



Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

IT-инфраструктура офиса 20-50 РМ: как мы её строим

Наш стек: AD DS на WS2025, Proxmox VE 9.2, Veeam 13.1,
Zabbix 7.0 LTS, 3-2-1-1-0

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

Суть проблемы

К нам приходят офисы, где 1С стоит на рабочей станции бухгалтера, общие папки раскиданы по трём ПК, а «бэкап» — архив на том же диске. Мы приводим офис к предсказуемой схеме: домен AD DS, виртуализация, сегментированная сеть, копии по правилу 3-2-1-1-0 и мониторинг, который сообщает об отказе раньше пользователя. Укладываемся в 2-4 недели и одно окно простоя.

Почему это важно бизнесу

- Простой 1С на 30 человек стоит дороже всей серверной: считаем RTO/RPO до закупки, а не после аварии
- Без AD увольнение сотрудника не закрывает доступ к данным — блокировка учётки должна отзывать всё сразу
- Шифровальщик приходит через пользовательский ПК: спасает только неизменяемая офлайн-копия, а не RAID
- 152-ФЗ и приказ ФСТЭК № 21 требуют управления доступом и регистрации событий — это GPO, NTFS и журналы
- Предсказуемая инфраструктура снимает зависимость от «того самого админа, который всё знал»

Ключевые параметры реализации

RTO 4 ч

целевое время восстановления 1С и файлового сервера из бэкапа, закладываем в проект

Регламент внедрения ITfresh

RPO 1 ч

глубина потерь по 1С: полный дамп ночью + архив WAL каждый час

Регламент внедрения ITfresh

3-2-1-1-0

3 копии, 2 типа носителей, 1 копия вне офиса, 1 неизменяемая, 0 ошибок верификации

Наша схема резервирования

2 DC

минимум два контроллера домена на разных физических хостах — иначе домен = SPOF

Наш обязательный минимум

5 VLAN

mgmt/серверы/пользователи/гости/печать — базовая сегментация офиса

Наш типовой L2-дизайн

1 раз/кв

полное тестовое восстановление 1С и AD на изолированный стенд, с протоколом

Наш регламент обслуживания



Проектное бюро: пять «серверов» из десктопов сведены в один узел

Что настраиваем

Проектная организация, 38 рабочих мест, Москва, тяжёлые файлы CAD/BIM до 2 ГБ, домена и бэкапа не было

Как мы это делаем

- 1 Неделя 1: инвентаризация, замер IOPS и профиля доступа к шарам, схема VLAN, согласование окна простоя и матрицы RTO/RPO по сервисам
- 2 Неделя 2: хост Proxmox VE 9.2 (ZFS-зеркала NVMe под БД, RAIDZ2 SATA под архив), DC01 на Windows Server 2025, DNS AD-integrated, DHCP-failover
- 3 Неделя 3: миграция шар на FS01 с NTFS-правами только по группам, Shadow Copies каждые 2 часа (MaxShadowCopies поднят с 64, потолок 512), DFS-namespace
- 4 Неделя 4: Veeam B&R 13.1 на hardened-репозиторий Linux XFS с immutability, GFS 4 недели/12 месяцев, реплика в наш ЦОД, Zabbix 7.0 LTS с алертами в Telegram

РЕЗУЛЬТАТ

Домен вместо локальных учёток, единая точка выдачи прав, восстановление файла пользователем через «Предыдущие версии». Первое тестовое восстановление БД прошло по протоколу за 40 минут. Сеть разведена на 5 VLAN: гостевой Wi-Fi не видит серверный сегмент.

КЛЮЧЕВОЙ НЮАНС

Начинать надо не с сервера, а с замера профиля нагрузки: если бы мы взяли «мощный» SATA-RAID6 под тяжёлые файлы вместо ZFS-зеркал под БД и RAIDZ2 под архив, деньги ушли бы не туда.



Торговая компания: 1С в файловом режиме переведена в клиент-сервер

Что настраиваем

Оптовая торговля, 26 пользователей 1С, база УТ выросла до 180 ГБ, ежедневные блокировки и «зависания» проведения

Как мы это делаем

- 1 Разнесли роли: отдельная VM сервера 1С (8 vCPU / 24 ГБ) и отдельная VM СУБД PostgreSQL на NVMe, обе на одном хосте, но с разными дисковыми пулами
- 2 Настроили ночной полный дамп базы плюс архивацию WAL с интервалом 1 час — это и дало RPO в один час без остановки работы
- 3 Завели мониторинг Zabbix 7.0 LTS: очередь к диску, время отклика СУБД, свободное место в пулах, доступность службы 1С, триггеры в Telegram
- 4 Вынесли копии на отдельный репозиторий с неизменяемостью, чтобы шифровальщик с ПК бухгалтера не дотянулся до архивов

РЕЗУЛЬТАТ

Файловый режим убран как класс: конкурентная работа больше не упирается в блокировки на уровне SMB. Регламентные задания перенесены на ночное окно, дневной профиль нагрузки стал ровным. Инциденты «база не открывается» ушли, рост базы виден на графике заранее.

КЛЮЧЕВОЙ НЮАНС

Клиент-сервер на PostgreSQL закрывает потребность офиса до сотни пользователей, но только если СУБД реально живёт на NVMe и имеет свою VM — иначе получите те же тормоза, что и в файловом режиме.



