Ich versuche gerade, einen User zu erstellen, mit dem man eine PHP-Seite gegen UCS authentifizieren kann

Hier eine kleine Anleitung

PHP-Binding gegen UCS

User erstellen

Zunächst braucht man einen User, der sehr wenige Rechte hat. Dieser wird über „Domäne - LDAP-Verzeichnis - Users - Hinzufügen“ erstellt. Der Kontotyp soll „Einfaches Authentisierungskonto“ sein. Dieser User kann nur in der Domäne suchen. Ein Nutzername und ein Passwort festlegen (Passwort-History ignorieren kann man aktivieren, Passwort-Prüfungen ignorieren kann man auch aktivieren, da man ja sowieso starke Passwörter benutzt) und schon ist er fertig.

Apropos Passwort:

Diese kann ruhig lang und durch einen Generator erzeugt worden sein. Man braucht es nur zur Authentifizierung und muss es nur einmal eingeben.

Logindaten herausfinden

LDAP-usernamen sind etwas kryptisch, sowie case sensitve. Deshalb sollte man sich die distingishedNames auflisten lassen und kopieren. Auf der UCS sollte man mit diesem Kommando den dn angezeigt bekommen

```
univentions-ldapsearch uid=<Kontenname> dn
```

User testen

Jetzt muss der Benutzername auch noch von außen zugänglich sein

```
ldapsearch -x -h <ad-server>
```

Es sollte eine positive Rückmeldung kommen. Dies zeigt, dass hier ein LDAP-Server arbeitet.

Jetzt kann man den User testen:

```
ldapsearch -x -h <ad-server> -D <uid=test,dc=domain> -W
```

Hier muss exakt der dn von der ucs genommen werden (case sensitive).

Sollte eine positivie Rückmeldung kommen, passt alles. Sollte diese Rückmeldung negative sein (invalid credentials) gibt es folgende Möglichkeiten

- Passwort ist falsch
- dn ist falsch geschrieben
- irgendetwas blockiert die verbindung (Firewall?)
- ist der Port für das LDAP richtig (UCS LDAP)

Jetzt

username in der php-Applikation testen

Sollte hier die Meldung invalid credentials kommen, kann es an selinux liegen.

```
getsebool httpd_can_connect_ldap
httpd_can_connect_ldap --> off
```

Hier ist es per selinux-Boolean verboten, dass der httpd-Server auf ldap zugreifen kann. Dies löst man über

```
setsebool httpd_can_connect_ldap on
```

Quellen

- https://wiki.univention.de/index.php/Cool_Solution_-_LDAP_search_user