

Интеграция WordPress со службой каталога ALD Pro



11/26/2025

Содержание

1 Введение	2
2 Подготовка сервисной учетной записи	3
3 Настройка доверия сертификатов	4
4 Настройка WordPress	5
5 Настройка плагина authLDAP	6

1 Введение

WordPress – одна из самых используемых систем управления контентом (CMS), которая позволяет создавать и управлять сайтами без необходимости писать код. Это бесплатная платформа с открытым исходным кодом.

Данная интеграция позволяет синхронизировать пользователей и группы из LDAP в пользователей и роли WordPress, что позволит пользователям входить в портал управления WordPress с доменными учетными записями.

2 Подготовка сервисной учетной записи

Аутентификация и авторизация выполняются методом LDAP Bind, для чего необходимо создать в ALD Pro сервисную учётную запись, которая не является POSIX-пользователем, не имеет прав на вход в домен и не отображается в портале управления, а используется только для чтения LDAP.

Для этого нужно подключиться по SSH к контроллеру домена и выполнить следующие шаги:

1. Создать файл с именем **ldap-bind.update**.
2. Внести в файл следующее содержимое:

```
dn: uid=wordpress,cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan
add:objectclass: account
add:objectclass: simplesecurityobject
add:uid: ldap-bind
add:userPassword: SecretPass
add:passwordExpirationTime: 20380119031407Z
add:nsIdleTimeout: 0
```

Разъяснения:

- **dn** – уникальный идентификатор записи пользователя в LDAP,
 - **add:objectclass: account** – добавляет базовый класс для учётной записи,
 - **add:objectclass: simplesecurityobject** – добавляет класс для хранения пароля и других атрибутов безопасности,
 - **add:uid: ldap-bind** – уникальный идентификатор пользователя,
 - **add:userPassword:SecretPass** – пароль для учётной записи, заменить на желаемый,
 - **add:passwordExpirationTime: 20380119031407Z** – время истечения пароля (можно адаптировать под политики безопасности),
 - **add:nsIdleTimeout: 0** – отключает тайм-аут простоя для этой учётной записи.
3. Выполнить добавление пользователя следующей командой:

```
kinit admin && ipa-ldap-updater ldap-bind.update
```

3 Настройка доверия сертификатов

Если WordPress развернут на сервере, который не введен в домен ALD Pro, необходимо настроить доверие к корневому сертификату сервера для безопасного подключения к LDAPS без ошибок о недоверенном сертификате.

Добавление CA-сертификата домена

1. Скопировать CA-сертификат с удалённого сервера:

```
scp <remote_user>@<remote_host>:/etc/ipa/ca.crt /tmp/ald_ca.crt
```

Разъяснения:

- **<remote_user>** – пользователь на удалённом сервере,
- **<remote_host>** – адрес или имя контроллера домена,
- **/etc/ipa/ca.crt** – путь к CA-сертификату на контроллере домена,
- **/tmp/ald_ca.crt** – временный файл на локальной машине.

2. Перенести сертификат в системное хранилище:

```
sudo cp /tmp/ald_ca.crt /usr/local/share/ca-certificates/ald_ca.crt
```

Разъяснения:

- **/usr/local/share/ca-certificates/** – каталог для локальных доверенных сертификатов

3. Обновить системное хранилище доверенных сертификатов:

```
sudo update-ca-certificates
```

Создание групп WordPress

Для управления пользователями WordPress используются встроенные группы. Во время настройки LDAP-подключения можно включить функцию выстраивания соответствия групп каталога и групп WordPress. Для удобного управления пользователями нужно создать несколько групп в ALD Pro:

```
ipa group-add wp_admin  
ipa group-add wp_editors  
ipa group-add wp_authctors
```

4 Настройка WordPress

⊗ Предупреждение!

Во время настройки плагина рекомендуется, не выходя из сессии администратора, открыть новое окно браузера в режиме инкогнито. Так как неверные настройки могут вызывать ошибки, затрудняющие любую авторизацию на портале управления, такой способ позволит при обнаружении ошибки вернуть или исправить введенные настройки в основной сессии администратора WordPress.

