Интеграция и синхронизация пользователей с ALD Pro

04/15/2026

Содержание

1 Введение

Astra Linux Directory Pro (ALD Pro) — это централизованная служба каталога, построенная на базе FreeIPA и предназначенная для управления учетными записями, группами и политиками безопасности в корпоративной инфраструктуре. ALD Pro поддерживает протоколы LDAP и Kerberos, реализует ролевую модель управления доступом (RBAC) и предоставляет возможность организации единого входа (SSO) для пользователей. Синхронизация информации о пользователях с внешними сервисами по протоколу LDAP позволяет упростить администрирование, централизовать контроль доступа и повысить уровень защищённости информационной системы.

2 Настройка LDAP Bind

Для интеграции внешних сервисов со службой каталогов Astra Linux Directory Pro (ALD Pro) рекомендуется использовать защищённое соединение по протоколу LDAPS (порт: 636). Это обеспечивает шифрование передаваемых данных и соответствует требованиям информационной безопасности.

2.1 Протокол и порт подключения

- Используйте **LDAPS (LDAP over SSL/TLS)** — стандартный порт: **636**.
- Сторона-клиент должна доверять SSL-сертификату LDAP-сервера. При необходимости установите корневой сертификат удостоверяющего центра, выдавшего сертификат сервера, в хранилище доверенных корневых сертификатов на стороне клиента.

2.2 Параметры подключения

- Тип сервера: **389 Directory Server**
- Адрес сервера: **FQDN контроллера домена ALD Pro или имя домена**
- Base DN (базовый DN): **dc=ald,dc=company,dc=lan**, где ald.company.lan — доменное имя LDAP-домена ALD Pro

2.3 Аутентификация

- Метод: **Simple Bind**
- Учетная запись: сервисная с правами только на чтение
- Формат DN учётной записи:

```
uid=ldap-bind,cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan
```

Разъяснения:

- **uid=ldap-bind** — имя учётной записи;
- **cn=sysaccounts,cn=etc** — путь в структуре LDAP;
- **dc=ald,dc=company,dc=lan** — компоненты домена.

3 Настройка сервисной учетной записи

3.1 Создание 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.

3.1.1 Порядок создания сервисной учетной записи

1. Перед выполнением команды необходимо задать следующие параметры:

```
PASS='Pa$$w0rd'
LDAP_USER='system'
LDAP_BASE_DN='dc=ald,dc=company,dc=lan'
```

Разъяснения:

- `PASS` — пароль сервисной учётной записи,
- `LDAP_USER` — имя создаваемой сервисной LDAP-учётной записи,
- `LDAP_BASE_DN` — базовый DN вашего домена LDAP.

Примеры базового DN:

```
ald.company.lan → dc=ald,dc=company,dc=lan
```

2. Подключитесь по SSH к контроллеру домена и выполните следующую команду:

```
PASS='Pa$$w0rd'
LDAP_USER='system'
LDAP_BASE_DN='dc=ald,dc=company,dc=lan'

sudo bash -c '
PW_B64=$(printf "%s" "'"$PASS"'" | base64 -w0)
LDAP_USER="'"$LDAP_USER"'"
LDAP_BASE_DN="'"$LDAP_BASE_DN"'"
EXPIRATION=$(date -u -d "+5 years" +"%Y%m%d%H%M%SZ")

cat > /tmp/${LDAP_USER}.update <<EOF
dn: uid=${LDAP_USER},cn=sysaccounts,cn=etc,${LDAP_BASE_DN}
add:objectclass: account
add:objectclass: simplesecurityobject
add:uid: ${LDAP_USER}
add:userPassword:: ${PW_B64}
add:passwordExpirationTime: ${EXPIRATION}
add:nsIdleTimeout: 0
EOF
```

```
kinit admin && ipa-ldap-updater /tmp/${LDAP_USER}.update
'
```

Команда выполняет следующие действия:

- кодирует указанный пароль в Base64 и сохраняет его в переменную `PW_B64;`
- создаёт файл `/tmp/${LDAP_USER}.update`, содержащий LDIF-описание сервисной учётной записи;
- получает Kerberos-билет администратора (`kinit admin`);
- применяет изменения из созданного LDIF-файла к LDAP-каталогу с помощью `ipa-ldap-updater` .

