WHITE PAPER

НАСТРОЙКА ИНТЕГРАЦИИ СЛУЖБЫ КАТАЛОГОВ FREEIPA 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 FREEIPA 6
   - 3.1. Создание сервисной учетной записи 6
   - 3.2. Подготовка LDAP-групп 7
   - 3.3. Получение информации о домене FreeIPA 8
4. НАСТРОЙКА ДОСТУПА АДМИНИСТРАТОРОВ К WEBUI ЧЕРЕЗ LDAP 9
   - 4.1. Доступ к WebUI 9
   - 4.2. Настройка подключения к LDAP-серверу 9
   - 4.3. Использование шифрования (опционально) 11
   - 4.4. Расширенные фильтры (опционально) 11
5. НАСТРОЙКА ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ К S3 ЧЕРЕЗ LDAP 11
   - 5.1. Настройка подключения к LDAP-серверу 12
   - 5.2. Использование шифрования (опционально) 13
6. НАСТРОЙКА ПРИВЯЗКИ LDAP-ГРУПП К IAM-ГРУППАМ 13
   - 6.1. Создание IAM-групп (при отсутствии созданных групп) 13
   - 6.2. Настройка привязки 14
   - 6.3. Важные замечания 14
   - 6.4. Проверка привязки через FreeIPA 15
7. ПРОВЕРКА РАБОТЫ ИНТЕГРАЦИИ 16
   - 7.1. Проверка подключения к LDAP 16
   - 7.2. Проверка аутентификации в WebUI 16
   - 7.3. Проверка доступа к S3 16
8. ЗАКЛЮЧЕНИЕ 17
9. ИСТОЧНИКИ ДАННЫХ 17

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 службой каталогов FreeIPA через протокол LDAP

ВЕРСИИ ИСПОЛЬЗУЕМОГО ПО	
TATLIN.OBJECT	1.9
FREEIPA	4.9.x+
CentOS	8

ПОДГОТОВКА FREEIPA

Создание сервисной учетной записи

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

Требования:

- FreeIPA версии 4.9.0 или выше.
- Операционная система RHEL/CentOS/Rocky Linux 8.x или выше.
- Доступ к серверу FreeIPA с правами администратора.

Шаг 1. Подключитесь по SSH к серверу FreeIPA 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=example,dc=com
add:objectclass: account
add:objectclass: simplesecurityobject
add:uid: srv-tatlin-bind
add:userPassword: SecurePassword123!
add:passwordExpirationTime: 203801190314O7Z
add:nsIdleTimeout: 0
```

Параметры:

- uid=srv-tatlin-bind — имя сервисной учетной записи (рекомендуется оставить неизменным);
- userPassword: SecurePassword123! — пароль (необходимо заменить на надежный);
- dc=example,dc=com — параметры домена (необходимо заменить на параметры вашего домена FreeIPA);
- passwordExpirationTime: 203801190314O7Z — срок действия пароля (установленный срок действия истекает в 2038 году);
- nsIdleTimeout: 0 — таймаут простоя, в секундах (таймаут отключен).

Чтобы узнать ваш Base DN, запросите информацию о домене:

```
ipa config-show | grep "IPA domain"
```

Пример Base DN для домена "corp.local": dc=corp,dc=local
Пример вывода для домена "corp.local":

```
dn: uid=srv-tatlin-bind,cn=sysaccounts,cn=etc,dc=corp,dc=local
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 root:

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

При успешном выполнении будет выведено сообщение:

```
Update complete
The ipa-ldap-updater command was successful
```

Шаг 6. Проверьте создание учетной записи:

```
ldapsearch -x -H ldap://localhost:389 \
  -D "uid=srv-tatlin-bind,cn=sysaccounts,cn=etc,dc=example,dc=com" \
  -w "SecurePassword123!" \
  -b "dc=example,dc=com" \
  "(objectClass=*)" dn | head -20
```

Шаг 7. Замените dc=example,dc=com и пароль на свои значения.

Возвращение командой списка DN свидетельствует об успешном создании учетной записи.

Подготовка LDAP-групп

Убедитесь, что в FreeIPA созданы необходимые группы для разграничения доступа к TATLIN.OBJECT.

Примеры групп:

- tatlin-admins — администраторы хранилища (полный доступ);
- tatlin-users — пользователи с доступом на чтение/запись;
- tatlin-readonly — пользователи с доступом только на чтение;

Шаг 1. Создайте группы одним из доступных способов.

Через IPA CLI

1. Войдите с правами администратора:

```
kinit admin
```

2. Создайте группы:

```
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"
```

Через WebUI

1. Откройте WebUI FreeIPA и перейдите по ссылке: https://<freeipa-server>/ipa/ui.
2. Перейдите в **Identity → Groups.**
3. Нажмите **Add.**
4. Заполните **Group name и Description.**
- Group name: tatlin-admins
- Description: Tatlin Storage Administrators
5. Сохраните и повторите для остальных групп.

