WHITE PAPER

НАСТРОЙКА ИНТЕГРАЦИИ СЛУЖБЫ КАТАЛОГОВ ALD PRO И TATLIN.OBJECT

О WHITE PAPER

Данный документ описывает архитектурные принципы и подходы, а также рекомендации по их применению при построении корпоративных решений на основе продуктов производства компании YADRO.

Документ предназначен для широкой аудитории, но также может включать материалы, требующие специальной профессиональной подготовки, ориентированные на системных архитекторов, администраторов, сервисных инженеров и других ИТ-специалистов, участвующих в планировании, проектировании и внедрении комплексных решений.

! Представленная информация основана на результатах исследований, а также экспертизе специалистов YADRO. Документ носит не предписывающий, а информационный характер, целью которого является информирование получателей документа о предмете произведенного исследования и о его результатах. При этом конкретные результаты и эффективность конечных решений зависят от множества факторов, которые могут различаться в зависимости от особенностей инфраструктуры и условий эксплуатации. Ни при каких обстоятельствах YADRO не несет ответственности за последствия применения получателем документа рекомендаций, инструкций, подходов и решений, указанных в документе.

Запрещается копировать, воспроизводить, изменять, публиковать, передавать, распространять, продавать информацию (часть информации), содержащуюся в документе, или создавать производные работы на основе содержания документа без предварительного письменного разрешения YADRO.

Любая информация или утверждения относительно возможностей, емкости, производительности или других характеристик продукции, указанной в документе, предоставляются исключительно на условиях «как есть» и приведена исключительно в целях описания произведенного исследования. YADRO оставляет за собой право вносить изменения/обновлять информацию в документе без уведомления.

«YADRO» является зарегистрированным товарным знаком ООО «КНС ГРУПП». Другие названия продуктов и компаний, упомянутые здесь, могут быть товарными знаками или торговыми наименованиями их соответствующих владельцев.

Актуальные версии документации публикуются на информационном ресурсе YADRO по адресу service.yadro.com.

ОГЛАВЛЕНИЕ

1. ОБ ЭКСПЕРТАХ 4
2. ВВЕДЕНИЕ 5
3. ПОДГОТОВКА ALD PRO 6
   - 3.1. Создание сервисной учетной записи 6
   - 3.2. Подготовка LDAP-групп 7
4. НАСТРОЙКА ДОСТУПА АДМИНИСТРАТОРОВ К WEBUI ЧЕРЕЗ LDAP 7
   - 4.1. Доступ к WebUI 8
   - 4.2. Настройка подключения к LDAP-серверу 8
   - 4.3. Использование шифрования (опционально) 9
5. НАСТРОЙКА ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ К S3 ЧЕРЕЗ LDAP 9
   - 5.1. Настройка подключения к LDAP-серверу 9
   - 5.2. Использование шифрования (опционально) 11
6. НАСТРОЙКА ПРИВЯЗКИ LDAP-ГРУПП К IAM-ГРУППАМ 11
   - 6.1. Создание IAM-групп (при отсутствии созданных групп) 11
   - 6.2. Настройка привязки 11
   - 6.3. Важные замечания 12
7. ЗАКЛЮЧЕНИЕ 13
8. ИСТОЧНИКИ ДАННЫХ 13

ОБ ЭКСПЕРТАХ

Антон Морозов — ведущий ИТ-инженер и системный архитектор с более чем 15-летним опытом проектирования и внедрения высоконагруженных отказоустойчивых решений.
Начинал карьеру с глубокого погружения в Windows-экосистемы, что позволило сформировать уникальную экспертизу в построении сложных гибридных инфраструктур. В рамках сотрудничества с Microsoft и Ericsson реализовывал масштабные проекты по развертыванию IPTV-платформ для международных телеком-операторов (Vodafone Greece, TDC Denmark, Oi Brazil), где особое внимание уделял аспектам высокой доступности и бесперебойной миграции сервисов.
Сейчас в YADRO занимает позицию ведущего специалиста отдела объектных систем хранения данных, где фокусируется на:

- Оптимизации интеграции TATLIN.OBJECT со сторонним ПО
- Внедрении best practices по работе с распределенными системами хранения

ВВЕДЕНИЕ

Данная инструкция описывает процесс интеграции объектного хранилища TATLIN.OBJECT с системой централизованного управления доступом ALD Pro (Astra Linux Directory) через протокол LDAP.