Подводные камни

✗ Один контроллер домена

Смерть единственного DC останавливает вход, печать и доступ к шарам. Мы ставим второй DC на другом хосте и разносим FSMO.

✗ Бэкап на тот же массив

RAID — не резервная копия. Нужен отдельный носитель, копия вне офиса и хотя бы одна неизменяемая или офлайн-копия.

✗ Бэкап без тестов восстановления

Задание «зелёное», а база не поднимается. Мы восстанавливаем 1C и AD на изолированный стенд раз в квартал с протоколом.

✗ Плоская сеть без VLAN

Гостевой Wi-Fi, камеры и серверы в одном broadcast-домене. Любое заражённое устройство видит SMB на файловом сервере.

✗ Права раздаются на пользователей

Через год NTFS-права нечитаемы, а увольнение никого ни от чего не отрезает. Только доменные группы и наследование.

✗ ИБП без корректного выключения

Батарея есть, а агента выключения нет: при разряде хост гаснет по питанию и ломает базу. Настраиваем shutdown по порогу заряда.

✗ Мониторинг «по звонку пользователя»

Без Zabbix отказ диска, разросшийся лог или сдохший бэкап видны только постфактум. Агент — на все серверы и на шлюз.

✗ Локальный админ с общим паролем

Один пароль на всём парке = одна украденная хеш-строка на всю сеть. Ставим Windows LAPS и выключаем SMBv1.



Как правильно

МИНИМУМ

- Домен AD DS на Windows Server 2025, второй DC на другом хосте, AD-integrated DNS
- Veeam (Community Edition — до 10 инстансов) на отдельный носитель плюс офлайн-копия
- Управляемый коммутатор и минимум 3 VLAN: серверы, пользователи, гости
- ИБП на серверную с агентом корректного выключения хоста и NAS

НОРМАЛЬНО

- Гипервизор Proxmox VE 9.2 или Hyper-V, роли разнесены по ВМ, снапшот перед работами
- 1С в клиент-сервере на PostgreSQL, СУБД на NVMe, WAL-архив с RPO 1 час
- Zabbix 7.0 LTS: агенты на серверах, SNMP с коммутатора и ИБП, алерты в Telegram
- Shadow Copies на шарах каждые 2 часа, права только через доменные группы

ХОРОШО

- Hardened-репозиторий на Linux XFS с immutability и GFS 4 недели / 12 месяцев
- Реплика ВМ в наш ЦОД, отработанный план переключения с замеренным RTO
- Windows LAPS, отдельные учётки администрирования, запрет SMBv1, SMB signing
- 5 VLAN с ACL на L3, WireGuard для удалёнки, сертификаты вместо паролей



Чек-лист самопроверки

- | | |
|---|--|
| ☐ Зафиксированы RTO и RPO по каждому сервису и подписаны заказчиком до закупки железа | ☐ Резервные копии соответствуют 3-2-1-1-0, есть неизменяемая копия вне периметра офиса |
| ☐ Два контроллера домена на разных хостах, FSMO разнесены, AD-integrated DNS проверен dcdiag | ☐ Тестовое восстановление 1С и файлового сервера выполнено и оформлено протоколом |
| ☐ DHCP настроен в failover, резервирования и области выгружены, аренда согласована с VLAN | ☐ Zabbix закрывает хосты, ВМ, коммутатор, ИБП и сами задания бэкапа, алерты доходят в Telegram |
| ☐ Файловые права выданы только доменным группам, наследование не сломано, есть карта доступа | ☐ ИБП рассчитан на корректное выключение, батареи протестированы, дата замены в паспорте |
| ☐ Shadow Copies включены на шарах, MaxShadowCopies поднят с дефолтных 64 под нужную глубину | ☐ Паспорт сети сдан: схема VLAN, IP-план, маркировка портов, пароли — в зашифрованном хранилище |

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).

- Проводим аудит и считаем RTO/RPO, отдаём схему и смету по трём уровням: минимум, норма, хорошо
- Разворачиваем домен, виртуализацию и 1С клиент-сервер, мигрируем данные в одно окно простоя
- Настраиваем Veeam с неизменяемым репозиторием и репликой в наш ЦОД, проверяем восстановление
- Подключаем ваш офис к нашему Zabbix 7.0 LTS: дежурный видит алерт раньше, чем пользователь
- Ведём инфраструктуру на аутсорсе: регламентные работы, обновления, документация и паспорт сети

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** Windows Server 2025: жизненный цикл и функциональные уровни AD DS (learn.microsoft.com — 2026)
- 02** Registry Keys for Backup and Restore: MaxShadowCopies (64, макс. 512) (learn.microsoft.com — 2026)
- 03** Zabbix Life Cycle: 7.0 LTS — полная поддержка до 30.06.2027 (zabbix.com — 2026)
- 04** KB4738: Release Information for Veeam B&R 13 (13.1, июль 2026) (veeam.com — 2026)
- 05** Veeam Community Edition: ограничение 10 инстансов (veeam.com — 2026)
- 06** Proxmox VE 9.2 release notes: Debian 13.5, ZFS 2.4, QEMU 11 (proxmox.com — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.

