# Интеграция Orion soft zVirt со службой каталога ALD Pro


04/07/2026

**zVirt** - это платформа виртуализации, основанная на oVirt Engine, которая обеспечивает управление виртуальными машинами, хостами и инфраструктурой виртуализации на уровне предприятия.

Интеграция позволяет вести базу пользователей централизованно в ALD Pro, а также перенести функции аутентификации и авторизации на ALD Pro через LDAP или Keycloak. Это позволит пользователям аутентифицироваться в zVirt с использованием учетных записей из ALD Pro и получать доступы в соответствии с группами и ролями. Интеграция выполняется путем настройки подключения к службе каталога ALD Pro через AAA JDBC или Keycloak и поддерживает протоколы LDAP и LDAPS.

Инструкция по интеграции разработана компанией OrionSoft.

# Инструкция по интеграции zVirt со службой каталога ALD Pro

#orionsoft/zvirt/prodintegra

Расширенно руководство по управлению Keycloak с описанием всех параметров: https://wiki.orionsoft.ru/zvirt/latest/keycloak/management-guide/#_подключение_слу жб_каталогов_к_keycloak

**Содержание**



## Вводные данные

Предварительно выполнена установка и настройка :

- платформа виртуализации zVirt с Engine oVirt Engine AAA JDBC

- платформа виртуализации zVirt с Keycloak
- служба каталога ALD Pro
- resolve.conf и /etc/hosts на сервере управления zVirt

> **Примечание: для подключения к LDAP рекомендуется использовать отдельную сервисную учетную запись с минимальными правами**

Перед началом настройки подготовьте следующую информацию:

**zVirt:**

- **Engine**: engine.zvirt.local

**ALD Pro:**

- **LDAP-сервер**: dc.aldpro.local
- **Пользователь для подключения**: ldapuser
- **Пароль для подключения**: ldappass
- **Группы и пользователи ALD Pro для zVirt**:
  - GRP-zVirtAdmins - Группа администраторы zVIrt
    - zvirtadmin - Администоратор zVirt
  - GRP-zVirtUsers - Группа пользователей zVirt
    - zvirtuser - Пользователь zVirt
- **Base DN вашего домена**: dc=aldpro,dc=local

# Подготовка сертификатов ALD Pro для LDAPS

## Получить сертификат с сервера ALD Pro

```
# Получить сертификат с сервера ALD Pro
openssl s_client -connect dc.aldpro.local:636 -showcerts </dev/null
2>/dev/null | openssl x509 -outform PEM > aldpro_ca.pem
```

## Установка сертификата ALD Pro на сервер zVirt Engine

```
# Для RHEL/CentOS/Oracle Linux
sudo cp aldpro_ca.pem /etc/pki/ca-trust/source/anchors/aldpro-ca.crt
sudo update-ca-trust

# Для Debian/Ubuntu
## sudo cp aldpro_ca.pem /usr/local/share/ca-certificates/aldpro-ca.crt
```

```
## sudo update-ca-certificates

# Добавить корневой сертификат в доверенные
update-ca-trust enable
update-ca-trust extract

# Перезагрузить портал Keycloak
systemctl restart ovirt-engine-keycloak.service

# Проверить корректность сертификата и убедиться, что сертификат валиден и
не вызывает ошибок
openssl s_client -connect dc.aldpro.local:636 -showcerts

## Вариант установки сертификата в Keycloak
# В админ-консоли Keycloak перейдите в [Realm Settings → Keys → Providers]
# Добавьте новый провайдер типа "java-truststore"
# Загрузите файл aldpro_root_ca.pem
# Перезапустите Keycloak

## Вариант добавление сертификата в truststore Java (используется zVirt)
# sudo keytool -import -trustcacerts \
#   -alias aldpro-ca \
#   -file /path/to/ald-pro-cert.pem \
#  -keystore $JAVA_HOME/jre/lib/security/cacerts
```

# Настройка интеграции zVirt с ALD pro через AAA JDBC

## Настройка 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 домени 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=ldapuser,cn=sysaccounts,cn=etc,dc=aldpro,dc=local
add:objectclass: account
add:objectclass: simplesecurityobject
add:uid: ldapuser
add:userPassword: ldappass
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: simplesecurityobjec**t - добавляет класс для хранения пароля и других атрибутов безопасности,*
***add:uid: ldap-bind** - уникальный идентификатор пользователя,*
***add:userPassword: securePassword** - пароль для учётной записи, заменить на желаемый,*
***add:passwordExpirationTime: 20380119031407Z** - время истечения пароля (можно адаптировать под политики безопасности),*
***add:nsIdleTimeout: 0** - отключает таймаут простоя для этой учетной записи.*