ВЕРСИИ ИСПОЛЬЗУЕМОГО ПО	
TATLIN.OBJECT	1.9
ALD PRO	2.4.0
Astra Linux Special Edition	1.7.4 (Ядро Linux: 5.15)

ПОДГОТОВКА ALD PRO

Создание сервисной учетной записи

Сервисная учетная запись используется для подключения TATLIN.OBJECT к LDAP-серверу ALD Pro с правами только на чтение.

Требования

- ALD Pro версии 2.4.0 или выше
- Операционная система Astra Linux Special Edition (1.7 или выше)
- Доступ к контроллеру домена с правами администратора

Шаг 1. Подключитесь по SSH к контроллеру домена ALD Pro от имени пользователя root.

Шаг 2. Создайте файл конфигурации:

```
nano srv-tatlin-bind.update
```

Шаг 3. Добавьте в файл строки:

```
dn: uid=srv-tatlin-bind,cn=sysaccounts,cn=etc,dc=test,dc=local
add:objectclass: account
add:objectclass: simplesecurityobject
add:uid: srv-tatlin-bind
add:userPassword: 1234567q!
add:passwordExpirationTime: 203801190314O7Z
add:nsIdleTimeout: 0
```

Параметры:

- uid=srv-tatlin-bind — имя сервисной учетной записи (рекомендуется оставить неизменным)
- userPassword: 1234567q! — пароль (необходимо заменить на надежный)
- dc=test,dc=local — параметры домена (необходимо заменить на параметры вашего домена, например dc=company,dc=lan)
- passwordExpirationTime: 203801190314O7Z — срок действия пароля (установленный срок действия истекает в 2038 году)
- nsIdleTimeout: 0 — таймаут простоя, в секундах (таймаут отключен)

Пример для домена company.lan:

```
dn: uid=srv-tatlin-bind,cn=sysaccounts,cn=etc,dc=company,dc=lan
add:objectclass: account
add:objectclass: simplesecurityobject
add:uid: srv-tatlin-bind
add:userPassword: MySecurePass123!@#
add:passwordExpirationTime: 203801190314O7Z
add:nsIdleTimeout: 0
```

Шаг 4. Сохраните файл (**Ctrl+O — Enter — Ctrl+X**).

Шаг 5. Выполните команду для создания учетной записи от имени пользователя root:

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

При успешном выполнении будет выведено сообщение об обновлении LDAP.

Шаг 6. Проверьте создание учетной записи:

```
ldapsearch -x -H ldap://localhost:389 \
  -D "uid=srv-tatlin-bind,cn=sysaccounts,cn=etc,dc=test,dc=local" \
  -w "1234567q!" \
  -b "dc=test,dc=local" \
  "(objectClass=*)" dn | head -20
```

Шаг 7. Замените dc=test,dc=local и пароль на свои значения.

Подготовка LDAP-групп

Шаг 1. Убедитесь, что в ALD Pro созданы необходимые группы для разграничения доступа к TATLIN.OBJECT.

Примеры групп:

- tatlin-admins — администраторы хранилища
- tatlin-users — пользователи с доступом на чтение/запись
- tatlin-readonly — пользователи с доступом только на чтение

Шаг 2. Проверьте наличие групп:

```
ldapsearch -x -H ldap://localhost:389 \
  -D "uid=srv-tatlin-bind,cn=sysaccounts,cn=etc,dc=test,dc=local" \
  -w "1234567q!" \
  -b "cn=groups,cn=accounts,dc=test,dc=local" \
  "(objectClass=groupOfNames)" cn
```

Шаг 3. Замените домен и пароль на свои значения.

Шаг 4. При необходимости создайте группы в ALD Pro:

```
ipa group-add tatlin-admins --desc="Tatlin Storage Administrators"
ipa group-add tatlin-users --desc="Tatlin Storage Users"
ipa group-add tatlin-readonly --desc="Tatlin Storage Read-Only Users"
```

НАСТРОЙКА ДОСТУПА АДМИНИСТРАТОРОВ К WEBUI ЧЕРЕЗ LDAP

Данный раздел описывает настройку аутентификации **администраторов** в WebUI TATLIN.OBJECT через LDAP. После настройки администраторы смогут входить в веб-интерфейс с использованием доменных учетных записей.

