Интеграция WordPress со службой каталога ALD Pro

11/26/2025

Содержание

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 учетной 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_authtors
```

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.

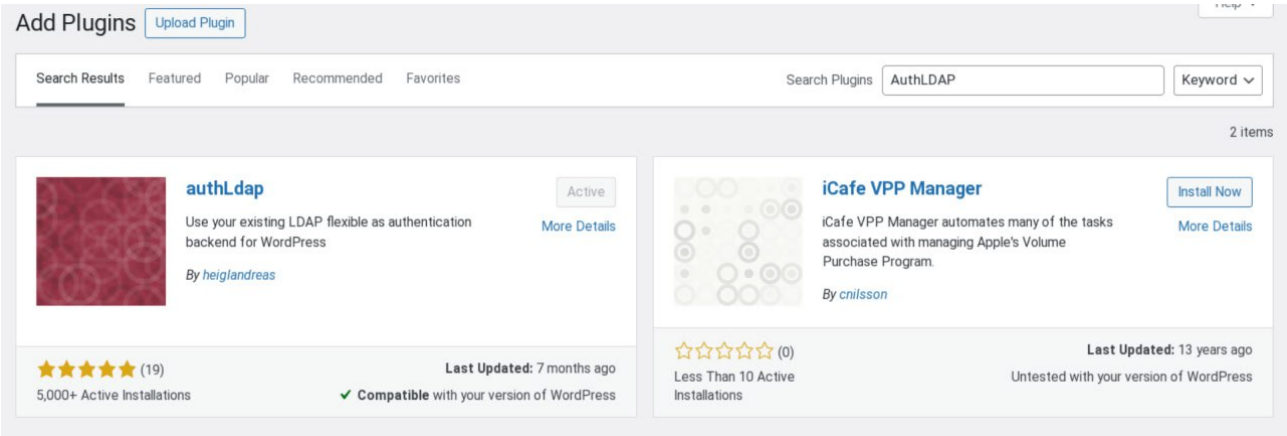

Рисунок 1 – Поиск плагина authLDAP

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.

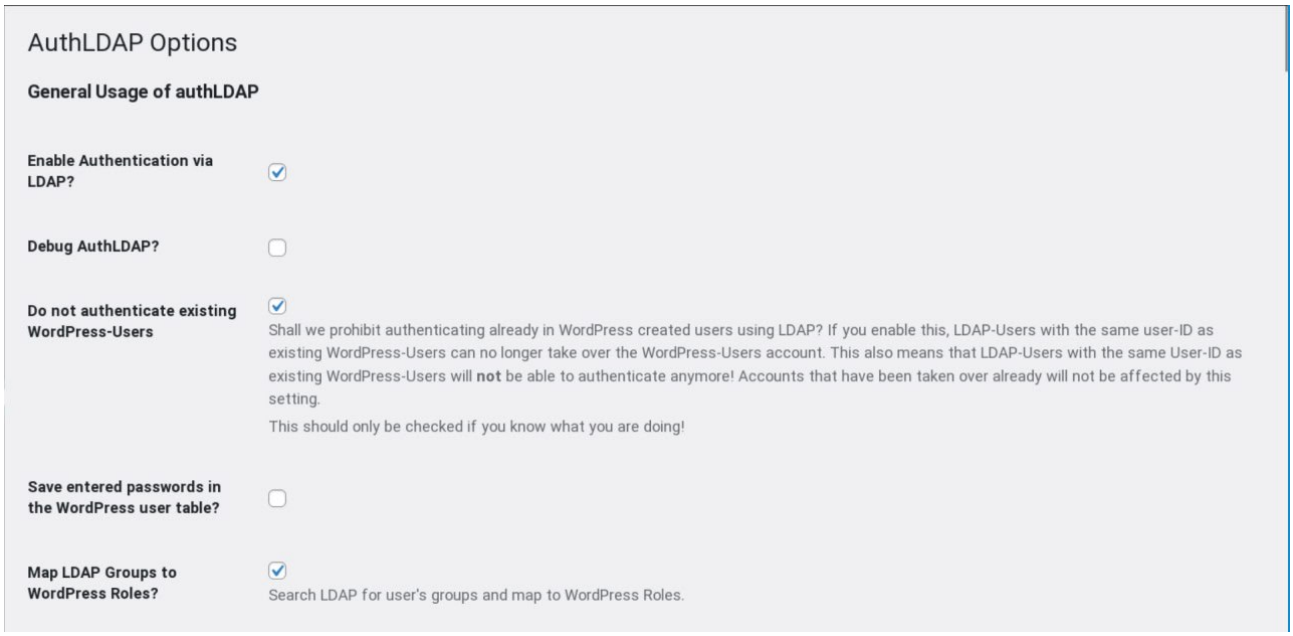

Рисунок 2 - Пример конфигурации раздела AuthLDAP Options

Далее нужно указать LDAP URI, например:

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

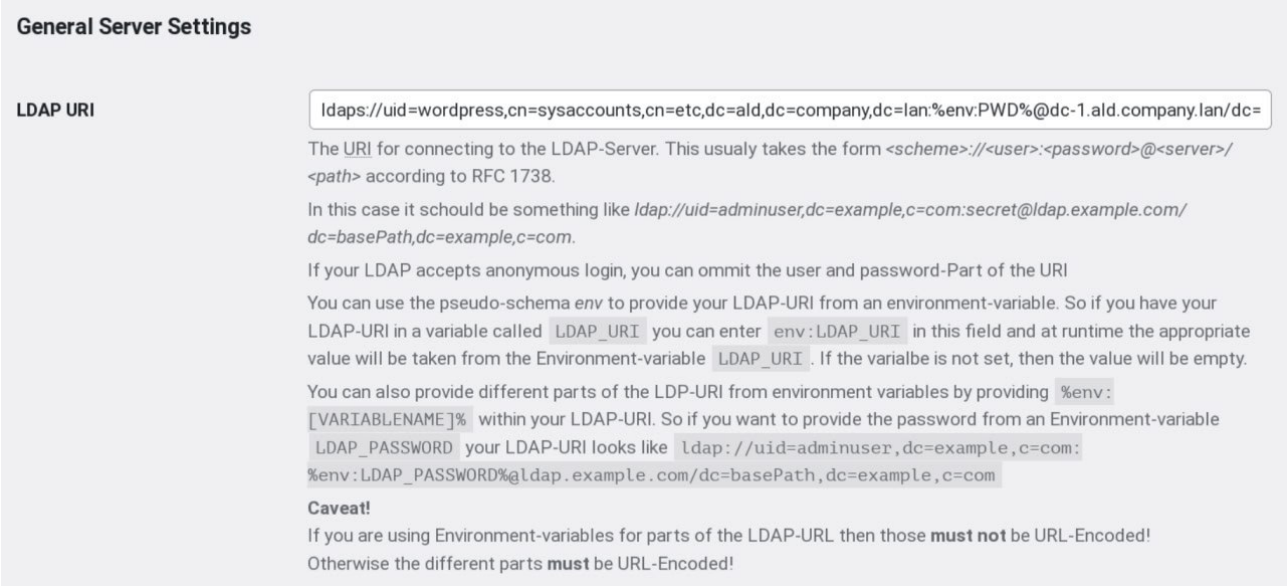

Рисунок 3 - Пример конфигурации раздела General Server Settings

В поле Filter указать следующее:

