Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Authentik или Keycloak: как мы строим SSO для SMB в 2026

Оба IdP изнутри: критерии выбора и наш типовой деплой — AD-синк, OIDC, forward auth, 2FA

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

У клиента на 30–60 РМ обычно 8–14 внутренних сервисов: почта, файлы, CRM, вики, Git, мониторинг, VPN. Без SSO это десятки паролей, ручные блокировки при увольнении (кто-то всегда остаётся с доступом) и ноль аудита входов. Мы сводим всё к одному IdP — authentik или Keycloak: одна учётка из AD, централизованный 2FA, а блокировка в домене гасит доступ везде за минуту.

Почему это важно бизнесу

- Уволенный сотрудник с живым паролем к CRM или файлам — прямой риск утечки клиентской базы и претензий по 152-ФЗ
- Сброс забытых паролей по 12 сервисам съедает часы админа и простои сотрудников каждую неделю
- Один слабый пароль без 2FA открывает сразу почту, CRM и файлы — фишинг окупается с первой попытки
- Аудит входов в одном месте: кто, откуда и когда входил — без этого разбор инцидента невозможен

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

26.7

Актуальная ветка Keycloak (Quarkus): SCIM API и multi-cluster HA без внешнего Infinispan — обе...

keycloak.org, июль 2026

2026.5

Ветка authentik: server+worker в Docker, PostgreSQL 14+, Redis не нужен с 2025.10; релиз раз в...

docs.goauthentik.io

2–4 ГБ

RAM под IdP: authentik стартует на 2 ГБ (минимум по requirements), под Keycloak (JVM) закладыв...

docs.goauthentik.io + наш sizing

10 ч

Единый таймаут: SSO Session Idle и сессии приложений выравниваем, иначе логауты расходятся

наш стандарт

60 мин

Periodic Changed Users Sync из AD: инкрементальный LDAP-синк, полный (Periodic Full Sync) — ра...

Keycloak User Federation

5 неудач

Наш порог Max Login Failures в Brute Force Detection (дефолт realm — 30) — включаем в каждом r...

Keycloak Realm settings

РЕАЛИЗАЦИЯ 1 ИЗ 3

Разворачиваем authentik: ядро и связка с AD

Что настраиваем

VPS 2 vCPU / 4 ГБ: контейнеры authentik server + worker, PostgreSQL 16 — типовой SMB-контур до 200 PM

Как мы это делаем

1. Официальный docker-compose: server и worker (ghcr.io/goauthentik/server) плюс PostgreSQL 16; Redis не нужен — с 2025.10 очереди и кэш живут в Postgres; AUTHENTIK_SE...
2. LDAP Source к AD: bind под сервисной УЗ с минимальными правами поверх LDAPS, регулярный фоновый синк юзеров и групп; пароли проверяются LDAP-биндом в AD и в authent...
3. Обязательный 2FA в default-authentication-flow: стадия TOTP/WebAuthn с enrollment при первом входе; администраторам — только аппаратный WebAuthn
4. Конфиг как код: Flows, Stages и Policies экспортируем в YAML-blueprints и храним в Git — стенд повторяемо поднимается на чистой VM

РЕЗУЛЬТАТ

Рабочая админка и синк 50+ учёток из AD — в первый день; дальше добавление приложения — это 5–20 минут на OIDC-клиент, а не отдельный проект. Увольнение = блокировка в AD, доступ гаснет во всех сервисах при следующей проверке сессии.

КЛЮЧЕВОЙ НЮАНС

Пароли пользователей не должны реплицироваться в IdP — держим проверку через LDAP-бинд в AD. И сразу решаем, что будет при недоступности DC: вошедших держит кэш сессий, но новые логины встанут.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Подключаем 10+ приложений: OIDC, SAML и forward auth

Что настраиваем

Nextcloud, GitLab, Grafana, Rocket.Chat, Wiki.js по OIDC; Synology/BookStack по SAML2; легаси — через Proxy Outpost

Как мы это делаем

1. На каждое приложение — отдельный OAuth2/OIDC-провайдер: свой client_id/secret, redirect URI точным списком, группы отдаём claim'ом через scope mapping
2. Легаси без OIDC/SAML закрываем Proxy Outpost: forward auth через nginx auth_request или Traefik forwardAuth — SSO поверх приложения без его доработки
3. SAML2 (Synology, BookStack): подписанные assertion, правильный NameID format и NTP на обеих сторонах — 90% проблем SAML это clock skew и сертификаты
4. Доступ по группам: group membership / expression policy на binding приложения — бухгалтерия не видит Grafana, подрядчики видят только трекер

РЕЗУЛЬТАТ

14 сервисов за один логин с 2FA; в портале My applications пользователь видит только своё. Старый Redmine и Portainer живут за forward auth без единой строчки их доработки, а матрица доступа управляется группами AD, а не паролями.

КЛЮЧЕВОЙ НЮАНС

Точное имя claim'а групп и формат redirect URI сверяем с докой конкретного приложения: половина «SSO не работает» — это опечатка в redirect URI или неподхваченный groups-claim.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Когда ставим Keycloak: Kerberos, SPI и рост

Что настраиваем

Keycloak 26.7 (Quarkus) — клиенты с Windows-SSO без пароля, кастомной логикой на Java и планами роста за 200 PM

Как мы это делаем

1. Сборка Quarkus-дистрибутива: kc.sh build --db=postgres, запуск kc.sh start --optimized; за реверс-прокси — --proxy-headers=xforwarded и явный --hostname
2. User Federation → LDAP + Kerberos/SPNEGO: с доменной машины браузерный вход без пароля; SPNEGO есть и в authentik (Kerberos source), но у Keycloak это одна связка с...
3. Realm: Brute Force Detection (блокировка после 5 неудач), SSO Session Idle/Max = 10/24 ч, обязательный OTP шагом в Authentication flow
4. Наблюдаемость: --health-enabled=true --metrics-enabled=true — health и Prometheus-метрики на management-порту 9000, забираем в Zabbix/Grafana

РЕЗУЛЬТАТ

Windows-SSO без пароля для доменных PC, кастомная логика через Java SPI, готовый путь к HA — с 26.7 multi-cluster (preview) без внешнего Infinispan. Инсталляция переживает рост клиента до сотен PM без смены платформы.

