Konfiguracja autentykacji LDAP / Active Directory

Menu

Wprowadzenie

System eDokumenty umożliwia oprócz wbudowanego mechanizmu autentykcji, uwierzytelnianie użytkowników systemu w katalogu LDAP (w tym również ActiveDirectory).

Użytkownik po wejściu na stronę logowania podaje login i hasło które są zgodne z nazwą i hasłem w katalogu LDAP. System przekazuje dane do serwera LDAP który przeprowadza wyszukiwanie w swoim katalogu. W przypadku pomyślnego przebiegu procesu autentykacji następuje wejście do systemu oraz automatyczna aktualizacja podanego hasła w bazie eDokumenty.

Automatyczne tworzenie konta w eDokumenty po pierwszym logowaniu

Jeżeli user jest w ActiveDirectory i zaloguje się pierwszy raz do systemu z użyciem poprawnego hasła wówczas system eDokumenty utworzy jego konto w bazie eDokumenty i doda tego użytkownika do tych **grup** do których jest przypisany w LDAP i które również obecne są w systemie eDokumenty. Niestety takie konto nie będzie jeszcze pozwalało na pracę w systemie gdyż wymagane jest przypisanie nowego użytkownika do stanowiska w strukturze organizacyjnej. Może to zrobić jedynie administrator w panelu *Pracownicy*.

Przejdź do Menu

Instalacja wymaganych bibliotek

Do współpracy eDokumentów z LDAP oraz Active Directory wymagane jest zainstalowanie obsługi LDAP przez PHP. Obsługę taką zawiera pakiet php5-ldap (dla linuksa). Szczegóły są dostępne na stronie http://www.php.net/ldap.

Jeżeli pakiet w Debianie nie jest zainstalowany, to należy wykonać następujące polecenia (z poziomu użytkownika root):

1. Odświeżenie repozytoriów

```
root@pc# apt-get update
```

1. Odświeżenie repozytoriów

```
root@pc# apt-get install php5-ldap
```

1. Po instalacji należy zrestartować serwer Apache'a

```
root@pc# /etc/init.d/apache2 restart
```

W systemie Windows w katalogu `C:\Program Files\php\ext` powinien znajdować się plik `php-ldap.dll`. Aby parser php mógł skorzystać z tej biblioteki nalezy w pliku php.ini odkomentować rozszerzenie: `;extension=php_ldap.dll` usuwając symbol średnika sprzed wyrażenia. Ostatnim krokiem jest zrestartowanie serwera Apache.

Przejdź do Menu

Autentykacja przy pomocy LDAP

Ta część niniejszego artykułu dotyczyć będzie autentykacji przy pomocy protokołu LDAP. Zakłada się tutaj, iż mamy w systemie Windows bądź Linux zainstalowany serwer LDAP - przykładowo: OpenLDAP http://www.openldap.org/ (linux) oraz http://www.userbooster.de/en/download/openldap-for-windows.aspx (windows).

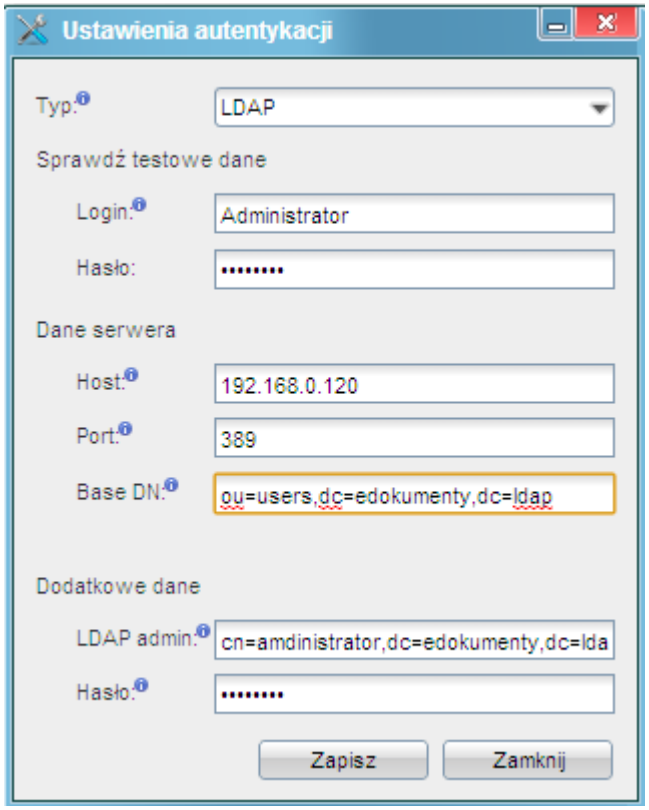
Przejdź do Menu

konfiguracja eDokumentów do autentykacji LDAP

Po zdefiniowaniu użytkowników na serwerze LDAP, należy przejść do eDokumentów, i zdefiniować sposób autentykacji. Wykonuje się to w menu *Ustawienia* > *Panel Sterowania* > *Autentykacja*. Otwiera się okienko, gdzie wybieramy *Typ: LDAP*. Pojawiają się nam pola, gdzie wprowadzamy:

- Dane serwera, w tym:
  - Host - adres IP lub nazwę serwera LDAP
  - Port - port serwera LDAP, domyślnie 389.
  - BaseDN: - adres bazy danych, w której będą wyszukiwaniu użytkownicy LDAP. Należy sprawdzić w konfiguracji LDAP. Przykład: *OU=users,DC=edokumenty,DC=ldap*.
- Dodatkowe dane:
  - LDAP admin - dane użytkownika, który posiada uprawnienia do przeszukiwania zasobów LDAP, np. CN=amdinistrator,DC=edokumenty,DC=ldap
  - Hasło - hasło dla powyższego użytkownika.

Dodatkowo warto przetestować połączenie wprowadzając dane użytkownika, dla którego zostanie przeprowadzona testowa autentykacja.



(Rys.1)

Dane z powyższego formularza są wprowadzone do pliku `config.inc`, którego fragment dotyczący autentykacji został przedstawiony w dalszej części artykułu.

Po ustawieniu i przetestowaniu połączenia do eDokumentów będzie się mógł zalogować tylko ten użytkownik, który posiada konto na serwerze LDAP.

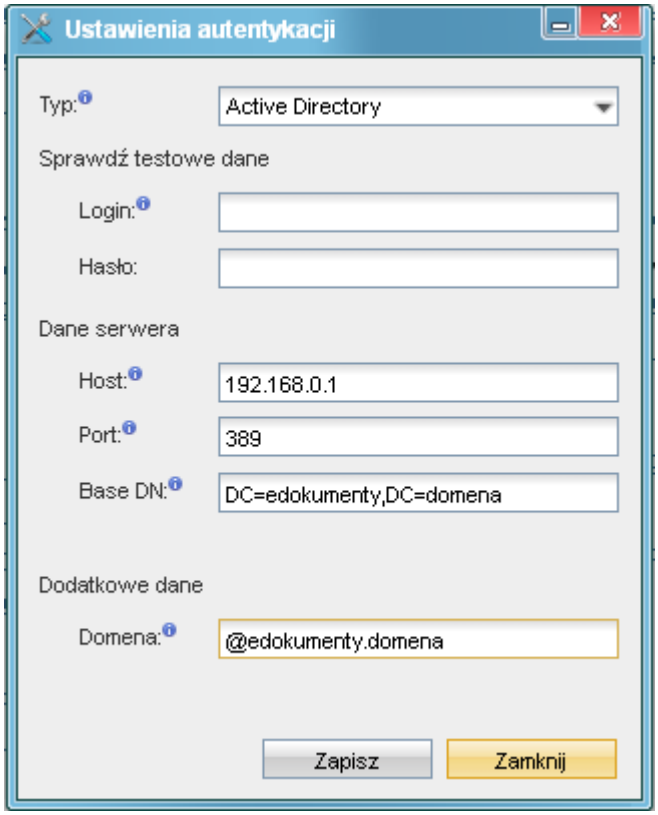
Przejdź do Menu

Autentykacja przy pomocy Active Directory

W niniejszej części artykułu zajmiemy się autentykacją przy pomocy Active Directory. System eDokumenty może być zainstalowany albo na serwerze Microsoft Windows lub też na serwerze Linuksowym np. Debian.

Konfiguracja systemu eDokumenty do współpracy z Active Directory

Aby móc skorzystać z dobrodziejstw uwierzytelniania poprzez LDAP (Active Directory na Windows) należy skonfigurować podstawowe dane przy użyciu formularza umieszczonego w *Panelu Sterowania* > *Autentykacja*.



(*Rys.2*)

W formularzu wybieramy rodzaj autoryzacji, następnie wpisujemy adres hosta - komputera, który jest kontrolerem domeny. Base DN - jest wyjaśnione w dalszej części artykułu. Ważne jest, aby w polu Domena wpisać pełny adres domeny poprzedzony znakiem @ np. @edokumenty.firma.