> ! Настройка не предоставляет пользователям доступ к S3. Для настройки доступа к данным через S3 см. Раздел 5.

Доступ к WebUI

Шаг 1. Откройте браузер и перейдите по адресу:

https://<Management-URL-TATLIN.OBJECT>

Шаг 2. Войдите в систему с учетной записью, имеющей роль SECURITY_ADMINISTRATORS.

Требования:

- TATLIN.OBJECT версии 1.9.0 или выше
- Учетная запись с ролью SECURITY_ADMINISTRATORS

Настройка подключения к LDAP-серверу

Шаг 1. Перейдите в раздел **Настройки → Внешние службы → LDAP → Настройка.**

Шаг 2. Выберите в качестве типа службы каталогов **стандартный LDAP** или **Active Directory.**

Шаг 3. Заполните параметры подключения:

ПАРАМЕТР	ОПИСАНИЕ	ПРИМЕР
СЕРВЕР	IP-адрес контроллера домена ALD Pro	192.168.1.10
DN ДЛЯ ПОДКЛЮЧЕНИЯ	Distinguished Name сервисной учетной записи	uid=srv-tatlin-bind,cn=sysaccounts,cn=etc,dc=test,dc=local
ПАРОЛЬ ДЛЯ ПОДКЛЮЧЕНИЯ	Пароль сервисной учетной записи	MySecurePass123!
БАЗА ПОИСКА	Корень поиска в структуре каталога	cn=accounts,dc=test,dc=local
ФИЛЬТР ПОЛЬЗОВАТЕЛЯ	LDAP-фильтр для поиска учетных записей администраторов	(objectClass=*)
ФИЛЬТР ГРУПП	LDAP-фильтр для поиска групп	(objectClass=groupOfNames)

! Настройте фильтры так, чтобы количество возвращаемых пользователей не превышало 1000, а групп — 100. Слишком большое количество объектов может привести к ошибке авторизации.

Шаг 4. Выберите режим шифрования:

РЕЖИМ	ОПИСАНИЕ
ОТКЛЮЧЕНО	Соединение без шифрования (порт 389)
ВКЛЮЧЕНО	Шифрование по протоколу SSL (порт 636)
STARTTLS	Обновление соединения до TLS (порт 389)

Шаг 5. Нажмите **Сохранить.**

Шаг 6. Нажмите **Включить** для активации интеграции.

Шаг 7. Перейдите в **Настройки → Учетные записи → Учетные записи LDAP.** Проверьте подключение и наличие пользователей.

Использование шифрования (опционально)

Если хост TATLIN.OBJECT не введен в домен ALD Pro, добавьте CA-сертификат контроллера домена в системное хранилище доверенных сертификатов.

Шаг 1. Скопируйте CA-сертификат с контроллера домена:

```
scp <admin>@<dc-host>:/etc/ipa/ca.crt /tmp/ald_ca.crt
```

Шаг 2. Добавьте сертификат в системное хранилище:

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

Для LDAPS (SSL): порт — 636, переключатель — **Включено.**
Для StartTLS: порт — 389, переключатель — **STARTTLS.**

> ! В базовой конфигурации используется порт 389 без шифрования. Для production-среды рекомендуется LDAPS.

НАСТРОЙКА ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ К S3 ЧЕРЕЗ LDAP

Данный раздел описывает настройку доступа **пользователей** к S3 data path TATLIN.OBJECT с использованием доменных учетных записей ALD Pro. После настройки пользователи смогут получать S3-ключи самостоятельно, без обращения к администратору, а права доступа будут синхронизироваться с группами в домене.

> ! Настройка не связана с доступом к WebUI. Для настройки входа администраторов в веб-интерфейс см. Раздел 4.

Настройки доступны для редактирования как в корневом (root), так и в дочерних неймспейсах. Задать конфигурацию по умолчанию для всех новых неймспейсов можно только из корневого неймспейса.

Настройка подключения к LDAP-серверу

Шаг 1. Перейдите в раздел **IAM → Интеграция с LDAP.**

По умолчанию конфигурация не задана.

