

LDAP / LDAPS Authentifizierung BelWü Moodle

Seit kurzem ist, für ein bei Belwue gehostetes Moodle, die Authentifizierung per ldaps gegenüber einem Server der paedML Linux in der Schule möglich. Durch die Änderung auf ldaps werden nun die Passwörter verschlüsselt übertragen, so dass sie nicht mehr abgehört werden können.

Sicherheitshalber sollte man aber immer einen administrativen Zugang zum Moodle vorsehen, der von Hand eingetragen wurde und bei dem die Authentifizierung von Moodle intern durchgeführt wird. Dies ist sinnvollerweise der bei der Erstinstallation schon eingerichtete Admin Nutzer, der sowieso nur für Notfälle eingesetzt werden sollte.

Anmerkung: Die Einstellungen in Moodle sind wohl für alle paedMLs identisch. Einzige Ausnahme: Einstellung zur Nutzerüberprüfung (user lookup settings): die Pfade im LDAP Server dürften sich wohl je nach paedML unterscheiden. Die Hinweise in Abschnitt 1.: Einstellungen im Netzwerk beziehen sich rein auf die paedML Linux.

1. Einstellungen im eigenen Netzwerk

Damit das Moodle bei Belwue mit dem LDAP / LDAPS Server der ML kommunizieren kann, muss moodle den Server der paedML4.x erreichen können, deswegen sind folgende Einstellungen erforderlich:

Am Router zum Provider (Belwue):

- Portweiterleitung für die Ports 389 (LDAP) und 636 (LDAPS) im Router von Belwue einrichten lassen bzw. einrichten

Am IPCOP des Schulnetzes:

- Im Webfrontend des IPCop muss unter „Firewall“ - „Port Weiterleitung“ eine neue Regel erstellt werden, die den Port 389 TCP für LDAP bzw. den Port 636 TCP für LDAPS auf den server (normalerweise 10.16.1.1) weiterleitet. Es ist darauf zu achten, dass diese Regel auch aktiviert ist (Häkchen im Kasten am Ende der Zeile).

2. Umstellen auf LDAP

Folgende Einstellungen sind im Moodle vorzunehmen, um die Benutzerauthentifizierung über den LDAP / LDAPS -Server der paedML Linux einzurichten:

Melden Sie sich als admin (s.o.) an Ihrem Moodle an. Gehen Sie im Block Website-Administration auf Nutzer /innen – Authentifizierung – Übersicht. „Öffnen“ Sie dort in der Zeile LDAP Server „das Auge“ und wählen Sie dann Einstellungen.



The screenshot shows the Moodle Website Administration interface. On the left is a navigation menu with categories like 'Mittellungen', 'NutzerInnen', 'Authentifizierung', 'Übersicht', 'Kein Login', 'LDAP-Server', 'Manuelle Zugänge', 'Nutzerkonten', 'Zugriffsrechte', 'Kurse', 'Bewertungen', 'Lokales', 'Sprache', 'Module', 'Sicherheit', and 'Darstellung'. The main content area is titled 'Übersicht' and contains a table 'Aktive Plugins zur Authentifizierung'.

Name	Aktivieren	Aufwärts/Abwärts	Einstellungen
Manuelle Zugänge			Einstellungen
Kein Login			Einstellungen
LDAP-Server	<input checked="" type="checkbox"/>		Einstellungen
CAS-Server (SSO)	<input type="checkbox"/>		Einstellungen
Externe Datenbank	<input type="checkbox"/>		Einstellungen

3. LDAP Server Einstellungen

Auf der Konfigurationsseite sind folgende Einstellungen vorzunehmen:

LDAP-Server

Diese Methode bietet die Authentifizierung gegenüber einem externen LDAP-Server. Wenn der vergebene Nutzernamen und Passwort gültig sind, erstellt Moodle einen neuen Nutzereintrag in seiner Datenbank. Dieses Modul kann Nutzereinträge aus LDAP lesen und gewünschte Felder in Moodle vorlegen. Für die nachfolgenden Zugänge werden nur Nutzernamen und Passwort überprüft.

LDAP Server-Einstellungen

Host URL: Geben Sie einen LDAP Server in URL-Form an wie 'ldap://ldap.myorg.de/' oder 'ldaps://ldap.myorg.de/'

Version: Diese Version des LDAP Protokolls nutzt Ihr Server.