Для работы LDAP требуется установить php-ldap на сервере с WordPress:

```
sudo apt install php-ldap
```

Для расширения стандартных функциональных возможностей в WordPress используются плагины. Для интеграции с ALD Pro также потребуется установить плагин, который работает с LDAP. В каталоге плагинов есть большой выбор доступных плагинов, но в данной инструкции будет описан способ с использованием плагина authLDAP, так как он обеспечивает необходимый набор функций, имеет обновления для актуальной версии и бесплатен в использовании. Для его установки нужно перейти в раздел плагинов и в поиске ввести название authLDAP. Результат поиска должен быть таким, как показано на рисунке 1.

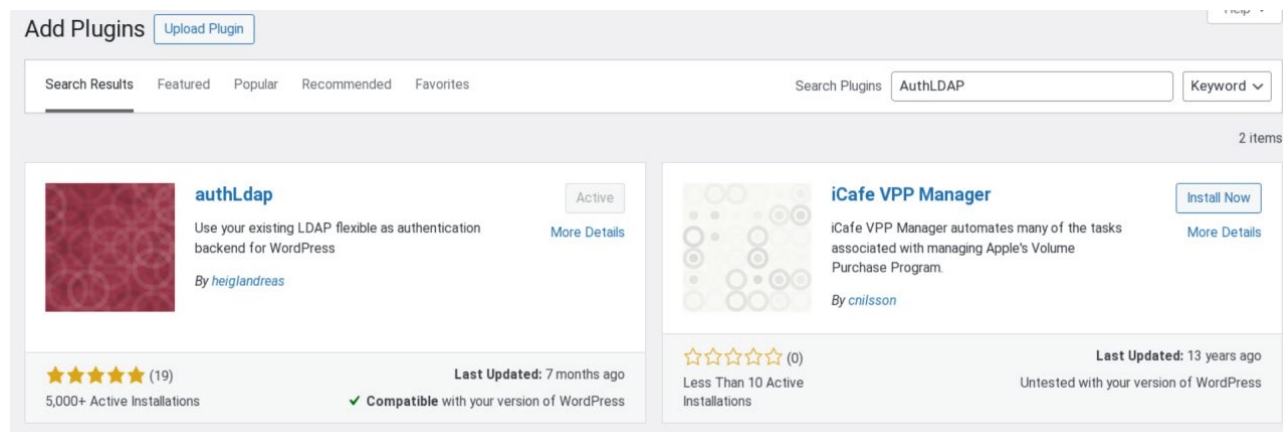


Рисунок 1 – Поиск плагина authLDAP

Далее нужно перейти в раздел Settings и его подраздел authLDAP.

5 Настройка плагина authLDAP



Важно!

