



Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Dovecot Sieve в офисе: серверная фильтрация почты

Как мы ставим Pigeonhole на Dovecot 2.4: LMTP,
global-скрипты, ManageSieve

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

Суть проблемы

Правила Outlook живут в профиле клиента: не работают на смартфоне и при выключенном ноутбуке, теряются после переустановки Windows, не видят серверных заголовков антиспама и DMARC. Сотрудники пропускают письма от налоговой и контрагентов, а восстановление 40-60 правил на каждого съедает часы админа. Мы переносим логику на сервер — в Sieve, срабатывающий при доставке по LMTP.

Почему это важно бизнесу

- Требование ФНС, утонувшее в общем INBOX, — это штраф и блокировка счёта; серверный фильтр кладёт его в отдельную папку до открытия почты.
- Правила на сервере переживают переустановку Windows и смену ноутбука: админ не тратит полдня на восстановление 40-60 фильтров сотрудника.
- Отпуск и болезнь не рвут коммуникацию: vacation и переадресация отрабатывают на сервере, когда компьютер сотрудника выключен.
- Один общий скрипт на отдел вместо правок в четырёх Outlook-профилях: смена адресов банк-клиента или оператора ЭДО занимает минуты.
- Утечка через самодельную пересылку на личный ящик закрывается лимитом сервера, а не устной договорённостью с сотрудником.



Ключевые параметры реализации

2.4.4

Актуальный релиз Dovecot и Pigeonhole (май 2026): новые внедрения ставим только на 2.4.x

по докам Dovecot CE 2.4

4190

Порт ManageSieve: пользователь правит фильтры сам из Roundcube, без SSH и без FTP

RFC 5804 / Pigeonhole

4

sieve_max_redirects по умолчанию: потолок пересылок, чтобы ящик не стал ретранслятором

по докам Pigeonhole

1M

sieve_max_script_size: длинные перечни доменов выносим в include, а не раздуваем скрипт

по докам Pigeonhole

1d

sieve_vacation_min_period по умолчанию: защита от петли автоответов между серверами

по докам Pigeonhole

60 мин

Интервал сапагу-письма: проверяем не сервис, а факт попадания письма в нужную папку

наш стандарт



Доставка через Dovecot LMTP и включение Pigeonhole

Что настраиваем

Почтовый узел офиса: Postfix 3.11 на приёме, Dovecot 2.4 в роли LDA/LMTP, база Debian 13 или Ubuntu 24.04 LTS

Как мы это делаем

- 1 В main.cf переводим доставку на Dovecot: mailbox_transport и virtual_transport = lmtp:unix:private/dovecot-lmtp, procmail и mbox-обработчик убираем.
- 2 В service lmtp поднимаем unix_listener /var/spool/postfix/private/dovecot-lmtp с mode=0600 и владельцем postfix, иначе Postfix молча не достигнется.
- 3 Плагин включаем новым синтаксисом: в protocol lmtp и protocol lda пишем mail_plugins { sieve = yes }; секции plugin { } в 2.4 больше нет.
- 4 Хранилище описываем блоками sieve_script: тип personal с sieve_script_path=~/.sieve и sieve_script_active_path=~/.dovecot.sieve, плюс блок sieve_script_type=default.
- 5 Проверяем тестовым скриптом с fileinto :create и меткой в теме; разбор — mail.log плюс sieve-test при sieve_trace_level=actions.

РЕЗУЛЬТАТ

Письмо обрабатывается один раз на сервере до попадания в IMAP, поэтому Outlook, Apple Mail, мобильный клиент и Roundcube видят одинаковую раскладку по папкам. Сортировка перестаёт зависеть от того, включён ли компьютер сотрудника, и не слетает при переустановке системы.

КЛЮЧЕВОЙ НЮАНС

Sieve вызывается только тогда, когда доставку ведёт Dovecot LDA или LMTP. Остался в Postfix локальный transport или procmail — скрипты компилируются, но не выполняются: симптом «всё падает в INBOX».



