

Beratung und Support
Technische Plattform
Support-Netz-Portal



paedML® – stabil und zuverlässig vernetzen

Anleitung

Anbindung eines externen LDAP-Dienstes am Beispiel von Moodle

Stand 10.07.2015

paedML® Linux

Version: 6.0

Impressum

Herausgeber

Landesmedienzentrum Baden-Württemberg (LMZ)
Support-Netz
Rotenbergstraße 111
70190 Stuttgart

Autoren

der Zentralen Expertengruppe Netze (ZEN),
Support-Netz, LMZ
Roland Walter

Endredaktion

Wird von der Redaktion eingetragen.

Bildnachweis Titelbilder:

Thinkstock

Weitere Informationen

www.support-netz.de
www.lmz-bw.de

Änderungen und Irrtümer vorbehalten.

Veröffentlicht: 2015

Die Nutzung dieses Handbuches ist ausschließlich für eigene Zwecke zulässig. Die Nutzung sowie die Weitergabe dieses Handbuches zu kommerziellen Zwecken wie z.B. Schulungen ist nur nach ausdrücklicher Einwilligung durch das LMZ erlaubt.

© Landesmedienzentrum Baden-Württemberg

Inhaltsverzeichnis

1.	Übersicht	5
2.	Portweiterleitung und Anpassung der Firewall.....	6
3.	Anpassungen an der paedML.....	9
4.	Konfiguration des externen Dienstes	12

Vorwort

In dieser Anleitung soll exemplarisch am Beispiel des bei BelWü gehosteten Programmes Moodle aufgezeigt werden, wie die Anbindung eines externen LDAP-Dienstes an die paedML Linux eingerichtet werden kann.

Voraussetzungen

1. Zunächst einmal muss ein externer Server eingerichtet sein, auf dem eine LDAP-Anmeldung konfiguriert werden kann. Für das Erstellen dieser Anleitung wurde bei www.belwue.de ein Moodle¹ gebucht, das so eingerichtet wird, dass sich Benutzer der paedML an dem externen Dienst anmelden können.

(Ein solcher Service kann natürlich auch im Schulnetz bereitgestellt werden, wobei die Einstellungen für den Zugriff auf den paedML-LDAP-Service entsprechend geändert werden müssen.)

2. Um den externen Zugriff auf den paedML LDAP zuzulassen, muss ein Port in Router und Firewall geöffnet werden.



Weder die Bereitstellung des externen Dienstes, noch die Konfiguration und die Bedienung eines externen Dienstes sind im Leistungspaket der paedML enthalten.

Die Mitarbeiter der Hotline können Sie lediglich in der Umsetzung der hier beschriebenen Anbindung eines externen Dienstes unterstützen.

Zielgruppe	Schwierigkeitsgrad
Händler, erfahrene Administratoren	mittel

¹ <http://www.belwue.de/produkte/dienste/moodle1.html>

1. Übersicht

Die Anmeldung an dem externen Service geschieht über eine Authentifizierung am paedML-Server. Hierfür muss der externe Service auf den LDAP-Dienst der paedML zugreifen können.

Mit seinen paedML-Zugangsdaten kann sich ein paedML-Benutzer an dem Service anmelden (1).

Der externe Server greift auf den LDAP-Baum der paedML zu und prüft, ob die Anmeldung zulässig ist (2).

Wenn die Anmeldedaten stimmen, wird dies von LDAP bestätigt (3) und der Benutzer wird am externen Dienst angemeldet (4).