*3. Выполнить добавление пользователя следующей командой:*

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

## Запуск мастера настройки интеграции

```
# Войдите в терминальную оболочку сервера управления - zVirt Engine
ssh root@engine.zvirt.local

# Запустите утилиту для запуска мастера настройки интеграции
ovirt-engine-extension-aaa-ldap-setup
```

## Настройка параметров подключения

- Выберите тип подключения: `IPA`
- Укажите наличие DNS-сервера: `Yes` (если DNS настроен)
- Тип подключения: `Single Server`
- Адрес хоста: `dc.aldpro.local`
- Протокол подключения: `LDAPS` (если используются сертификаты) или `LDAP`

- Доменный путь до администратора домена: `uid=ldapuser,cn=users,cn=accounts,dc=aldpro,dc=local`
- Базовый DN: `dc=aldpro,dc=local`
- Имя профиля подключения: `aldpro.local`

## Проверка подключения

```
# Проверьте корректность подключения с помощью AAA LDAP
ovirt-engine-extension-aaa-ldap-authn --profile=aldpro.local --
username=ldapuser --password=ldappass

# Проверка LDAPS соединения
ldapsearch -x -H ldaps://dc.aldpro.local:636 \
  -D "uid=ldapuser,cn=users,cn=accounts,dc=aldpro,dc=local" \
  -w ldappass \
  -b "dc=aldpro,dc=local" \
  "(cn=GRP-zVirtAdmins)"

# Проверка членства в группе
ldapsearch -x -H ldaps://dc.aldpro.local:636 \
  -D "uid=ldapuser,cn=users,cn=accounts,dc=aldpro,dc=local" \
  -w ldappass \
  -b "cn=GRP-zVirtAdmins,cn=groups,cn=accounts,dc=aldpro,dc=local" \
  "(objectClass=*)"
```

# Настройка интеграции zVirt с ALD Pro через Keycloak

## Настройка LDAP-провайдера

Для настройки LDAP-провайдера для интеграции zVirt с ALD Pro через Keycloak:

- Открыть портал администрирования zVirt и перейти в Портал Keycloak
- Выполнить вход в Портал Keycloak и перейти "**Configure** → **User Federation**"
- Нажать добавить провайдера - **Add Provider** → выбрать тип: **LDAP**

Раздел конфигурации **General Options**:

- Отображаемое имя - **UI display name**: `aldpro.local`
- Тип провайдера - **Vendor**: `Other`

Раздел конфигурации **Connection and authentication settings**:

- Адрес URL - **Connection URL**: `ldaps://dc.aldpro.local`

- Использовать **Truststore SPI**: `Always`
- Для проверки соединения нажать **Test connection**
- Тип аутентификации - **Bind Type**: `simple`
- Путь к объекту в LDAP каталоге - **Bind DN**: `uid=ldapuser,cn=users,cn=accounts,dc=aldpro,dc=local`
- Пароль для аутентификации - **Bind credentials**: `ПАРОЛЬ`
- Для проверки аутентификации нажать **Test authentication**

Раздел конфигурации **LDAP searching and updating**:

- Режим взаимодействия - **Edit mode**: `READ_ONLY`
- Пользовательский DN - **Users DN**: `dc=aldpro,dc=local`
- Атрибуты:
  - **Username LDAP attribute**: `uid`
  - **RDN LDAP attribute**: `uid`
  - **UUID LDAP attribute**: `uid`
- Классы объектов пользователя - **User object classes**: `rbra-org-unit`

Остальные разделы конфигурации настраиваются по умолчанию или опционально.
Для создание провайдера LDAP нажмите **Save**
После сохранения выполняется синхронизация, по окончании которой в разделе **Users** появятся пользователи, полученные с LDAP.

## Настройка сопоставления групп пользователей из службы каталогов ALD Pro

Для настройки сопоставления групп пользователей из LDAP-провайдера:

- Открыть портал администрирования zVirt и перейти в Портал Keycloak
- Выполнить вход в Портал Keycloak и перейти **Configure → User Federation**
- Выбрать целевой провайдер: `aldpro.local`
- Перейти на вкладу **Mappers**

Создание нового правила сопоставления групп пользователей:

- Название правила сопоставления - **Name**: `Groups Mapping`
- Тип атрибута сопоставления - **Mapper type**: `group-ldap-mapper`
- Местоположение групп в LDAP дереве - **LDAP Groups DN**: `cn=groups,cn=accounts,dc=aldpro,dc=local`
- Отключите опцию иерархии наследования групп - **Preserve Group Inheritance**: `ВЫКЛ`
- Режим взаимодействия - **Mode**: ==`READ_ONLY

- Стратегия для извлечения информации о группах пользователя - **User Groups Retrieve Strategy**: `GET_GROUPS_FROM_USER_MEMBEROF_ATTRIBUTE`
- Остальные параметры: `ПО УМОЛЧАНИЮ`
- Для создание правила нажать **Save**

