



Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Уходим с Exchange на Postfix + Dovecot без потери писем

Регламент ITfresh: imapsync 2.314, doveadm sync -1, LMTP, DKIM/DMARC, SOGo вместо EAS

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

Суть проблемы

Exchange 2016 и 2019 вышли из поддержки 14.10.2025: обновлений безопасности нет, а преемник Exchange SE лицензируется по схеме server+CAL с обязательной Software Assurance, которую в РФ не оплатить. У клиента остаётся почтовый сервер на периметре: 30-150 ящиков, общие календари, публичные папки, Outlook на всех столах. Переносим контур на Postfix 3.11 и Dovecot 2.4 без простоя.

Почему это важно бизнесу

- Сервер без обновлений на периметре — прямой путь к шифровальщику: почта смотрит в интернет и держит весь архив переписки.
- Вендорской поддержки нет: сбой базы Exchange чиним своими силами, без гарантии, что store вообще смонтируется обратно.
- Лицензии CAL и Software Assurance под Exchange SE в РФ не оплачиваются — почтовый контур становится юридически непродлеваемым.
- Простой почты в бухгалтерии и юротделе останавливает ЭДО, банк-клиент и переписку с судами: счёт идёт на часы, а не на дни.
- Exchange требует Windows Server, AD и запаса дисков под ESE-базы и индексы; Postfix с Dovecot на 50 ящиков живут на 4 vCPU и 8 ГБ.



Ключевые параметры реализации

14.10.2025

Дата окончания поддержки Exchange 2016 и 2019: обновлений безопасности больше нет

learn.microsoft.com, Exchange EOS

3.11.6

Stable-ветка Postfix, на которой собираем новые узлы; 3.10.x держим как legacy

postfix.org, релиз 10.08.2026

2.4.4

Актуальный релиз Dovecot CE для новых узлов; на 2.3.21.1 идут только security-фиксы

doc.dovecot.org, релиз 12.05.2026

2.314

Версия imapsync, которой снимаем ящики с Exchange по IMAP4 через админ-прокси-логин

imapsync.lamiral.info, релиз 09.2025

2 msg/s

Наш потолок --maxmessagespersecond, чтобы не словить ThrottlingPolicy Exchange

imapsync FAQ.Exchange + наш стандарт

300 с

TTL на MX и A опускаем за сутки до переключения, после стабилизации возвращаем 3600

наш регламент переключения MX



Параллельный контур: поднимаем узел рядом с живым Exchange

Что настраиваем

Офис 40–60 ящиков, Exchange 2016 на Windows Server 2016, домен AD, Outlook 2019 у всех, общий календарь отдела

Как мы это делаем

- 1 Снимаем инвентарь: список ящиков и объём каждого, алиасы, группы рассылки, публичные папки, правила пересылки и внешние коннекторы.
- 2 Ставим узел: Postfix 3.11 и Dovecot 2.4, `virtual_transport = lmtp:unix:private/dovecot-lmtp`, `mail_driver = maildir`, `mail_path` в `/var/vmail`, SQL-мапы.
- 3 Поднимаем `message_size_limit` до фактического лимита Exchange: дефолтные 10240000 байт режут вложения, которые раньше проходили.
- 4 Включаем `MSExchangeIMAP4` и `MSExchangeIMAP4BE`, заводим сервисную учётку с Full Access (встроенному Administrator IMAP закрыт), гоняем `imapsync --dry`.
- 5 Ночной прогон: `imapsync --exchange1 --automap --maxmessagespersecond 2`, логин вида `domain\admin\ящик`, четыре потока по спискам из `users.csv`.

РЕЗУЛЬТАТ

Утром пользователь открывает привычный Outlook по IMAP и SMTP с теми же папками, флагами и датами писем. Простой ограничен временем распространения MX: при TTL 300 это минуты, а всё, что успело упасть на старый сервер, забирает финальная дельта через `doveadm sync -1`.

КЛЮЧЕВОЙ НЮАНС

Не переключаем MX, пока `imapsync` на контрольном ящике не покажет нулевую дельту по числу писем и по байтам. Любое расхождение означает, что папка не смапилась через `--automap`.



