Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

FreeIPA: единая учётка для парка Linux-серверов офиса

Как мы централизуем вход, sudo/HBAC и 2FA на 389-DS, MIT Kerberos и Dogtag CA

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

В офисе с 5+ Linux-серверами доступы расползаются: на каждом узле свои локальные учётки, SSH-ключи и пароли в passwords.txt на рабочем столе. Уволенный сотрудник месяцами сохраняет вход, онбординг превращается в ручной обход всех серверов, а на вопрос «кто заходил на 1С» ответа нет. Это прямая брешь в безопасности и неуправляемый доступ к данным компании.

Почему это важно бизнесу

- Учётка уволенного живёт на каждом сервере, где он был: забытый SSH-ключ — готовый канал утечки клиентской базы к конкурентам
- Пароли и ключи в passwords.txt на рабочем столе админа — одна украденная копия открывает весь парк серверов сразу
- Онбординг и офбординг вручную по каждому узлу: часы работы админа и человеческие ошибки при каждом изменении доступа
- Нет журнала входов — при инциденте или проверке невозможно показать, кто и когда заходил на критичные серверы

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

4.13

Актуальная серия FreeIPA (Modern WebUI, DNS over TLS); на проде держим security-ветку 4.12.5

по докам freeipa.org

300 с

Порог clockskew Kerberos: расхождение времени клиент↔KDC, сверх которого билет не выдаётся

MIT krb5, libdefaults

7 дн

Срок офлайн-кеша SSSD, который задаём явно; дефолт 0 = вечно (уволенный войдёт всегда)

по докам SSSD, sssd.conf

60

Максимум серверов-реплик в одном домене IdM; офису хватает мастер + реплика

по докам Red Hat IdM

4 ГБ

RAM на узел под ~10 000 юзеров и 100 групп + 4 ГБ swap — базовый сайзинг VM

Red Hat IdM, hardware

РЕАЛИЗАЦИЯ 1 ИЗ 3

Ядро: мастер + реплика на 389-DS, KDC и Dogtag CA

Что настраиваем

Две VM (2 vCPU/4 ГБ) на разных гипервизорах: LDAP-каталог, KDC, Dogtag CA и интегрированный DNS

Как мы это делаем

1. chrony на всех узлах ДО установки: без единого времени KDC не выдаст билет (порог clockskew 300 с)
2. FQDN нижним регистром (ipa1.corp.example.ru), затем ipa-server-install с --setup-dns и --setup-ca
3. ipa-replica-install на втором гипервизоре; топологию проверяем ipa topologysegment-find domain
4. DNS-зону офиса переносим на встроенный BIND + bind-dyndb-ldap: авторитативный DNS и SRV-автодискавери
5. ipa-backup по cron ночью + снапшоты VM; копию храним на NAS отдельно от мастера

РЕЗУЛЬТАТ

Отказ мастера не роняет вход: реплика автоматически подхватывает LDAP, Kerberos и DNS, пользователи не замечают простоя. Единый каталог учёток вместо десятков локальных /etc/passwd на каждом сервере.

КЛЮЧЕВОЙ НЮАНС

Мастер IdM критичен как AD и DNS: реплику закладываем сразу и проводим учения failover; SRV-записи в DNS должны указывать на оба сервера.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Клиенты: SSSD на каждом сервере и офлайн-кеш

Что настраиваем

12 серверов (1С, PostgreSQL, GitLab, веб, бэкап, Zabbix, Docker), заводим через ipa-client-install

Как мы это делаем

1. ipa-client-install одной командой настраивает SSSD, PAM, NSS и krb5.conf, вводит хост в домен
2. id_provider=ipa, cache_credentials=true — SSSD кеширует учётки для офлайн-входа при недоступности KDC
3. offline_credentials_expiration=7: осознанно ограничиваем кеш 7 днями (дефолт 0 = вечно)
4. krb5_store_password_if_offline=true — пароль сохраняется до восстановления связи с KDC
5. Проверяем id ivanov и getent passwd — NSS видит доменного пользователя

РЕЗУЛЬТАТ

Пользователь заходит ssh ivanov@bd1.local своей корпоративной учёткой на любой из 12 серверов; при недоступности мастера вход продолжается из локального кеша SSSD без простоя.

КЛЮЧЕВОЙ НЮАНС

Дефолт offline_credentials_expiration=0 (вечно) — риск: уволенный логинится из кеша бесконечно. Явно задаём срок и чистим кеш через sss_cache при блокировке.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Права и 2FA: sudo, HBAC и TOTP-токены

Что настраиваем

Разграничение по ролям: root у 2 инженеров, подрядчик — только веб-серверы, 2FA на 1С/GitLab/бэкап

Как мы это делаем

1. Отключаем дефолтное правило allow_all (ipa hbacrule-disable allow_all) — иначе HBAC не ограничивает
2. HBAC: ipa hbacrule-add + hbacrule-add-host/user — подрядчик видит только 2 веб-сервера, на 1С Permission denied
3. sudo: ipa sudorule-add с --cmdcat и привязкой команд — бухгалтеру только скрипты обновления 1С
4. 2FA: ipa otptoken-add (TOTP, RFC 6238), FreeOTP на смартфоне для базы 1С, GitLab и бэкапа
5. Офбординг: ipa user-disable petrov — доступ пропадает во всей инфраструктуре за минуту

РЕЗУЛЬТАТ

Доступ соответствует роли, а не памяти админа. Увольнение = одна команда вместо обхода 12 серверов; критичные узлы прикрыты вторым фактором через FreeOTP.

