

Модуль авторизации LDAP : примеры Active Directory

Ниже, пример конфигурации для работы с [LDAP](#) и сервером  [Active Directory](#).

Приятно отметить, что существует [модуль авторизации Active Directory](#) в котором гораздо легче настроить  [Single-Sign-On](#) посредством NTLM.

Замечание: Обращайте внимание на прописные буквы домена, если соединение работает, но группы Active Directory не будут активны, используйте такие инструменты, как [AD Explorer](#) для отладки.

Active Directory с группами

- Измените «mydomain» и «dom» на свой домен AD (dc).

```
$conf['authtype'] = 'ldap';
$conf['auth']['ldap']['server'] = 'mydomain.dom';
$conf['auth']['ldap']['binddn'] = '%{user}@%{server}';
$conf['auth']['ldap']['usertree'] = 'dc=mydomain,dc=dom';
$conf['auth']['ldap']['userfilter'] =
'(userPrincipalName=%{user}@%{server})';
$conf['auth']['ldap']['mapping']['name'] = 'displayname';
$conf['auth']['ldap']['mapping']['grps'] = array('memberof' =>
'/CN=(.+)ate, /i');
$conf['auth']['ldap']['grouptree'] = 'dc=mydomain,dc=dom'; # position
for find groups, at root here
$conf['auth']['ldap']['groupfilter'] =
'(&(cn=*)(Member=%{dn})(objectClass=group))'; # поиск групп для пользователя
(dn)
$conf['auth']['ldap']['referrals'] = 0; # отключение рефералов при
использовании Active Directory
$conf['auth']['ldap']['version'] = 3;
$conf['auth']['ldap']['debug'] = 0; # Установите в 1 для просмотра
действий авторизации (напр. отображение групп пользователя) на HTML-странице
```

Если у вас есть ошибки «LDAP: bind with xxx failed [ldap.class.php:90]», попробуйте это:

```
$conf['auth']['ldap']['binddn'] = 'domain\%{user}';
```

Замените имя домена вашим.

Различные установки

```
$conf['authtype'] = 'ldap';
```

```
$conf['auth']['ldap']['server']           =  
'ldap://servername.domain.tld:389';  
$conf['auth']['ldap']['binddn']           = '%{user}@domain.tld';  
$conf['auth']['ldap']['usertree']          = 'ou=Users,dc=domain,dc=tld';  
$conf['auth']['ldap']['userfilter']        = '(SAMAccountName=%{user})';  
$conf['auth']['ldap']['mapping']['name']   = 'displayname';  
$conf['auth']['ldap']['mapping']['grps']   = array('memberof' =>  
'/CN=(.+?),/i');  
$conf['auth']['ldap']['referrals']          = 0; # отключение рефералов при  
использовании Active Directory  
$conf['auth']['ldap']['version']           = 3;
```

Ограничения пользователей USR_*

```
$conf['authtype']                         = 'ldap';  
$conf['auth']['ldap']['server']           = '127.0.0.1:389';  
$conf['auth']['ldap']['binddn']           = '%{user}@yourfulldomainname';  
$conf['auth']['ldap']['usertree']          = ''; // место, содержащее  
пользователей, напр. OU=x, DC=y и подобное.  
$conf['auth']['ldap']['userfilter']        =  
'(userPrincipalName=%{user}@yourfulldomainname)';  
$conf['auth']['ldap']['grouptree']         = ''; // point this to container  
where your groups are ie CN=Users, DC=x etc  
$conf['auth']['ldap']['groupfilter']       =  
'(&(cn=USR_*)(Member=%{dn})(ObjectCategory=group))'; //selects only the  
groups with the user as a member  
// не забывайте, dn должен быть полным dn учетной записи пользователя - фильтры групп  
начинаются с USR_  
$conf['auth']['ldap']['mapping']['name']   = 'displayname';  
$conf['auth']['ldap']['mapping']['grps']   = 'array(\'memberof\' =>  
'/CN=(.+?),/i\')';  
$conf['auth']['ldap']['referrals']          = '0';  
$conf['auth']['ldap']['version']           = '3';
```

From:
<https://wwoss.ru/> - **worldwide open-source software**

Permanent link:
https://wwoss.ru/doku.php?id=wiki:auth:ldap_ad

Last update: **2024/08/15 01:53**

