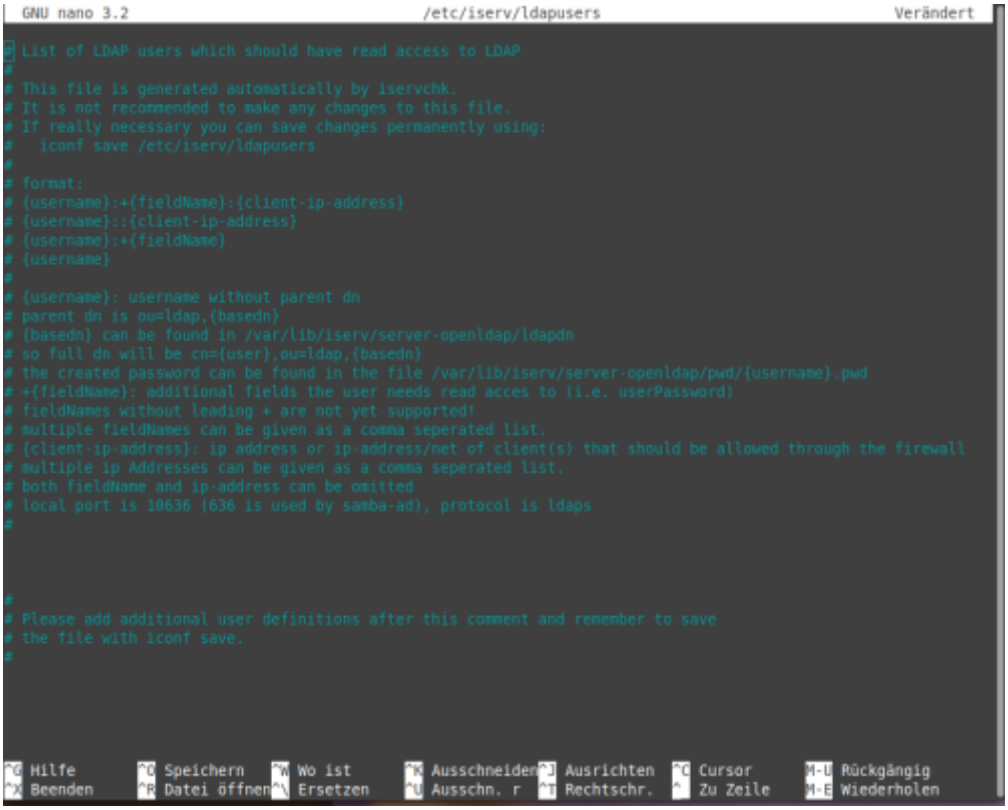
LDAP auf dem IServ vorbereiten

Dieser Schritt ist für jedes System notwendig, welches per LDAP angebunden werden soll. Man benötigt Zugriff zum Internetrouter der Schule und zur Kommandozeile von IServ. Ggf. ist die Einrichtung auch über den IServ-Support möglich.

Der Port 10636 muss auf dem Router oder der Firewall nach außen freigegeben werden. Über diesen Port findet die Kommunikation mit Moodle statt. IServ lässt dabei nur Verbindungen von IP-Adressen zu, die man vorher dafür freigegeben hat.

Nach dem Einloggen auf IServ, muss die Datei */etc/iserv/ldapusers* angepasst werden. Am leichtesten gelingt das mit nano:

```
nano /etc/iserv/ldapusers
```



Nun kommt ein Eintrag hinter dem Hinweis

```
# Please add additional user definitions after this comment an remember to save
# the file with iconf save
```

Also z.B.:

```
moodle:+userPassword:192.168.0.56
```

Der Benutzerzugang zum Verzeichnis lautet hier „moodle“. Die IP-Adresse (192.168.0.56) muss diejenige des Moodleservers sein. Der Lesezugriff auf den Passworthash und die Gruppenmitgliedschaften muss extra freigegeben werden.

Sie können jetzt mit STRG-x den Editor verlassen und mit

```
iconf save /etc/iserv/ldapusers
iservchk ldap ferm
```

die Änderungen im IServ permanent übernehmen.

Für die spätere Konfiguration jeder denkbaren Anwendung (also auch Moodle) benötigen Sie jetzt noch die sogenannte BaseDN und das Zugriffspasswort:

```
nano /var/lib/iserv/server-openldap/ldapdn
nano /var/lib/iserv/server-openldap/pwd/moodle.pwd
```

Notieren Sie sich beide Angaben.

