



**Ай-ТИ Фреш**

**ТЕХНИЧЕСКИЙ РАЗБОР**

# Мониторинг офиса на Zabbix: наш подход внедрения

Zabbix 7.x LTS и agent2 — что мы ставим, что смотрим и с какими порогом

---

Июль 2026

**itfresh.ru** · ИТ-аутсорсинг для юридических лиц

# Суть проблемы

Мы приходим на площадки, где 3-10 серверов и до полусотни рабочих мест живут без выделенного мониторинга: о падении диска, зависшем бэкапе или обрыве 1С узнают от бухгалтера, а не от системы. Инцидент, который триггер Zabbix ловит за минуту, без мониторинга превращается в простой на часы и разбор по логам постфактум.

## Почему это важно бизнесу

- Простой сервера 1С на несколько часов останавливает продажи и бухгалтерию целиком.
- Незамеченное заполнение диска до 100% валит СУБД и файловый сервис одновременно.
- Упавшее задание бэкапа обнаруживают только в день восстановления — поздно.
- Без SLA-метрик невозможно объективно показать заказчику качество обслуживания.
- Ручной обход серверов не масштабируется дальше 3-4 узлов на инженера.

# Ключевые параметры реализации

## 7.0 LTS

ветка Zabbix, которую мы ставим на новых площадках — поддержка вендора до 2029 года

Zabbix 7.0 LTS

## 60 с

интервал активных проверок agent2 по умолчанию — им закрываем большинство ключей

по докам Zabbix

## 3 знач.

берём min/avg по 3 последним значениям перед триггером, чтобы не ловить дребезг

наш стандарт

## 6 severity

уровней важности триггера от Not classified до Disaster — правило именования у нас единое

Zabbix 7.x

## 10 мин

нормативное время реакции инженера на severity High/Disaster по нашему SLA

наш стандарт

## до 5%

свободного места на томе — порог critical для vfs.fs.size, ниже — риск остановки СУБД

наш стандарт



# Базовый стек: сервер, рабочие места, каналы связи

## Что настраиваем

Типовой офис 15-50 рабочих мест, 1-2 физических/виртуальных сервера, 1 интернет-канал

## Как мы это делаем

- 1 Ставим Zabbix server 7.0 LTS + MySQL/PostgreSQL на отдельной VM, agent2 на все сервера и ключевые ПК.
- 2 На Windows-серверах — шаблон «Windows by Zabbix agent active» (perf\_counter, service.info, eventlog).
- 3 На Linux — «Linux by Zabbix agent active»: system.cpu.util, vm.memory.size[pavailable], vfs.fs.size[fs,pused] через LLD по файловым системам.
- 4 Доступность сервисов — net.tcp.service[tcp,,port] на RDP/SMB/1C-сервер/почтовый порт, net.dns для критичных доменов.
- 5 Канал и роутер — SNMP-шаблон на ifHCInOctets/ifOperStatus, если оборудование отдаёт SNMP.

## РЕЗУЛЬТАТ

Инженер видит все узлы офиса на одном экране Problems, а не узнаёт о простое из звонка. Время до обнаружения инцидента падает с часов до минуты интервала опроса.

## КЛЮЧЕВОЙ НЮАНС

Active-агент экономнее пассивного на нестабильных каналах: агент сам решает, когда слать данные, сервер не ждёт таймаутом недоступный хост.



# Мониторинг MSSQL и кластера 1С через RAS/RAC

## Что настраиваем

Сервер 1С:Предприятие 8.3 на MSSQL, до 20 одновременных сеансов

## Как мы это делаем

- 1 Разворачиваем нативный MSSQL-плагин agent2 (Go-плагин, конфиг mssql.conf, TLS к инстансу) и шаблон «MSSQL by Zabbix agent 2».
- 2 Смотрим deadlock-и, blocked-процессы, размер и автогровт баз, батч-запросы в секунду, page life expectancy.
- 3 Для кластера 1С поднимаем службу RAS рядом с сервером и опрашиваем её через ras-клиент по UserParameter.
- 4 LLD обходит список информационных баз кластера, дальше — количество активных сеансов, заблокированных сеансов, статус блокировки регламентных заданий.
- 5 Триггер на резкий рост числа сеансов сверх лицензионного лимита — сигнал до жалоб пользователей.

## РЕЗУЛЬТАТ

Просадку 1С по производительности видно по метрикам MSSQL раньше, чем по звонкам пользователей; блокировки лицензий и сеансов обнаруживаются автоматически, а не через ЦУП вручную.

## КЛЮЧЕВОЙ НЮАНС

RAS/RAC — не входит в стандартную поставку шаблонов Zabbix, обязательку под конкретную версию платформы 1С мы держим и обновляем сами.

# SMART дисков, UPS по SNMP и Telegram-эскалация

## Что настраиваем

Файловый сервер с RAID/ZFS + ИБП с сетевой картой в серверной без выделенного админа

## Как мы это делаем

- 1 SMART снимаем UserParameter-обвязкой вокруг smartctl -a с LLD по /dev/sdX, ключи Reallocated\_Sector\_Ct, Current\_Pending\_Sector, температура.
- 2 ИБП опрашиваем по SNMP (community или SNMPv3) — заряд батареи, статус линии, оставшееся время автономии, статус нагрузки.
- 3 Настраиваем media type Telegram через встроенный webhook-шаблон: bot token + chat\_id, api\_parse\_mode=markdown.
- 4 Эскалация в Action: severity Warning — уведомление ответственному инженеру, severity High/Disaster — рассылка в общий чат дежурных сразу.
- 5 Maintenance-периоды закрываем на плановые окна, чтобы регламентные работы не поднимали ложные тревоги.

