



Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Uptime Kuma: свой мониторинг сайтов, 1С и почты за 10 минут

Как мы разворачиваем self-hosted «светофор» с алертами в Telegram под ключ

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

Суть проблемы

Клиент узнаёт о падении сайта, недоступности сервера 1С или остановке почты от своих сотрудников — а не от нас. У компаний до 50 РМ штатного мониторинга обычно нет, а SaaS-сервисы режут проверки на бесплатном тарифе. Мы закрываем разрыв бесплатным self-hosted инструментом и настраиваем алерты раньше, чем сотрудник клиента заметит проблему.

Почему это важно бизнесу

- Простой сайта или 1С-сервера считается часами до звонка клиента, а не минутами до алерта
- SaaS-мониторинг (UptimeRobot, Pingdom) на бесплатном тарифе режет интервал проверки и число мониторов
- Бухгалтерия и отдел продаж не могут работать без 1С — падение сервера приложений критично в день сдачи отчётности
- Почтовый сервер «тихо» перестаёт принимать письма (диск, DKIM, блок IP) без видимых симптомов на клиенте
- Заказчику нужен публичный статус-пейдж для прозрачности перед своими клиентами и партнёрами



Ключевые параметры реализации

60 сек

интервал проверки (Heartbeat Interval) по умолчанию на мониторе Uptime Kuma 2.x, wiki

15+

типов мониторов: HTTP(s), Keyword, JSON Query, TCP Port, Ping, DNS Record, Docker, Push
Uptime Kuma 2.x, docs

90+

каналов уведомлений из коробки + Apprise-мост на остальные сервисы
Uptime Kuma 2.x, notification-providers

3001

порт веб-интерфейса контейнера по умолчанию — наш стандарт публикуем только за reverse-proxy наш стандарт

21 день

порог предупреждения об истечении TLS-сертификата, который мы включаем на HTTPS-мониторах
наш стандарт

0 руб/мес

лицензионные отчисления — весь стек open-source (MIT), платим только за VPS
наш стандарт



Мониторинг витрины и лендингов клиента

Что настраиваем

охват: публичные сайты и лендинги клиента + сертификаты TLS, узел — отдельный контейнер на нашем мониторинг-VPS

Как мы это делаем

- 1 Разворачиваем контейнер `louislam/uptime-kuma:2`, том `data` примонтирован в `/app/data` под SQLite-базу `kuma.db`
- 2 Публикуем интерфейс через `nginx reverse-проxy` с проксированием заголовков `Upgrade/Connection` под `WebSocket`
- 3 Заводим HTTP(s) монитор на каждый домен клиента с интервалом 60 сек и `Retries=2` перед пометкой `Down`
- 4 Включаем проверку TLS-сертификата с порогом уведомления за 21 день до истечения
- 5 Публикуем публичный статус-пейдж на поддомене `status.` для клиента и его партнёров

РЕЗУЛЬТАТ

Клиент и мы получаем алерт в Telegram раньше, чем посетитель напишет в поддержку «сайт не открывается»; просроченный сертификат ловим за 3 недели, а не в момент блокировки браузером.

КЛЮЧЕВОЙ НЮАНС

Публичный статус-пейдж снижает число «а что с сайтом» звонков клиента почти до нуля — он сам смотрит статус до звонка нам.

Контроль сервера приложений 1С и терминала

Что настраиваем

охват: сервер 1С:Предприятие (веб-публикация + RAS), терминальный сервер RDP, узел — тот же мониторинг-VPS по VPN

Как мы это делаем

- 1 Заводим TCP Port монитор на порты кластера 1С (1541 менеджер, 1560+ рабочие процессы) и RDP 3389
- 2 Добавляем HTTP(s) Keyword монитор на веб-публикацию 1С с проверкой строки на странице авторизации
- 3 Настраиваем Push-монитор: регламентное задание 1С раз в 15 минут дёргает push-URL монитора с токеном — тишина = алерт
- 4 Группируем мониторы 1С в отдельную группу на дашборде и привязываем Notification только на рабочий Telegram-чат клиента
- 5 Ставим Maintenance Window на плановые часы обновления конфигурации, чтобы не будить дежурного ложной тревогой

РЕЗУЛЬТАТ

Мы видим зависание кластера 1С или остановку регламентного задания за минуты, а не когда бухгалтер не смог провести документы к сдаче отчётности.

КЛЮЧЕВОЙ НЮАНС

Push-монитор закрывает главное слепое пятно — задачи, которые должны выполняться по расписанию сами, но никто не проверяет, выполнены ли они.

