Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Выгорание штатного админа МСБ: снимаем нагрузку технически

Как мы автоматизируем мониторинг, патчи, бэкапы и SLA, чтобы админ не был системой оповещения

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

В компании на 30-50 PM инфраструктура держится на одном человеке: он же helpdesk, патч-менеджмент, бэкапы и ночной приёмник алертов. Технически роль системы мониторинга и эскалации исполняет живой админ — без дежурств, порогов и автопроверок восстановления. Итог: незакрытые обновления, непроверенные бэкапы и уход единственного носителя знаний вместе с паролями и схемой сети.

Почему это важно бизнесу

- Уход единственного админа = потеря знаний об инфраструктуре: восстановление схемы и доступов занимает месяцы
- Бэкапы без автоматической верификации восстановления дают ложное чувство защиты до первого инцидента
- Пропущенные окна обновлений копят уязвимости на периметре: RDP, гипервизоры, контроллеры домена
- Ночные звонки вместо дежурной ротации превращают любой сбой в личный простой одного человека
- Рутина съедает время: проекты (RDS, DFS, MFA, сегментация) откладываются на годы

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

60 с

Минимальная длительность шага эскалации в Zabbix: короче нельзя, мы ставим 5 мин на L1

Zabbix 7.0, раздел Escalations

7.0 LTS

Ветка Zabbix под мониторинг клиента: полная поддержка до 30.06.2027, EOL 30.06.2029

Zabbix Life Cycle and Release Policy

7 дней

Минимальный период неизменяемости на hardened repository Veeam, наш стандарт — 14

Veeam B&R, Hardened Repository: How Immutability Works

43200 с

Дефолт frequency у Wazuh syscheck (12 ч); на серверных группах мы снижаем интервал

Wazuh 4.14, ossec.conf: syscheck frequency

20.09.2024

Дата объявления WSUS deprecated: новых функций не будет, роль в WS2025 работает

Microsoft Learn: deprecated features, Windows Server

TTO/TTR

Две метрики SLA в GLPI, по которым мы делим зоны штатного и нашей команды

GLPI 10.0, раздел Service Levels

РЕАЛИЗАЦИЯ 1 ИЗ 3

Мониторинг и маршрутизация алертов: Zabbix 7.0 LTS вместо человека

Что настраиваем

Все серверы, гипервизоры, DC и каналы клиента; сервер Zabbix и агенты на Windows/Linux-узлах

Как мы это делаем

1. Ставим Zabbix 7.0 LTS (полная поддержка до 30.06.2027), агенты на все серверы, официальные шаблоны Windows by Zabbix agent и Windows services by Zabbix agent
2. Задаём триггеры по свободному месту и службам, зависимости триггеров, чтобы падение узла не порождало каскад алертов
3. Настраиваем эскалацию: шаг 1 - дежурный инженер, шаг 2 через 15 мин - второй уровень; минимальная длительность шага по докам - 60 с
4. В медиа штатного админа задаём период активности 1-5,09:00-18:00 - вне этого окна уведомления ему не отправляются
5. Плановые работы закрываем периодами обслуживания (maintenance), чтобы не генерировать ложные инциденты

РЕЗУЛЬТАТ

Ночные и выходные алерты уходят в нашу дежурную ротацию, а не в телефон одного человека. Штатный админ видит ту же картину в режиме наблюдателя, но получает уведомления только в свои рабочие часы. Каскадный шум давится зависимостями триггеров, поэтому реальные инциденты не тонут в потоке.

КЛЮЧЕВОЙ НЮАНС

Ключевое не в установке Zabbix, а в разделении получателей: период активности в media пользователя и шаги эскалации в действии - именно они снимают ночную нагрузку. Раздел Escalations и настройки user media.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Патчи и бэкапы: автоверификация вместо ручных проверок

Что настраиваем

Контур обновлений Windows-парка и резервное копирование на hardened repository под Linux

Как мы это делаем

1. Инвентаризация патч-контура: WSUS объявлен deprecated 20.09.2024 (новых функций нет, роль входит в Windows Server 2025), фиксируем план перехода на Azure Update Man…
2. Разносим кольца обновлений: пилот на тестовых PM, затем рабочие станции, серверы — в отдельное окно с ребутом
3. Бэкапы кладём на hardened repository (только Linux) с immutability: диапазон по докам 7-9999 дней, наш стандарт 14; срок пишется в .veeam.N.lock рядом с файлом бэка…
4. Учитываем отсчёт: период неизменяемости стартует от создания последней точки активной цепочки, поэтому фактическая защита длиннее номинала
5. Ставим SureBackup-задание на регулярную автоматическую проверку восстановимости — отчёт уходит в наш дайджест, а не в память админа

РЕЗУЛЬТАТ

Проверка бэкапа перестаёт быть задачей, которую человек делает, когда дойдут руки: восстановимость подтверждается заданием по расписанию. Патчи ставятся по кольцам в согласованные окна, а не аврально после инцидента. Отчёт по обоим контурам приходит одним письмом.

