LDAP einrichten und konfigurieren unter Moodle

LDAP-SERVER EINRICHTEN

ZIEL

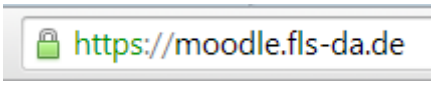
LDAP stellt einen Verzeichnisdienst zur Verfügung, der zur Speicherung und zum Wiederabruf von Informationen über einzelne Personen (z.B. ‚Lehrer und Schüler) einer Organisation genutzt werden kann. Die Bandbreite der Informationen, die auf diese Weise verfügbar gemacht werden können, ist recht groß: traditionelle Telefon- oder andere institutionelle Verzeichnisse (Lage von Büros, Telefonnummern usw.), Daten von LANiS-Benutzer-Accounts, persönlichere Daten, wie private Telefonnummern und Fotografien, zusammen mit weiteren spezifischen Daten.

HINWEIS IM BEREICH DATENSCHUTZ

LANiS stellt den Administratoren der Schulen LDAP Daten zur Verfügung, die dem Datenschutz unterliegen. Die Administratoren dürfen den privilegierten Zugang zu Daten der Schüler, Studierenden, Lehrkräften und Mitarbeiter ausschließlich für die Erleichterung schulinterner administrativer Abläufe einsetzen. Die Abfragen der Administratoren sind zudem nur auf Daten von Schüler, Studierenden, Lehrkräften und Mitarbeiter zu begrenzen, die direkt mit dem Lehrbetrieb ihrer entsprechenden Schule in Zusammenhang stehen.

Speziell ist zu beachten, dass das Führen einer oder mehrerer lokalen Kopien von Daten aus dem LDAP-Directory der Schule (z.B. Datenbank, lokales LDAP-Directory u.ä.) sowie die Nutzung der Daten für E-Mail oder andere Versände, die nicht unmittelbar mit dem Lehrbetrieb der Schule in Zusammenhang stehen untersagt sind. Untersagt ist auch die Weitergabe der spezifisch für die LDAP-Abfrage generierten Passörter und User-Accounts an Dritte.

Datenübertragung von Passwörtern sollte verschlüsselt erfolgen. Eine Möglichkeit zur Realisation eines solchen Datentransfers wäre z.B. eine von der Schule erstellte - SSL (https) geschützte! - Web-Seite, auf der sich interessierte Schüler, Studierenden, Lehrkräften und Mitarbeiter mit ihrem UID/Passwd einloggen, Ihre Daten aus dem LDAP-Directory abholen und andere Daten der Schule zur Verfügung stellen (eine entsprechende Bemerkung müsste auf der Web-Seite gut ersichtlich angebracht werden). Dies verlangt leider ein bisschen Programmierarbeit.



VORAUSSETZUNG

Installiertes Moodle in der Schule oder bei einen Web-Provider (wird empfohlen).

LDAP einrichten und konfigurieren unter Moodle

LDAP ABFRAGE EINRICHTEN

Melden Sie sich als Admin an und gehen Sie auf LDAP-Server.

LDAP-SERVER-EINSTELLUNGEN

Host URL	ldaps://10.0.249.2	Gib einen LDAP Server in URL-Form an wie 'ldap://ldap.myorg.de/' oder 'ldaps://ldap.myorg.de/' Bei externen Server die öffentliche Adresse eintragen.
Version	3	Diese Version des LDAP Protokolls nutzt dein Server.
TLS benutzen	Ja	LDAP-Service mit TLS (über Port 389) verschlüsseln
LDAP-Codierung	utf-8	Die Codierung des LDAP-Servers sollte standardmäßig utf-8 sein, aber das Microsoft ActiveDirectory v2 verwendet andere Codierungen, z.B. cp1252 oder cp1250.
Einträge pro Seite	250	Stellen Sie sicher, dass dieser Wert kleiner ist als die Obergrenze Ihres LDAP-Servers für eine einzelne Datenbankabfrage.