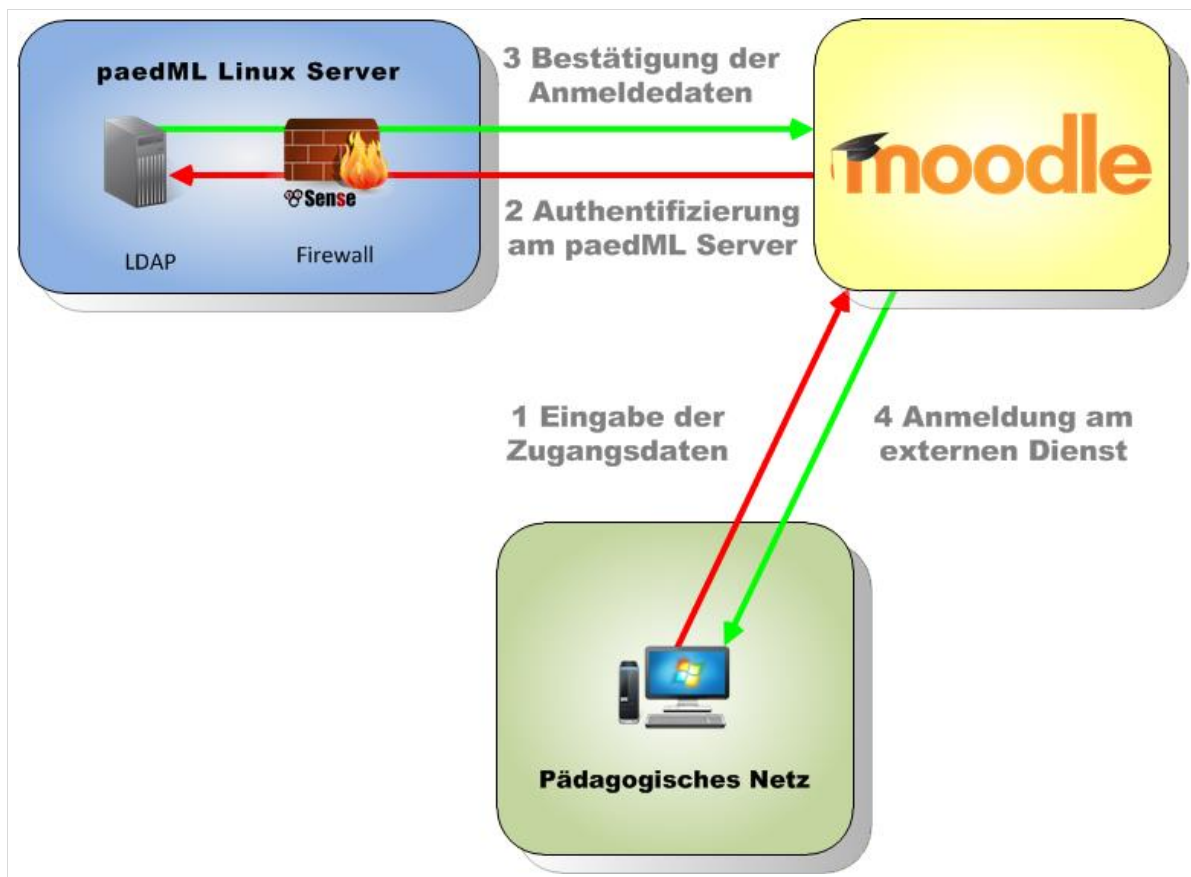


Abb. 1: Schematische Darstellung der Anmeldung an einem externen Dienst

2. Portweiterleitung und Anpassung der Firewall

Im ersten Schritt muss der externe Zugriff auf den LDAP-Server der paedML eingerichtet werden.

Um die Firewall einzurichten, müssen Sie sich als „Administrator“ unter <https://firewall.paedml-linux.lokal> an der pfSense-Firewall anmelden.

