Интеграция Сакура со службой каталога ALD Pro

04/07/2026

САКУРА − это программный комплекс для мониторинга и контроля удалённых рабочих мест с централизованным управлением политиками безопасности. Система защищает корпоративную инфраструктуру через контроль соответствия рабочих мест требованиям безопасности, инвентаризацию оборудования и ПО, управление доступом пользователей и автоматизацию реакции на нарушения.

Интеграция позволяет расширить управление доступом с использованием данных LDAP для определения ролей и групп пользователей. Реализация аутентификации через ALD Pro обеспечивает единообразие и безопасность управления доступом в организации, упрощает администрирование и поддерживает комплексный контроль политик безопасности на рабочих местах.

Инструкция по интеграции разработана компанией ИТ-Экспертиза.

Интеграция с ALD Pro

1. Создание роли для служебной УЗ в ALD Pro

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:

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

```
dn: uid=ald-service,cn=sysaccounts,cn=etc,dc=ald-pro,dc=lan
add:objectclass: account
add:objectclass: simplesecurityobject
add:uid: ald-service
add:userPassword: securePassword
add:passwordExpirationTime: 20380119031407Z
add:nsIdleTimeout: 0
```

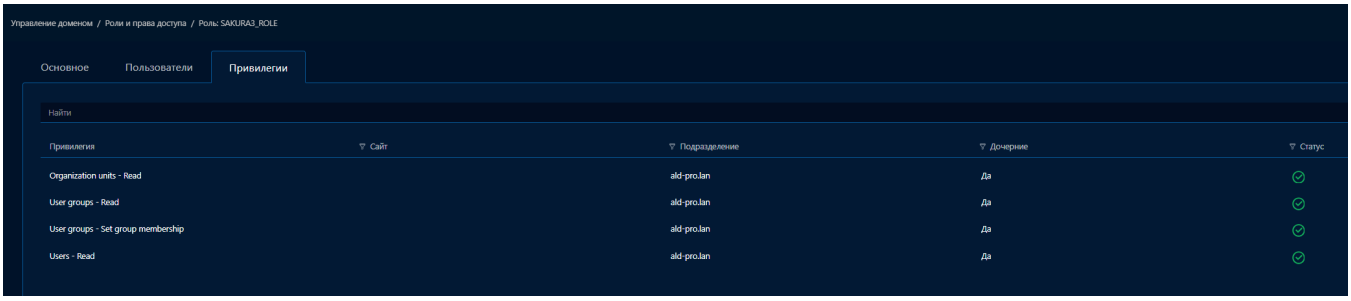
Разъяснения:

- **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: ald-service** — 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

Выполнить добавление пользователя следующей командой:

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

Список привилегий необходимый для функционирования служебной УЗ в рамках интеграции ALD Pro с САКУРА 3 (через портал ALD Pro)



Добавление сервисной учетной записи в роль через LDIF

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

```
dn: cn=SAKURA3,cn=roles,cn=accounts,dc=ald,dc=company,dc=lan
changetype: modify
add: member
member: uid=ald-service,cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan
```

Разъяснения по LDIF:

- **dn** — уникальный идентификатор роли в LDAP, куда добавляем участника
-

- **changetype: modify** — указывает, что запись изменяется
- **add: member** — операция добавления нового члена роли
- **member:** — DN пользователя, который будет участником роли

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 к команде:

