



Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Файловое хранилище для офиса: NAS, S3 или облако в 2026

Наша схема: Synology DSM 7.2, MinIO с erasure coding,
Nextcloud 34 и бэкап 3-2-1 с Object Lock

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

Суть проблемы

Офис на 10–50 PM хранит договоры и проекты на стареющем NAS или «шаре» на чьём-то ПК: RAID 5, бэкап на тот же диск, веб-интерфейс наружу. Один умерший диск или шифровальщик — простой на дни и безвозвратная потеря архива за годы. Разбираем, как мы выбираем и строим хранилище под задачи: NAS Synology, свой S3 на MinIO или облако с локальным кэшем.

Почему это важно бизнесу

- Простой файлового сервера останавливает всех: бухгалтерию, проекты, продажи — час простоя офиса на 30 PM дороже любого диска
- Шифровальщик через открытый NAS-интерфейс уносит и данные, и «бэкап» на том же массиве — восстанавливать нечего
- Переплата за неподходящую архитектуру: облако на терабайтах CAD за 5 лет выходит в разы дороже своего сервера
- Уволенные сотрудники с живым доступом к файлам — прямой риск утечки клиентской базы и договоров

Ключевые параметры реализации

ЕС:4

дефолтная чётность erasure coding
MinIO для пулов от 8 дисков:
данные читаются при отказе
любы...

MINIO_STORAGE_CLASS_STANDARD, доки MinIO

7.2

версия DSM, с которой доступны
неизменяемые (Immutable)
снапшоты на Btrfs — обновляем до
ввода...

Synology Snapshot Replication

60 мин

интервал снапшотов рабочих шар,
хранение 30 дней — окно отката
при шифровальщике

наш стандарт

3-2-1

схема бэкапа: локальная копия +
Hyper Backup в S3 вне офиса;
восстановление проверяем
ежемесяч...

наш стандарт + Hyper Backup

34

Nextcloud Hub 26 Spring: ставим
только поддерживаемые ветки
(32/33/34), поддержка 34-й — до
ию...

nextcloud, Maintenance and Release Schedule

10 Гбит/с

сеть до сервера хранения: SFP+
линк и SMB Multichannel, иначе
рендеры и CAD упрутся в
гигабит

наш стандарт



NAS Synology под документы: DSM 7.2, Btrfs и WORM-снапшоты

Что настраиваем

Офисы 15–35 PM: DS923+/DS1522+, 4–5 дисков в SHR-2, ввод в AD-домен, доступ снаружи только через VPN

Как мы это делаем

- 1 Собираем пул SHR-2 на Btrfs (переживает отказ 2 дисков), включаем контрольные суммы данных и ежемесячный data scrubbing
- 2 Включаем Snapshot Replication: снапшоты рабочих шар раз в 60 мин, хранение 30 дней, флаг Immutable Snapshots — их не удалит даже администратор DSM
- 3 Заводим NAS в AD: доступ по доменным группам, SMB3 с шифрованием, отключаем SMB1 и гостевой доступ
- 4 Hyper Backup в S3: ежедневное задание с клиентским шифрованием AES-256, ротация Smart Recycle, ежемесячная проверка целостности архива
- 5 Закрываем периметр: QuickConnect выключен, порты 5000/5001 наружу не пробрасываем, вход извне только через VPN, 2FA для администраторов DSM

РЕЗУЛЬТАТ

Отказ любых двух дисков не останавливает работу — замена на горячую. Шифровальщик или ошибочное удаление откатываются снапшотом за минуты, а не восстановлением из бэкапа за часы. Копия вне офиса закрывает сценарии пожара и кражи железа.

КЛЮЧЕВОЙ НЮАНС

Ключевое в доке Synology: неизменяемые снапшоты работают только на Btrfs и DSM 7.2+, а Hyper Backup не заменяет снапшоты — это разные слои защиты с разным временем восстановления.



S3-хранилище MinIO: erasure coding и Object Lock

Что настраиваем

Офисы 25–50 PM с бэкапами и интеграциями: 2U-сервер на 8–12 дисков, репозиторий Veeam, файлы 1С и CRM по S3 API

Как мы это делаем

- 1 Разворачиваем MinIO в режиме single-node multi-drive: диски отдаём как JBOD без RAID-контроллера, erasure coding сам считает чётность
- 2 Фиксируем класс хранения `MINIO_STORAGE_CLASS_STANDARD=EC:4` и включаем versioning на бакетах — перезапись и удаление файлов обратимы
- 3 Для бэкап-бакета включаем Object Lock в режиме COMPLIANCE на 30 дней: копии не удалит никто, включая root-учётку
- 4 Жизненный цикл через `mc ilm rule add` с `--noncurrent-expire-days 90`: неактуальные версии старше 90 дней удаляются, бакет не разрастается бесконтрольно
- 5 Мониторим endpoint `/minio/v2/metrics/cluster` в Prometheus/Zabbix: свободное место, статус healing, деградация дисков

РЕЗУЛЬТАТ

S3-эндпоинт внутри офиса: Veeam пишет бэкапы в immutable-репозиторий, 1С и портал хранят файлы по API. При EC:4 на 8 дисках отказ до 3 дисков переживается без остановки записи, при 4 отказавших данные ещё читаются. Шифровальщик не портит бэкапы даже с украденными ключами доступа.

КЛЮЧЕВОЙ НЮАНС

После разделения продукта на community и AIStor веб-консоль в бесплатной сборке урезана — закладываем управление через `mc` CLI и скрипты, а не кнопки в браузере, и фиксируем версию релиза в `docker-compose`.