КЛЮЧЕВОЙ НЮАНС

FreeIPA после установки создаёт правило allow_all — пока оно включено, все ходят везде. Первым делом отключаем и строим явные HBAC по ролям.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Hostname не FQDN или в верхнем регистре**
  IPA требует FQDN нижним регистром без подчёркиваний; IPA-Server01 роняет установку на проверке имени. Задаём ipa1.corp.example.ru заранее.

- ✕ **Рассинхрон времени ломает Kerberos**
  При расхождении > 300 с KDC не выдаёт билет. Ставим chrony на всех узлах ДО ipa-client-install и проверяем chronyc sources.

- ✕ **SELinux отключают вместо permissive**
  Отключённый SELinux потом не включают. На отладку переводим в permissive, собираем политику через audit2allow, возвращаем enforcing.

- ✕ **Забыли отключить HBAC allow_all**
  Стартовое правило allow_all пускает всех везде — HBAC не работает. Отключаем его сразу, иначе разграничение доступа только мнимое.

- ✕ **Нет реплики — единая точка отказа**
  Падение единственного мастера останавливает новые входы на всех серверах. Ставим реплику на другом гипервизоре и проверяем failover.

- ✕ **Офлайн-кеш SSSD живёт вечно**
  Дефолт offline_credentials_expiration=0 — уволенный логинится из кеша без ограничений. Задаём срок и чистим sss_cache при блокировке.

- ✕ **Нет бэкапа каталога IdM**
  Потеря мастера без ipa-backup = ручное пересоздание всех учёток и политик. Настраиваем ipa-backup по cron + снапшоты VM на отдельный NAS.

- ✕ **CA-сертификаты забывают контролировать**
  Внутренний Dogtag CA перевыпускает сертификаты сам, но при сбое certmonger вход по TLS падает. Мониторим getcert list и свежесть CA.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Один мастер FreeIPA (389-DS + KDC + CA), FQDN и chrony на всех узлах
- ipa-client на всех серверах, SSSD-кеш для офлайн-входа
- Отключён allow_all, базовые HBAC по ролям, ipa-backup по cron

НОРМАЛЬНО

- Мастер + реплика на разных гипервизорах, встроенный DNS с SRV
- sudo-правила и HBAC под каждую роль, offline_credentials_expiration=7
- 2FA (TOTP/FreeOTP) на 1С, GitLab и бэкап-сервер

ХОРОШО

- Учения failover раз в полгода, мониторинг репликации в Zabbix
- Ежемесячный аудит неактивных учёток, автоблок по офбордингу от HR
- Trust с AD для смешанного парка, DNS over TLS (FreeIPA 4.13)

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] На всех узлах настроен chrony и расхождение времени < 300 с до установки клиента?
- [ ] Hostname — FQDN нижним регистром без подчёркиваний и заглавных?
- [ ] Развёрнута реплика на отдельном гипервизоре и проверён failover?
- [ ] Отключено дефолтное правило HBAC allow_all?
- [ ] Заданы sudo-правила и HBAC под каждую роль, полный root ограничен?
- [ ] Включена 2FA (TOTP) на критичных серверах: база, репозиторий, бэкап?
- [ ] offline_credentials_expiration задан явно, а не оставлен 0 (вечно)?
- [ ] ipa-backup идёт по cron и копируется на отдельный NAS?
- [ ] SELinux в enforcing, политики собраны через audit2allow, не отключён?
- [ ] Есть регламент офбординга: ipa user-disable по заявке HR за минуту?

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 Linux-парка: инвентаризация учёток, поиск забытых доступов уволенных, письменное заключение со сметой
- Разворачиваем мастер + реплику FreeIPA, переносим DNS-зону, подключаем серверы через ipa-client
- Настраиваем sudo, HBAC по ролям и 2FA (FreeOTP) на критичные узлы
- Абонентка: заведение/блокировка по заявкам HR, аудит учёток, failover-учения, security-патчи
- Trust FreeIPA↔AD для смешанного парка Windows + Linux

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 FreeIPA 4.13 Release Notes и Downloads (freeipa.org — 4.13)

02 Tuning performance in IdM — Hardware recommendations (docs.redhat.com — RHEL 9)

03 Planning IdM — Planning the replica topology (docs.redhat.com — RHEL 9)

04 sssd.conf(5): cache_credentials, offline_credentials_expiration (sssd.io — SSSD)

05 MIT Kerberos krb5.conf — libdefaults, clockskew (web.mit.edu — krb5)

06 FreeIPA Workshop — HBAC и Sudo rule management (freeipa.readthedocs.io — 4.11)

Основано на официальной документации продуктов и нашей практике внедрения.