- **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

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=SAKURA3, cn=roles,cn=accounts,
dc=ald,dc=company,dc=lan" member
```

Разъяснения к команде:

- **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

2. Получение сертификата для LDAPS

Для настройки защищенного LDAP-соединения потребуется получить корневой сертификат контроллера домена ALD Pro

Корневой сертификат находиться в директории /etc/ipa/ca.crt

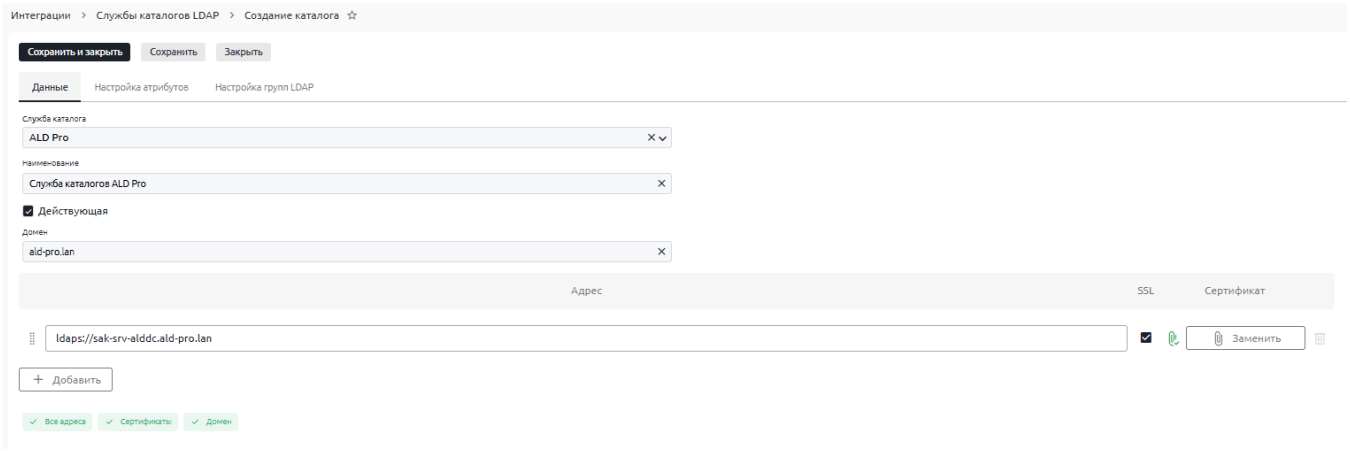
Данный сертификат понадобится далее для настройки интеграции

3. Создание службы каталогов LDAP

Во вкладке "Интеграции" "Службы каталогов LDAP" необходимо создать объект службы каталогов LDAP для ALD Pro

Список параметров:

- **Служба каталога:** выбираем ALD Pro
- **Наименование:** может быть любым
- **Действующая:** для работы необходимо ее отметить как действующую
- **Домен:** вводим домен следующим образом <поддомен>.<домен>
- **Адрес:** вводится в виде ldap://<DNS-имя контроллера домена>
- **SSL:** требуется загрузить сертификат полученный в пункте 2

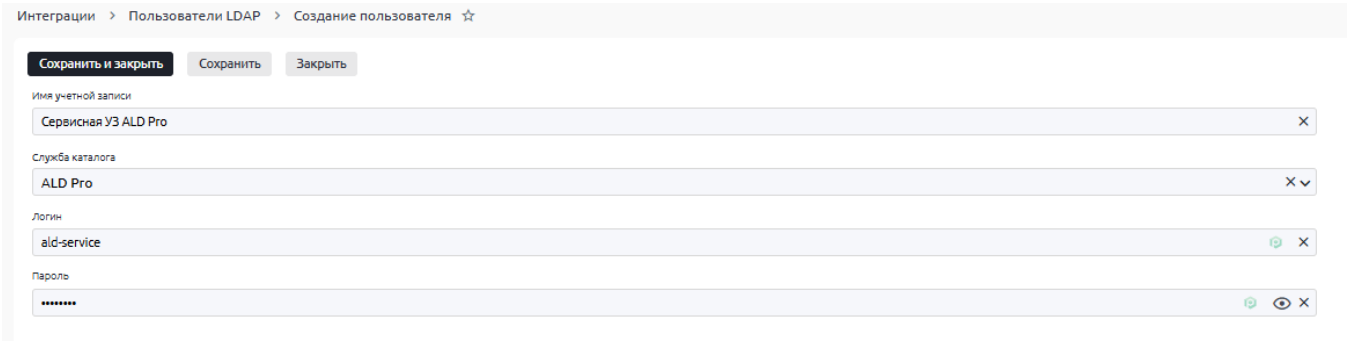


4. Создание пользователя LDAP