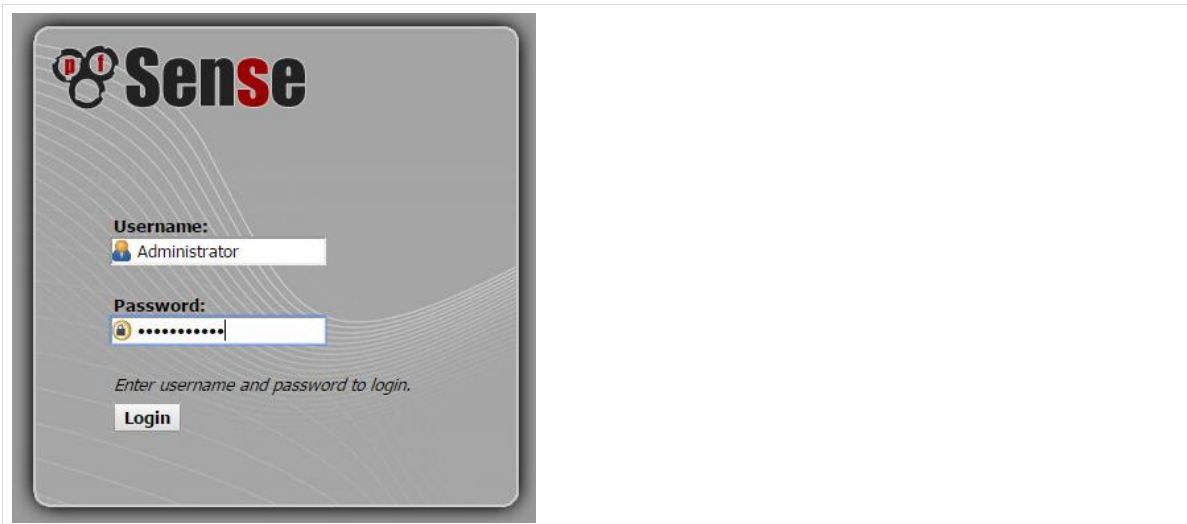


Abb. 2: Anmeldung an der Firewall

Über den Menüpunkt „**Firewall | NAT**“ gelangen Sie in die Konfigurationsmaske, in der das Port-Forwarding, also die Weiterleitung der externen Anfrage von Moodle, eingetragen wird.

Da die Firewall-Regel „**SSH-Zugriff auf den MASTER**“ als Vorlage genutzt werden kann, kopieren Sie diese Regel mit Hilfe der Kopier-Taste (Popup-Hilfetext „**add a new NAT based on this one**“).

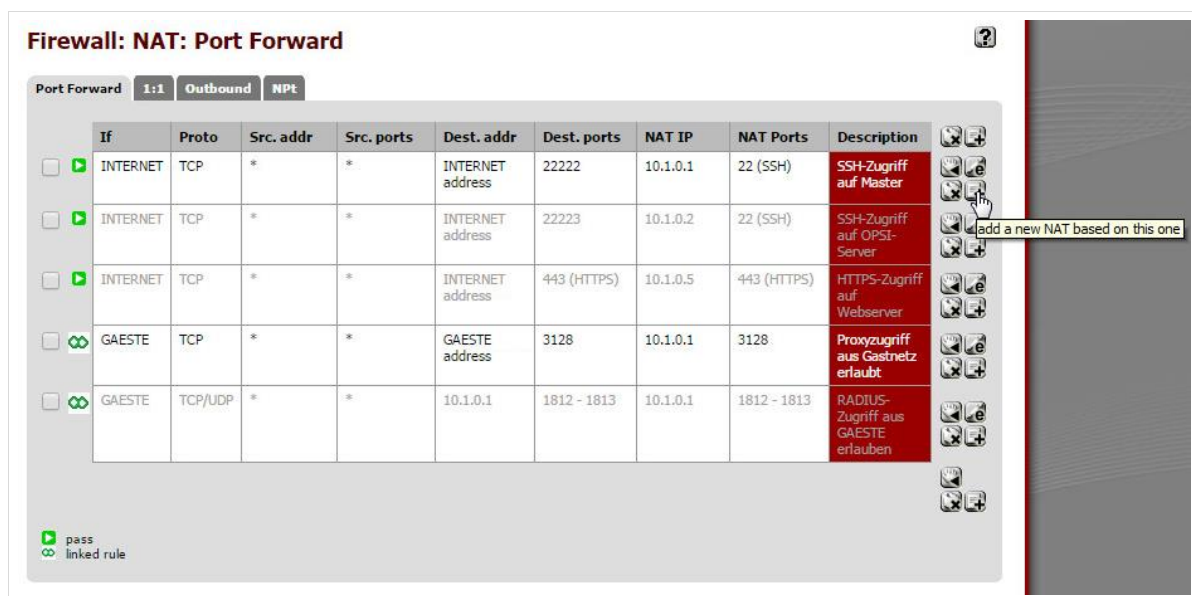


Abb. 3: Kopieren der vorhandenen NAT-Regel „SSH-Zugriff auf Master“

Es öffnet sich ein neuer Dialog, in dem die Einstellungen vorgenommen werden. Klicken Sie hier in der Zeile „Source“ zunächst auf „Advanced“, um weitere Optionen angezeigt zu bekommen.

Firewall: NAT: Port Forward: Edit

Edit Redirect entry	
Disabled	☐ Disable this rule Set this option to disable this rule without removing it from the list.
No RDR (NOT)	☐ Enabling this option will disable redirection for traffic matching this rule. Hint: this option is rarely needed, don't use this unless you know what you're doing.
Interface	INTERNET Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.
Protocol	TCP Choose which IP protocol this rule should match. Hint: in most cases, you should specify TCP here.
Source	Advanced Show source address and port range

Abb. 4: Anzeige weiterer Optionen über „Advanced“

Die kopierte Regel wird nun an die Anforderungen angepasst. Achten Sie im ersten Schritt darauf, dass die Checkbox bei „Disable this rule“ (1) nicht aktiv ist!