Календари, общие ящики и телефоны после отказа от Exchange

Что настраиваем

Стенды, где Exchange держал не только почту: календарь отдела, ресурсы-переговорки, общий ящик продаж и телефоны через ActiveSync

Как мы это делаем

- 1 Ставим SOGo поверх Dovecot: веб-почта, CalDAV и CardDAV плюс собственная реализация EAS, поэтому телефоны ходят привычным протоколом.
- 2 Публичные папки Exchange выгружаем в отдельные ящики и публикуем через shared namespace Dovecot с плагином acl, права выдаём на группу.
- 3 Календари и контакты экспортируем в ICS и vCard, заливаем в SOGo, переговорки пересобираем как ресурсы с автоматическим принятием.
- 4 Outlook на столах — IMAP/SMTP плюс CalDav Synchronizer к CalDAV SOGo: EAS десктопный Outlook к стороннему серверу не поддерживает с 2016.
- 5 iPhone и Android заводим в SOGo нативным EAS-профилем: почта, календарь и контакты в одной учётной записи, переустановка профиля не нужна.

РЕЗУЛЬТАТ

Групповой функционал не теряется при отказе от Exchange: свободен/занят, общие ящики и приглашения на встречи работают, телефоны остаются на одном профиле. Это снимает главное возражение клиента — «а календари мы куда денем».

КЛЮЧЕВОЙ НЮАНС

EAS в SOGo не эквивалент Exchange по делегированию: отправку «от имени» и правила уровня организации переносим на ACL Dovecot и на sieve, а не на клиентские надстройки.



Репутация нового IP: чтобы домен не уехал в спам

Что настраиваем

Любая миграция, где домен годами отправлял с IP Exchange, а новый узел стартует с нулевой репутацией у Gmail и mail.ru

Как мы это делаем

- 1 До переключения: PTR у провайдера на mail.<домен>, ключ DKIM 2048 бит новым селектором, старый селектор из DNS не убираем ещё месяц.
- 2 SPF расширяем сразу на оба выхода, DMARC поднимаем степенями `p=none` → `quarantine` → `reject` по отчётам rua, не быстрее двух недель.
- 3 Rspamd 4.1: классификатор bayes с autolearn (`spam_threshold 6.0`, `ham_threshold -0.5`), обучение из папки Спам через `imapsieve` и `sieve_pipe_bin_dir`.
- 4 Порты: `postscreen` на 25, `submission 587` с `smtpd_tls_security_level = encrypt`, `submissions 465` через `smtpd_tls_wrappermode = yes`, `managesieve 4190`.

РЕЗУЛЬТАТ

В первые сутки после смены MX домен не проваливается в спам: подпись валидна с обоих селекторов, SPF покрывает старый и новый выход, а rua-отчёты сразу показывают, кто ещё отправляет от имени домена. Байес Rspamd за две недели набирается на реальном потоке.

КЛЮЧЕВОЙ НЮАНС

Единственный по-настоящему необратимый шаг — DMARC `p=reject`. Ставим его только после того, как отчёты rua неделю подряд дают 100% pass по SPF и DKIM с обоих адресов.



Подводные камни

✗ Релей-политика не в том параметре

С Postfix 2.10 она живёт в `smtpd_relay_restrictions`. Оставив `reject_unauth_destination` только в `recipient_restrictions`, легко открыть релей.

✗ Забытый PTR и чужой HELO

Без обратной зоны на `mail.<домен>` и при HELO, не совпадающем с PTR, Gmail и mail.ru кладут письма в спам независимо от SPF и DKIM.

✗ Финальная дельта через `doveadm backup`

`backup` — односторонняя заливка, она откатывает изменения на приёмнике. Для добора последних писем нужен `doveadm sync -1`.

✗ IMAP4 на Exchange выключен

Службы `MSExchangeIMAP4` и `MSExchangeIMAP4BE` по умолчанию остановлены, а встроенному Administrator доступ по IMAP закрыт политикой.

✗ ThrottlingPolicy рвёт прогон

Exchange режет массовое чтение по IMAP. Держим `--maxmessagespersecond 2`, `--maxbytespersecond` и не более четырёх процессов `imapsync`.

✗ Конфиг 2.3 залит в Dovecot 2.4

В 2.4 обязательны `dovecot_config_version` и `dovecot_storage_version`, а `mail_location` распался на `mail_driver` и `mail_path` — старый файл не стартует.