Шаг 2. Добавьте пользователей в группы:

```
ipa group-add-member tatlin-admins --users=admin,user1
ipa group-add-member tatlin-users --users=user2,user3
ipa group-add-member tatlin-readonly --users=user4
```

Шаг 3. Проверьте группы:

Через IPA CLI

```
ipa group-show tatlin-admins
```

Через LDAP

```
ldapsearch -x -H ldap://localhost:389 \
  -D "uid=srv-tatlin-bind,cn=sysaccounts,cn=etc,dc=example,dc=com" \
  -w "SecurePassword123!" \
  -b "cn=groups,cn=accounts,dc=example,dc=com" \
  "(objectClass=groupOfNames)" cn
```

Шаг 4. Замените домен и пароль на свои значения.

Получение информации о домене FreeIPA

Получение домена:

```
ipa config-show | grep "IPA domain"
```

Пример вывода:

```
IPA domain: corp.local
```

Получение realm:

```
ipa config-show | grep "IPA realm"
```

Пример вывода:

```
IPA realm: CORP.LOCAL
```

Получение FQDN сервера:

```
hostname -f
```

Пример вывода:

```
ipa01.corp.local
```

Проверка доступности LDAP:

```
ss -tlnp | grep 389
```

Вывод должен отображать порт 389 (LDAP) или 636 (LDAPS).

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 используя доменные учетные записи FreeIPA.

> ! Настройка не дает 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-IP-адрес-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 тип службы каталогов: стандартный LDAP.

Шаг 3. Заполните параметры подключения:

ПАРАМЕТР	ОПИСАНИЕ	ПРИМЕР
СЕРВЕР	IP-адрес или FQDN сервера FreeIPA	192.168.1.10 или ipa01.corp.local
DN ДЛЯ ПОДКЛЮЧЕНИЯ	Distinguished Name сервисной учетной записи	uid=srv-tatlin-bind,cn=sysaccounts,cn=etc,dc=corp,dc=local
ПАРОЛЬ ДЛЯ ПОДКЛЮЧЕНИЯ	Пароль сервисной учетной записи	SecurePassword123!
БАЗА ПОИСКА	Корень поиска в структуре каталога	cn=accounts,dc=corp,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.

Пример конфигурации для домена corp.local с сервером FreeIPA 192.168.100.50:

```
Сервер:                  192.168.100.50
DN для подключения:      uid=srv-tatlin-bind,cn=sysaccounts,cn=etc,dc=corp,dc=local
Пароль для подключения:  SecurePassword123!
База поиска:             cn=accounts,dc=corp,dc=local
Фильтр пользователей:    (objectClass=*)
Фильтр групп:            (objectClass=groupOfNames)
Шифрование:              Отключено
```

Использование шифрования (опционально)

Если хост TATLIN.OBJECT не введен в домен FreeIPA, добавьте CA-сертификат сервера FreeIPA в системное хранилище доверенных сертификатов.

Шаг 1. Скопируйте CA-сертификат с сервера FreeIPA:

```
cp <admin>@<ipa-host>:/etc/ipa/ca.crt /tmp/ipa_ca.crt
```

Шаг 2. Добавьте сертификат в системное хранилище:

```
sudo cp /tmp/ipa_ca.crt /usr/local/share/ca-certificates/ipa_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.

Расширенные фильтры (опционально)

Фильтр для поиска только активных пользователей:

```
(&(objectClass=person)(!(nsAccountLock=TRUE)))
```

Фильтр для поиска пользователей из определенных групп:

```
(&(objectClass=person)(|
  (memberOf=cn=tatlin-admins,cn=groups,cn=accounts,dc=corp,dc=local)
  (memberOf=cn=tatlin-users,cn=groups,cn=accounts,dc=corp,dc=local)
))
```

Фильтр для исключения служебных учетных записей:

```
(&(objectClass=person)(!(uid=admin))(!(uid=srv-*)))
```

НАСТРОЙКА ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ К S3 ЧЕРЕЗ LDAP

Данный раздел описывает настройку доступа пользователей к S3 data path TATLIN.OBJECT с использованием доменных учетных записей FreeIPA. 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 *	URL 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=corp,dc=local
ПАРОЛЬ ДЛЯ ПОДКЛЮЧЕНИЯ	Пароль сервисной учетной записи	SecurePassword123!
БАЗА ПОИСКА *	Корень поиска в структуре каталога	cn=accounts,dc=corp,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.

* — поле обязательно для заполнения

Пример конфигурации для домена corp.local, сервер FreeIPA 192.168.100.50:

```
Адрес сервера:              ldap://192.168.100.50:389
DN для подключения:         uid=srv-tatlin-bind,cn=sysaccounts,cn=etc,dc=corp,dc=local
Пароль для подключения:     SecurePassword123!
База поиска:                cn=accounts,dc=corp,dc=local
Фильтр пользователя:        (&(objectClass=person)(uid={username}))
Атрибут группы:             cn
Макс. время жизни ключей:   86400
Таймаут поиска:             30
SSL:                        Отключено
```

Использование шифрования (опционально)

Если хост TATLIN.OBJECT не введен в домен FreeIPA, добавьте CA-сертификат сервера FreeIPA в системное хранилище.

Шаг 1. Скопируйте CA-сертификат с сервера FreeIPA:

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

Шаг 2. Добавьте в системное хранилище:

```
sudo cp /tmp/ipa_ca.crt /usr/local/share/ca-certificates/ipa_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:

IAM ГРУППА	ОПИСАНИЕ	ПРАВА
TATLIN-ADMINS	Администраторы хранилища	Полный доступ к управлению
TATLIN-POWER-USERS	Продвинутые пользователи	Чтение/запись в S3-бакетах
TATLIN-READERS	Пользователи на чтение	Только чтение данных

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-admins
```

Пример 2. Пользователи:

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

Пример 3. Только чтение:

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

Шаг 4. Нажмите **Сохранить.**

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

Управление привязками:

- Для редактирования — выберите запись в таблице.
- Для удаления — **Действия → Удалить**, подтвердите действие.

Важные замечания

- Имена LDAP-групп должны точно соответствовать атрибуту cn группы в FreeIPA.
- Предусмотрено указание нескольких LDAP-групп через запятую или по одной на строку.
- Регистр букв имеет значение (например, tatlin-admins и Tatlin-Admins не совпадают).
- Не разрешается использование более 1000 объектов в фильтрах.
- Привязка обновляется автоматически при каждом входе пользователя.

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 FreeIPA.

- 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 FreeIPA 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 FreeIPA.

Практические последствия:

- 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 FreeIPA **не снимает** блокировку в TATLIN.OBJECT.

Действия при блокировке

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

Проверка привязки через FreeIPA

Чтобы получить информацию о группе, выполните:

```
ipa group-show tatlin-admins
```

Чтобы увидеть имя пользователя, выполните:

```
ipa user-show username
```

Чтобы увидеть группы пользователя, выполните:

```
ipa user-show username --all | grep "Member of groups"
```

ПРОВЕРКА РАБОТЫ ИНТЕГРАЦИИ

Проверка подключения к LDAP

Через WebUI TATLIN.OBJECT

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

Шаг 2. Чтобы проверить статус подключения, убедитесь, что отображается статус "Connected" или "Enabled" и проверьте количество найденных пользователей.

Через командную строку на сервере FreeIPA

Шаг 1. Проверьте подключения и пользователей:

```
ldapsearch -x -H ldap://localhost:389 \
  -D "uid=srv-tatlin-bind,cn=sysaccounts,cn=etc,dc=corp,dc=local" \
  -w "SecurePassword123!" \
  -b "cn=accounts,dc=corp,dc=local" \
  "(objectClass=person)" uid cn | grep -E "^(uid|cn):"
```

Шаг 2. Проверьте группы:

```
ldapsearch -x -H ldap://localhost:389 \
  -D "uid=srv-tatlin-bind,cn=sysaccounts,cn=etc,dc=corp,dc=local" \
  -w "SecurePassword123!" \
  -b "cn=groups,cn=accounts,dc=corp,dc=local" \
  "(objectClass=groupOfNames)" cn member | grep -E "^(cn|member):"
```

Проверка аутентификации в WebUI

Шаг 1. Откройте новое окно браузера в режиме инкогнито.

Шаг 2. Перейдите по адресу TATLIN.OBJECT.

Шаг 3. Войдите с использованием доменной учетной записи. Используйте логин username (только имя пользователя, без @domain) и пароль пользователя в FreeIPA

Шаг 4. Проверьте доступ к соответствующим ресурсам согласно привязке групп.

Проверка доступа к S3

Шаг 1. Перейдите в **IAM → Интеграция с LDAP** и убедитесь, что статус **Включено.**

Шаг 2. Войдите в TATLIN.OBJECT как пользователь домена FreeIPA.

Шаг 3. Перейдите в **IAM → Пользователи → Ключи доступа** и убедитесь, что S3-ключи были выданы автоматически.

Шаг 4. Проверьте доступ к S3 с помощью клиента (например, aws s3 ls) с использованием полученных ключей.

ЗАКЛЮЧЕНИЕ

Результаты выполнения данной инструкции:

- Создание сервисной учетной записи для подключения TATLIN.OBJECT к FreeIPA.
- Настройка LDAP-интеграции в веб-интерфейсе TATLIN.OBJECT.
- Создание или использование существующих групп в FreeIPA для разграничения доступа.
- Настройка привязки между LDAP-группами FreeIPA и IAM-группами TATLIN.OBJECT.
- Проверка работоспособности интеграции и аутентификации пользователей.

Реализованное решение соответствует:

- Политике наименьших привилегий (сервисная УЗ имеет только права на чтение).
- Принципу разделения обязанностей (роли разграничены через группы).
- Требованиям аудита (логирование всех действий пользователей происходит в обеих системах).
- ГОСТ Р 57580.1 (идентификация и доступ находятся под управлением).

ИСТОЧНИКИ ДАННЫХ

1. Руководство администратора TATLIN.OBJECT
2. FreeIPA Official Documentation
3. Red Hat Identity Management Guide
4. LDAP Protocol RFC 4511