Es wird empfohlen den Zugriff auf die IP-Adresse des externen Services zu begrenzen. Wählen Sie hierfür in der Zeile „Source“ im Dropdown-Menü „Type“ den Eintrag „Single host or alias“ und tragen Sie im Feld „Address“ die IP-Adresse des externen Services, also bspw. der Moodle-Instanz, ein (2). **Wenn Sie unter „Source“ keine Einschränkungen vornehmen, dann wird der Zugriff auf den von Ihnen frei geschalteten Port NICHT auf eine IP-Adresse begrenzt. Wenn Sie mehrere externe Dienste an die paedML anbinden wollen, müssen Sie je externen Server eine eigene Firewall-Regel definieren.**

Die Zeile „Source port range“ muss auf die Werte „from any“ „to any“ eingestellt werden (3).

In der Zeile „Destination port range“ sind je Dropdown-Feld die Werte „other“ einzustellen. Anschließend müssen Sie in dem freien Feld den Port „7389“ (Port des openldap-Dienstes) eintragen (4).

Der Wert für „Redirect target IP“ muss auf den Server zeigen, also mit „10.1.0.1“ befüllt sein (5).

Im Feld „Redirect target port“ wählen Sie zunächst im Dropdown-Feld den Wert „(other)“ und tragen Sie anschließend wieder den Port „7389“ (Port des openldap-Dienstes) ein (6).

Unter „Description“ können Sie den Namen der Firewall-Regel eintragen, zum Beispiel „Moodle an Server“ (7).

Nachdem alle Werte gesetzt wurden, muss die Regel mit dem „Save“-Button, der sich ganz unten auf der Seite befindet, gespeichert werden.

Firewall: NAT: Port Forward: Edit

Edit Redirect entry

Disabled 1 ☐ **Disable this rule**
Set this option to disable this rule without removing it from the list.

No RDR (NOT) ☐ Enabling this option will disable redirection for traffic matching this rule.
Hint: this option is rarely needed, don't use this unless you know what you're doing.

Interface INTERNET
Choose which interface this rule applies to.
Hint: in most cases, you'll want to use WAN here.

Protocol TCP
Choose which IP protocol this rule should match.
Hint: in most cases, you should specify TCP here.

Source 2 ☐ **not**
Use this option to invert the sense of the match.

Type: Single host or alias
Address: 129.143.110.112 / ▼

Source port range 3
from: any to: any
Specify the source port or port range for this rule. This is usually random and almost never equal to the destination port range (and should usually be 'any').
Hint: you can leave the 'to' field empty if you only want to filter a single port.

Destination ☐ **not**
Use this option to invert the sense of the match.

Type: INTERNET address
Address: ▼

Destination port range 4
from: (other) 7389
to: (other) 7389
Specify the port or port range for the destination of the packet for this mapping.
Hint: you can leave the 'to' field empty if you only want to map a single port.

Redirect target IP 5 10.1.0.1
Enter the internal IP address of the server on which you want to map the ports.
e.g. 192.168.1.12

Redirect target port 6 (other) 7389
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
Hint: this is usually identical to the 'from' port above.

Description 7 Moodle an Server
You may enter a description here for your reference (not parsed).

No XMLRPC Sync ☒ Hint: This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

NAT reflection Use system default

Filter rule association Rule NAT Moodle an Server
[View the filter rule](#)

Abb. 5: Einstellungen der Port-Weiterleitung

Anschließend sehen Sie wieder auf die Übersichtsseite der Firewall-Regeln. Hier müssen abschließend alle Änderungen über den Knopf „**Apply changes**“ übernommen werden. Anschließend werden die Firewall-Regeln neu eingelesen.