Шаг 2. Нажмите **Настройка.** Откроется окно LDAP с параметрами подключения.

Шаг 3. Переведите переключатель **Статус** в режим **Включено.** Интеграция будет включена сразу после сохранения настроек.

Шаг 4. Заполните параметры подключения:

ПАРАМЕТР	ОПИСАНИЕ	ПРИМЕР
АДРЕС СЕРВЕРА *	URI LDAP-сервера	ldap://192.168.1.10:389
DN ДЛЯ ПОДКЛЮЧЕНИЯ *	Distinguished Name сервисной учетной записи	uid=srv-tatlin-bind,cn=sysaccounts,cn=etc,dc=test,dc=local
ПАРОЛЬ ДЛЯ ПОДКЛЮЧЕНИЯ	Пароль сервисной учетной записи	MySecurePass123!
БАЗА ПОИСКА *	Корень поиска в структуре каталога	cn=accounts,dc=test,dc=local
ФИЛЬТР ПОЛЬЗОВАТЕЛЯ	LDAP-фильтр поиска (должен содержать плейсхолдер {username})	(&(objectClass=person)(uid={username}))
АТРИБУТ ГРУППЫ	Атрибут LDAP-группы для привязки к IAM-группам	cn
МАКСИМАЛЬНОЕ ВРЕМЯ ЖИЗНИ КЛЮЧЕЙ	Срок действия S3-ключей, в секундах (минимум: 1)	86400 (1 сутки)
ТАЙМАУТ ПОИСКА	Лимит времени на операции поиска в LDAP, в секундах	30

Шаг 5. Выберите режим шифрования (переключатель SSL):

РЕЖИМ	ОПИСАНИЕ
ОТКЛЮЧЕНО	Соединение без шифрования (порт 389)
ВКЛЮЧЕНО	Шифрование по протоколу SSL (порт 636)
STARTTLS	Обновление соединения до TLS (порт 389)

При использовании самоподписанного сертификата переведите переключатель **Пропускать проверку TLS-сертификата** в положение **Да.**

Шаг 6. Нажмите **Сохранить.**

Шаг 7. Для активации интеграции нажмите **Включить** и подтвердите действие.

Пример конфигурации для домена test.local, контроллер домена 192.168.100.50:

```
Адрес сервера:              ldap://192.168.100.50:389
DN для подключения:         uid=srv-tatlin-bind,cn=sysaccounts,cn=etc,dc=test,dc=local
Пароль для подключения:     MySecurePass123!
База поиска:                cn=accounts,dc=test,dc=local
Фильтр пользователя:        (&(objectClass=person)(uid={username}))
Атрибут группы:             cn
Макс. время жизни ключей:   86400
Таймаут поиска:             30
SSL:                        Отключено
```


* — поле обязательно для заполнения

Использование шифрования (опционально)

Если хост TATLIN.OBJECT не введен в домен ALD Pro, добавьте CA-сертификат контроллера домена в системное хранилище.

Шаг 1. Скопируйте CA-сертификат с контроллера домена:

```
scp <admin>@<dc-host>:/etc/ipa/ca.crt /tmp/ald_ca.crt
```

Шаг 2. Добавьте в системное хранилище:

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

Для **LDAPS:** адрес — ldaps://host:636, переключатель — **SSL → Включено.**
Для **StartTLS:** адрес — ldap://host:389, переключатель — **SSL → STARTTLS.**

При использовании самоподписанного сертификата без добавления CA в системное хранилище переведите переключатель **Пропускать проверку TLS-сертификата** в положение **Да.** В режиме **Нет** соединение не будет установлено, если сертификат не пройдет проверку.

> ! В базовой конфигурации используется ldap:// без шифрования. Для production-среды рекомендуется LDAPS.

НАСТРОЙКА ПРИВЯЗКИ LDAP-ГРУПП К IAM-ГРУППАМ

Создание IAM-групп (при отсутствии созданных групп)

Шаг 1. Перейдите в раздел **IAM → Группы.**

Шаг 2. Создайте необходимые IAM-группы с соответствующими правами.

