LDAP-аутентификации

Этот модуль позволяет производить проверку подлинности посредством LDAP, используя списки контроля доступа. Он включён в текущий релиз «ДокуВики».

Пользователь может войти в вики, используя свои имя и пароль, определённые на LDAP-сервере. Добавление новых пользователей в LDAP данным модулем не поддерживается.

 Не пытайтесь писать здесь о багах и проблемах. Вместо этого используйте багтрекер, списки рассылки или форум.

Настройка

Вот пример того, как изменить `conf/local.php`, чтобы использовать аутентификации через LDAP.

```
$conf['useacl']      = 1;
$conf['openregister']= 0;
$conf['authtype']    = 'ldap';

#$conf['auth']['ldap']['server']     = 'localhost';
#$conf['auth']['ldap']['port']       = 389;
$conf['auth']['ldap']['server']      = 'ldap://server.tld:389'; #instead of
the above two settings
$conf['auth']['ldap']['usertree']    = 'ou=People, dc=server, dc=tld';
$conf['auth']['ldap']['grouptree']   = 'ou=Group, dc=server, dc=tld';
$conf['auth']['ldap']['userfilter']  =
'(&(uid=%{user})(objectClass=posixAccount))';
$conf['auth']['ldap']['groupfilter'] =
'(&(objectClass=posixGroup)(|(gidNumber=%{gid})(memberUID=%{user})))';

# This is optional but may be required for your server:
#$conf['auth']['ldap']['version']    = 3;

# This enables the use of the STARTTLS command
#$conf['auth']['ldap']['starttls']   = 1;

# This is optional and is required to be off when using Active Directory:
#$conf['auth']['ldap']['referrals']  = 0;

# Optional bind user and password if anonymous bind is not allowed
(develonly)
#$conf['auth']['ldap']['binddn']     = 'cn=admin, dc=my, dc=home';
#$conf['auth']['ldap']['bindpw']     = 'secret';

# Mapping can be used to specify where the internal data is coming from.
```

```
#$conf['auth']['ldap']['mapping']['name']  = 'displayname'; # Name of
attribute Active Directory stores it's pretty print user name.
#$conf['auth']['ldap']['mapping']['grps']  = array('memberof' =>
'/CN=(.+?),/i'); # Where groups are defined in Active Directory

# Optional debugging
#$conf['auth']['ldap']['debug']      = 1;
```

Можно использовать параметр *version*, чтобы заставит PHP использовать протокол LDAP 3-й версии для подключения к вашему серверу. По умолчанию — 2.

Свойство *userfilter* определяет LDAP-фильтр, который будет использоваться для поиска контактов. *groupfilter* используется для получения групп, в которые входит пользователь.

Следующие переменные можно использовать в *userfilter* и *groupfilter*:

Переменная	**Значение**
%{user}	имя, под которым пользователь пытается подключиться
%{server}	сервер, указанный в $conf['auth']['ldap']['server']

Также в *groupfilter* можно использовать все атрибуты объекта *user*:

Переменная	**Значение**
%{dn}	dn пользователя, например, uid=user,ou=People,dc=server,dc=dk
%{uid}	uid пользователя, например, user
%{...}	

Свойство *mapping* используется для каталогов, использующих «нестандартные» имена атрибутов, отображаемый атрибут может быть обработан регулярным выражением перед тем, как будет подставлен в целевую переменную. Для всех переменных, кроме 'grps', используется только первое значение атрибута, если их предоставлено несколько.

Переменная	**Отображение**	**Назначние**
grps	array('memberof' => '/CN=(.+?),/i')	Заменяет значение 'grps', тем, что предоставлено в атрибуте memberof и применяет регулярное выражение /CN=(.+?),/i к каждому его элементу.
name	'displayname'	Заменяет значение 'name' первым элементом атрибута 'displayname'.

Аутентификация проходит в три этапа:

1. First see if we need to do an anonymous bind by looking in the usertree for a %{user}:
   - Если нашли — устанавливаем usertree как DN.
   - Если нет — пытаемся найти DN для введенного логина, осуществляя поиск в *usertree* с указанным *userfilter*. Должен быть найден только один вариант.
2. Пытаемся подключиться с найденным DN и указанным паролем. Если удалось — доступ разрешён.
3. Для получения списка групп, в которых состоит пользователь, осуществляется поиск с использованием *groupfilter*.

Замечания

- В процессе настройки LDAP вам может быть полезно установить свойство *debug* для вывода сообщений об ошибках, присланных вашим LDAP-сервером. По завершении обязательно выключите это свойство.
- Свободный LDAP-браузер (написан на Java) может быть полезен, чтобы подобрать правильные значения `$conf['auth']['ldap']` и определиться со структурой вашего LDAP-сервера.
- Имена полей и отображений (mapping) всегда указываются в нижнем регистре, вне зависимости от регистра, используемого LDAP-сервером.
- Убедитесь, что у вас установлено расширение PHP LDAP.

Реальные примеры

Ниже приведён список примеров конфигураций, используемых различными пользователями для различных LDAP-серверов. Это всего лишь примеры. Перед использованием обязательно подправьте под свои настройки сервера.

- OpenLDAP
- Active Directory
- Lotus Domino (Notes)
- Open Directory (Mac OS X Server)
- Univention Corporate Server (UCS)
- Oracle Internet Directory
- Novell eDirecotry
- tinyldap