КЛЮЧЕВОЙ НЮАНС

Keycloak выпускает минорные релизы раз в квартал (26.5 → 26.7 за полгода) — апгрейдим только через Upgrading Guide и тестовый realm-export/import: «просто поднять новый образ» периодически ломает темы и кастом...

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **IdP стал единой точкой отказа**
  Лёг IdP — лежат все 14 сервисов. Мониторим /health/ready на management-порту 9000 (Keycloak) или /-/health/ready/ (authentik), бэкап с проверкой восс…

- ✕ **Нет break-glass входа мимо SSO**
  В каждом критичном сервисе оставляем локальную админ-УЗ вне SSO с паролем в сейфе — иначе при падении IdP не войти даже чинить

- ✕ **Сессии разъезжаются по сервисам**
  IdP 8 ч, Nextcloud 15, GitLab 24 — пользователя выкидывает вразнобой. Выравниваем SSO Session Idle и таймауты приложений к одному значению

- ✕ **Бэкап только снапшотом VPS**
  Снапшот раз в сутки = потеря дня изменений. Ставим pg_dump ежесуточно + WAL-G непрерывным WAL-архивом в S3 и квартально проверяем restore

- ✕ **Wildcard в redirect URI**
  Звёздочка в Valid redirect URIs позволяет увести код авторизации на чужой хост. Прописываем точные URI на каждый клиент

- ✕ **Синк AD под доменным админом**
  Компрометация IdP отдаёт домен целиком. Bind — сервисная УЗ read-only по LDAPS, права только на нужные OU

- ✕ **Легаси-клиенты не умеют OIDC**
  Старые Outlook и толстый клиент 1С в браузерный OIDC не ходят. Оставляем им пароли приложений/IMAP или прокси-связку nginx auth_request

- ✕ **Апгрейд мимо migration notes**
  Релизы меняют дефолты (hostname, прокси-опции). Читаем Upgrading Guide, катаем на тестовом стенде, потом в прод

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- authentik по официальному docker-compose: 2 vCPU / 4 ГБ, PostgreSQL 16 рядом
- LDAP-синк из AD, OIDC на 3–5 ключевых сервисов, точные redirect URI
- Обязательный TOTP для всех, ежесуточный pg_dump базы IdP

НОРМАЛЬНО

- Выбор по задаче: authentik до ~200 PM; Keycloak — Java SPI, Kerberos в одной LDAP-фе…
- Forward auth (Proxy Outpost) для легаси, доступ к приложениям по группам AD
- WAL-G в S3, алерт на health-эндпоинт, break-glass админ вне SSO
- Blueprints / realm-export в Git — конфигурация как код

ХОРОШО

- WebAuthn/passkey вместо TOTP минимум для админов и бухгалтерии
- Выделенная PostgreSQL с репликой; для Keycloak — 2 ноды за HAProxy
- Регламент апгрейдов: тестовый стенд, release notes, окно раз в квартал
- Проверка восстановления IdP из бэкапа на чистой VM раз в квартал

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Все сервисы с поддержкой OIDC/SAML заведены через IdP, а не по локальным паролям?
- [ ] Блокировка учётки в AD реально закрывает доступ во все сервисы — проверяли на живом тесте?
- [ ] 2FA обязателен для всех, у админов — аппаратный WebAuthn-ключ?
- [ ] Есть break-glass доступ к каждому критичному сервису на случай падения IdP?
- [ ] Таймауты сессий выровнены между IdP и всеми приложениями?
- [ ] Redirect URI в каждом OIDC-клиенте прописаны точно, без wildcard?
- [ ] База IdP бэкапится (pg_dump + WAL-архив) и восстановление проверялось?
- [ ] Мониторинг health-эндпоинта IdP с алертом дежурному заведён?
- [ ] Синк с AD идёт по LDAPS под ограниченной сервисной УЗ, а не под админом домена?
- [ ] План апгрейдов IdP есть, migration notes читаются до обновления, а не после?

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).

- Бесплатный аудит: какие из ваших сервисов умеют OIDC/SAML, что закроем forward auth, что оставить вне SSO
- Внедрение под ключ за 3–4 дня: IdP, AD-синк, обязательный 2FA, 10+ приложений, обучение сотрудников
- Бэкап и мониторинг IdP: pg_dump + WAL-G в S3, алерты на health, break-glass регламент
- Абонентка: подключение новых приложений, апгрейды после теста, разбор инцидентов входа

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 Keycloak Server Guides: database, reverse proxy, health/metrics (keycloak.org — 26.7)

02 Keycloak Server Administration: User Federation, Sessions, Brute Force (keycloak.org — 26.7)

03 authentik Docs: Docker Compose installation, Requirements, Configuration (docs.goauthentik.io — 2026.5)

04 authentik Docs: Providers OAuth2/SAML, Proxy Outpost (forward auth), Kerbe… (docs.goauthentik.io — 2026.5)

05 authentik Docs: Flows, Stages, Blueprints (docs.goauthentik.io — 2026.5)

06 Наш шаблон деплоя IdP: docker-compose + WAL-G + Zabbix-мониторинг (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.