```
(&(uid=%s)(nsAccountLock=False))
```

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.

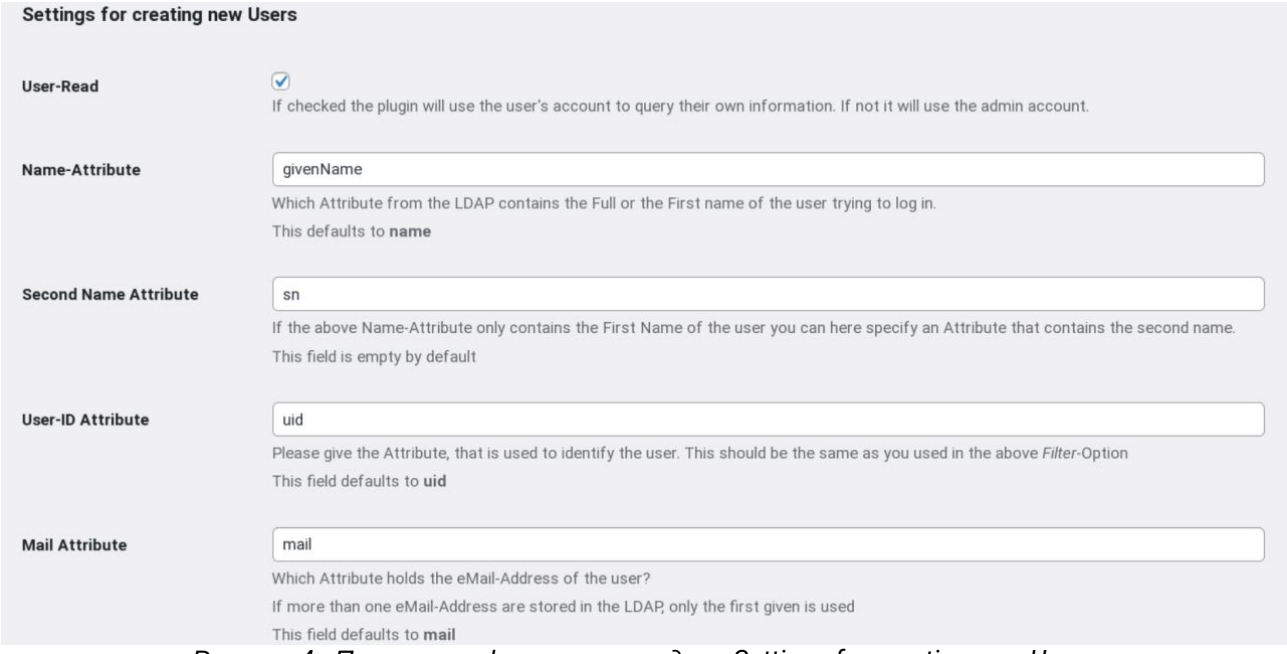

Рисунок 4 - Пример конфигурации раздела Settings for creating new Users

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))
```

