Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Keycloak SSO: один вход для корпоративных сервисов

Как мы разворачиваем Keycloak 26.7, федерируем Active Directory и подключаем сервисы по OIDC и…

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

В офисе на 30-80 человек сотрудник держит 8-12 паролей: почта, портал, GitLab, Nextcloud, Grafana, Zabbix, CRM, VPN. Пароли повторяются, живут на стикерах и не отзываются при увольнении: учётка в AD блокируется, а вход в веб-сервисы остаётся. Мы закрываем это одним Identity Provider на Keycloak: единая точка входа, единый отзыв доступа, обязательная 2FA и общий журнал входов.

Почему это важно бизнесу

- Уволенный теряет доступ ко всем сервисам одной операцией в AD, а не десятью ручными правками в разных панелях
- Один сильный пароль плюс TOTP вместо десятка одинаковых паролей, разложенных по несвязанным системам
- Заявки «забыл пароль» уходят в self-service сброс через почту, админ не тратит на рутину часы каждую неделю
- Единый журнал входов и событий даёт доказуемую картину доступа для проверок и внутренних разбирательств
- Новый сервис подключается созданием клиента в realm, а не заведением отдельной базы учёток со своим циклом жизни

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

26.7

Ветка Keycloak для новых инсталляций (актуальный патч 26.7.3): SCIM API и упрощённый multi-clu…

релиз-ноты Keycloak 26.7

900 с

Periodic changed users sync у LDAP-провайдера: правки в AD доезжают в realm за 15 минут

наш стандарт

9000

Порт management-интерфейса по умолчанию (http-management-port): /health и /metrics отделены от…

Keycloak, Management interface

30 мин

SSO Session Idle в realm corp при SSO Session Max 10 ч: сессия не живёт сутками

наш стандарт

5 мин

Access Token Lifespan: короткий токен сужает окно использования украденной сессии

наш стандарт

x2

Две реплики Keycloak за HAProxy с общим кэшем сессий: рестарт узла не роняет вход

наш стандарт

РЕАЛИЗАЦИЯ 1 ИЗ 3

Развёртывание Keycloak и терминация TLS

Что настраиваем

Отдельная VM 4 vCPU / 8 ГБ / 50 ГБ, docker compose: Keycloak 26.7 и PostgreSQL 16, nginx как фронт TLS

Как мы это делаем

1. Поднимаем PostgreSQL 16 отдельным контейнером под базу keycloak, серверу задаём db=postgres, db-url, db-username, db-password через переменные KC_DB, KC_DB_URL, KC_…
2. Собираем оптимизированный образ: kc.sh build с нужными features, запуск командой kc.sh start --optimized, без пересборки конфигурации на каждом рестарте
3. За прокси включаем proxy-headers=xforwarded (парсинг X-Forwarded-*), задаём hostname=https://sso.example.ru и hostname-strict=true, чтобы issuer и редиректы не подм…
4. Включаем health-enabled=true и metrics-enabled=true: /health/ready и /metrics поднимаются на management-порту 9000 и доступны только из сети мониторинга
5. TLS терминируем на nginx с сертификатом Let's Encrypt и HSTS, сам Keycloak слушает http только во внутренней docker-сети

РЕЗУЛЬТАТ

Стенд воспроизводим: docker-compose.yml и .env без секретов лежат в Git, подъём с нуля занимает минуты. Health-пробы отдают состояние старта и БД, Prometheus снимает метрики логинов и сессий, при этом служебные эндпоинты наружу не открыты.

КЛЮЧЕВОЙ НЮАНС

Главный источник поломок за прокси — hostname. Без явного hostname и с proxy-headers, которому доверяют лишние узлы, issuer берётся из запроса, и клиенты начинают отвергать токены и подпись SAML; адрес фиксиру…

РЕАЛИЗАЦИЯ 2 ИЗ 3

Федерация с Active Directory и роли из групп

Что настраиваем

Realm corp, LDAP-провайдер к контроллеру домена по ldaps://dc01:636, мапперы групп и статуса учёток