Firewall: NAT: Port Forward

The NAT configuration has been changed. You must apply the changes in order for them to take effect. Apply changes

Port Forward		1:1	Outbound	NPT								
	If	Proto	Src. addr	Src. ports	Dest. addr	Dest. ports	NAT IP	NAT Ports	Description			
☐	INTERNET	TCP	*	*	INTERNET address	22222	10.1.0.1	22 (SSH)	SSH-Zugriff auf Master			
☐	INTERNET	TCP	129.143.110.112	*	INTERNET address	389 (LDAP)	10.1.0.1	7389	Moodle an Server			

Abb. 6: Übernahme mit „Apply changes“



Die Portweiterleitung muss – wie hier beschrieben – an der pfSense-Firewall sowie am Router Ihres Schulnetzes eingerichtet werden.

Die Konfiguration des Routers ist Aufgabe des Dienstleisters.

Wenn Sie Ihren Internet-Zugang über BelWü beziehen, dann muss BelWü diesen Port auf dem Router frei schalten.

Abb. 7: Port-Weiterleitung im Router (hier am Beispiel einer Fritz!Box)

3. Anpassungen an der paedML

Im nächsten Schritt muss ein Nutzer für die Authentifizierung erstellt werden. Melden Sie sich hierfür an der Schulkonsole ein und rufen Sie das Menü „**Domäne | Benutzer**“ auf.



Lehrer und Schüler dürfen NUR über das Schulkonsolen-Menü „**Schul-Administration | Benutzer (Schulen)**“ verwaltet werden.

In unserem Fall handelt es sich um einen Domänen-Benutzer.

Klicken Sie auf den Knopf „**Hinzufügen**“, um einen neuen Nutzer anzulegen.

Name	Pfad
Administrator	lokal.paedml-linux:/users
aproflehrer	lokal.paedml-linux:/users/templates
aprofschueler	lokal.paedml-linux:/users/templates
b.cullmann	lokal.paedml-linux:/schule/users/schueler
b.hoelzenbein	lokal.paedml-linux:/schule/users/schueler
b.vogts	lokal.paedml-linux:/schule/users/schueler

Abb. 8: Anlegen eines neuen Domänen-Benutzers über Hinzufügen

Im nächsten Dialog werden Sie nach einem „**Container**“ gefragt. Wählen Sie im Drop-Down-Feld den Eintrag „**lokal.paedml-linux:/users**“. Drücken Sie anschließend auf „**Weiter**“.

Container:

- lokal.paedml-linux:/schule/users/admins
- lokal.paedml-linux:/schule/users/admins
- lokal.paedml-linux:/schule/users/lehrer
- lokal.paedml-linux:/schule/users/lehrer und mitarbeiter
- lokal.paedml-linux:/schule/users/mitarbeiter
- lokal.paedml-linux:/schule/users/schueler
- lokal.paedml-linux:/users**
- lokal.paedml-linux:/users/templates

Abbrechen Weiter

Abb. 9: Auswahl des Benutzer-Containers

Im nächsten Dialogfeld wählen Sie „**Erweitert**“ aus. Anschließend kann ein neuer Domänen-Benutzer angelegt werden.

Im Reiter „**Allgemein**“ müssen die Felder „**Nachname**“, „**Benutzername**“ und die „**Passwort**“-Felder befüllt werden. Merken Sie sich das verwendete Passwort, da es später bei der Einrichtung der externen Moodle-Instanz benötigt wird.

Abb. 10: Reiter „Allgemein“

Wechseln Sie anschließend in den Reiter „**Optionen**“ und deaktivieren Sie alle Checkboxes, bis auf den Eintrag „**Einfaches Authentisierungskonto**“ (vgl. Screenshot).

Abb. 11: Auswahl der LDAP-Objekt-Eigenschaft

Wenn Sie alle Werte angepasst haben, können Sie mit dem Knopf „Benutzer anlegen“ den Vorgang abschließen.

4. Konfiguration des externen Dienstes

Nachdem die Konfiguration der paedML abgeschlossen ist, muss abschließend der externe Server für den Zugriff auf die paedML eingerichtet werden.



Die Konfiguration externer Dienste wird nicht durch die Mitarbeiter der Hotline des Support-Netzes unterstützt!

Melden Sie sich an dem externen Server (zum Beispiel an Moodle) an.

Abb. 12: Anmeldung an einem BelWü-Moodle



Bei der ersten Anmeldung an Moodle müssen Sie auf der Startseite Namen und Mailadresse des Moodle-Administrators hinterlegen (vgl. Abschnitt „General“ im folgenden Screenshot).

Erst danach können Sie mit der Konfiguration von Moodle fortfahren.

