Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

SSO для офиса на 15-50 PM: единый вход в 1С, почту и CRM

Как мы связываем AD, Keycloak, RADIUS и 2FA в один контур входа за 3-4 недели

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Семь паролей на сотрудника превращаются в стикеры на мониторах, забытые блокировки при увольнении и поток заявок «сбросьте пароль». Мы решаем это единым контуром аутентификации: один каталог (AD/LDAP), брокер Keycloak для SAML/OIDC-сервисов, Kerberos для 1С и RADIUS для Wi-Fi. Отключение одной учётки закрывает доступ ко всему; вход и аудит — из одной точки.

Почему это важно бизнесу

- При увольнении блокируем одну учётку в AD — доступ ко всем 6-10 сервисам исчезает мгновенно, без забытых активных аккаунтов и утечки базы
- Заявки «забыл пароль от 1С/почты/портала» сводятся к одной точке сброса — нагрузка на инженера хелпдеска падает кратно
- Один длинный пароль плюс 2FA вместо семи слабых вариаций: подбор одной учётки больше не открывает сразу все системы
- Единый журнал входов вместо семи разрозненных — отчёт для аудита 152-ФЗ собирается из одной точки за минуты

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

26.6.3

Актуальная версия Keycloak на Quarkus, которую мы ставим брокером SAML/OIDC для облачных и веб-сервисов

по докам keycloak.org

5 мин

Access Token Lifespan по умолчанию: короткий токен ограничивает ущерб при перехвате, оставляем в этом диапазоне

Keycloak 26, Realm Tokens

30 мин

SSO Session Idle: неактивная сессия гасится, повторный вход требует пароля — баланс удобства и риска

Keycloak 26 default

10 ч

SSO Session Max — абсолютный потолок жизни сессии за рабочий день независимо от активности

Keycloak 26 default

10

Порог блокировки учётки по базовому профилю безопасности Microsoft; задаём на уровне AD-политики

MS Security Baseline

JDK 21

Среда исполнения Keycloak 26; на ней собираем оптимизированный образ и поднимаем федерацию LDAP и Kerberos/SPNEGO

по докам keycloak.org

РЕАЛИЗАЦИЯ 1 ИЗ 3

Наведение порядка в каталоге AD и парольной политике

Что настраиваем

Контроллеры домена, все действующие сотрудники, OU и группы безопасности под роли доступа

Как мы это делаем

1. Инвентаризируем учётки: удаляем «мёртвые», заводим действующих, раскладываем по OU и группам безопасности под роли доступа
2. Default Domain Policy: минимум 10-14 символов, история паролей, порог блокировки 10 попыток и сброс счётчика ~10 минут
3. Оставляем Kerberos основным протоколом, отключаем устаревшие NTLMv1/SMBv1, проверяем репликацию через dcdiag и repadmin
4. Готовим служебные учётки и SPN для сервисов, которые будут аутентифицировать пользователей через каталог

РЕЗУЛЬТАТ

Каталог становится единым источником истины: одна учётка на человека, предсказуемая парольная политика и мгновенная блокировка при увольнении. На этот фундамент садятся почта, 1С, Wi-Fi и брокер.

КЛЮЧЕВОЙ НЮАНС

Порог блокировки на уровне AD держим не ниже порога NPS/RADIUS, иначе Wi-Fi-клиент со старым паролем в кэше заблокирует человека раньше, чем сработает штатная защита от перебора.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Keycloak-брокер для облачных и веб-сервисов (SAML/OIDC)

Что настраиваем

ВМ 2 vCPU / 4 GB, Keycloak 26 на Quarkus + PostgreSQL, федерация с AD по LDAP

Как мы это делаем

1. Разворачиваем в продакшен-режиме: kc.sh build --db=postgres, затем start --optimized с заданным hostname и HTTPS/TLS
2. Подключаем User Federation к AD по LDAP, включаем Kerberos/SPNEGO с провайдером Negotiate для прозрачного входа из домена
3. Заводим клиентов: Битрикс24 и вики — по SAML 2.0, самописный портал 1С — по OIDC; для каждого настраиваем mapper атрибутов
4. В Realm→Tokens включаем Revoke Refresh Token и Max Reuse=0, back-channel logout, оставляем короткий Access Token Lifespan

РЕЗУЛЬТАТ

Вошедший в домен попадает в Битрикс24, вики и порталы без повторного ввода пароля; выход и отзыв сессии — из одной консоли. Секреты клиентов хранятся централизованно.

КЛЮЧЕВОЙ НЮАНС

Продакшен-режим Keycloak требует явного hostname и TLS и разделяет build/start — конфиг БД фиксируется на этапе build. Меняете вендора или параметры БД — пересобираете образ, иначе start падает.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Персональный Wi-Fi WPA2-Enterprise и второй фактор

Что настраиваем

NPS/RADIUS на контроллере домена, точки доступа, 2FA для бухгалтерии, руководства и админов

Как мы это делаем

1. Ставим роль NPS, регистрируем в AD, заводим RADIUS-клиентов (точки доступа) и сетевую политику PEAP-MSCHAPv2 для WPA2-Enterprise
2. MaxDenials на NPS задаём примерно вполовину от порога AD, чтобы перебор гасился на RADIUS раньше доменной блокировки
3. 1С переводим на аутентификацию ОС (провайдер Negotiate первым) — пользователь не вводит пароль в 1С вообще
4. 2FA: приложение-аутентификатор всей компании, аппаратные токены — бухгалтерии и руководству, админам обязательно

РЕЗУЛЬТАТ

Каждый подключается к Wi-Fi под своим доменным именем — общих ключей нет, доступ уволенного отзывается той же блокировкой учётки. Критичные системы прикрыты вторым фактором.