BIND-EINSTELLUNGEN

Kennworte nicht cachen	Ja	Wähle ja, um Passwörter nicht in der Moodle-Datenbank zu speichern
Anmeldename	CN=Administrator,CN=Users,DC	Möchtest du Bind-User für die Nutzersuche verwenden, so gib dies hier an. Normalerweise etwas wie 'cn=ldapuser,ou=public,o=org' Die Struktur Ihrer internen AD beachten.
Kennwort	**********	Kennwort des Bind-Users
	☐ Klartext	

NUTZERSUCHE (USER LOOKUP)

Nutzertyp	MS ActiveDirectory	Wählen Sie, wie die Nutzerdaten in LDAP hinterlegt sind. Diese Einstellungen legen auch fest, wie das Gültigkeitsende für Kennworte, die GraceLogins und das Anlegen neuer Nutzer in LDAP funktionieren.
Kontexte	ou=lanis-ldap,dc=domain,dc=loc	Liste der Umgebungen, in denen sich Nutzer/innen befinden. Trenne verschiedene Umgebungen durch ';'. Beispiel: 'ou=users,o=org; ou=others,o=org' lanis-ldap wird durch das LANiS-Tool zur Verfügung gestellt (siehe LANiS-Support)
Subkontexte	Ja	Nutzersuche auch in Subkontexten durchführen
Aliase berücksichtigen	Nein	Legt fest wie Aliasbezeichnungen bei der Suche behandelt werden. Wähle einen der folgenden Werte: "No" (LDAP_DEREF_NEVER) or "Yes" (LDAP_DEREF_ALWAYS)
Nutzermerkmal	samaccountname	Optional: Merkmal zur Nutzerbenennung und -suche ändern. Normalerweise 'cn'.

KENNWORTÄNDERUNG FORDERN

Kennwortänderung fordern	Nein	Nutzer/innen werden aufgefordert, ihr Kennwort beim ersten Anmelden zu ändern. Nein=da immer die Änderung von LANiS einfließen.
Standardseite zur Kennwortänderung nutzen	Nein	Stelle Ja ein, wenn das externe Authentifizierungssystem eine Änderung des Passwortes durch Moodle zulässt. Die Einstellungen überschreiben 'Passwort-URL ändern' Achtung: Es wird dringend empfohlen, LDAP ausschließlich SSL-verschlüsselt zu benutzen (ldaps://), wenn ein externer LDAP-Server verwendet wird.
Kennwortformat	MD5-Verschlüsselung	Geben Sie das Format für neue Kennworte auf dem LDAP-Server an.
URL zur Kennwortänderung		Hier kannst du 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 du dieses Feld leer lässt, wird die Option nicht angeboten.

GÜLTIGKEITSABLAUF VON KENNWORTEN

Gültigkeitsende	no	Setze Nein (no), um die Überprüfung abgelaufener Kennworte abzuschalten, oder LDAP, um sie direkt über LDAP abzuwickeln.
Warnung zum Gültigkeitsende	10	Diese Zahl gibt an, wie viele Tage vor dem Gültigkeitsende von Kennworten eine Warnung versendet wird.
Merkmal für Gültigkeitsende		Optional: Merkmal für Gültigkeitsende ändern
GraceLogins	Nein	LDAP-GraceLogin aktivieren. Wenn das Gültigkeitsende von Kennworten erreicht ist, können sich die Nutzer/innen noch solange weiter einloggen, bis der GraceLogin-Zähler den Wert 0 hat. Nach dem Aktivieren der Einstellung wird eine GraceLogin-Mitteilung angezeigt, sobald die Gültigkeitsende erreicht ist.
Merkmal für GraceLogin		Optional: Merkmal für GraceLogin ändern

