



Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Корпоративный мессенджер вместо Telegram: наш разбор

Self-hosted Mattermost: AD-синхронизация, сроки хранения,
выгрузка и свой push

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

Суть проблемы

Рабочая переписка компании до 50 мест живёт в личных Telegram-аккаунтах: история, договорённости и сканы документов принадлежат физлицу, а не юрлицу, и уходят вместе с сотрудником. Мы переносим коммуникацию на свой сервер Mattermost: учётные записи из Active Directory, свои сроки хранения, выгрузка переписки за период и бэкап в общем контуре резервного копирования.

Почему это важно бизнесу

- Уход сотрудника не уносит историю: учётка деактивируется из AD, каналы и файлы остаются у компании
- Персональные данные и сканы лежат на сервере организации, а не в чужом облаке вне юрисдикции РФ
- Онбординг менеджера ускоряется: он получает доступ к архиву каналов клиента с первого дня
- Блокировка внешнего сервиса или потеря телефона не останавливает внутреннюю коммуникацию
- Выгрузка переписки за период готовится штатным заданием, а не собирается скриншотами

Ключевые параметры реализации

v11.7 ESR

Ветка с продлённой поддержкой: жизненный цикл v10.11 ESR закрыт 15.08.2026, ставим v11.7+

докум. Mattermost

PG 14+

PostgreSQL 14.x — минимум с ESR v11.7; MySQL с v11 не развивается, новые стенды только на PG

докум. Mattermost

2 GB/1 vCPU

Профиль сервера приложения до 1000 пользователей; на 50 мест берём запас 4 GB / 2 vCPU

докум. Mattermost

60 мин

LdapSettings.SyncIntervalMinutes по умолчанию; в офисе до 50 мест ставим 15 минут

наш стандарт ITfresh

100 МБ

FileSettings.MaxFileSize по умолчанию (104857600 байт); режим до 52428800 и правим nginx

докум. Mattermost

50 / 100

SqlSettings.MaxIdleConns / MaxOpenConns по умолчанию — сверяем с max_connections в PostgreSQL

докум. Mattermost



Базовый стенд: сервер, БД, обратный прокси, файлы

Что настраиваем

Одна Linux-VM (Ubuntu LTS) в контуре клиента или на нашей площадке: Mattermost Server + PostgreSQL

Как мы это делаем

- 1 PostgreSQL 14+: отдельная роль mmuser и БД mattermost, `SqlSettings.DriverName=postgres`, `DataSource` с `sslmode` и `binary_parameters=yes`
- 2 Ставим mattermost-server из tar.gz в `/opt/mattermost`, отдельный системный пользователь mattermost, юнит mattermost.service
- 3 nginx как reverse proxy: TLS, `proxy_set_header Upgrade $http_upgrade` и `Connection "upgrade"`, `client_max_body_size` и `proxy_read_timeout` под вложения
- 4 `ServiceSettings.SiteURL` — внешний FQDN строго по https: по нему строятся ссылки в письмах, OAuth-редиректы и запросы мобильных клиентов
- 5 Файлы: `FileSettings.DriverName=local` на отдельный том либо amazons3 на MinIO; смена драйвера — только с рестартом сервиса

РЕЗУЛЬТАТ

Получаем управляемую точку хранения рабочей переписки: данные в PostgreSQL и на дисках клиента, бэкап входит в общий контур резервного копирования, обновление ветки — заменой бинарников с миграцией схемы при старте сервиса.

КЛЮЧЕВОЙ НЮАНС

`SqlSettings` и смена `FileSettings.DriverName` применяются только при рестарте; `MaxFileSize` подхватывается на лету, но лимит nginx `client_max_body_size` поднимается отдельно и требует reload.



Учётные записи: AD/LDAP, группы и отзыв доступа

Что настраиваем

Контроллер домена + Mattermost: единый источник правды по людям; AD/LDAP-синхронизация — лицензируемая функция

Как мы это делаем

- 1 BaseDN на OU сотрудников, UserFilter отсекает служебные и отключённые учётки:
(!(userAccountControl:1.2.840.113556.1.4.803:=2))
- 2 Маппинг: IdAttribute=objectGUID (неизменяемый), LoginIdAttribute=sAMAccountName, Email/FirstName/LastName берём из AD
- 3 SyncIntervalMinutes=15: отключённая в AD учётка деактивируется, активные сессии отзываются; срочно — кнопка AD/LDAP Synchronize Now
- 4 Каналы отделов собираем из групп AD (group sync): состав чатов меняется вместе с кадровыми приказами, а не руками админа
- 5 Тест увольнения на стенде: disable в AD, цикл синхронизации, проверка отказа входа, отзыва сессии и сохранности истории в каналах

РЕЗУЛЬТАТ

Отключение сотрудника в домене закрывает ему мессенджер в пределах одного цикла синхронизации, сообщения и файлы остаются в каналах компании. Исчезает ручной чек-лист «выгнать из чатов» и риск, что кто-то останется в группе после ухода.

КЛЮЧЕВОЙ НЮАНС

Привязка к неизменяемому objectGUID критична: маппинг на email или логин ломается при переименовании сотрудника и плодит вторые учётки без истории.