Здоровье почтового сервера и очередей

Что настраиваем

охват: почтовый сервер клиента (Postfix/Dovecot или mailcow), узел — контейнер на мониторинг-VPS с доступом по SMTP/IMAP портам

Как мы это делаем

- 1 Заводим TCP Port мониторы на 25/465/587 (SMTP) и 993 (IMAPS) с интервалом 60 сек
- 2 Добавляем DNS Record монитор на MX и TXT (SPF/DKIM/DMARC) записи домена — ловим случайное удаление записи регистратором
- 3 Настраиваем Docker Container монитор через socket-proxu для контейнеров postfix/dovecot/rsnamd на mailcow-хостах
- 4 Включаем Resend Notification каждые 3 цикла, чтобы авария не потерялась среди других сообщений в чате
- 5 Настраиваем канал Telegram через собственного бота с персональным chat_id дежурного инженера

РЕЗУЛЬТАТ

Отказ приёма почты или пропaja DKIM-записи обнаруживается до жалоб клиентов о недоставленных письмах, а не постфактум через разбор логов.

КЛЮЧЕВОЙ НЮАНС

DNS-мониторинг записей так же важен, как мониторинг портов — большинство «поломок почты» на практике это случайно изменённая TXT/MX запись у регистратора.



Подводные камни

✗ **Мониторинг на том же сервере**

Ставить Uptime Kuma на тот же хост, что и сайт — при падении хоста падает и монитор, алерта не будет

✗ **Retries=0 на нестабильных каналах**

Первый же таймаут при неровном канале клиента даёт ложный алерт и приучает игнорировать уведомления

✗ **NFS-том под данными**

SQLite-база Uptime Kuma не работает поверх сетевой файловой системы — том обязан быть локальным диском

✗ **Публикация 3001 без прокси**

Голый порт без reverse-proxy и TLS отдаёт панель управления и логи в открытый интернет

✗ **Без Maintenance Window**

Плановые работы без окна обслуживания заваливают чат ложными алертами и приучают их не читать

✗ **Один Telegram-чат на всё**

Смешение алертов сайта, 1С и почты в один канал без групп мониторов размывает ответственность дежурного

✗ **Нет бэкапа каталога /app/data**

История аптайма, настройки уведомлений и сертификаты живут в каталоге /app/data (kuma.db + конфиги) — бэкапить нужно весь том, иначе потеряете всё пр...

✗ **Забыли про 2FA админки**

Панель управления мониторингом видит все секреты уведомлений (токены ботов, SMTP-пароли) — без 2FA это отдельная точка входа

Как правильно

МИНИМУМ

- Docker-контейнер Uptime Kuma на отдельном VPS вне сети клиента
- HTTP(s) мониторы на публичные сайты, интервал 60 сек
- Один канал Telegram-уведомлений на все алерты

НОРМАЛЬНО

- Reverse-proxy с TLS перед панелью + 2FA для входа администратора
- TCP-мониторы портов 1С и почты, DNS Record на MX/SPF/DKIM
- Группировка мониторов и разделение Telegram-чатов по зонам ответственности
- Регулярный бэкап каталога /app/data с kuma.db и конфигами

ХОРОШО

- Push-мониторы на регламентные задания 1С и cron-бэкапы
- Docker Container монитор через socket-proxy для критичных контейнеров
- Публичный статус-пейдж для клиента с историей инцидентов
- Maintenance Window, привязанные к календарю регламентных работ

Чек-лист самопроверки

- Uptime Kuma развёрнут вне хоста, который сам мониторится?
- Данные (/app/data с kuma.db) лежат на локальном томе, а не на NFS?
- Панель управления закрыта reverse-proxy с TLS и 2FA?
- Настроены Retries и Retry Interval, а не голый Retries=0?
- Есть TCP/HTTP мониторы на 1C-сервер и терминал клиента?
- DNS Record монитор проверяет MX/SPF/DKIM почтового домена?
- Настроен Telegram-бот с отдельными чатами по зонам ответственности?
- Включена проверка истечения TLS-сертификатов с запасом от 14 дней?
- Есть Maintenance Window на плановые регламентные работы?
- Настроен регулярный бэкап всего каталога /app/data контейнера?

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).

- Развернём Uptime Kuma под ключ на своём или клиентском VPS за один визит инженера
- Настроим мониторы под конкретный стек клиента: 1С-кластер, почта, сайты, VPN-шлюзы
- Подключим Telegram-бота и разведём алерты по чатам ответственных сотрудников
- Настроим публичный статус-пейдж для клиентов заказчика
- Возьмём мониторинг на сопровождение: реагируем на алерты по регламенту SLA

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** [GitHub repository louislam/uptime-kuma \(github.com — 2026\)](#)
- 02** [Wiki: How to Install \(github.com/louislam/uptime-kuma/wiki — 2026\)](#)
- 03** [Wiki: Notification Methods \(github.com/louislam/uptime-kuma/wiki — 2026\)](#)
- 04** [Wiki: Reverse Proxy \(github.com/louislam/uptime-kuma/wiki — 2026\)](#)
- 05** [Wiki: Status Page \(github.com/louislam/uptime-kuma/wiki — 2026\)](#)
- 06** [Docker Hub image louislam/uptime-kuma \(hub.docker.com — 2026\)](#)
- 07** [Wiki: Migration From v1 To v2 \(github.com/louislam/uptime-kuma/wiki — 2026\)](#)

Основано на официальной документации продуктов и нашей практике внедрения.