LDAP Codierung: Geben Sie die Codierung des LDAP Servers an. Meist ist dies utf-8. MS AD v2 verwendet andere Codierung wie cp1252, cp1250, etc.

Bind-Einstellungen

Kennwörter verbergen: Wählen Sie ja, um Passwörter **nicht** in der Moodle-Datenbank zu speichern

Gekennzeichneter Name: Möchten Sie Bind-User für die Nutzersuche verwenden, so geben Sie dies hier an. Normalerweise etwas wie 'cn=ldapuser,ou=public,o=org'

Kennwort: Passwort für Bind-User.

Einstellung zur Nutzerüberprüfung (user lookup settings)

Nutzertyp: Auswahl, wie Nutzer in LDAP hinterlegt werden. Die Einstellungen legen fest wie der Login-Ablauf, grace Logins und Nutzererstellung ablaufen.

Kontexte: Liste der Umgebungen, in denen sich Nutzer/innen befinden. Trennen Sie verschiedene Umgebungen durch ';'. Beispiel: 'ou=users,o=org; ou=others,o=org'

Subkontexte suchen: Nutzer/innen in Teilumgebungen suchen

Alias berücksichtigen: Legt fest wie Aliasbezeichnungen bei der Suche behandelt werden. Wählen Sie einen der folgenden Werte: "No" (LDAP_DEREF_NEVER) or "Yes" (LDAP_DEREF_ALWAYS)

Nutzerattribut: Verwendete Eigenschaften, um Nutzer zu benennen/suchen. Normalerweise 'cn'.

Mitgliedsattribut: Geben Sie die Mitgliedsoptionen an, wenn Nutzer/innen zu einer Gruppe gehören. Normalerweise 'member'

Mitgliedsattribut nutzt dn: Optional: Überschreib-Handlung für Mitgliedsattribut-Werte, entweder 0 oder 1

Objekt Class: Filter für die Suche nach Nutzernamen. Normalerweise tragen Sie ein: objectClass=posixAccount . Defaults to objectClass=* what will return all objects from LDAP.

LDAP Server Einstellungen

Host URL:	<i>ldaps: //<IPAdresse></i> (falls man sich mit der einfacheren Authentifizierung per ldap begnügt, genügt hier einfach: ldap: //<IPAdresse> dies ist auch der einzige Unterschied zur Authentifizierung per ldaps)
Version:	3
LDAP Codierung:	<i>utf-8</i>

Bind-Einstellungen

Kennwörter verbergen (ldap-preventpassindb):	<i>nein</i>
Gekennzeichneter Name (ldap bind dn)	<i>Leer lassen</i>
Kennwort (ldap bind_pw):	<i>Leer lassen</i>



Einstellung zur Nutzerüberprüfung (user lookup settings)

Nutzertyp (ldap user type):	<i>posixAccount (rfc2307)</i>
Kontexte (ldap contexts)	<i>ou=accounts, dc=linuxmuster, dc=local</i> (der komplette Pfad muss wie oben eingetragen werden. Die Information für den fettgedruckten Teil muss in der Datei /etc/resolv.conf am Server nachgeschaut werden. Der Eintrag nach search muss entsprechend umgeschrieben werden. Die Zeile in der resolv.conf für das obige Beispiel lautet also: <i>search linuxmuster.local</i> d.h. Der Eintrag ou=accounts ist immer erforderlich. Für jeden durch Punkt getrennten Eintrag in der resolv.conf muss ein Eintrag dc=xxx vorhanden sein. Die Einträge müssen durch Leerzeichen und Komma getrennt werden.
Suchkontexte: (ldap_search_sub):	<i>ja</i>
Alias berücksichtigen: (ldap opt deref)	<i>nein</i>
Nutzerattribut: (ldap user attribute)	<i>uid</i>
Mitgliedsattribut: (ldap-memberattribute)	<i>member</i>
Mitgliedsattribut nutzt dn	<i>leer</i>
Objekt Class (ldap objectclass)	<i>objektClass=posixAccount</i>

Verbindliche Änderung des Passwortes

Verbindliche Änderung des Passwortes

Nutzer werden aufgefordert, ihr Passwort beim ersten Login zu ändern

Standardseite zur Passwortänderung nutzen

Stellen Sie Ja ein, wenn das externe Authentifizierungssystem eine Änderung des Passwortes durch Moodle zulässt. Die Einstellungen überschreiben 'Passwort-URL ändern'

Anmerkung: Es wird empfohlen LDAP über einen SSL verschlüsselten Tunnel (ldaps://) zu nutzen, wenn der LDAP Server remote verwendet wird.

