



Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Резервная копия файлового сервера: наша схема 3-2-1

Veeam B&R 13, снимоты VSS/ZFS, restic в S3,
hardened-репозиторий, автотесты восстановления

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

Суть проблемы

Файловый сервер — единая рабочая память компании: договоры, первичка, макеты, архивы. Мы регулярно принимаем инфраструктуры, где «бэкап» — это копия на втором диске того же сервера, и при тестовом восстановлении она не читается. Отказ RAID или шифровальщик в такой схеме — недели простоя. Разбираем нашу типовую схему 3-2-1 с immutable-копией и автотестами восстановления.

Почему это важно бизнесу

- Простой файлового сервера останавливает продажи, бухгалтерию и юристов одновременно — RTO напрямую конвертируется в потерянную выручку
- Шифровальщик без immutable-копии вне домена — это выбор между выкупом и потерей архива за годы работы
- Без снимотов удалённый файл восстанавливает инженер часами; со снимотами — сам пользователь за минуты
- Непроверенный бэкап даёт ложное чувство защищённости: правда выясняется в момент аварии, когда исправлять поздно



Ключевые параметры реализации

13.0.2

актуальная сборка Veeam B&R 13 (build 13.0.2.29): Linux software appliance, а с 13.0.1 доступн...

Veeam KB4738, 2026

3-2-1-1-0

наша схема хранения: 3 копии, 2 носителя, 1 оффсайт, 1 неизменяемая, 0 ошибок верификации

наш стандарт по докам Veeam

60 мин

интервал инкрементов Veeam на локальный репозиторий — RPO не хуже часа для офисных данных
наш стандарт (RPO)

7-30 дн

период неизменяемости Linux Hardened Repository (XFS + immutable-флаг) против шифровальщика; м...

по докам Veeam

64

максимум теневых копий VSS на том для «Предыдущих версий» — закладываем 3 снимка/день на ~3 не...

по докам Microsoft VSS

0.19.1

restic для оффсайт-копии в S3: AES-256 шифрование на клиенте, дедупликация блоков и сжатие

restic.net, июль 2026



Локальный контур: Veeam B&R и hardened-репозиторий

Что настраиваем

Файловый сервер Windows/Hyper-V + отдельный бэкап-узел (Linux-сервер или NAS) в другом помещении

Как мы это делаем

- 1 Разворачиваем Veeam B&R 13 (software appliance или установка на Windows Server); под репозиторий — отдельный Linux-хост: XFS с reflink=1, роль Hardened Repository,...
- 2 Джоб на файловый сервер: forward incremental каждые 60 минут, synthetic full по субботам, GFS-етенция 14 дней + 8 недель + 6 месяцев
- 3 Еженедельный health check (storage-level corruption guard) + шифрование бэкапа паролем из нашего менеджера секретов
- 4 Учётка репозитория — single-use credentials вне домена, без доменного админа; SSH на репозитории после деплоя отключаем
- 5 SureBackup: ежемесячный автозапуск ВМ из бэкапа в изолированной virtual lab, отчёт о boot-тесте — инженеру и директору клиента

РЕЗУЛЬТАТ

Локальная точка восстановления не старше часа; повреждение цепочки ловится health check'ом до аварии, а не во время неё. Immutable-репозиторий переживает компрометацию домена: даже с правами администратора нельзя удалить или перезаписать точки восстановления в течение периода неизменяемос...

КЛЮЧЕВОЙ НЮАНС

Hardened Repository по докам Veeam требует нерутового пользователя и отключённого SSH после установки — если оставить root-доступ «для удобства», защита бэкапов от удаления превращается в фикцию.



Оффсайт: шифрованная копия в S3 через restic

Что настраиваем

Российское S3-совместимое объектное хранилище; источник — файловый сервер или его реплика на NAS

Как мы это делаем

- 1 Инициализируем репозиторий: `restic -r s3:<endpoint>/<bucket> init`; пароль репозитория и ключи доступа — только в менеджере секретов, не в скриптах
- 2 Ночной systemd-timer: `restic backup` с `--exclude-file` для временных файлов; в облако уходят только изменённые блоки (дедупликация + сжатие)
- 3 Ретенция еженедельно: `restic forget --keep-daily 30 --keep-weekly 12 --keep-monthly 12`; `prune` — отдельным ежемесячным заданием в своё окно
- 4 Ежемесячно `restic check --read-data-subset=5%` — реально вычитываем часть данных из облака, а не только метаданные
- 5 Ключ S3 — отдельный сервисный, с политикой только на бакет бэкапов; на бакете включено версионирование против перезаписи

РЕЗУЛЬТАТ

Оффсайт-копия зашифрована до отправки — провайдер видит только зашифрованные блоки. Первичная загрузка 1 ТБ — одна ночь, дальше инкременты по 5-20 ГБ. При пожаре или краже железа восстанавливаемся из облака на любое новое железо, включая арендованный сервер.

КЛЮЧЕВОЙ НЮАНС

`restic forget` без `prune` не освобождает место — данные остаются в репозитории и счёт за хранилище растёт; `prune` гоняем отдельным окном: он тяжёлый по трафику и числу API-запросов к S3.