## РЕЗУЛЬТАТ

Деграцию диска и потерю сети на ИБП замечаем до отказа оборудования, а не после инцидента; уведомление доходит инженеру в Telegram за секунды вместо разбора наутро.

## КЛЮЧЕВОЙ НЮАНС

Готового плагина под smartctl в agent2 нет — обвязка через UserParameter остаётся рабочим и предсказуемым вариантом для малого офиса.

## Подводные камни

### × Один порог на все диски

Системный и файловый том растут по-разному — задаём макросы `{$VFS.FS.PUSED.MAX.CRIT}` персонально через контекст LLD, а не глобально.

### × Пассивные проверки через NAT/VPN

Passive-агент требует, чтобы сервер сам достучался до хоста; за NAT и на нестабильном канале ставим Active checks.

### × Триггер по одному значению

Единичный всплеск CPU или сети — не авария; берём `min()/avg()` за окно 3-5 минут, иначе шлём ложные тревоги.

### × Нет разделения severity

Все триггеры на Warning — дежурный перестаёт реагировать на алерты вообще; используем полную шкалу до Disaster.

### × Забыли про Maintenance

Плановая перезагрузка без периода обслуживания рождает ложный инцидент и портит статистику доступности.

### × Мониторим сервер, но не сервис

Хост жив, а служба 1C или SQL упала — добавляем `net.tcp.service` и `proc.num` по конкретному процессу, не только `agent.ping`.

### × SNMP-community публичная по умолчанию

«public» на ИБП и коммутаторах в один клик читает любой в сети — меняем community и переходим на SNMPv3, где поддерживается.

### × Нет владельца алерта

Уведомление падает в общий чат без ответственного — эскалацию строим по ролям и рабочим часам в Zabbix User group/Escalation.



# Как правильно

## МИНИМУМ

- Zabbix agent2 на серверах: CPU, память, диск, служба 1C/SQL
- Telegram-алерт на severity High/Disaster дежурному инженеру
- Проверка бэкапа: свежесть файла и код завершения задания

## НОРМАЛЬНО

- Плюс мониторинг рабочих станций и сетевого оборудования по SNMP
- Шаблон MSSQL by Zabbix agent 2 и базовые метрики кластера 1C
- Разделение severity и эскалация по ролям, maintenance-окна
- SMART дисков и статус ИБП с прогнозом автономии

## ХОРОШО

- RAS/RAC-обвязка: сеансы, блокировки, лицензии 1C по каждой базе
- Дашборды SLA для заказчика с историей доступности за месяц
- Distributed monitoring через Zabbix проху на удалённых площадках
- Автодискавери новых хостов и сервисов (LLD + network discovery)

# Чек-лист самопроверки

---

- Стоит ли agent2 хотя бы на всех серверах, а не только на роутере?
- Есть ли отдельный триггер на службу 1C/SQL, а не только на доступность хоста?
- Настроены ли пороги vfs.fs.size индивидуально по разделам через LLD-макросы?
- Приходит ли алерт в Telegram/почту, а не только в веб-интерфейс Zabbix?
- Разведены ли severity по критичности, а не все на одном уровне?
- Есть ли мониторинг SMART и ИБП, а не только «сервер пингуется»?
- Закрываете ли плановые работы Maintenance-периодом?
- Проверяется ли фактическое выполнение бэкапа, а не просто факт задания в планировщике?
- Знаете ли вы, кто и за сколько минут реагирует на Disaster-триггер?
- Обновляется ли Zabbix server/agent2 в рамках LTS-цикла вендора?

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 Zabbix server 7.x LTS и agent2 под ключ на вашей инфраструктуре.
- Настраиваем шаблоны под 1С/MSSQL, SMART, ИБП и сетевое оборудование конкретно под ваш стек.
- Подключаем Telegram-эскалацию с разделением по ролям и рабочим часам.
- Ведём мониторинг на абонентском обслуживании: реагируем на алерты, актуализируем пороги.
- Делаем аудит существующего Zabbix, если он уже стоит, но 'просто пингует'.

**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** Zabbix agent (active checks, интервалы, конфигурация) ([zabbix.com/documentation — 7.0](https://zabbix.com/documentation/7.0))
- 02** MSSQL plugin для Zabbix agent 2 ([zabbix.com/documentation — 7.0](https://zabbix.com/documentation/7.0))
- 03** Шаблон Windows/Linux by Zabbix agent active ([github.com/zabbix](https://github.com/zabbix) — 7.0)
- 04** Webhook-медиатип Telegram ([zabbix.com/integrations — 7.0](https://zabbix.com/integrations/7.0))
- 05** vfs.fs.size, LLD файловых систем, макросы порогов ([zabbix.com/documentation — 7.0](https://zabbix.com/documentation/7.0))
- 06** Триггеры, severity, escalations ([zabbix.com/documentation — 7.0](https://zabbix.com/documentation/7.0))
- 07** Наш стандарт внедрения Zabbix в малых офисах (ITfresh — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.