Общий скрипт отдела и персональные правила в ManageSieve

Что настраиваем

Бухгалтерия и юротдел: серверный before-скрипт плюс personal-скрипт каждого ящика, правка через Roundcube 1.7

Как мы это делаем

- 1 Общие правила выносим в `/etc/dovecot/sieve/global/buh.sieve` и подключаем блоком `sieve_script` с `sieve_script_type=before` — он идёт до пользовательского.
- 2 Персональные шаблоны строим на `require ["fileinto","mailbox","imap4flags","envelope","variables"]`: `imapflags` устарел, берём `imap4flags`.
- 3 Включаем `protocols = imap Imtp sieve` и `service managesieve-login с inet_listener sieve` на порту 4190; наружу порт не публикуем.
- 4 В Roundcube ставим плагин `managesieve` и указываем `127.0.0.1:4190`; скрипт пользователя сохраняется в `~/sieve/roundcube.sieve`.
- 5 Ограничиваем аппетиты: `sieve_quota_script_count` и `sieve_quota_storage_size` (в 2.3 это `sieve_quota_max_scripts` и `sieve_quota_max_storage`).

РЕЗУЛЬТАТ

Смена адреса банк-клиента или оператора ЭДО — правка одного файла на сервере вместо обхода четырёх Outlook-профилей. Сотрудник сам собирает типовую сортировку по отправителю и теме в веб-интерфейсе, инженера зовут только под `regex` и условия по нескольким полям.

КЛЮЧЕВОЙ НЮАНС

Порядок исполнения жёсткий: `before`, затем `personal`, затем `after`. Если `before` обрывается на `stop`, персональные правила не отработают — в общих блоках ставим `stop` только там, где сортировка финальная.



Контроль исполнения: логи, doveadm и canary-ящик

Что настраиваем

Все ящики домена: мониторинг Sieve на почтовом узле, алерты в Telegram, аудит скриптов через doveadm

Как мы это делаем

- 1 Собираем ошибки Sieve: персональный sieve_user_log_path плюс разбор mail.log; больше 5 ошибок за час — алерт в Telegram.
- 2 Инвентаризация без входа в ящики: doveadm sieve list -A, doveadm sieve get для выгрузки, doveadm sieve activate для отката.
- 3 Canary-ящик: раз в час отправляем письмо с меткой в теме и через минуту проверяем, что оно легло в целевую папку, иначе алерт.
- 4 Жалобу «правило не сработало» разбираем sieve-test на реальном .eml при sieve_trace_level=matching и sieve_trace_dir во временный каталог.
- 5 Пересылки держим в узде: sieve_max_redirects=4 и sieve_redirect_envelope_from=orig_recipient вместо дефолтного sender, плюс разбор адресов в логах.

РЕЗУЛЬТАТ

Фильтрация перестаёт быть чёрным ящиком: видно, что скрипт скомпилирован, вызван и положил письмо туда, куда задумано. Сломанное правило ловим по canary раньше, чем пользователь заметит пропажу писем, а массовые ошибки компиляции — по счётчику в алерте.

КЛЮЧЕВОЙ НЮАНС

Тихий отказ — штатное поведение Sieve: скрипт с ошибкой прав или синтаксиса не роняет доставку, письмо просто уходит в INBOX. Поэтому мониторим не состояние службы, а факт попадания письма в папку.



Подводные камни

✗ Доставка идёт мимо Dovecot LMTP

Остался procmail или локальный transport — Sieve не вызывается. Переводим mailbox_transport и virtual_transport на lmtp:unix:private/dovecot-lmtp.

✗ Права на каталог ~/sieve

Каталог не принадлежит vmail или открыт шире 0700 — тихий отказ, письма падают в INBOX без обработки. Владельца сверяем с учёткой LMTP.

✗ Скрипты без предварительной компиляции

Без sievec Dovecot компилирует скрипт при каждой доставке — лишний CPU на потоке в тысячи писем. Компилируем заранее и следим за правами на .svbin.

✗ Фильтр написан под чужой заголовок

Rspamd ставит X-Spam-Result и X-Spam-Level, а правило ждёт X-Spam-Status от SpamAssassin. Сначала фиксируем milter_headers, потом пишем Sieve.

✗ Vacation без :days и :addresses

Автоответ уходит на каждое письмо и закидывается с чужим роботом. Держим sieve_vacation_min_period на 1d и перечисляем свои адреса в :addresses.

✗ addheader без расширения editheader

Расширения, меняющие письмо, выключены по умолчанию. Без блока sieve_extensions { editheader = yes } и без require скрипт не компилируется целиком.

