Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Мониторинг ИТ-инфраструктуры: узнавать о сбоях раньше клиентов

Почему простои дорожают и как мы предсказываем аварию за две недели до звонка клиента

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

О сбоях в компании до 50 рабочих мест чаще всего узнают не от ИТ-службы, а от сотрудников и клиентов: с утра не открывается 1С, не уходит почта, «лежит» сайт. Причину ищут часами вслепую — хотя диск заполнялся неделями, а бэкап молча не выполнялся. Мониторинг считают роскошью крупных компаний, при этом час простоя малого бизнеса стоит от десятков до сотен тысяч рублей.

Почему это важно бизнесу

- Час простоя компании в 50 человек — от 40 тыс. ₽ прямых потерь на оплату труда; с упущенной выручкой и штрафами — сотни тысяч
- Большинство отказов предсказуемы: заполнение диска, деградация RAID, истекающий TLS-сертификат видны за дни и недели до аварии
- Когда о сбое сообщает клиент, а не система, к прямым потерям добавляются репутационный ущерб и отток заказчиков
- Западные системы мониторинга ушли из РФ, но open source (Zabbix 7.0 LTS, Prometheus) бесплатен, легален и стал стандартом де-факто

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

500+

серверов и сетевых устройств под единым мониторингом Zabbix 7.0 LTS + Prometheus в нашем конту…

1 мин

интервал опроса ключевых метрик (CPU, память, файловые системы, RAID) агентом Zabbix; доступно…

14 дней

горизонт прогноза заполнения диска и деградации RAID предиктивными функциями timeleft()/foreca…

7 дней

порог раннего оповещения об истечении TLS-сертификата (шаблон «Website certificate by Zabbix a…

6

уровней важности триггеров Zabbix; ночной звонок — только High/Disaster, Warning/Average копят…

< 2 мин

целевое время обнаружения инцидента (MTTD) при blackbox-пробе раз в 30 с — против 30–60 мин в…

РЕАЛИЗАЦИЯ 1 ИЗ 3

Предиктивный контроль дисков и RAID: авария видна за две недели

Что настраиваем

Наш контур мониторинга: 500+ серверов и СХД под Zabbix 7.0 LTS

Как мы это делаем

1. На каждый сервер ставим Zabbix agent 2 и шаблон «Linux by Zabbix agent» или «Windows by Zabbix agent» — метрики CPU, памяти, файловых систем и SMART снимаются раз в…
2. Заполнение диска ловим не порогом «90%», а прогнозом: timeleft(/host/vfs.fs.size[/,free],1h,0)<14d — триггер срабатывает, когда до заполнения остаётся меньше двух н…
3. Состояние массива берём через SMART и утилиты контроллера (storcli/perccli); деградацию RAID и rebuild выносим отдельным триггером важности High
4. TLS-сертификаты сайтов и почты закрываем шаблоном «Website certificate by Zabbix agent 2» — алерт за 7 дней до истечения

РЕЗУЛЬТАТ

Заполненный том, умирающий диск в массиве и истекающий сертификат перестают быть внезапностью: инженер получает задачу за дни-недели до отказа и меняет диск или чистит логи в плановое окно, а не ночью по аварии.

КЛЮЧЕВОЙ НЮАНС

Мониторить нужно не факт «диск на 90%», а прогноз времени до отказа: функции timeleft()/forecast() в Zabbix превращают метрику в раннее предупреждение.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Бэкапы и события ИБ под наблюдением, а не «делаются сами»

Что настраиваем

Наш регламент: контроль восстановимости и журналов безопасности на всех серверах

Как мы это делаем

1. Успех задания бэкапа отдаём в Zabbix трапом через zabbix_sender прямо из скрипта копирования; нет свежего успешного трапа за сутки → триггер «бэкап не выполнен»
2. Раз в неделю запускаем тестовое восстановление контрольной выборки и сверяем контрольные суммы — мониторим сам факт успешного restore, а не наличие файла копии
3. Журналы (Windows Event Log, syslog, auth.log) собираем в Grafana Loki; всплеск отказов аутентификации, массовое шифрование/переименование файлов, остановку службы б…
4. Критичные события ИБ (удаление или шифрование копий, отключение антивируса) маршрутизируем отдельным каналом с немедленной эскалацией

РЕЗУЛЬТАТ

Молчаливо падающая копия и подозрительная активность в сети перестают всплывать «в момент аварии»: расхождение видно на следующий день, а не через месяц.

КЛЮЧЕВОЙ НЮАНС

Контролировать надо и успешность заданий, и восстановимость данных, и журналы безопасности — доступность (ping и CPU) скрытную проблему не покажет.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Приоритеты алертов, инвентаризация и runbook-и вместо шквала писем

Что настраиваем

Наша эксплуатация: маршрутизация оповещений и дежурство по всему парку серверов

Как мы это делаем

1. Шесть уровней важности Zabbix используем осмысленно: Disaster/High → звонок и Telegram ночью, Warning/Average → до утра, Information → только в журнал
2. Дедупликация и группировка алертов на стороне Alertmanager и Zabbix, чтобы один инцидент не рождал сотню писем
3. Держим актуальную инвентаризацию (CMDB): какие сервисы на каком узле и их зависимости — чтобы при сбое сразу видеть радиус поражения
4. На каждый типовой алерт готов runbook: диск, зависшая 1С, недоставка почты, деградация RAID — с точными командами диагностики и восстановления

РЕЗУЛЬТАТ

Дежурный видит не «сотни писем», а несколько приоритизированных инцидентов с готовой инструкцией; время локализации падает с десятков минут до единиц.