✗ Вложения режет `message_size_limit`

У Postfix по умолчанию 10240000 байт, у Exchange лимит обычно выше. Не подняв его, получаем отбивки на письмах, которые раньше ходили.

✗ Квота отдаётся отбивкой

Без сервиса `quota-status` письмо в переполненный ящик принимается и отбивается своим bounce. Подключаем `check_policy_service` на этапе RCPT.



Как правильно

МИНИМУМ

- Postfix + Dovecot, maildir, LMTP, TLS от Let's Encrypt, ночной дамп в Borg
- SPF, DKIM 2048 бит, DMARC p=none и PTR на mail.<домен> у провайдера
- Rspamd с базовыми правилами и обучением из папки Спам через imapsieve
- Старый Exchange держим read-only семь суток как страховку отката

НОРМАЛЬНО

- SQL-мапы доменов и ящиков, quota-status в Postfix, postscreen на 25 порту
- SOGo: веб-почта, CalDAV и CardDAV, EAS для телефонов вместо Exchange
- DMARC quarantine с приёмом rua-отчётов и разбором раз в неделю
- Zabbix: очередь Postfix, срок TLS-сертификата, заполнение раздела vmail

ХОРОШО

- Второй узел с doveadm sync и резервный приём по MX 20
- DANE: smtp_tls_security_level = dane и smtp_dns_support_level = dnssec
- MTA-STS и TLS-RPT на домене, DMARC p=reject по чистым отчётам
- Borg на отдельную площадку плюс горячая реплика maildir



Чек-лист самопроверки

- | | |
|---|---|
| ☐ Снят инвентарь: число ящиков и объём, алиасы, группы рассылки, публичные папки, внешние коннекторы | ☐ <code>virtual_transport = lmtp:unix:private/dovecot-lmtp</code> , доставка проверена тестовым письмом |
| ☐ На Exchange запущены MExchangeIMAP4 и MExchangeIMAP4BE, заведена сервисная учётка с Full Access | ☐ Релей закрыт: <code>smtpd_relay_restrictions</code> выставлен, внешняя проверка <code>open relay</code> отрицательна |
| ☐ <code>imapsync --dry</code> прошёл на трёх тестовых ящиках без ошибок маппинга папок | ☐ Финальная дельта снята через <code>doveadm sync -1</code> или повторный <code>imapsync</code> с нулевым остатком |
| ☐ PTR у провайдера настроен, DKIM-селектор опубликован, SPF покрывает старый и новый IP | ☐ Квоты и <code>message_size_limit</code> выставлены, <code>quota-status</code> отвечает Postfix на этапе RCPT TO |
| ☐ TTL на MX и A снижен до 300 секунд минимум за 24 часа до переключения | ☐ Exchange переведён в <code>read-only</code> , бэкап баз снят и хранится отдельно от нового узла |

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).

- Считаем миграцию по фактическому инвентарю Exchange, а не по числу сотрудников в штатке
- Разворачиваем параллельный узел Postfix + Dovecot + Rspamd + SOGo и отдаём на тест до смены MX
- Гоняем imapsync ночью с контролем дельты по каждому ящику и держим окно отката семь суток
- Настраиваем PTR, SPF, DKIM и DMARC, доводим домен до p=reject по реальным rua-отчётам
- Берём почту на сопровождение: очередь, бэкапы Borg, обновления Postfix и Dovecot

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** Exchange Server 2019/2016 End of Support Roadmap (learn.microsoft.com — 2025)
- 02** postfix(5): smtpd_relay_restrictions, message_size_limit, TLS (postfix.org — 3.11)
- 03** Upgrading Dovecot CE 2.3 → 2.4: конфиг, mail_driver, quota (doc.dovecot.org — 2.4.4)
- 04** dovecadm-sync(1) и dovecadm-backup(1): режим -1 при миграции (doc.dovecot.org — 2.4.4)
- 05** Postfix and Dovecot LMTP, плагин quota и сервис quota-status (doc.dovecot.org — 2.4.4)
- 06** Statistics settings: bayes, autolearn, обратная связь IMAPSieve (docs.rspamd.com — 4.1)
- 07** imapsync FAQ.Exchange: прокси-логин, пресеты, лимиты скорости (imapsync.lamiral.info — 2.314)
- 08** SOGo Installation Guide: EAS, CalDAV/CardDAV, клиенты (sogo.nu — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.