An der linken Seite befindet sich ein Navigationsmenü. Drücken Sie hier auf den Eintrag „Administration | Site administration | Plugins | Authentication | Manage Authentication“.

Abb. 13: Navigation zu den Authentifizierungs-Plugins

Deaktivieren Sie alle Plugins bis auf „**LDAP Server**“. Das (De-)Aktivieren der Plugins geschieht über einen Mausklick auf das **Auge**.

Nachdem alle Werte der Maske angepasst wurden, klicken Sie ganz unten auf den Knopf „**Save changes**“.

Name	Users	Enable	Up/Down	Settings	Test settings	Uninstall
Manual accounts	2			Settings		
No login	0			Settings		
LDAP server	0			Settings		
CAS server (SSO)	0			Settings		Uninstall

Abb. 14: Deaktivieren der Plugins

Bearbeiten Sie anschließend die Einstellungen für den LDAP-Server. Klicken Sie hierfür auf „**Settings**“.

Die folgende Maske umfasst einige Einstellungen, die jedoch nicht alle bearbeitet werden müssen. Im Folgenden wird die Maske in kleinere Abschnitte unterteilt. Zu jedem Abschnitt gibt es Erklärungen.

LDAP server settings

Als erstes muss die „**Host URL**“ eingetragen werden. Dies ist die externe Adresse unter der der paedML-Server erreichbar ist. Als Protokoll wird immer **ldap://**, verwendet, gefolgt vom DynDNS-Namen oder der IP-Adresse des Servers und dem Port **7389**.

Beispiele: „**ldap://meine-schule.dyndnsprovider.de:7389**“, „**ldap://129.143.110.112:7389**“

Die Version des LDAP-Protokolls ist „**3**“.

TLS sollte genutzt werden. Somit sollte der Wert „**Use TLS**“ auf „**Yes**“ gestellt werden.

Die Werte „LDAP encoding“ und „Page size“ bedürfen keiner Anpassung.

Bind settings

Unter „Bind Settings“ wird im Feld „Distinguished name“ der Name des in Kapitel 3 erstellten Domänennutzers, sowie der Pfad, unter dem der Benutzer im LDAP-Verzeichnis angelegt wurde, eingetragen.

Beispiel: „uid=moodle,cn=users,dc=paedml-linux,dc=lokal“

Dort wird auch das oben erstellte Passwort hinterlegt.

LDAP server

This method provides authentication against an external LDAP server. If the given username and password are valid, Moodle creates a new user entry in its database. This module can read user attributes from LDAP and prefill wanted fields in Moodle. For following logins only the username and password are checked.

LDAP server settings

Host URL Specify LDAP host in URL-form like 'ldap://ldap.myorg.com/' or 'ldaps://ldap.myorg.com/' Separate multipleservers with ';' to get failover support.

Version The version of the LDAP protocol your server is using.

Use TLS Use regular LDAP service (port 389) with TLS encryption

LDAP encoding Specify encoding used by LDAP server. Most probably utf-8, MS AD v2 uses default platform encoding such as cp1252, cp1250, etc.

Page Size Make sure this value is smaller than your LDAP server result set size limit (the maximum number of entries that can be returned in a single query)

Bind settings

Don't cache passwords Select yes to prevent passwords from being stored in Moodle's DB.

Distinguished name If you want to use bind-user to search users, specify it here. Something like 'cn=ldapuser,ou=public,o=org'

Password Password for bind-user.

☐ Unmask

Abb. 15: Konfiguration LDAP-Server (1)

User lookup settings

Hier wird der Wert für „User Type“ auf „Default“ belassen

In das Feld „Contexts“ tragen Sie den Container ein, in dem nach Benutzern gesucht wird. In dieses Feld muss „cn=users,ou=schule,dc=paedml-linux,dc=lokal“ eingetragen werden.

Der Wert „Search subcontexts“ sollte auf „Yes“ gestellt werden, „Dereference aliases“ ebenso.

Im Feld „User attribute“ wird der Eintrag „uid“ gewählt. Damit wird der Benutzername der paedML-Benutzer referiert.

Der Eintrag für das Feld „Member attribute“, wird auf „uniqueMember“ gesetzt.

Tragen Sie bei „Member attribute uses dn“ den Wert „1“ ein.

Alle Schüler und Lehrer teilen sich die „Object Class“ „univentionPerson“. Dieser Wert ist ebenfalls entsprechend einzutragen.