КЛЮЧЕВОЙ НЮАНС

Immutability работает только на hardened repository под Linux с одноразовыми креденшелами и без прав на удаление у учётки задания; на SMB-шаре флага неизменяемости нет. Раздел Hardened Repository.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Helpdesk и разграничение зон: GLPI 10 с SLA и OLA

Что настраиваем

Единая точка входа для 30-50 пользователей, правила маршрутизации между штатным админом и нашей командой

Как мы это делаем

1. Разворачиваем GLPI 10, заводим SLA с метриками TTO (время реакции) и TTR (время решения) по категориям заявок
2. На внутренние зоны ответственности заводим OLA: рутина L1 — штатному, серверы, сеть и ИБ — нашей команде
3. Добавляем escalation levels: за 1 ч до истечения TTR тикет автоматически меняет приоритет и переназначается на второй уровень
4. Включаем автоматическое действие slaticket (Настройки - Автоматические действия) и уведомление TicketRecall - просрочка не зависит от того, посмотрел ли кто-то в оч...
5. Wazuh 4.14 подключаем к тому же контуру: FIM с дефолтным <frequency>43200</frequency>, на серверных группах интервал сокращаем через агентские группы

РЕЗУЛЬТАТ

Заявки перестают жить в мессенджере и голове одного человека. Каждая категория имеет измеримое время реакции и решения, а просрочка эскалируется автоматически. Руководитель видит реальную нагрузку в цифрах, а не по фразе «всё нормально».

КЛЮЧЕВОЙ НЮАНС

SLA без OLA не разделяет ответственность: наружу клиенту обещается одно время, а внутренние переходы между исполнителями остаются неизмеримыми. Заводим оба уровня сразу.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- **Алерты идут всем и круглосуточно**
  Один список получателей без окон активности возвращает ночные звонки штатному админу. Разводим медиа по расписанию и эскалацию по шагам.
- **Шум алертов без зависимостей**
  Падение гипервизора рождает десятки триггеров. Настраиваем зависимости триггеров и периоды обслуживания на плановые работы.
- **Бэкап есть, восстановления не было**
  Успешное задание не равно восстановимости. Ставим SureBackup по расписанию и храним отчёт вне головы администратора.
- **Immutability на обычной шаре**
  Неизменяемость даёт только hardened repository под Linux с корректными правами; на SMB-шаре защиты от удаления нет.
- **Ставка на WSUS без плана ухода**
  Роль объявлена deprecated 20.09.2024: работает и поддерживается в Windows Server 2025, но новых функций не будет. Заранее закладываем миграцию патч-к…
- **Пароли и схема сети в одной голове**
  Уход админа обнуляет доступ. Ведём хранилище секретов с разграничением и актуализируем схему при каждом изменении.
- **Мониторинг без владельца триггера**
  Алерт без назначенного дежурного никто не берёт. В операции шага эскалации указываем конкретную группу пользователей, а не список всех получателей.
- **SLA без внутренних OLA**
  Ответственность между штатным и аутсорсом размывается. Разделяем категории заявок и внутренние сроки переходов.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Zabbix 7.0 LTS с шаблоном Windows by Zabbix agent на всех серверах и media-типом e-m…
- Бэкапы по расписанию под отдельной учёткой, репозиторий вне продуктивного домена
- Единая точка регистрации заявок (GLPI) вместо мессенджера, с категориями
- Хранилище паролей с разграничением доступа и актуальная схема сети

НОРМАЛЬНО

- Эскалация в 2 шага и окна активности медиа: ночью алерт не идёт штатному
- Hardened repository с immutability не менее 7 дней и задание SureBackup по расписанию
- Кольца обновлений с фиксированным окном перезагрузки серверов
- GLPI с SLA по TTO/TTR и категориями заявок

ХОРОШО

- Зависимости триггеров и периоды обслуживания против шума алертов
- OLA и автоэскалация уровней в GLPI, автодействие slaticket
- Wazuh 4.14: FIM и Vulnerability Detection, frequency под серверные группы
- План ухода с WSUS и дежурная ротация 24/7 на критичные инциденты

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Есть ли у вас окна активности уведомлений, чтобы ночные алерты не шли штатному админу?
- [ ] Настроена ли эскалация хотя бы в два шага с указанием конкретной группы на каждом шаге?
- [ ] Заданы ли зависимости триггеров, чтобы падение узла не рождало каскад алертов?
- [ ] Проверяется ли восстановимость бэкапа автоматическим заданием, а не вручную раз в квартал?
- [ ] Настроена ли неизменяемость точек восстановления и на какой срок (минимум по докам — 7 дней)?
- [ ] Может ли сервис-аккаунт задания удалить бэкапы из репозитория?
- [ ] Есть ли план ухода с WSUS (deprecated с 20.09.2024, новых функций не будет)?
- [ ] Измеряются ли TTO и TTR по категориям заявок, или сроки существуют только на словах?
- [ ] Разделены ли зоны штатного сотрудника и аутсорса внутренними OLA?
- [ ] Где лежат пароли и схема сети, если единственный админ завтра не выйдет?

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).

- Разворачиваем Zabbix 7.0 LTS с шаблонами, эскалацией по шагам и окнами активности медиа
- Ставим бэкапы на hardened repository с immutability и регулярной проверкой SureBackup
- Готовим патч-контур: кольца обновлений, окна перезагрузки, план ухода с WSUS
- Внедряем GLPI с SLA/OLA и разграничением зон между штатным админом и нашей командой
- Берём дежурство 24/7 на критичные инциденты и ведём актуальную документацию инфраструктуры

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. Configuration - Notifications - Actions - Escalations (zabbix.com — 7.0 LTS)

02 Zabbix Life Cycle and Release Policy (7.0 LTS: 30.06.2027 / 30.06.2029) (zabbix.com — 2024-2029)

03 Veeam B&R User Guide. Hardened Repository. How Immutability Works (helpcenter.veeam.com — 12.x)

04 Microsoft Learn. Deprecated features / WSUS deprecation (learn.microsoft.com — 2024)

05 Wazuh. Local configuration (ossec.conf): syscheck; Grouping agents (documentation.wazuh.com — 4.14)

06 GLPI Help Center. Service Levels (SLA/OLA), Automatic actions (help.glpi-project.org — 10.0)

07 Внутренний регламент ITfresh: гибридная модель и дежурство (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.