Passwortformat

Format für neue oder geänderte Passworte auf LDAP-Server

URL zur Kennwortänderung

Hier können Sie eine Adresse angeben, unter der die Nutzer ihren Nutzernamen/Passwort ändern können, sofern sie dies vergessen haben. Diese Option wird den Nutzern als Schaltfläche auf der Anmeldungsseite angeboten. Wenn Sie dieses Feld leer lassen, wird die Option nicht angeboten.

LDAP PasswortablaufEinstellung

Ablauf

Setzen Sie Nein (no) um die Überprüfung abgelaufener Passworte abzuschalten oder LDAP um sie direkt über LDAP abzuwickeln.

Ablaufhinweis

Zahl der Tage vor dem Ablauf der Gültigkeit des Passwortes an denen eine Nachricht versandt wird.

Ablauf-Attribut

optional: Ändert die LDAP-Attribute zur Speicherung der Passwortgültigkeitsdauer passwordExpirationTime

Frist Login

Aktiviert LDAP graclelogin Unterstützung. Wenn das Passwort abgelaufen ist, können die Nutzer/innen sich weiter einloggen bis graclelogin den Wert 0 hat. Nach dem Aktivieren der Einstellung wird eine graclelogin Mitteilung angezeigt, wenn das Passwort abgelaufen ist.

grace Login Attribute

optional: Ändert die graclelogin Attribute

Nutzer-Erstellung aktivieren

Nutzer extern anlegen

Neue (anonyme) Nutzer können Nutzer-Accounts erstellen außerhalb der Authentifizierungsquelle und per E-Mail bestätigen. Sofern Sie dies aktivieren, achten Sie darauf, ebenso modulspezifische Optionen für die Modulerstellung zu konfigurieren.

Kontext für neue Nutzer

Wenn Sie die Nutzererstellung mit E-Mail-Bestätigung aktivieren, geben Sie die Umgebung an, wo die Nutzer/innen erstellt werden sollen. Diese Umgebung sollte sich von der anderer Nutzer/innen unterscheiden, um Sicherheitsrisiken zu vermeiden. Sie brauchen diese Umgebung nicht zur ldap_context Variable hinzuzufügen, Moodle sucht in dieser Umgebung automatisch nach Nutzer/innen.



Verbindliche Änderung des Passwortes

Verbindliche Änderung des Passwortes:	<i>nein</i>
Standardseite zur Passwortänderung nutzen:	<i>nein</i>
Passwortformat:	<i>Reiner Text</i>
URL zur Kennwortänderung:	<i>Leer lassen</i>

LDAP Passwortablaufeinstellung

Ablauf: (ldap expiration)	<i>no</i>
Ablaufhinweis: (ldap expiration warning)	<i>10</i>
Ablaufattribut: (ldap expireattr)	<i>Leer lassen</i>
Frist Login: (ldap_gracelogins)	<i>nein</i>
grade Login Attribute: (ldap_graceattr)	<i>Leer lassen</i>

Nutzer Einstellung aktivieren

Nutzer extern anlegen:	<i>nein</i>
Kontext für neue Nutzer: (ldap_create_context)	<i>Leer lassen</i>

Kursverwalter/in

Kursverwalter/innen: (ldap_creators):	<i>Leer lassen</i>
---------------------------------------	--------------------

Cron-Synchronisierungsskrip

Entfernte externe Nutzer	<i>Nur intern zugänglich</i>
--------------------------	------------------------------

NTLM SSO

Aktivieren	<i>nein</i>
Subnet	<i>Leer lassen</i>
MS IE fast path?	<i>nein</i>

Data mapping

Hier alles so lassen, außer einem Text im Textfeld, das über das Loginverfahren informiert.

Noch ein Hinweis: am moodle kann man sich dann aber nur anmelden, wenn die eigene paedML auch erreichbar ist!