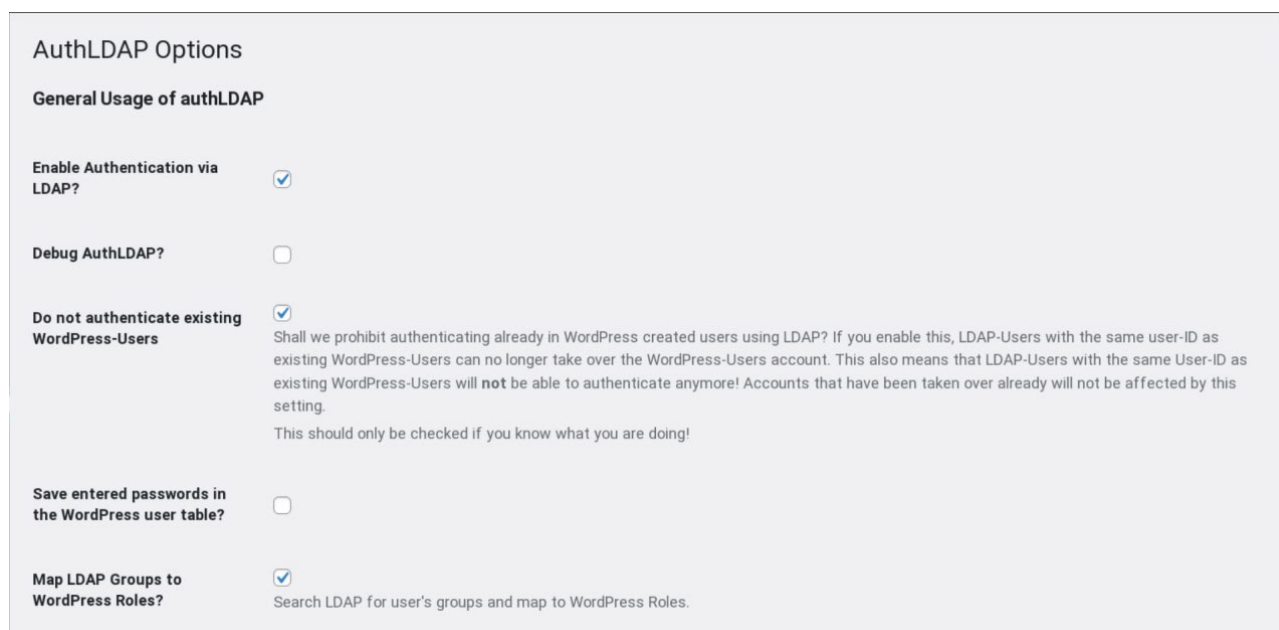
При настройке LDAP-подключения для указания пароля рекомендуется использовать переменные окружения. Для объявления такой переменной нужно на сервере WordPress в файле `/etc/apache2/envvars` добавить строку

```
export ENVNAME=<Пароль сервисной учетной записи>
```

, где ENVNAME - это название переменной окружения.

В разделе Settings => требуется включить следующие опции (рис. 2):

- Enable Authentication via LDAP,
- Do not authenticate existing Wordpress-Users,
- Map LDAP Groups to WordPress Roles.



AuthLDAP Options

General Usage of authLDAP

Enable Authentication via LDAP?

Debug AuthLDAP?

Do not authenticate existing WordPress-Users
 Shall we prohibit authenticating already in WordPress created users using LDAP? If you enable this, LDAP-Users with the same user-ID as existing WordPress-Users can no longer take over the WordPress-Users account. This also means that LDAP-Users with the same User-ID as existing WordPress-Users will **not** be able to authenticate anymore! Accounts that have been taken over already will not be affected by this setting.
 This should only be checked if you know what you are doing!

Save entered passwords in the WordPress user table?

Map LDAP Groups to WordPress Roles?
 Search LDAP for user's groups and map to WordPress Roles.

Рисунок 2 - Пример конфигурации раздела AuthLDAP Options

Далее нужно указать LDAP URI, например:

```
ldaps://uid=wordpress,cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan:%env:PWD%@dc-1.a  
ld.company.lan/dc=ald,dc=company,dc=lan
```

Данный URI включает в себя следующие компоненты (рис. 3):

- способ подключения (ldap/ldaps),
- DN ранее созданной сервисной учетной записи,
- пароль указанной учетной записи (можно указать при помощи переменной окружения, в данном примере используется переменная окружения PWD),

- доменное имя ALD Pro,
- базовый суффикс для поиска в каталоге.

General Server Settings

LDAP URI

The URI for connecting to the LDAP-Server. This usually takes the form `<scheme>://<user>:<password>@<server>/<path>` according to RFC 1738.

In this case it should be something like `ldap://uid=adminuser,dc=example,c=com:secret@ldap.example.com/dc=basePath,dc=example,c=com`.