Назначение групп пользователей на роли zVirt:

- Перейте в меню - **Realm roles**
- Выбрать целевую роль по умолчанию для zVirt: `default-roles-zvirt-internal`
- Перейти на вкладу группы по умолчанию - **Default Groups**
- Нажать добавить групп - **Add group**
- Выберите целевую группу и назначьте ей роль "default-roles-zvirt-internal"
- В меню "Пользователи" добавьте нужных доменных пользователей в целевую группу

Назначение пользователей на роли zVirt:

- Перейдите в меню пользователи - **Users**
- Выбрать целевого пользователя, к примеру: `zvirtadmin`
- Перейти на вкладу сопоставления ролей - **Roles mapping**
- Назначить целевую роль - **Assign role***
- Установить фильтр по сопоставляемым ролям - **Realm roles**
- Выберите целевую группу и назначьте ей роль: `default-roles-zvirt-internal`
- Назначить роль - **Assign**

# Настройка прав доступа в zVirt

## Добавление доменных групп

Для добавления доменных групп:

- Войти в портал администрирования zVirt под административной учетной записью
- Перейти: **Управление - Настройка - Системный разрешения**
- Нажать: **Добавить**
- Выбрыть для системных разрешений: **Группа**
- В поле поиск выбрать: `internalsso` и нажать **Поиск**
- Выбрать целевую групп: ==`GRP-zVirtAdmins
- Назначить целевую роль: `SuperUser` и нажать **ОК**

## Проверка аутентификации

1. Попробуйте войти в zVirt под учетной записью из ALD Pro

2. Убедитесь, что назначенные права работают корректно
3. **Настройка прав доступ пользователей и групп с ALD Pro в zVirt**

# Часть 5: Устранение неполадок

## 5.1 Ошибки сертификатов

```
# Просмотр сертификата
openssl x509 -in aldpro_root_ca.pem -text -noout

# Проверка цепочки
openssl verify -CAfile aldpro_root_ca.pem aldpro_root_ca.pem
```

## 5.2 Проблемы с подключением

```
# Проверка доступности порта
telnet dc.aldpro.local 636
nc -zv dc.aldpro.local 636

# Проверка без TLS
ldapsearch -x -H ldap://dc.aldpro.local:389 -LLL -s base -b ""
namingContexts
```

## 5.3 Журналы событий

```
# zVirt
tail -f /var/log/ovirt-engine/engine.log

# zVirt - journalctl
journalctl -u ovirt-engine

# LDAP-запросов ALD Pro
tail -f /var/log/dirsrv/slapd-aldpro/access
```

# ПРИЛОЖЕНИЕ. Параметры настройки

## Параметры для настройки zVirt AAA JDBC:

**Основные параметры LDAP:**

```
Тип  LDAP:  FreeIPA
Использовать DNS: Да
Тип подключения: Single Server
Адрес сервера: dc.aldpro.local
Протокол: ldaps://
Порт: 636
Bind DN: uid=ldapuser,cn=sysaccounts,cn=etc,dc=aldpro,dc=local
Пароль: <ldappass>
Base DN: dc=aldpro,dc=local
Имя профиля: aldpro_ldaps_integration
```

**Параметры группы:**

```
Группа для доступа: GRP-zVirtAdmins
Уровень прав: SuperUser
```

# Параметры для настройки Keycloak

**Основные параметры LDAP:**

```
Console Display Name: ALD Pro LDAPS
Vendor: Red Hat Directory Server
Connection URL: ldaps://dc.aldpro.local:636
Use Truststore SPI: ALWAYS
Bind Type: simple
Bind DN: uid=ldapuser,cn=sysaccounts,cn=etc,dc=aldpro,dc=local
Bind Credential: <ldappass>
```

**Параметры пользователей:**

```
Users DN: cn=users,cn=accounts,dc=aldpro,dc=local
User Object Classes: inetOrgPerson, organizationalPerson
Username LDAP Attribute: uid
RDN LDAP Attribute: uid
UUID LDAP Attribute: entryUUID
User Search Scope: Subtree
Import Users: ON
Sync Registrations: ON
```

**Параметры групп:**

```
Mapper Name: ALD Pro Groups
LDAP Groups DN: cn=groups,cn=accounts,dc=aldpro,dc=local
Group Name LDAP Attribute: cn
Preserve Group Inheritance: OFF
Mode: READ_ONLY
User Groups Retrieve Strategy: GET_GROUPS_FROM_USER_MEMBEROF_ATTRIBUTE
```

**Параметры ролей:**

```
Группа: GRP-zVirtAdmins
Назначенные роли: default-roles-zvirt-internal, admin
```