3.1.2 Срок действия пароля

Срок действия пароля задаётся автоматически в формате **текущая дата + 5 лет**.

Это значение рассчитывается следующей командой:

```
date -u -d "+5 years"
```

Если в вашей инфраструктуре используются другие требования к сроку действия паролей, значение можно изменить, например:

```
+1 year
+3 years
+10 years
```

3.2 Выдача дополнительных прав через роль и LDIF

Если сервисной учетной записи нужно дополнительно управлять объектами (например, изменять группы), права назначаются через **роль**.

3.2.1 Создание роли через портал ALD Pro

- Имя роли: `ServiceAccountsGroupMgr`
- Назначенные привилегии: например `User groups – Modify`
- Роль создается через портал управления ALD Pro

3.2.2 Добавление сервисной учетной записи в роль через LDIF

1. Создать файл `add-ldap-bind-to-role.ldif` :

```
dn: cn=ServiceAccountsGroupMgr,cn=roles,cn=accounts,dc=ald,dc=company,dc=lan
changetype: modify
add: member
member: uid=ldap-bind,cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan
```

Разъяснения:

- **dn** — уникальный идентификатор роли в LDAP, куда добавляем участника,
- **changetype: modify** — указывает, что запись изменяется,
- **add: member** — операция добавления нового участника роли,
- **member:** — DN пользователя, который будет участником роли.

2. Применение LDIF через CLI:

```
ldapmodify -x -D "uid=admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan" -W -f add-ldap-bind-to-role.ldif
```

Разъяснения:

- **ldapmodify** — утилита для изменения LDAP-записей,
- **-x** — использовать простой LDAP Bind,
- **-D** — DN пользователя, выполняющего изменения (`admin`),
- **-W** — запрос пароля при подключении,
- **-f** — файл LDIF с инструкцией для изменения.

3. Проверка, что сервисная учетная запись добавлена в роль

```
ldapsearch -x -D "uid=admin,cn=users,cn=accounts,dc=ald,dc=company,dc=lan" -W -b "cn=ServiceAccountsGroupMgr,cn=roles,cn=accounts,dc=ald,dc=company,dc=lan" member
```

Разъяснения:

- **ldapsearch** — утилита для поиска записей в LDAP,
- **-x** — использовать простой LDAP Bind,
- **-D** — DN пользователя с правами на чтение ролей,
- **-W** — запрос пароля при подключении,
- **-b** — база поиска (DN роли).

В выводе должна появиться строка `member: uid=ldap-bind,...` , что подтверждает успешное добавление.

4 Настройка доверия сертификатов

Если сервис 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.

4.1 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
```

5 Настройка дополнительных параметров LDAP-подключения

Для корректной работы внешних сервисов с ALD Pro рекомендуется задать следующие параметры LDAP. Они обеспечивают правильную фильтрацию и отображение групп, а также расширяют профиль пользователя за счёт дополнительных атрибутов.

LDAP-параметр	Значение	Описание
Filter Disabled	(!(nsAccountLock=TRUE))	Исключение заблокированных учётных записей
Filter Login	(objectClass=inetOrgPerson)	Фильтр для определения учётных записей пользователя
Filter Group	(objectClass=groupofnames)	Фильтр для определения LDAP-групп
Group Member	member	Атрибут, определяющий состав группы
Member Of	memberOf	Атрибут групп, в которых состоит пользователь
Login	uid	Логин пользователя
Display Name	displayName	Отображаемое полное имя пользователя
First Name	givenName	Имя пользователя
Last Name	sn	Фамилия пользователя
Middle Name	rbtamiddlename	Отчество
Email	mail	Электронная почта пользователя
Mobile Phone	mobile	Мобильный телефон
Work Phone	telephoneNumber	Рабочий телефон
Home Phone	employeeNumber	Внутренний/добавочный номер

IPA Unique ID	ipaUniqueID	Уникальный идентификатор LDAP-объекта (UUID для пользователя)

6 Настройка Kerberos

В ALD Pro сервисная служба (SPN) связывается с уже существующей A-записью сервера на DNS-сервере. Поэтому перед настройкой Kerberos SSO рекомендуется добавить сервер в домен ALD Pro. В крайнем случае — создать A-запись сервера, как указано ниже в инструкции, если ввод в домен не предполагается.

6.1 Создание keytab-файла

> Важно: шаги, описанные в пункте **c.**, необходимо выполнять, только если сервер ещё не добавлен в домен ALD Pro. Если узел уже существует, переходите к следующему шагу.

a. Получите Kerberos-билет администратора домена, выполнив команду в терминале:

```
kinit admin
```

Разъяснения:

- **admin** - имя доменного администратора.

b. Задайте переменные с нужными значениями (без пробелов):

```
IP_ADDRESS=10.10.10.10
HOSTNAME=service.ald.company.lan
DOMAIN_CONTROLLER=dc-1.ald.company.lan
```

Разъяснения:

- **IP_ADDRESS** - IP-адрес сервера службы;
- **HOSTNAME** - Полное доменное имя сервера;
- **DOMAIN_CONTROLLER** - FQDN контроллера домена ALD Pro.

c. Если сервер ещё не добавлен в домен, создайте запись узла с помощью:

```
sudo ipa host-add --force --ip-address=$IP_ADDRESS $HOSTNAME
```

d. Добавьте сервисную службу (SPN):

```
sudo ipa service-add service/$HOSTNAME
```

Разъяснения:

- **service** - это тип службы (service principal), который нужно заменить на конкретный сервис, который вы хотите зарегистрировать, существуют стандартные типы сервисов, такие как host, http, ldap, postgres, но это не полный список, можно использовать и другие сервисы в

зависимости от задач и возможностей клиента, создаваемый принципал будет использоваться вашим сервисом для аутентификации в домене Kerberos.

e. Сгенерируйте keytab-файл:

```
sudo ipa-getkeytab -s $DOMAIN_CONTROLLER -p service/$HOSTNAME -k service.keytab
```

6.2 Настройка единого входа (SSO)

a. Загрузите сгенерированный keytab-файл в систему аутентификации используемого сервиса.

b. Активируйте Kerberos SSO (единый вход).

После этих действий клиенты, подключённые к домену ALD Pro, смогут автоматически проходить аутентификацию через Kerberos SSO без повторного ввода пароля.

7 Настройка SASL и GSSAPI для LDAP-аутентификации

Для надёжной и безопасной интеграции с Astra Linux Directory Pro (ALD Pro) рекомендуется реализовать поддержку аутентификации LDAP с использованием SASL и механизма GSSAPI (Kerberos). Это позволит обеспечить единую аутентификацию (SSO) и повысить уровень безопасности.

Рекомендации для разработчиков сервисов

- Обеспечить поддержку SASL с механизмом GSSAPI в LDAP-клиенте сервиса.
- Реализовать корректную обработку Kerberos-билетов для аутентификации пользователей.
- Настроить конфигурацию Kerberos-клиента на стороне сервиса, включая файл krb5.conf с параметрами домена ALD Pro.
- Использовать LDAPS (порт 636) для защиты канала передачи данных.
- Проверять корректность синхронизации времени между клиентом и KDC для успешной аутентификации.
- Обеспечить возможность загрузки и использования keytab-файлов для сервисных учётных записей при необходимости автоматической аутентификации.
- В логах сервиса предусмотреть информативные сообщения об ошибках SASL/GSSAPI для облегчения диагностики.

Реализация этих рекомендаций позволит сервисам максимально эффективно интегрироваться с ALD Pro, обеспечивая удобство и безопасность пользователей.