Как мы это делаем

1. Заводим сервисную учётку только на чтение, Bind DN в OU=Services, соединение ldaps://dc01.corp.example.ru:636 с корневым сертификатом домена в truststore
2. Vendor: Active Directory, Edit Mode: READ_ONLY, Username LDAP attribute: sAMAccountName, UUID LDAP attribute: objectGUID — мастером учёток остаётся домен
3. Periodic changed users sync 900 с, periodic full sync раз в сутки, Batch Size подбираем так, чтобы полный синк не держал соединение к DC дольше минуты
4. Добавляем group-ldap-mapper: LDAP Groups DN=OU=Groups, Mode=READ_ONLY, User Groups Retrieve Strategy=LOAD_GROUPS_BY_MEMBER_ATTRIBUTE_RECURSIVELY для вложенных групп…
5. Проверяем, что в мапперах провайдера есть msad-user-account-control-mapper: без него отключённая в AD учётка продолжает проходить аутентификацию в Keycloak

РЕЗУЛЬТАТ

Отключение сотрудника делается один раз, в AD: учётка в realm становится неактивной, а живые сессии снимаем действием Sessions → Sign out all active sessions. Права в приложениях едут от групп домена, отдельные списки доступа в каждом сервисе больше не ведём.

КЛЮЧЕВОЙ НЮАНС

READ_ONLY — сознательный выбор: писать в AD из Keycloak мы не даём. Маппер msad-user-account-control-mapper проверяем руками после каждой правки провайдера: без него блокировка в домене не закрывает вход.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Подключение сервисов и вторая проверка входа

Что настраиваем

Клиенты realm corp: OIDC для Nextcloud, Grafana, Proxmox; SAML для GitLab; политика 2FA на браузерном флоу

Как мы это делаем

1. Для OIDC создаём confidential-клиент: Standard flow, точный Valid redirect URI без wildcard, Web origins по домену сервиса, client secret — в менеджере паролей
2. Добавляем protocol mapper Group Membership в claim groups и Audience mapper, в Grafana роль вычисляется из этого claim через role_attribute_path в секции auth.gener…
3. SAML-клиент для GitLab: подписанные assertion, NameID format persistent, отпечаток сертификата IdP прописываем в idp_cert_fingerprint в gitlab.rb и ставим на контро…
4. В realm включаем Required Action Configure OTP и добавляем OTP Form в browser flow, администраторам дополнительно даём WebAuthn/passkey
5. По каждому клиенту проверяем сценарии: вход, single logout, поведение после истечения сессии и после Sign out all active sessions

РЕЗУЛЬТАТ

Сотрудник вводит пароль один раз и переходит между сервисами без повторной авторизации, а поддержка получает единый журнал событий входа по всем приложениям. Новый сервис подключается созданием клиента и маппера, без своей базы пользователей.

КЛЮЧЕВОЙ НЮАНС

Wildcard в redirect URI и открытый Web origins — самая дорогая ошибка в конфигурации клиента. Отпечаток SAML-сертификата IdP надо отслеживать: его ротация молча ломает вход в GitLab.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **hostname-strict выключен «чтобы заработало»**
  Issuer и редиректы начинают зависеть от заголовков запроса. Фиксируем hostname, включаем строгий режим, а прокси доверяем через proxy-headers.

- ✕ **Wildcard в Valid redirect URI**
  Звёздочка расширяет поверхность атаки на код авторизации. Прописываем полный путь callback каждого сервиса отдельной строкой и закрываем Web origins.

- ✕ **Нет msad-user-account-control-mapper**
  Без него отключение учётки в AD не переносится в realm и бывший сотрудник входит по SSO. Ставим маппер сразу при создании LDAP-провайдера.

- ✕ **Синхронизация вместо снятия сессий**
  Синк меняет статус учётки, но выданная SSO-сессия живёт до таймаута. При увольнении дополнительно делаем Sign out all active sessions и отзываем offl…

- ✕ **Нет резервной копии realm**
  Дамп PostgreSQL поднимает всё, но долго. Держим рядом экспорт realm: клиенты, флоу и мапперы восстанавливаются за минуты.

- ✕ **Секреты клиентов лежат в Git**
  docker-compose.yml и .env версионируем, но пароли БД и client secret выносим в менеджер паролей и переменные окружения хоста.