Force change password

In diesem Abschnitt müssen keine Änderungen vorgenommen werden.

User lookup settings

User type:

Contexts:

Search subcontexts:

Dereference aliases:

User attribute:

Member attribute:

Member attribute uses dn:

Object class:

Force change password

Force change password:

Use standard page for changing password:

Password format:

Password-change URL:

Select how users are stored in LDAP. This setting also specifies how login expiration, grace logins and user creation will work.

List of contexts where users are located. Separate different contexts with ','. For example: 'ou=users,o=org; ou=others,o=org'

Search users from subcontexts.

Determines how aliases are handled during search. Select one of the following values: "No" (LDAP_DEREF_NEVER) or "Yes" (LDAP_DEREF_ALWAYS)

Optional: Overrides the attribute used to name/search users. Usually 'cn'.

Optional: Overrides user member attribute, when users belongs to a group. Usually 'member'

Optional: Overrides handling of member attribute values, either 0 or 1

Optional: Overrides objectClass used to name/search users on ldap_user_type. Usually you dont need to change this.

Force users to change password on their first login to Moodle.

If the external authentication system allows password changes through Moodle, switch this to Yes. This setting overrides 'Change Password URL'.

NOTE: It is recommended that you use LDAP over an SSL encrypted tunnel (ldaps://) if the LDAP server is remote.

Specify the format of new or changed passwords in LDAP server.

Here you can specify a location at which your users can recover or change their username/password if they've forgotten it. This will be provided to users as a button on the login page and their user page. If you leave this blank the button will not be printed.

Abb. 16: Konfiguration LDAP-Server (2)

LDAP password expiration settings

In diesem Abschnitt müssen keine Änderungen vorgenommen werden.

Enable user creation

In diesem Abschnitt müssen keine Änderungen vorgenommen werden.

Course Creator

Da Lehrkräfte Kurse und/oder Klassen erstellen dürfen, muss im Feld „**Creators**“ der der entsprechende LDAP-Verzeichnispfad eingetragen werden:

„**cn=lehrer-schule,cn=groups,ou=schule,dc=paedml-linux,dc=lokal**“

Cron synchronization script

Unter „**Cron synchronization script**“ wählen sie als Wert für das Feld „**Removed ext user**“ den Wert „**Suspend internal**“ aus. Hiermit so werden nicht mehr vorhandene Nutzer zwar deaktiviert, Ihre Inhalte bleiben aber erhalten, auch wenn die Nutzer die Schule verlassen.

LDAP password expiration settings.

Expiration	no	Select No to disable expired password checking or LDAP to read passwordexpiration time directly from LDAP
Expiration warning	10	Number of days before password expiration warning is issued.
Expiration attribute		Optional: overrides ldap-attribute that stores password expiration time
Grace logins	No	Enable LDAP gracelogin support. After password has expired user can login until gracelogin count is 0. Enabling this setting displays grace login message if password is expired.
Grace login attribute		Optional: Overrides gracelogin attribute
Enable user creation		
Create users externally	No	New (anonymous) users can create user accounts on the external authentication source and confirmed via email. If you enable this , remember to also configure module-specific options for user creation.
Context for new users		If you enable user creation with email confirmation, specify the context where users are created. This context should be different from other users to prevent security issues. You don't need to add this context to ldap_context-variable, Moodle will search for users from this context automatically. Note! You have to modify the method user_create() in file auth/ldap/auth.php to make user creation work
Course creator		
Creators	cn=lehrer-schule,cn=groups,ou=schu	List of groups or contexts whose members are allowed to create new courses. Separate multiple groups with ','. Usually something like 'cn=teachers,ou=staff,o=myorg'
Cron synchronization script		
Removed ext user	Suspend internal	Specify what to do with internal user account during mass synchronization when user was removed from external source. Only suspended users are automatically revived if they reappear in ext source.

Abb. 17: Konfiguration LDAP-Server (3)

NTLM SSO

In diesem Abschnitt müssen keine Änderungen vorgenommen werden.