Снапшоты и мониторинг: VSS, ZFS и контроль свежести

Что настраиваем

Том с общими папками на Windows Server + Linux/NAS-реплика; наш Zabbix-контур мониторинга

Как мы это делаем

- 1 Включаем VSS на томе данных: хранилище 15% тома, расписание 07:00/12:00/17:00 — пользователи сами достают файлы через «Предыдущие версии»
- 2 На ZFS-реплике — снапшоты по расписанию через sanoid: hourly×24, daily×30; они read-only и недоступны для изменения через SMB
- 3 Репликация на резервный узел: DFS-R для Windows (staging quota считаем от 32 крупнейших файлов) или rsync+lsyncd на Linux
- 4 Zabbix: триггеры на возраст последней успешной точки (старше 26 ч — авария), статус джобов Veeam, свободное место репозитория менее 20%
- 5 Квартальный регламент: восстановление случайного файла и целой VM на стенд с замером фактического RTO; результат — в паспорт клиента

РЕЗУЛЬТАТ

До 80% обращений «случайно удалил файл» закрывают сами пользователи за минуты без инженера. Мониторинг превращает бэкап из «настроили и забыли» в контролируемый сервис: о протухшей копии мы узнаём в день сбоя из алерта, а не через месяцы — на аварии.

КЛЮЧЕВОЙ НЮАНС

Репликация (DFS-R, lsyncd) — не бэкап: удаление и шифрование файлов уезжают на реплику за секунды. Реплика работает только в паре со снапшотами с ретенцией на принимающей стороне.



Подводные камни

✗ Бэкап на диске того же сервера

Умирает вместе с RAID-контроллером и шифруется вместе с оригиналом. Минимум — отдельный узел в другом помещении плюс обязательная оффсайт-копия.

✗ Реплика вместо бэкапа

DFS-R и Isyncd мгновенно тиражируют и удаление, и шифрование. Реплику всегда дополняем снапшотами с ретенцией на принимающей стороне.

✗ Одна учётка на всё

Доменный админ с доступом к бэкапам — шифровальщик удалит и их. Репозиторий держим вне домена, со своими кредами и периодом неизменяемости.

✗ Восстановление никогда не тестировали

Битая цепочка видна только при restore. Закладываем health check еженедельно, SureBackup или тест на стенде — ежемесячно, с отчётом.

✗ Облако без клиентского шифрования

Данные лежат у провайдера открытым текстом. restic и Veeam шифруют до отправки; пароль репозитория храним отдельно от самого сервера.

✗ Ретенция «пока есть место»

Репозиторий заполняется — джобы молча падают. Считаем ёмкость: full + инкременты × срок хранения × прирост ~20%/год, алерт на <20% свободного.

✗ Надежда на теньевые копии Windows

Малварь с правами администратора штатно удаляет VSS-снимки. Это сервис удобства пользователей; последняя линия — immutable-копия вне домена.



Как правильно

МИНИМУМ

- Veeam Community Edition (до 10 рабочих нагрузок) + ежедневный бэкап на NAS в другом...
- Ночная копия в S3-облако через restic с шифрованием на клиенте
- Снапшоты VSS 3 раза в день на томе с общими папками
- Ручной тест восстановления файла раз в квартал с записью результата

НОРМАЛЬНО

- Veeam B&R: инкременты каждый час + synthetic full, GFS-ретенция 14д/8н/6м
- Hardened-репозиторий на Linux вне домена, immutability 14 дней
- restic в облако ежедневно + restic check --read-data-subset ежемесячно
- Zabbix-контроль возраста точек, статуса джобов и места в репозитории

ХОРОШО

- SureBackup: ежемесячный автотест загрузки VM из бэкапа в изолированной среде
- S3 с версионированием/Object Lock и отдельным сервисным ключом на бакет
- Горячая реплика (DFS-R или rsync+lsyncd) + ZFS-снапшоты на приёмнике
- Паспорт восстановления: замеренные RPO/RTO, runbook и годовые DR-учения



Чек-лист самопроверки

- | | |
|---|---|
| ☐ Есть ли копия вне офиса, которая переживёт пожар или кражу серверной? | ☐ Шифруется ли облачная копия до отправки и хранится ли пароль репозитория отдельно от сервера? |
| ☐ Есть ли хотя бы одна копия, которую нельзя удалить даже с правами администратора домена (immutable)? | ☐ Отделены ли учётные данные бэкап-системы от доменных административных? |
| ☐ Известен ли фактический RPO: какого возраста будет последняя точка, если сервер упадёт прямо сейчас? | ☐ Приходит ли алерт при падении джоба и при устаревании последней копии более чем на сутки? |
| ☐ Замерен ли RTO на практике: за сколько часов сервер реально поднимается из бэкапа на стенде? | ☐ Могут ли пользователи сами вернуть вчерашний файл через «Предыдущие версии», не дёргая инженера? |
| ☐ Проводился ли за последний квартал тест восстановления с документированным результатом? | ☐ Хватит ли места в репозитории на рост данных в ближайший год? |

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).

- Аудит текущих бэкапов за 1 день: тестовое восстановление, замер RPO/RTO, письменный отчёт с приоритетами
- Внедрение схемы 3-2-1 под ключ: Veeam B&R + hardened-репозиторий + restic в российское S3-облако
- Настройка снапшотов VSS/ZFS и самообслуживания пользователей через «Предыдущие версии»
- Мониторинг бэкапов в Zabbix с алертами в Telegram и ежемесячным отчётом руководителю
- Квартальные тесты восстановления и DR-учения с замером фактического времени подъёма

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** Veeam B&R 13 User Guide — Hardened Repository, SureBackup (helpcenter.veeam.com — v13)
- 02** Veeam KB4738 — Release Information for Veeam B&R 13 (veeam.com — 2026)
- 03** restic Docs — Backing up, Removing snapshots, check (restic.readthedocs.io — 0.19.1)
- 04** Volume Shadow Copy Service — лимиты и настройка (learn.microsoft.com — 2025)
- 05** DFS Replication — staging folder guidance (learn.microsoft.com — 2025)
- 06** OpenZFS — zfs-snapshot(8), zfs-send(8) (openzfs.github.io — 2.3)
- 07** Наш шаблон «Паспорт резервного копирования клиента» (itfresh.ru — 2026)

