LDAP Authentifizierung an einem paedML Windows Server

Standardmäßig verwendet openSchulportfolio eine eigene Benutzerverwaltung. Benutzer können vom Administrator des Portfoliosangelegt, verändert oder gelöscht werden, nähere Informationen hierzu finden Sie auf der Seite "Benutzer verwalten" der Dokumentation.

Dies bedeutet, dass sich Lehrer zusätzliche Benutzerdaten merken müssen. Komfortabler ist es, wenn ein Lehrer sich mit seinem **Benutzerkonto aus dem Schulnetz anmelden kann**. Die hierfür notwendigen Schritte werden hier dargestellt.

Technischer Hintergrund

Nachdem ein Lehrer seine Benutzerdaten eingegeben hat, sendet openSchulportfolio eine sogenannte LDAP Abfrage an das Active Directory des paedML Windows Server. Als Antwort erhält openSchulportfolio dann die Informationen, ob der Benutzer mit dem eingegebenen Kennwort im Active Directory existiert und welchen Gruppen er angehört. So wird dann entscheiden, ob der Benutzer sich anmelden kann und welche Berechtigungen er erhält.

Voraussetzungen

- Im Router muss der Port 389 für LDAP geöffnet werden (LDAPS noch nicht gelöst).

Konfigurationsdateien auf dem Webserver (z.B. Belwue) ersetzen und anpassen

Zunächst muss die Konfiguration von openSchulportfolio geändert werden.

- Ersetzen sie hierfür die die beiden Dateien `acl.auth.php` und `local.php` aus dem Verzeichnis `\portfolio\conf` durch die aus dem ZIP Paket conf_paedml_windows_belwue.zip
  - Hintergrund: In der Datei `acl.auth.php` stehen die Zugriffsberechtigungen der verschiedenen Gruppen. Hier wird z.B. festgelegt, dass die Projektgruppe portfoliored (Redakteure des Portfolios) die zum Verfassen von Artikeln notwendigen Berechtigungen hat. Man sieht die Einstellungen im Adminbereich des Portfolios unter Zugangsverwaltung. Hier lassen sich auch einfach Änderungen vornehmen.
  - Hintergrund: In der Datei `localh.php` stehen wichtige Konfigurationseinstellungen des Portfolios. Diese Datei sollten Sie möglichst nicht direkt editieren, mit Ausnahme der unten dargestellten Änderungen.
- Öffnen Sie die Datei local.php mit WinSCP (z.B. per Doppelklick)
- Nehmen Sie im oberen Bereich der Datei folgende Änderungen vor:
  - Zeile 13: `$conf['auth']['ad']['domain_controllers'] = '141.10.111.222';` Tragen Sie hier die IP Adresse der externen Netzwerkkarte des paedML Servers ein

- Zeile 14: `$conf['auth']['ad']['ad_password'] = 'muster';` ersetzen Sie *muster* durch ein möglichst sicheres Passwort. Dieses Passwort geben Sie später einem neu anzulegenden Benutzer (*ldapabfrage*), unter dessen Account openSchulportfolio eine LDAP Abfrage an das Active Directory ausführt.
- Zeile 15: `$conf['auth_security_timeout'] = 60;` Dieser Wert legt in Sekunden fest, nach welcher Zeit man sich mit einem anderen Benutzerkonto anmelden kann. Stellen Sie nach erfolgreicher Installation und Konfiguratin den Wert `60` wieder auf die Voreinstellung `900`.

Kommt es bei der Authentifizierung via LDAP zu Fehlermeldungen, so tragen Sie bei `$conf['manager'] = ' ';` einen beliebigen Wert ein, offenbar muss hier bei manchen Konstellationen etwas drinstehen.

Arbeiten am paedML Windows Server

Neue Zugriffsregel für den ISA Server erstellen

Erstellen Sie im ISA Server eine neue Zugriffsregel mit folgenden Einstellnungen.

- Name: Ldap ermöglichen
- Aktion: Zulassen
- Protokolle: LDAP
- Von: Extern
- Bis: Local Host (bei Drei-Serverlösung reicht das vermutlich nicht, da auf dem S3 kein AD installiert ist.)

Benutzer für LDAP Abfrage

Openschulportfolio sendet eine LDAP Abfrage ans Active Directory. Hierfür werden die Benutzerdaten eines Benutzers der Domäne verwendet. Es wird empfohlen, hierfür einen neuen Benutzer namens ldapabfrage anzulegen.

- Erstellen Sie im Active Directory in der OU Users einen neuen Benutzer mit folgenden Einstellungen:
  - *Vollständiger Name* und *Benutzeranmeldename*: `ldapabfrage`
  - Kennwort: gleiches Kennwort, das Sie in der Datei local.php eingegeben haben
  - Kennwort läuft nie ab
  - kein Exchange Konto

Wie sie eine Zugriffsregel erstellen, wird in dieser Anleitung beschrieben:
http://lehrerfortbildung-bw.de/netz/muster/win2000/material/basis30/pdf/isa06tipps.pdf

Projektgruppen in der Schulkonsole

Die Zugriffssteuerung auf das Portfolio erfolgt über die Zugehörigkeit zu Gruppen im Active Directory.

Beschreibung	Name der Benutzergruppe im AD	Berechtigungen

Alle außer Lehrer	-	Kein Zugriff
Lehrer	`G_Lehrer`	Lesen
Redakteure = Projektgruppe `portfoliored`	`g_projekt_portfoliored`	Artikel verfassen
Superuser mit Adminrechten = Projektgruppe `portfolioadm`	`g_projekt_portfolioadm`	Konfiguration

Hierfür müssen Sie nun die zwei oben beschriebenen Projektgruppen über die Schulkonsole erstellen. Achten Sie auf die Schreibweise! Fügen Sie den Projektgruppen die gewünschten Lehrer hinzu.

- `portfoliored`
- `portfolioadm`

Anleitung erstellt von Andreas Mayer. Danke an Tamer Berber, ohne dessen Vorarbeit und Unterstützung diese Anleitung nicht möglich gewesen wäre.