Во вкладке "Интеграции" "Пользователи LDAP" необходимо создать объект сервисной УЗ ALD Pro

Список параметров:

- **Имя учетной записи:** может быть любым
- **Служба каталогов:** из выпадающего списка выбираем созданный в п.2 службу каталогов
- **Логин:** необходимо ввести логин учетной записи служебной УЗ из ALD Pro
- **Пароль:** пароль от служебной УЗ

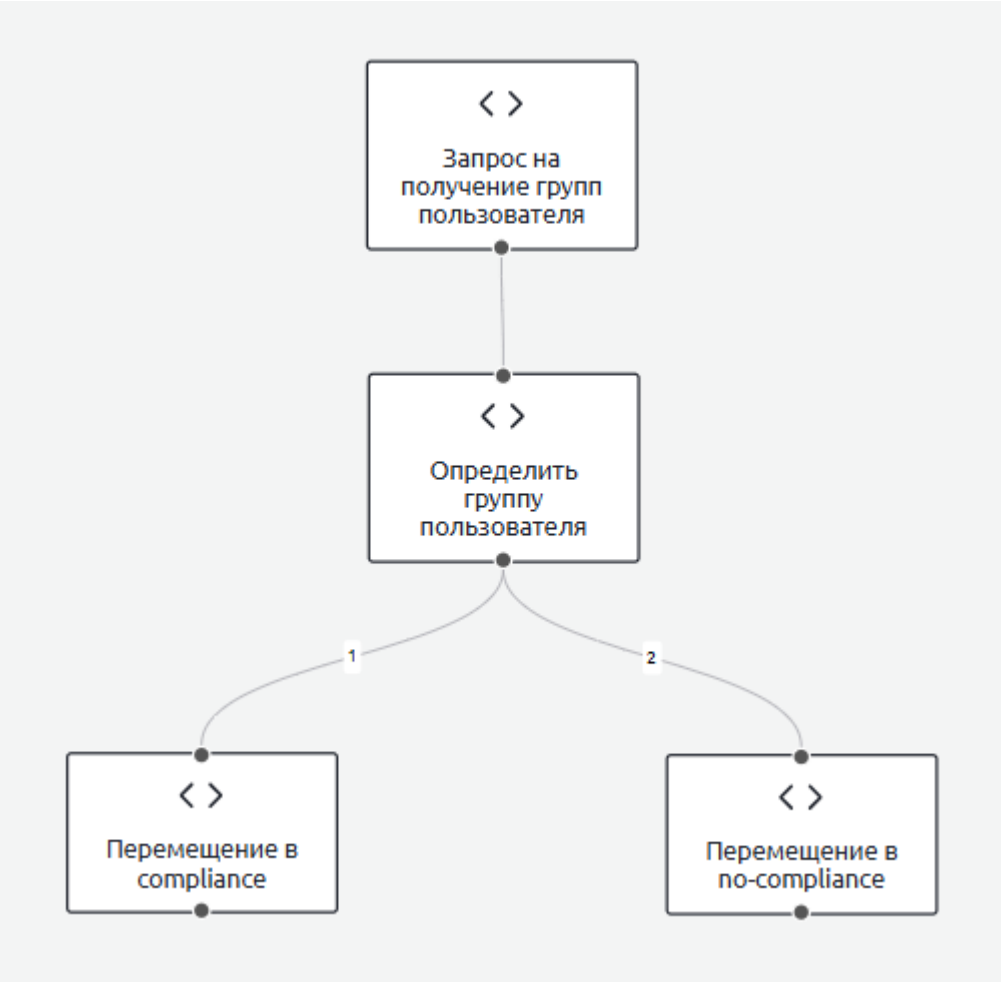


5. Создание сценариев

В САКУРА 3 существует только 2 операции при взаимодействии с ALD Pro:

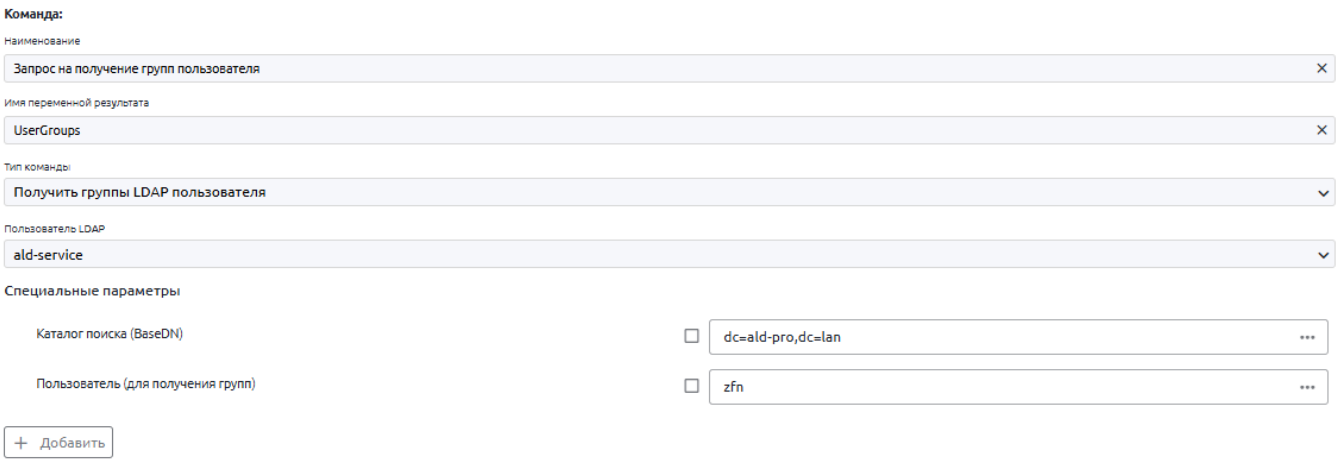
- Получить группы LDAP пользователя
- Управление группами LDAP пользователя

Пример сценария:



Запрос на получение групп выглядит следующим образом:

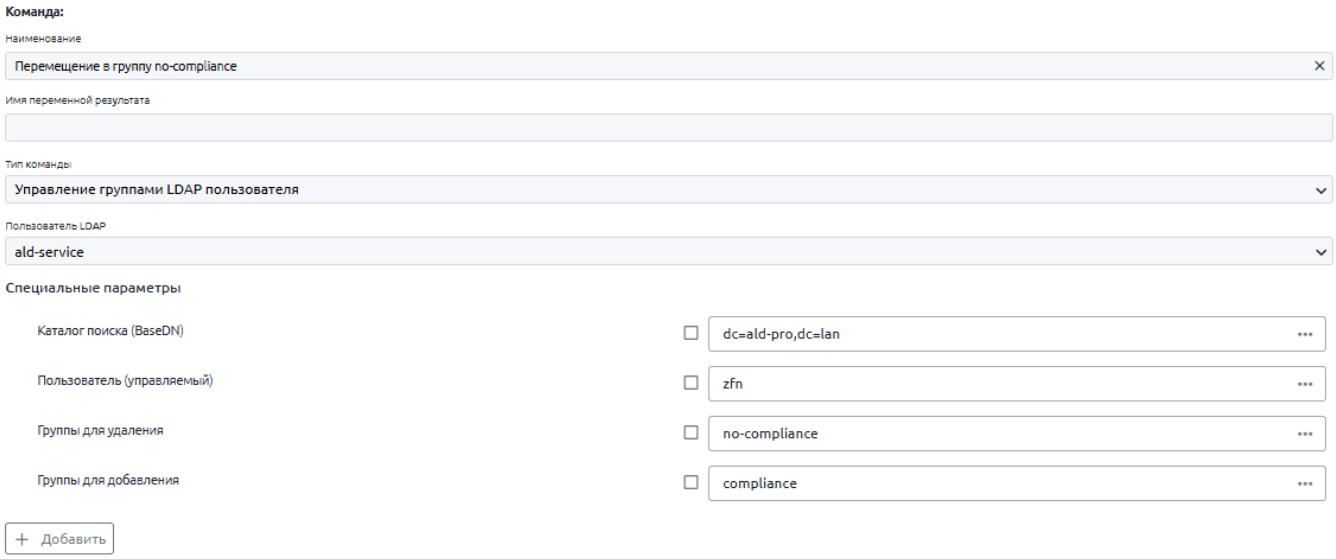
- **Наименование:** может быть любым
- **Имя переменной результата:** используется в сложных сценариях с дополнительными условиями
- **Тип команды:** Получить группы LDAP пользователя
- **Пользователь LDAP:** выбираем пользователя, созданного в п.3
- **Специальные параметры:**
  - **Каталог поиска:** ищем по всему домену
  - **Пользователь:** делаем вычисляемым, если только с PM мы можем получить имя пользователя (например, username в NAC является и именем пользователя в ALD Pro)



"Определить группу пользователя" - условие (команда ветвление), по которому проверяется входит ли пользователь в группу "no-compliance" из переменной UserGroups

Запрос на перемещение по группам:

- **Наименование:** может быть любым
- **Имя переменной результата:** используется в сложных сценариях с дополнительными условиями
- **Тип команды:** Получить группы LDAP пользователя
- **Пользователь LDAP:** выбираем пользователя, созданного в п.3
- **Специальные параметры:**
  - **Каталог поиска:** ищем по всему домену
  - **Пользователь:** делаем вычисляемым, если только с PM мы можем получить имя пользователя (например, username в NAC является и именем пользователя в ALD Pro)
  - **Группа для удаления:** пользователь будет удален из этой группы
  - **Группа для добавления:** пользователь будет добавлен в эту группу



6. Аутентификация в панель управления САКУРА

Для использования LDAP аутентификации в панель управления САКУРА необходимо выполнить настройку соответствия ролей созданных в меню "Администрирование" "Роли" с существующими ролями в ALD Pro. Соответствие ролей настраивается в меню "Интеграции" "Службы каталогов" "ALD Pro" вкладка "Настройка групп LDAP"