Der LDAP-Verzeichnisbaum des IServ

Damit man versteht, was man jeweils in den Konfigurationseinstellungen bewirkt, ist ein Blick in den

Verzeichnisbaum des LDAP-Verzeichnisses im IServ aufschlussreich. Dieser hält sich mustergültig an RFC-Vorgaben, so dass eigentlich jedes per LDAP angebundenes System damit zurechtkommen müsste.

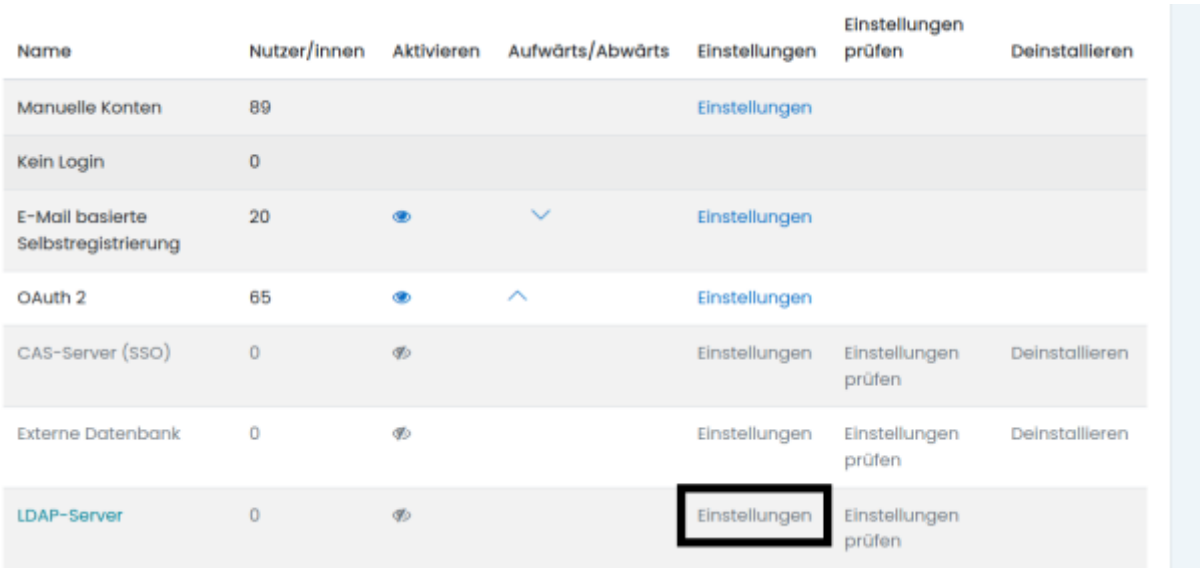
- Verzeichnisaufbau des IServ

Einstellungen in Moodle

Moodle ermöglicht eine Authentifizierung aus unterschiedlichen Quellen. Das wird über Module realisiert. Im ersten Schritt wird die LDAP-Authentifizierung eingerichtet. Sie finden die notwendigen Einstellungen unter:

> *Website-Administration ⇒ Plugins ⇒ Authentifizierung ⇒ Übersicht ⇒ LDAP-Server (Einstellungen)*

Schneller geht es immer über die Suchfunktion - hier wäre der Suchbegriff „LDAP-Server“ der geeignete.



Nun müssen verschiedene Einstellungen erfolgen. Die nicht aufgeführten Einstellungen können auf Standard verbleiben.

LDAP-Serverenstellungen	**Eintrag oder Einstellung**	**Erläuterung/Kommentar**
Host URL	*ldaps://<adresse-ihres-iserv>:10636/*	
Version	*3*	
TLS benutzen	*Ja*	
Kennwort-Caching verhindern	*Ja*	
Anmeldename	*cn=moodle, ou=ldap, dc=<iserv-url>, dc=<tld>*	
Kennwort	*Anmeldepasswort (s.o., 64-stellig)*	
Nutzersuche (user lookup)	**Eintrag oder Einstellung**	**Erläuterung/Kommentar**
Nutzertyp	*posixAccount (rfc2307)*	
Kontexte	*ou=users, dc=<iserv-url>, dc=<tld>*	
Nutzermerkmal	*uid*	
Mitgliedsmerkmal	*memberuid*	
ObjectClass	*uuidObject*	
Synchronisierung von Nutzerkonten	**Eintrag oder Einstellung**	**Erläuterung/Kommentar**