Примеры групп:

tatlin-admins — полные права на управление;
tatlin-power-users — чтение/запись в S3-бакетах;
tatlin-readers — только чтение.

Настройка привязки

Шаг 1. Перейдите в раздел **IAM → Интеграция с LDAP → Привязка.**

По умолчанию привязки не заданы.

Шаг 2. Нажмите **Создать.** Откроется окно **Изменить привязку.**

Шаг 3. Заполните форму:

Группа IAM: выберите из выпадающего списка IAM-группу, для которой нужно назначить права.

Группы LDAP: введите точные имена LDAP-групп (по одной на строку или через запятую). Имена должны соответствовать значению атрибута, указанного в поле **Атрибут группы** при настройке подключения.

Пример 1. Администраторы:

```
Группа IAM: tatlin-admins
Группы LDAP: tatlin-object-admins
```

Пример 2. Пользователи:

```
Группа IAM: tatlin-power-users
Группы LDAP: tatlin-object-users, developers, devops
```

Пример 3. Только чтение:

```
Группа IAM:   tatlin-readers
Группы LDAP:  tatlin-object-readonly, auditors
```

Шаг 4. Нажмите **Сохранить.**

Шаг 5. Повторите шаги 2–4 для всех необходимых привязок.

Управление привязками:

Для редактирования выберите запись в таблице.
Для удаления выберите **Действия → Удалить** и подтвердите действие.

Важные замечания

- Имена LDAP-групп должны точно соответствовать атрибуту cn группы в ALD Pro.
- Предусмотрено указание нескольких LDAP-групп через запятую или по одной на строку.
- Не разрешается использование более 1000 объектов в фильтрах.

Время жизни S3-ключей доступа

S3-ключи (Access Key / Secret Key), выданные пользователю для доступа к data path, **не привязаны к состоянию учетной записи в домене**. Ключи остаются активными, если пользователь заблокирован или удален в ALD Pro.

- Уволенный или заблокированный в домене сотрудник сохраняет доступ к данным через S3-ключи до их явной инвалидации.
- Удаление пользователя из LDAP-группы не отзывает ранее выданные ключи автоматически.

Рекомендации

- Всегда задавайте время жизни S3-ключей при их создании: **IAM → Пользователи → Ключи доступа → TTL.**
- При увольнении или блокировке сотрудника вручную инвалидируйте его ключи в TATLIN.OBJECT: **IAM → Пользователи → Ключи доступа → Удалить.**
- Настройте регулярный аудит активных ключей, срок действия которых не ограничен.

Политики блокировки учетных записей

TATLIN.OBJECT и ALD Pro применяют **независимые** политики блокировки при неверном вводе пароля. Это означает, что пользователь может быть заблокирован на стороне TATLIN.OBJECT, оставаясь при этом активным в домене ALD Pro.

- Если пользователь сообщает об ошибке входа в TATLIN.OBJECT, но успешно аутентифицируется в других сервисах домена, это является признаком блокировки на уровне TATLIN.OBJECT, а не домена.
- Сброс пароля в ALD Pro **не снимает** блокировку в TATLIN.OBJECT

Действия при блокировке

При блокировке необходимо разблокировать пользователя в интерфейсе TATLIN.OBJECT: **IAM → Пользователи → выбрать пользователя → Разблокировать.**

ЗАКЛЮЧЕНИЕ

Результаты выполнения данной инструкции:

- Создание сервисной учетной записи для подключения TATLIN.OBJECT к ALD Pro.
- Настройка LDAP-интеграции в веб-интерфейсе TATLIN.OBJECT.
- Создание привязки между LDAP-группами ALD Pro и IAM-группами TATLIN.OBJECT.
- Настройка разграничения доступа на основе групповой принадлежности.

Реализованное решение соответствует:

- Требованиям ФСТЭК (централизованное управление доступом).
- Политике наименьших привилегий (использование сервисной учетной записи только для чтения).
- Принципу разделения обязанностей (разграничение ролей через группы).
- Требованиям к аудиту (логирование всех действий пользователей в обеих системах).

ИСТОЧНИКИ ДАННЫХ

1. Руководство администратора TATLIN.OBJECT
2. Руководство администратора ALD Pro
3. RFC 4511 (LDAP Protocol)
4. FreeIPA Documentation