Aby przetestować wpisy, należy wprowadzić użytkownika z prawami administratora domeny i jego hasło.

Powyższy formularz uzupełnia poniższe stałe zawarte w pliku `config.inc` w katalogu głównym apps\edokumenty. W przypadku jeśli którejś z tych stałych nie ma należy dodać ją ręcznie korzystając z edytora teksu (zalecany Notepad++, VIM).

```
define('AUTHENTICATION_METHOD', 'PG');
// znacznik określający sposób autentykacji opcje: PG, LDAP, AD

define('LDAP_HOST', ''); // adres IP serwera
define('LDAP_PORT', 389); // port najczęściej 389

// ścieżka do wyszukania danych usera który ma prawo do
// przeglądania zasobów ldap włącznie z hasłami np.: cn=root,ou=BetaSoft,ou=Users,dc=firma,dc=local
define('LDAP_AUTH_USER', '');
define('LDAP_AUTH_PASS', ''); // haslo dla usera powyzej
define('LDAP_BASE_DN', ''); // ścieżka wyszukiwanie np ou=BetaSoft,ou=Users,dc=firma,dc=local

define('LDAP_USE_TLS', FALSE);

// specyficzne wartości dla Active Directory
define('ACTIVE_DIRECTORY_ACCOUNT_SUFFIX', '@firma.local'); // nazwa domeny poprzedzona @
```

W przypadku korzystania z TLS a gdy w AD mamy certyfikat podpisany przez nas samych w konfigruacji LDAP na serwerze eDokumentów należy edytować plik

```
/etc/ldap/ldap.conf
```

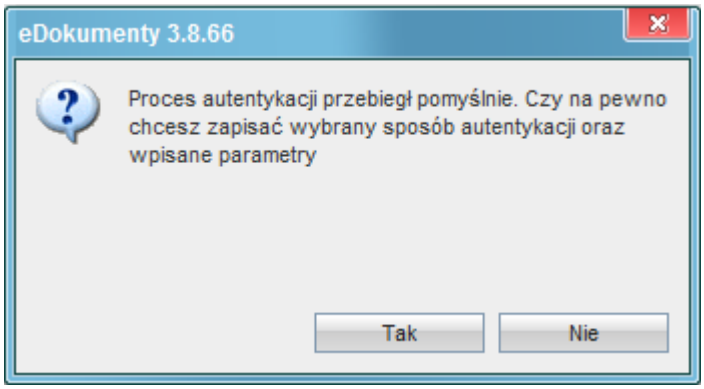
od dodać następujący wpis

```
TLS_REQCERT never
```

Odnośnie LDAP_BASE_DN najczęściej jest to ciąg postaci DC=firma,DC=local - każdy kolejny DC określa człon domeny np. edokumenty.firma.local będzie wyglądać DC=edokumenty,DC=firma,DC=local. Co do OU=betasoft jest to oznaczenie symboliczne oraz nazwa korzenia w którym nastąpi wyszukiwanie użytkowników.

Wyśmienitym narzędziem do pobrania tych danych jest Softerra LDAP Browser (Windows), phpLDAPadmin (PHP).

Po wprowadzeniu danych do powyższego formularza/pliku config.inc należy przetestować połączenie i zapisać ustawienia:



(Rys.3)

Przejdź do Menu

Typowy sposób dołączania użytkownika do eDokumentów

Dodawanie użytkownika do eDokumentów, w przypadku autentykacji AD wymaga dodatkowej pracy związanej z założeniem użytkownika w AD. Dopiero po założeniu użytkownika na kontrolerze AD oraz w eDokumentach pozwoli użytkownikowi uruchomić system eDokumenty na swoim stanowisku.

Przejdź do Menu

Dodatkowe operacje

W plikach /var/tpl/ad_column_map.ini oraz /var/tpl/ldap_column_map.ini można zadeklarować mapowanie pozostałych pól z LDAP/AD na pola z systemu eDokumenty (domyślnie ustawienia są gotowe po instalacji systemu eDokumenty).

```
; Mapa kolumn
;
; Kolumny firnam i lasnam zawsze musza byc
; Nalezy dopilnowac aby w ldapie kolumny
; mapowane na firnam i lasnam nie byly puste
[map]
samaccountname = usrnam
mail = e_mail
telephonenumber = phone_
givenname = firnam
sn = lasnam
initials = initls
description = commen
```

Przejdź do Menu