✗ Пересылка наружу без ограничений

Сотрудник заворачивает всю почту на личный ящик — утечка базы. Держим sieve_max_redirects=4, задаём sieve_redirect_envelope_from, смотрим логи.

✗ Конфиг 2.3 переносят в 2.4 как есть

sieve, sieve_before, sieve_default ушли в блоки sieve_script. Готового конвертера нет: переносим руками и сверяем вывод doveconf -n.

Как правильно

МИНИМУМ

- Доставка только через Dovecot LMTP, procmail и mbox-обработчики убраны
- Один default-скрипт: спам в Junk, системные уведомления в свою папку
- Каталог ~/sieve принадлежит vmail, режим 0700, скрипты собраны sievec
- Согласованы заголовки антиспама, по которым реально фильтруем письма

НОРМАЛЬНО

- ManageSieve 4190 на localhost и плагин managesieve в Roundcube 1.7
- Общий before-скрипт на отдел, персональные правила ложатся поверх него
- vacation с :days и :addresses, sieve_max_redirects оставлен на значении 4
- Ошибки Sieve из mail.log и sieve_user_log_path уходят в дежурный алерт

ХОРОШО

- Dovecot и Pigeonhole 2.4.4, конфиг в новом синтаксисе блоков sieve_script
- Canary-ящик с почасовой проверкой попадания письма в нужную папку
- Квоты sieve_quota_script_count и sieve_quota_storage_size на каждый ящик
- Разбор инцидентов через sieve-test при sieve_trace_level=matching



Чек-лист самопроверки

- | | |
|---|---|
| ☐ Доставка в ящики идёт через Dovecot LMTP, а не через procmail или локальный transport Postfix? | ☐ У автоответов заданы :days и :addresses, а sieve_vacation_min_period не занижен ниже 1d? |
| ☐ Плагин включён блоком mail_plugins { sieve = yes } и для protocol lmtp, и для protocol lda? | ☐ Ограничены ли пересылки наружу: sieve_max_redirects и заданный sieve_redirect_envelope_from? |
| ☐ Каталог ~/sieve принадлежит пользователю, под которым работает LMTP, и закрыт режимом 0700? | ☐ Есть ли у сотрудников самообслуживание фильтров через ManageSieve и Roundcube? |
| ☐ Активные скрипты скомпилированы sieves заранее, а не пересобираются при каждой доставке? | ☐ Настроены ли алерт на ошибки Sieve и canary-проверка фактической доставки в папку? |
| ☐ Правила написаны под те заголовки, которые реально проставляет ваш антиспам и DMARC-проверка? | ☐ Конфигурация переведена на блоки sieve_script синтаксиса 2.4 и проверена doveconf -n? |

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 Postfix, Dovecot 2.4, Pigeonhole, Rspamd и Roundcube под ключ, вместе с SPF, DKIM и DMARC
- Переносим правила из Outlook в общие и персональные Sieve-скрипты с обкаткой на тестовом ящике
- Мигрируем конфигурацию с Dovecot 2.3 на 2.4: блоки sieve_script, сверка doveconf -n, план отката
- Ставим мониторинг Sieve: алерты по ошибкам, canary-ящик, регулярный аудит скриптов через doveadm sieve
- Обучаем сотрудников редактору фильтров в Roundcube и оставляем шаблоны для бухгалтерии и руководства

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** Dovecot CE: плагин sieve — хранилище скриптов и блоки sieve_script (doc.dovecot.org — 2.4.4)
- 02** Dovecot CE: лимиты и квоты Sieve, trace- и log-настройки плагина (doc.dovecot.org — 2.4.4)
- 03** Upgrading Dovecot CE from 2.3 to 2.4: новый синтаксис конфигурации (doc.dovecot.org — 2.4)
- 04** doveadm-sieve(1): list, get, put, activate, deactivate (doc.dovecot.org — 2.4.4)
- 05** Dovecot CE: ManageSieve Server (RFC 5804), сервисы и порт 4190 (doc.dovecot.org — 2.4.4)
- 06** Dovecot CE: расширение editheader и sieve_extensions (doc.dovecot.org — 2.4.4)
- 07** Postfix: lmtp(8) и настройка транспорта доставки в main.cf (postfix.org — 3.11)
- 08** Rspamd: модуль milter_headers и состав служебных заголовков (docs.rspamd.com — 3.x)

Основано на официальной документации продуктов и нашей практике внедрения.