- ✕ **Management-порт 9000 опубликован наружу**
  Management-интерфейс с /health и /metrics раскрывает состояние узла и БД. Наружу отдаём только основной порт через прокси, 9000 держим в LAN для Prom…

- ✕ **2FA включена только у админов**
  TOTP на админах не защищает почту и файлы рядового сотрудника. Configure OTP делаем обязательным для всего realm, passkey — для IT.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Один узел Keycloak 26.7 на PostgreSQL 16, TLS на nginx, hostname задан явно и hostna…
- LDAP-провайдер к AD в режиме READ_ONLY с msad-user-account-control-mapper
- Обязательный TOTP для административных учёток realm
- Ежедневный pg_dump базы keycloak на отдельное хранилище

НОРМАЛЬНО

- Экспорт realm рядом с дампом БД, хранение копий вне узла Keycloak
- Роли из групп AD: group-ldap-mapper и claim groups в токене клиента
- TOTP для всех, короткий Access Token Lifespan и лимиты SSO-сессии
- Мониторинг /health/ready и метрик логинов с management-порта 9000 внутри сети

ХОРОШО

- Две реплики за HAProxy с общим кэшем сессий и проверкой /health/ready
- WebAuthn/passkey для IT и владельцев критичных сервисов
- Тестовое восстановление realm и БД на staging раз в квартал
- Разбор событий входа в Zabbix/SIEM: всплески отказов и перебор паролей

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Задан hostname и включён hostname-strict, а доверие прокси описано через proxy-headers?
- [ ] LDAP-провайдер работает по ldaps:636 с проверкой сертификата контроллера домена?
- [ ] Стоит msad-user-account-control-mapper и блокировка в AD реально закрывает вход?
- [ ] Есть регламент: увольнение = блокировка в AD плюс Sign out all active sessions в realm?
- [ ] У всех клиентов redirect URI без wildcard, а client secret хранится не в Git?
- [ ] Configure OTP включён как Required Action для всех пользователей realm, а не только для админов?
- [ ] Включена Brute force detection в Realm settings → Security defenses и задан порог временной блокировки при пере...
- [ ] Делается и pg_dump базы keycloak, и экспорт realm по расписанию, в разные хранилища?
- [ ] Проводилось тестовое восстановление Keycloak на отдельном стенде за последние три месяца?
- [ ] Management-порт 9000 с /health и /metrics закрыт от внешней сети и отдан мониторингу?

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.

ЧТО МЫ ДЕЛАЕМ

Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Разворачиваем Keycloak 26.7 с PostgreSQL, TLS и оптимизированной сборкой kc.sh build + start --optimized
- Настраиваем федерацию с Active Directory: мапперы групп, статусы учёток, синк каждые 15 минут
- Подключаем сервисы по OIDC и SAML: GitLab, Nextcloud, Grafana, Zabbix, Proxmox, портал, CRM
- Внедряем TOTP для всех и passkey для админов, пишем регламент отзыва доступа при увольнении
- Ставим бэкап БД и экспорт realm, мониторинг узла и тестовое восстановление по графику

15+
лет в ИТ-поддержке

50
рабочих мест — наш профиль

МТС
дата-центр, Москва

КОНТАКТЫ

Обсудить вашу задачу

Сайт	**itfresh.ru**
Телефон	**+7 903 729-62-41**
Telegram	**@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.

itfresh.ru

ДОКУМЕНТАЦИЯ И НАШ СТЕК

Техническая база

01 Server Administration Guide — User federation: LDAP-провайдер и мапперы (keycloak.org — 26.7)

02 All configuration — параметры db, health, metrics, http-management-port (keycloak.org — 26.7)

03 Configuring the hostname (v2) — hostname и hostname-strict (keycloak.org — 26.7)

04 Using a reverse proxy — значения proxy-headers, blueprints HAProxy/nginx (keycloak.org — 26.7)

05 Management interface — /health и /metrics на порту 9000 (keycloak.org — 26.7)

06 Release notes Keycloak 26.7 — SCIM API и multi-cluster HA в статусе preview (keycloak.org — 2026)

07 Importing and exporting realms — kc.sh export (keycloak.org — 26.7)

08 Шаблон ITfresh: realm corp и чек-лист подключения клиента (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.