Entfernte externe Nutzer	*intern sperren*	
Datenzuordnung	**Eintrag oder Einstellung**	**Erläuterung/Kommentar**
Daten übernehmen (Vorname)	*givenName*	
Lokal aktualisieren (Vorname)	*Bei jedem Login*	
Feld sperren (Vorname)	*Gesperrt*	
Daten übernehmen (Nachname)	*sn*	
Lokal aktualisieren (Nachname)	*Bei jedem Login*	
Feld sperren (Nachname)	*Gesperrt*	
Daten übernehmen (E-Mailadresse)	*mail*	
Lokal aktualisieren (E-Mailadresse)	*Bei jedem Login*	
Feld sperren (E-Mailadresse)	*Bearbeitbar*	
Daten übernehmen (ID-Nummer)	*uidNumber*	
Lokal aktualisieren (ID-Nummer)	*Bei jedem Login*	
Feld sperren (ID-Nummer)	*Gesperrt*	

Am Schluss klicken Sie auf den Button „Änderungen sichern“.

Das Plugin muss in der Plugin-Liste jetzt noch aktiviert werden.

Wenn das LDAP-Plugin die einzige Methode ist, mit der sich Schüler:innen und Lehrkräfte an Moodle anmelden, sollte es an die dritte Stelle in der Liste mit den Pfeilen „hochgeschoben“ werden.

Eine Anmeldung am Moodle mit IServ-Daten sollte jetzt möglich sein (bitte testen).

Nutzer:innenverwaltung in Moodle

Nutzer:innen können sich jetzt zwar in Moodle anmelden, sind aber keinen Gruppen zugeordnet. Auch werden nur Teilnehmer:innenrechte zugewiesen. Das ist bei kleinen Schulen noch beherrschbar, in großen Systemen ufert der Verwaltungsaufwand jedoch aus. Daher ist eine Automatisierung wünschenwert. Dies geht in Moodle über sogenannte Einschreibeplugins.

Für das Entfernen von Nutzer:innen gibt es noch keine technische Möglichkeit der Automatisierung.

Mit dem OSS-Plugin

Empfohlen wird die Nutzung des Plugins OSS-Enrolement. Im Gegensatz zum LDAP-Enrolment-Plugin von Moodle gibt es für den schulischen Bereich einige

sinnvolle Einstellungsmöglichkeiten

mehr. Man muss sich aber vor Augen halten, dass dieses Plugin für die Zusammenarbeit mit dem OpenSchoolServer und nicht für IServ konzipiert wurde. Das LDAP-Verzeichnis des OpenSchoolServer unterscheidet sich vom LDAP-Verzeichnis des IServ.

LDAP-Settings	**Eintrag oder Einstellung**	**Erläuterung/Kommentar**
contexts	*ou=groups, dc=<iserv-url>, dc=<tld>*	
abject class	*posixGroup*	
group name attribute	*cn*	
group attribute	*memberuid*	
member attribute is dn	*No*	
Teacher settings	**Eintrag oder Einstellung**	**Erläuterung/Kommentar**
teachers group	*lehrer*	Name der Lehrkräftegruppe auf IServ, meist „lehrer“
teachers course role	*Student*	
teachers course prefix	*(leer lassen)*	
teacher category	*lehrer*	
teachers category role	*Course creator*	
teachers course teacher rolle	*Teacher*	
autocreate	*Yes*	
autoremove	*Yes*	
removed courses category	*attic*	
ignored teachers	*<leer lassen>*	
class settings	**Eintrag oder Einstellung**	**Erläuterung/Kommentar**
classes enabled	*No*	
classes category	*Klassenkursbereich*	
autocreate class category	*Yes*	
autocreate classes	*Yes*	
autoremove classes	*Yes*	
all students class	*Yes*	
age group class	*Yes*	
class template name	*none*	
class attribute	*memberOf*	
Use prefixes	*No*	
class prefixes	*05*	
attribute value	*departmentNumber*	
class teachers tole	*Teacher*	
class students role	*Student*	
class parents role	*Student*	
use groups	*No*	
teachers description	*Lehrer:in der Klasse*	
students description	*Schüler:in der Klasse*	
parents description	*Eltern der Klasse*	
Student settings	**Eintrag oder Einstellung**	**Erläuterung/Kommentar**
students group	*lehrer*	Name der Schueler:innengruppe auf IServ, meist „schueler“
grade numbers	*Student*	

other groups	*IServ-spezifisch*	Prefixe für weitere Schüler:innengruppen
project prefix	*lehrer*	
student role	*Student*	
parents settings	**Eintrag oder Einstellung**	**Erläuterung/Kommentar**
parents enabled	*No*	
create parents accounts	*No*	
remove parents accounts	*No*	
parents role	*Manager*	
parents prefix	*eltern_*	
child attribute	*uniqueidentifier*	