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».

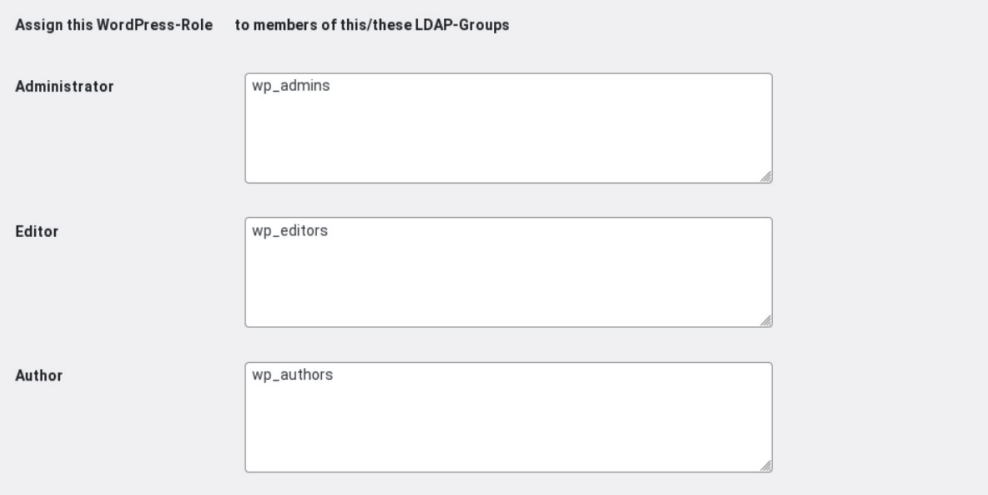

Рисунок 6 - Пример конфигурации раздела Role − group mapping

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.