LDAP integratie

context

dit document beschrijft hoe je DokuWiki instelt zodat gebruikers voortaan met hun LDAP gebruiker/wachtwoord kunnen aanmelden. Biedt het grote voordeel dat je bestaande gebruikers kunt gebruiken en dus geen extra DokuWiki gebruikers moet aanmaken. Ook toegangsrechten op DokuWiki kunnen we op die manier instellen.

systeemvereisten

- verbindingsinstellingen van LDAP:
  - naam van de server en poort waarop die luistert
  - gebruiker die de BIND maakt (indien geen anonieme LDAP)
  - plaats in LDAP waar gebruiker/groepen te vinden zijn
- een LDAP browser waarmee je je LDAP kunt bevragen. Apache Directory Studio is goed gerief.
- beheerder toegang op DokuWiki
- root toegang op de Linux waarop DokuWiki draait.

installatie

Linux server

- meld aan als root
- installeer volgende pakketten:
  - php-ldap
  - php-net-ldap3
  - ldap-utils
  - tshark
- controleer verbinding naar je LDAP server: `telnet <ip_ldapserver> 389 (of 636)`
- voer een LDAP query uit (lijst van gebruiker): ''ldapsearch -H “ldaps:<ip_ldapserver>” -x -b “ou=Users,o=<BASEDIR>,dc=<jouwdomein>,dc=<extentie>” -D ”<BIND gebruiker>“ -W ”(objectClass=posixGroup)“ ''

Belangrijk is dat je vanaf je Linux LDAP queries kunt uitvoeren. Zorg dat dit probleemloos werkt voor je DokuWiki configureert. Troubleshoot voor je verdergaat!

Dokuwiki

1. meld aan als admin
2. ga naar **Admin** > **Extension Manager** > **LDAP Auth Plugin**: **Enable**
3. ga naar **Admin** > **Configuration Settings** > **Authentication** > **Authentication backend**: authldap

4. ga naar **Admin** > **Configuration Settings** > **Authentication** > **Superuser**: @<ldap_groep>
5. ga naar **Admin** > **Configuration Settings** > **Plugin ** > **Authldap**
6. vul de gegevens van je LDAP in.
7. De voorgestelde waarden zijn in grote mate bruikbaar. In mijn geval gaven de groupfilters geen resultaten weer, waardoor ik het groepsprofiel van de aangemelde gebruiker niet terug kreeg. Start in dat geval je LDAP browser en zoek daar de correct waarden op.
8. zet zeker de waarde **Display additional debug information on errors“** aan. Dat helpt om fouten bij de verbinding op te lossen.
9. hieronder een voorbeeld van mijn LDAP configuratie voor mijn Jumpcloud LDAP. (ik weet dat ik zou moeten obfusceren, maar dat maakt je screenshot zo vies en de LDAP is toch met BINDuser beveiligt ...)

1. ga naar **Admin** > **Configuration Settings** > **Authentication** > **Authentication backend**: authldap
2. ga naar **Admin** > **Configuration Settings** > **Authentication** > **Password encryption method**: md5
3. meld af als admin
4. meld nu aan met een LDAPgebruiker.
5. analyseer de debug output.
    1. LDAP server gaat op zoek naar de gebruiker
    2. resultaat van de zoekactie
    3. LDAP server zoekt groepen van betreffende gebruiker op
    4. resultaat van de zoekactie

post installatie

Als alles goed blijkt te werken, zet debug dan uit:

1. ga naar **Admin** > **Configuration Settings** > **Plugin ** > **Authldap**
2. zet de waarde **Display additional debug information on errors”** uit.

problemen, problemen

Niets lukt meteen. Bovenstaand voorbeeld was dan ook het resultaat van behoorlijk wat proberen. Hieronder de eerste hulp

authenticatie

als de authenticatie module volledig kapot is, kan je best je aanpassing terug draaien door onderstaande bestanden te hernoemen:

1. /var/www/dokuwiki/conf/local.php.bak > /var/www/dokuwiki/conf/local.php
2. /var/www/dokuwiki/conf/plugins.php.bak > /var/www/dokuwiki/conf/plugins.php

3. /var/www/dokuwiki/conf/users.auth.php.bak > /var/www/dokuwiki/conf/users.auth.php

LDAP verbinding

1. monitor het netwerk verkeer tussen Linux en LDAP: `tshark -f "host <ip_ldap>"`
2. thark toont je de hele verbinding tussen Linux server en je LDAP server. Vaak vind je daar al een eerste aanwijzing

LDAP query

1. voer de query die door DokuWiki wordt uitgevoerd uit in je LDAP browser.
2. controleer of de ingestelde filters/paden overeenkomen met de structuur van je LDAP tree. Zo staan in Jumpcloud LDAP groepen niet in de OU **Groups**, maar in de OU **Users**. Groeplidmaatschap wordt niet uitlezen in de objectclass PosixGroepen maar in groupOfNames. Zoek en ge zult vinden, mijn zoon.

From:
https://louslab.be/ - **Lou's lab**

Permanent link:
https://louslab.be/doku.php?id=dokuwiki:security:ldap&rev=1731780894

Last update: **2024/11/16 18:14**