КЛЮЧЕВОЙ НЮАНС

Побеждает не тот, у кого не бывает аварий, а тот, кто быстрее их видит и локализует: приоритезация, инвентаризация и runbook сокращают простой в разы.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Мониторинга нет — «узнаём от людей»**
  Первый сигнал о сбое — звонок сотрудника или клиента. Обнаружение занимает 30–60 минут вместо 2, и ущерб растёт с каждой минутой.

- ✕ **Мониторят серверы, а не сервисы**
  Ping отвечает, CPU в норме, а 1С не пускает пользователей. Проверять нужно работу глазами пользователя: вход, проведение документа, отправку письма.

- ✕ **Шквал алертов без приоритетов**
  Сотни писем в день приучают игнорировать всё, включая критичное. Без уровней важности и дедупликации на Alertmanager/Zabbix дежурный тонет в шуме и п…

- ✕ **Бэкапы вне мониторинга**
  Копия месяцами «делается» с ошибкой, и это выясняется в момент аварии. Контролировать нужно и успешность заданий (zabbix_sender-трап), и восстановимо…

- ✕ **Алерты уходят в никуда**
  Оповещения падают в почтовый ящик, который никто не читает. Без ответственного, срока реакции и эскалации алерт равен его отсутствию.

- ✕ **Пороги настроили и забыли**
  Инфраструктура меняется, пороги — нет. Ложные срабатывания растут, доверие к системе падает, и реальную аварию пропускают.

- ✕ **Нет runbook-ов на типовые аварии**
  Что делать при алерте, знает один админ. Он в отпуске или уволился — и простой затягивается с минут до часов.

- ✕ **Сертификаты и сроки вне контроля**
  Истёкший TLS-сертификат или неоплаченный домен кладут сайт и почту на день. Автопроверка через шаблон «Website certificate by Zabbix agent 2» настраи…

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Внешняя uptime-проверка сайта, почты и 1С (blackbox probe_success) с оповещением в Т…
- Контроль дисков, RAID и успешности бэкапов на каждом сервере
- Автопроверка сроков TLS-сертификатов, доменов и лицензий
- Назначенный ответственный и норматив времени реакции на алерт

НОРМАЛЬНО

- Zabbix/Prometheus на всю инфраструктуру: серверы, сеть, ИБП, виртуализация
- Уровни важности алертов: Disaster/High — звонок и Telegram ночью, остальное — до утра
- Проверки «глазами пользователя»: вход в 1С, отправка письма, оплата на сайте
- Ежемесячный разбор инцидентов и корректировка порогов и предиктивных триггеров

ХОРОШО

- Метрики и логи в одном месте (Grafana + Loki): причина сбоя за минуты
- SLO по ключевым сервисам, согласованные с бизнесом, а не «99,9% вообще»
- Дежурства с эскалацией и runbook на каждый типовой алерт
- Мониторинг ИБ-событий + регулярное тестовое восстановление из бэкапа

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Узнаёте ли вы о сбоях раньше, чем сотрудники и клиенты начинают звонить?
- [ ] Знаете ли вы, во сколько компании обходится час простоя 1С, почты или сайта?
- [ ] Придёт ли автоматическое оповещение, если ночной бэкап не выполнился?
- [ ] Предупредит ли система за две недели о заполнении диска или истечении TLS-сертификата?
- [ ] Определено ли, кто и за сколько минут обязан отреагировать на критический сбой?
- [ ] Есть ли письменные инструкции (runbook) на типовые аварии: диск, 1С, почта, сеть?
- [ ] Разбираете ли вы причины каждого инцидента, чтобы он не повторился?
- [ ] Проверяется ли работа сервисов «глазами пользователя», а не только доступность серверов?
- [ ] Переживёт ли ваш мониторинг уход единственного системного администратора?

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 инфраструктуры и мониторинга: находим слепые зоны и считаем цену часа простоя ваших сервисов
- Внедрение под ключ: Zabbix 7.0 LTS/Prometheus + Grafana, алерты в Telegram по уровням важности, без лицензионных п…
- Контроль бэкапов: мониторинг успешности копий (zabbix_sender-трапы) и регулярные тестовые восстановления
- Runbook-и и регламент реагирования: понятные инструкции на типовые аварии для вашей команды
- Абонентское сопровождение: инженеры ITfresh реагируют на алерты вашей инфраструктуры, вам — отчёты

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 Zabbix 7.0 LTS — руководство: шаблоны «Linux by Zabbix agent» и «Windows b… (zabbix.com — 2026)

02 Zabbix 7.0 LTS — предиктивные триггерные функции timeleft() и forecast() (zabbix.com — 2026)

03 Zabbix 7.0 LTS — мониторинг TLS-сертификатов (Website certificate by Zabbi… (zabbix.com — 2026)

04 Prometheus — правила алертинга и Alertmanager (prometheus.io — 2026)

05 Prometheus Blackbox exporter — probe_success, probe_ssl_earliest_cert_expi… (prometheus.io — 2026)

06 Grafana Loki — сбор, хранение и запросы логов (LogQL) (grafana.com — 2026)

07 Grafana — дашборды и unified alerting (grafana.com — 2026)

08 Шаблон ITfresh: контроль успешности бэкапов через zabbix_sender (itfresh.ru — 2026)

09 Регламент ITfresh: уровни важности алертов и runbook-и дежурства (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.