NUTZERERSTELLUNG AKTIVIEREN

Nutzer/innen extern anlegen	Nein	Neue (anonyme) Nutzer können Nutzer-Accounts erstellen außerhalb der Authentifizierungsquelle und per E-Mail bestätigen. Sofern du dies aktivierst, achte darauf, ebenso modulspezifische Optionen für die Modulerstellung zu konfigurieren. Ja=wenn Sie auch externen den Zugang geben möchten. Kurse etc.
Kontext für neue Nutzer/innen		Wenn du die Nutzererstellung mit E-Mail-Bestätigung aktivierst, gib die Umgebung an, wo die Nutzer/innen erstellt werden sollen. Diese Umgebung sollte sich von der anderer er Nutzer/innen unterscheiden, um Sicherheitsrisiken zu vermeiden. Du brauchst diese Umgebung nicht zur ldap_context Variable hinzuzufügen, Moodle sucht in dieser Umgebung automatisch nach Nutzer/innen.

Kursersteller/in

Kursersteller/innen	OU=LANiS-LDAP,DC=domain,DC=lo	Eine Liste von Gruppen, denen es erlaubt ist, neue Kurse zu erstellen. Trenne mehrere Gruppen durch ';'. Normalerweise etwas wie 'cn=teachers, ou=staff, o=myorg'

Cron-Synchronisierungsskript

Entfernte externe Nutzer	Nur intern zugänglich	Legen Sie fest, was mit einem internen Nutzerprofil passieren soll, wenn bei einer Massensynchronisierung dieser Account im externen System entfernt wurde. Nur gesperrte Nutzer werden automatisch reaktiviert, wenn sie in der externen Quelle wieder erscheinen.

NTLM-SSO

Aktivieren	Nein	Aktivieren Sie diese Einstellung, um die einmalige Anmeldung (Single Sign On) mit der NTML-Domain zu versuchen. Anmerkung: Zusätzlich sind Einstellungen für den Webserver notwendig. Siehehttp://docs.moodle.org/en/NTLM_authentication
Subnet		Tragen Sie in dieses Feld eine Maske für ein Subnet ein, um NTLM-SSO auf IP-Adressen aus diesem Subnet zu beschränken. Mehrere Subnetze werden kommagetrennt angegeben. Format: xxx.xxx.xxx.xxx/bitmask

MS IE fast path?	NTLM mit allen Brow sern versuchen	Wenn diese Option aktiviert ist, wird der 'NTLM SSO fast path' zugelassen. Das funktioniert nur mit dem Internet Explorer.
Authentifizierungsart	NTLM	Diese Methode ist beim Webserver eingestellt, um Nutzer/innen zu authentifizieren. Falls Sie sich nicht sicher sind, wählen Sie bitte NTLM.
Format externer Nutzernamen		Wenn Sie 'NTLM' als 'Authentifizierungstyp' verwenden, können Sie hier das Format von externen Nutzernamen angeben. Bleibt der Eintrag leer wird das Standardformat verwendet. Verwenden Sie den optionalen%domain% Platzhalter, um festzulegen wo der Domainname erscheint und den erforderlichen Platzhalter %username% für den Nutzernamenort. Häufig genutzte Formate sind%domain%%username% (MS Windows default), %domain%/%username%,%domain%+%username% und einfach%username% (wenn kein Domainteil verwendet wird).

LDAP DATEN ZUORDNEN

Vorname	givenName
Nachname	sn
E-Mail-Adresse	Mail
Institution	company
Abteilung	department
Klassenbezeichnung	department

Andere Informationen sind aus Datenschutzgründen nicht interessant und zu vernachlässigen.

Bei diesen Feldern sollten Sie folgende Einstellungen vornehmen:

Lokal aktualisieren	Beim Anlegen
Extern aktualisieren	Nie
Feld sperren	Bearbeitbar (w enn leer)

Grundsätzlich zählt hier die Regel, wenn Sie diese Felder leer lassen, wird nichts von LDAP transferiert und die Moodle Voreinstellungen werden verwendet.