Konfiguracja autentykacji LDAP / Active Directory

Wprowadzenie

System eDokumenty umożliwia autentykację użytkowników systemu w trzech wariantach:

- poprzez autentykację serwera PostgreSQL,
- protokół LDAP
- odmianę protokołu LDAP dla Windows - Active Directory

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

Do współpracy z AD 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

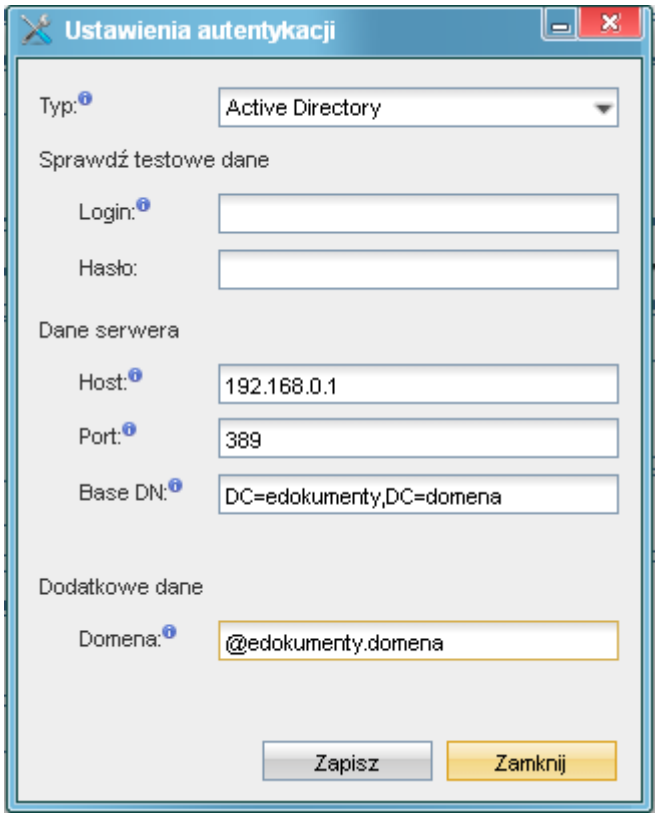
```
root@pc# apt-get install php5-ldap
```

1. Po instalacji należy zrestartować serwer Apache'a

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

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.1*)

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.

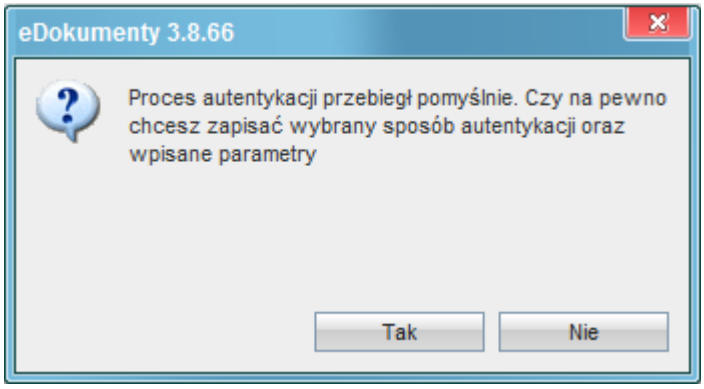
Powyższy formularz uzupełnia poniższe stałe zawarte w pliku `config.inc` w katalogu głównym apps\edokumenty. W przypadku jeśli którejś z tych stałych nie ma należy dodać ją ręcznie korzystając z edytora teksu (zalecany Notepad++, VIM).

```
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

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

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.2)

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.