Хранение, выгрузка, поиск и мобильные уведомления

Что настраиваем

Сроки хранения, compliance-выгрузка и push-контур; retention и export доступны на Enterprise-планах

Как мы это делаем

- 1 DataRetentionSettings: MessageRetentionHours и FileRetentionHours задаём отдельно, удаление физическое и необратимое
- 2 Срок хранения фиксируем письменно до включения политики: ночное задание чистит и записи в БД, и файлы на диске
- 3 Compliance export в формате CSV (есть также Actiance XML и Global Relay EML); батчи пишутся в подкаталог exports файлового хранилища
- 4 Push на телефоны: подписка на HPNS либо свой mattermost-push-proxu с ключами APNs/FCM и пересборкой мобильных клиентов
- 5 Поиск по русскому тексту на объёме от года переводим на Elasticsearch 8/9 или OpenSearch 2/3 вместо поиска средствами БД

РЕЗУЛЬТАТ

Компания получает предсказуемую глубину архива, штатный механизм выгрузки переписки за период, рабочий поиск по русской морфологии и уведомления на телефонах без завязки на внешний облачный сервис.

КЛЮЧЕВОЙ НЮАНС

Свой push-прокси требует собственных сертификатов APNs, ключа FCM и пересборки с подписью мобильных приложений — это проектная работа, а не галочка в системной консоли.



Подводные камни

✗ SiteURL пустой или на http

По ServiceSettings.SiteURL строятся ссылки в письмах, OAuth-редиректы и запросы клиентов. Внешний https-FQDN задаём до подключения пользователей.

✗ Прокси без WebSocket

Без заголовков Upgrade и Connection клиент уходит в long-poll: сообщения идут с задержкой. Правим location в nginx, проверяем ws:// в devtools.

✗ MySQL под новый стенд

MySQL с v11 не развивается, дальше v10.11 нужна миграция на PostgreSQL. Все новые внедрения ставим сразу на PostgreSQL 14 и новее.

✗ Ретенция без регламента и лицензии

DataRetentionSettings и compliance export есть на Enterprise-планах. Сначала письменный срок хранения и проверка редакции, потом включение политики.

✗ Каталог data на системном диске

Вложения растут быстрее ожиданий и забивают корень, сервис встаёт. Выносим data на отдельный том или в S3-совместимое хранилище с алертом по месту.

✗ Бэкап без согласованной пары

Дамп PostgreSQL без снимка каталога data даёт битые вложения. Снимаем БД и файлы одним окном, раз в квартал проверяем восстановление на стенде.

✗ Локальные учётки вместо AD

Ручные аккаунты переживают увольнение. Включаем LDAP-синхронизацию и отключаем самостоятельную регистрацию: EnableSignUpWithEmail=false.

✗ Подрядчики в общих каналах

Внешние участники видят лишнее. Заводим их гостевыми учётками в отдельной команде и приватных каналах, состав ревизуем на каждой синхронизации.



Как правильно

МИНИМУМ

- Mattermost Server v11.7 ESR и новее на PostgreSQL 14+, TLS завершает nginx
- ServiceSettings.SiteURL по https и рабочий WebSocket на десктопе и телефоне
- Ежедневный бэкап БД и каталога data, ежеквартальная проверка восстановления
- Учётки из AD/LDAP, регистрация по email отключена: EnableSignUpWithEmail=false

НОРМАЛЬНО

- SyncIntervalMinutes=15: деактивация в AD отзывает сессии в том же цикле
- Каналы отделов из групп AD, приватные каналы под проекты и подрядчиков
- Файлы на отдельном томе или MinIO, MaxFileSize согласован с лимитом nginx
- Метрики Prometheus и Grafana: размер БД, место под data, ошибки входа

ХОРОШО

- DataRetentionSettings: сроки по сообщениям и файлам под регламент компании
- Compliance export в CSV с проверкой полноты батчей в каталоге exports
- Мобильный push: подписка HPNS либо свой mattermost-push-proxy в контуре
- Поиск на OpenSearch или Elasticsearch, интеграции ботами и вебхуками из 1C



Чек-лист самопроверки

- | | |
|---|---|
| ☐ Задан ли ServiceSettings.SiteURL внешним https-адресом и совпадает ли он с именем в сертификате? | ☐ Согласован ли срок хранения и внесён ли он в MessageRetentionHours и FileRetentionHours? |
| ☐ Работает ли WebSocket через обратный прокси на десктопном и мобильном клиенте? | ☐ Лежит ли каталог data на отдельном томе и есть ли алерт по свободному месту? |
| ☐ Стоит ли под сервером PostgreSQL 14 или новее, а версия сервера — v11.7 ESR и выше? | ☐ Восстанавливали ли за последний квартал пару «дамп БД + каталог data» на стенде? |
| ☐ Заведены ли пользователи из AD/LDAP с маппингом IdAttribute на objectGUID? | ☐ Настроены ли мобильные уведомления и известно ли, через какой push-контур они идут? |
| ☐ Проверено ли, что disable учётки в AD блокирует вход и отзывает активные сессии? | ☐ Есть ли регламент выгрузки переписки за период по запросу руководителя или юриста? |

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



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 self-hosted Mattermost под ключ: сервер, PostgreSQL, TLS, файловое хранилище, бэкап
- Подключаем AD/LDAP, строим каналы по группам домена и отработываем сценарий увольнения
- Настраиваем сроки хранения и выгрузку переписки за период под регламент компании
- Поднимаем мобильные уведомления и десктоп-клиенты, переводим сотрудников с Telegram
- Берём на сопровождение: мониторинг, обновления ветки ESR, проверки восстановления

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



Техническая база

- 01** Software and hardware requirements (docs.mattermost.com — v11)
- 02** Environment configuration settings (config.json) (docs.mattermost.com — v11)
- 03** Database configuration settings (SqlSettings) (docs.mattermost.com — v11)
- 04** AD/LDAP setup and synchronization (docs.mattermost.com — v11)
- 05** Data retention policy (docs.mattermost.com — v11)
- 06** Compliance export (docs.mattermost.com — v11)
- 07** Host your own push proxy service (docs.mattermost.com — v11)
- 08** Чек-лист внедрения корпоративного мессенджера ITfresh (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.