If your LDAP accepts anonymous login, you can omit the user and password-Part of the URI

You can use the pseudo-schema `env` to provide your LDAP-URI from an environment-variable. So if you have your LDAP-URI in a variable called `LDAP_URI` you can enter `env:LDAP_URI` in this field and at runtime the appropriate value will be taken from the Environment-variable `LDAP_URI`. If the variable is not set, then the value will be empty.

You can also provide different parts of the LDAP-URI from environment variables by providing `%env:[VARIABLENAME]%` within your LDAP-URI. So if you want to provide the password from an Environment-variable `LDAP_PASSWORD` your LDAP-URI looks like `ldap://uid=adminuser,dc=example,c=com:%env:LDAP_PASSWORD@ldap.example.com/dc=basePath,dc=example,c=com`

Caveat!
If you are using Environment-variables for parts of the LDAP-URL then those **must not** be URL-Encoded! Otherwise the different parts **must** be URL-Encoded!

Рисунок 3 - Пример конфигурации раздела General Server Settings

В поле Filter указать следующее:

Данный фильтр не позволит заблокированным пользователям авторизоваться в веб-портале WordPress.

Заполнить Settings for creating new Users указанными значениями для полей, изображенных на рисунке 4:

- givenName,
- sn,
- uid,
- mail.

Settings for creating new Users

User-Read
If checked the plugin will use the user's account to query their own information. If not it will use the admin account.

Name-Attribute
Which Attribute from the LDAP contains the Full or the First name of the user trying to log in.
This defaults to **name**

Second Name Attribute
If the above Name-Attribute only contains the First Name of the user you can here specify an Attribute that contains the second name.
This field is empty by default

User-ID Attribute
Please give the Attribute, that is used to identify the user. This should be the same as you used in the above Filter-Option
This field defaults to **uid**

Mail Attribute
Which Attribute holds the eMail-Address of the user?
If more than one eMail-Address are stored in the LDAP, only the first given is used
This field defaults to **mail**

Рисунок 4 - Пример конфигурации раздела Settings for creating new Users

Заполнить Groups for Roles, как показано на рисунке 5.

Group-Base

cn=groups,cn=accounts,dc=ald,dc=company,dc=lan

Group-Attribute

cn

Group-Filter

(&(objectClass=ipausergroup)(member=uid=%s,cn=users,cn=accounts,dc=ald,dc=company,dc=lan))

Groups for Roles

LDAP Groups override role of existing users? If role determined by LDAP Group differs from existing WordPress User's role, use LDAP Group.

Group-Base
 This is the base dn to lookup groups.
 If empty the base dn of the LDAP URI will be used

Group-Attribute
 This is the attribute that defines the Group-ID that can be matched against the Groups defined further down
 This field defaults to **gidNumber**

Group-Separator
 This attribute defines the separator used for the Group-IDs listed in the Groups defined further down. This is useful if the value of Group-Attribute listed above can contain a comma (for example, when using the memberof attribute)
 This field defaults to , (comma)

Group-Filter
 Here you can add the filter for selecting groups for their currently logged in user
 The Filter should contain the string `%s` which will be replaced by the login-name of the currently logged in user
 Alternatively the string `%dn%` will be replaced by the DN of the currently logged in user. This can be helpfull if group-memberships are defined with DNs rather than UIDs
 This field defaults to (&(objectClass=posixGroup)(memberUid=%s))

Рисунок 5 – Пример конфигурации раздела Groups for Roles

В разделе Role – group mapping указать название групп, которые были созданы ранее в разделе «Создание групп WordPress».

Assign this WordPress-Role to members of this/these LDAP-Groups

Administrator	<input type="text" value="wp_admins"/>
Editor	<input type="text" value="wp_editors"/>
Author	<input type="text" value="wp_authors"/>

Рисунок 6 - Пример конфигурации раздела Role – group mapping

В завершении нужно сохранить настройки. Теперь при входе пользователя в WordPress с учетными данными из каталога ALD Pro будет создан пользователь, наделенный соответствующими правами той группы, к которой он относится. Посмотреть созданных пользователей можно в разделе Users панели администрирования WordPress.