NTLM SSO

Enable	No	Set to yes to attempt Single Sign On with the NTLM domain. Note: this requires additional setup on the webserver to work, see http://docs.moodle.org/en/NTLM_authentication
Subnet		If set, it will only attempt SSO with clients in this subnet. Format: xxx.xxx.xxx.xxx/bitmask. Separate multiple subnets with ',' (comma).
MS IE fast path?	Attempt NTLM with all browsers	Set to enable the NTLM SSO fast path (bypasses certain steps if the client's browser is MS Internet Explorer).
Authentication type	NTLM	The authentication method configured in the web server to authenticate the users (if in doubt, choose NTLM)
Remote username format		If you have chosen 'NTLM' in 'Authentication type', you can specify the remote username format here. If you leave this empty, the default DOMAIN\username format will be used. You can use the optional %domain% placeholder to specify where the domain name appears, and the mandatory %username% placeholder to specify where the username appears. Some widely used formats are %domain%\%username% (MS Windows default), %domain%/%username%, %domain%+username% and just %username% (if there is no domain part).

Abb. 18: Konfiguration LDAP-Server (4)

Data mapping

Im letzten Abschnitt, „Data mapping“, werden die LDAP Einträge eingestellt, die beim Anlegen der Nutzer ausgewertet werden.

Hierfür müssen drei Felder bearbeitet werden:

1. Vorname („First Name“)
2. Nachname („Surname“)
3. „ID number“

Für jeden Eintrag müssen in den Drop-Down-Menüs die gleichen Einstellungen getätigt werden.

- Dabei sollten alle Werte lokal aktualisiert werden „Update local“ und dies bei jedem Login „On every login“.

- Jedoch niemals aus Moodle heraus im LDAP, d.h. für „Update external“ muss der Wert „Never“ gewählt werden.
- Des Weiteren sollten die Schüler und Lehrer keine Abweichungen zwischen LDAP und Moodle produzieren. Daher sollte für alle oben genannten Werte das Feld „Lock Value“ auf „Locked“ gesetzt werden.

Feldbezeichnung	Wert	Update local	Update external	Lock Value
First Name	givenName			
Surname	sn	On every login	never	Locked
ID number				

Data mapping

First name: givenName
 Update local: On every login
 Update external: Never
 Lock value: Locked

Surname: sn
 Update local: On every login
 Update external: Never
 Lock value: Locked

Email address:
 Update local: On creation
 Update external: Never
 Lock value: Unlocked

City/town:
 Update local: On creation
 Update external: Never
 Lock value: Unlocked

ID number: uidnumber
 Update local: On every login
 Update external: Never
 Lock value: Locked

These fields are optional. You can choose to pre-fill some Moodle user fields with information from the LDAP fields that you specify here. If you leave these fields blank, then nothing will be transferred from LDAP and Moodle defaults will be used instead. In either case, the user will be able to edit all of these fields after they log in.

Update local: If enabled, the field will be updated (from external auth) every time the user logs in or there is a user synchronization. Fields set to update locally should be locked.

Lock value: If enabled, will prevent Moodle users and admins from editing the field directly. Use this option if you are maintaining this data in the external auth system.

Update external: If enabled, the external auth will be updated when the user record is updated. Fields should be unlocked to allow edits.

Note: Updating external LDAP data requires that you set binddn and bindpw to a bind-user with editing privileges to all the user records. It currently does not preserve multi-valued attributes, and will remove extra values on update.

Abb. 19: Konfiguration LDAP-Server (5)

Nachdem alle Werte der Maske angepasst wurden, klicken Sie ganz unten auf den Knopf „Save changes“.

Die Konfiguration ist damit abgeschlossen. Sofern keine Fehler bestehen, können sich paedML-Benutzer nun an Moodle anmelden und damit arbeiten.

5. Einrichtung anderer Dienste

Das hier beschriebene Verfahren ist übertragbar auf sämtliche externen Anwendungen, die sich über LDAP gegen den paedML Linux Server authentifizieren.

Als Alternative können Sie auch lokal, im Netzwerk der paedML Linux eigene Dienste bereitstellen. Im Administrator-Handbuch ist beschrieben, welche IP-Adressen hierfür genutzt werden können.

Für vmware gibt es virtuelle Maschinen, in denen schon vorkonfigurierte Anwendungen sind, die für die Arbeit in der Schule genutzt werden können (z.B. <https://bitnami.com/stack/moodle/virtual-machine>).

Landesmedienzentrum Baden-Württemberg (LMZ)
Support Netz
Rotenbergstraße 111
70190 Stuttgart

© Landesmedienzentrum Baden-Württemberg, 2015