КЛЮЧЕВОЙ НЮАНС

Российские сервисы без SAML/OIDC (СБИС, Контур, ФНС) в SSO силой не втягиваем — кладём их в корпоративный менеджер паролей, доступ к которому открывает та же доменная учётка.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

✕ Порог блокировки AD ниже, чем на NPS

Wi-Fi-клиент со старым паролем в кэше перебирает попытки и блокирует человека на уровне домена раньше защиты RADIUS. Держим AD-порог выше NPS MaxDenials.

✕ Keycloak запущен в dev-режиме

Без явного hostname, TLS и связки kc.sh build/start --optimized брокер работает нестабильно и небезопасно. В прод — только оптимизированная сборка с HTTPS.

✕ Смена драйвера БД без пересборки

Конфиг БД фиксируется на этапе build. Поменяли вендора или параметры Postgres и запустили start — сервер падает. Пересобираем образ после любой правки БД.

✕ Мёртвые учётки в каталоге

Если AD не чистили годами, уволенные логинятся локально и остаются в сервисах. Сначала инвентаризация и удаление, потом федерация — иначе тянем мусор во все системы.

✕ SSO без второго фактора

Единый пароль становится единой точкой отказа: утёк — открылось всё. 2FA обязательна минимум для бухгалтерии, руководства и администраторов.

✕ Длинные токены и вечные сессии

Большой Access Token Lifespan и отключённый Revoke Refresh Token дают долгую жизнь украденному токену. Оставляем ~5 мин, включаем отзыв и Max Reuse=0.

✕ Российские сервисы силой в SAML

СБИС, Контур и портал ФНС не поддерживают SAML и OIDC. Попытка «прикрутить» ломает вход; правильно — менеджер паролей под той же доменной учёткой.

✕ NTLM вместо Kerberos для 1С

Браузеры по умолчанию идут в NTLM. Для прозрачного входа в 1С и веб ставим провайдер Negotiate первым и проверяем SPN, иначе OS-аутентификация не срабатывает.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Единый каталог AD: одна учётка на человека, OU и группы под роли доступа
- Парольная политика: 10-14 символов, порог блокировки 10, история паролей
- Windows-аутентификация в 1С и почте — вход без повторного ввода пароля

НОРМАЛЬНО

- Keycloak-брокер на ВМ 2 vCPU/4 GB + PostgreSQL для SAML/OIDC-сервисов
- Wi-Fi WPA2-Enterprise через NPS/RADIUS с персональными учётками
- 2FA-приложение для всей компании, отзыв сессий из одной консоли

ХОРОШО

- Аппаратные токены для бухгалтерии, руководства и админов (обязательно)
- Back-channel logout, Revoke Refresh Token, короткий Access Token Lifespan
- Единый журнал входов и регламент парольной политики под аудит 152-ФЗ

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Удалены ли из AD все «мёртвые» учётки уволенных и заведены ли действующие сотрудники по OU и группам?
- [ ] Задан ли порог блокировки учётки (10 по базовому профилю) и держится ли он выше порога NPS/RADIUS?
- [ ] Запущен ли Keycloak в продакшен-режиме — с hostname, TLS и сборкой kc.sh build/start --optimized?
- [ ] Настроена ли федерация Keycloak с AD по LDAP и Kerberos/SPNEGO с провайдером Negotiate?
- [ ] Включён ли в 1С вход по аутентификации ОС, чтобы пользователь не вводил пароль вручную?
- [ ] Переведён ли корпоративный Wi-Fi на WPA2-Enterprise с персональными учётками через RADIUS?
- [ ] Включена ли 2FA для бухгалтерии, руководства и администраторов, и выданы ли аппаратные токены?
- [ ] Настроены ли отзыв refresh-токена, back-channel logout и короткий Access Token Lifespan?
- [ ] Собирается ли единый журнал входов и отчёт для аудита 152-ФЗ из одной точки?

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).

- Аудит инфраструктуры и каталога AD с письменным планом SSO под ваш набор сервисов и лицензий
- Разворачиваем и настраиваем Keycloak-брокер на ВМ, подключаем Битрикс24, вики и порталы по SAML/OIDC
- Наводим порядок в AD и парольной политике, включаем Windows-аутентификацию в 1С и почте
- Переводим Wi-Fi на WPA2-Enterprise через NPS/RADIUS и подключаем 2FA с аппаратными токенами
- Настраиваем журналы аудита и готовим регламент парольной политики под требования 152-ФЗ

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 — Identity Brokering (SAML/OIDC) (keycloak.org — 26.x)

02 Configuring Keycloak — Production, kc.sh build/start (keycloak.org — 26.x)

03 Server Administration Guide — LDAP/Kerberos User Federation (keycloak.org — 26.x)

04 Realm Settings — Sessions and Token Timeouts (keycloak.org — 26.x)

05 Аутентификация операционной системы (Windows) в 1С:Предприятии (v8.1c.ru — 8.3)

06 Configure remote access client account lockout (NPS) (learn.microsoft.com — 2026)

07 Security baseline — Account lockout threshold (=10) (learn.microsoft.com — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.