Nextcloud 34 как файловый портал с AD и офисным редактором

Что настраиваем

Распределённые команды: Docker-стек Nextcloud 34 + PostgreSQL + Redis, до 50 пользователей, SSO из AD

Как мы это делаем

- 1 Ставим Nextcloud 34 (Hub 26 Spring) в Docker: PHP 8.3, PostgreSQL 16, Redis под memcache.locking — без него совместная работа ловит конфликты блокировок
- 2 Подключаем AD через user_ldap: фильтр по группе доступа, автодеактивация уволенных при выпадении из группы
- 3 Интегрируем ONLYOFFICE Docs: совместное редактирование DOCX/XLSX в браузере, JWT-секрет между сервисами
- 4 Фоновые задания переводим на системный cron раз в 5 минут, превью генерируем по расписанию ночью
- 5 Большие шары отдаём через External Storage (SMB к NAS) — портал един, тяжёлые CAD-файлы не переезжают внутрь портала

РЕЗУЛЬТАТ

Удалёнка работает с файлами по HTTPS без VPN-тормозов: desktop-клиент синхронизирует локальную копию, правки уходят фоном. Учётные записи едины с доменом — увольнение в AD мгновенно отзывает доступ к файлам.

КЛЮЧЕВОЙ НЮАНС

По докам Nextcloud держимся только поддерживаемых веток и обновляемся строго последовательно по мажорным версиям (32→33→34) — прыжок через версию ломает миграции базы.



Подводные камни

✗ RAID 5 на дисках 8 ТБ+

Ребилд большого диска идёт сутки и добивает соседний. Ставим SHR-2/RAID 6 либо erasure coding с чётностью не ниже EC:2.

✗ NAS-интерфейс наружу

QuickConnect и проброс портов 5000/5001 — главный вектор шифровальщиков. Доступ извне только через VPN, администраторам — 2FA.

✗ Снапшоты без Immutable

Шифровальщик с правами администратора удаляет обычные снапшоты вместе с данными. Включаем Immutable Snapshots DSM 7.2 на критичных шарах.

✗ Versioning вместо бэкапа

Версии в MinIO/Nextcloud живут на том же массиве. Отдельная копия вне офиса по 3-2-1 обязательна — пожар и кража железа забирают всё.

✗ MinIO поверх RAID-контроллера

Erasure coding требует прямого доступа к дискам: RAID под ним прячет отказы и ломает healing. Диски отдаём в JBOD/HBA-режиме.

✗ Nextcloud без Redis-блокировок

Без memcache.locking параллельное редактирование даёт ошибки «file is locked». Redis ставим сразу, в одном стеке с порталом.

✗ Бэкап без тестового восстановления

Битые архивы находят в день аварии. Ежемесячно восстанавливаем контрольную папку и сверяем суммы — по календарю, а не «по возможности».

✗ Учётки без отзыва

Уволенные сохраняют доступ месяцами. Права только через группы AD: блокировка учётки гасит NAS, портал и S3-ключи разом.

Как правильно

МИНИМУМ

- NAS на Btrfs с SHR-2/RAID 6, никакого RAID 5 на дисках от 8 TB
- Снапшоты раз в час с хранением 30 дней на всех рабочих шарах
- Доступ снаружи только через VPN, веб-интерфейс наружу закрыт
- Ежедневный бэкап в S3 вне офиса с шифрованием на стороне клиента

НОРМАЛЬНО

- Immutable-снапшоты (WORM) на критичных шарах, 2FA для администраторов
- Права через группы AD, квартальная сверка учёток со штатом
- Object Lock COMPLIANCE 30 дней на бэкап-бакете S3
- Мониторинг места, SMART и статуса RAID/healing с алертами в Telegram

ХОРОШО

- MinIO с EC:4 под бэкапы и S3-интеграции, Nextcloud 34 как портал с AD SSO
- Сеть 10 Гбит/с до хранилища для CAD/медиа, SSD-кэш под метаданные
- Ежемесячное тестовое восстановление с протоколом по календарю
- ILM-политики mc ilm rule add: неактуальные версии старше 90 дней — в expiration, арх...



Чек-лист самопроверки

- | | |
|---|---|
| ☐ Переживёт ли массив одновременный отказ двух дисков — проверяли на практике, а не по паспорту? | ☐ Отзывается ли доступ к файлам автоматически при блокировке учётной записи в AD? |
| ☐ Закрыт ли веб-интерфейс NAS и панелей из интернета, а VPN — единственный вход снаружи? | ☐ Кто получает алерт при деградации диска и через сколько минут после события? |
| ☐ Есть ли неизменяемые снапшоты или Object Lock, которые не удалит даже администратор? | ☐ Хватит ли места на 12 месяцев вперёд при текущем приросте данных? |
| ☐ Лежит ли вторая копия данных физически вне офиса и шифруется ли она до отправки? | ☐ Есть ли у вас пароли и документация от собственного хранилища, а не только у подрядчика? |
| ☐ Когда последний раз реально восстанавливали файлы из бэкапа и есть ли протокол проверки? | |

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 хранения: объёмы, прирост, узкие места сети, состояние RAID и бэкапов — с письменным отчётом
- Внедрение под ключ: NAS Synology, сервер MinIO/Nextcloud или гибрид — от закупки железа до передачи паролей
- Миграция без простоя: перенос шар, прав и версий со старого NAS или сервера на новое хранилище
- Защита данных: WORM-снапшоты, Object Lock, VPN-периметр, бэкап 3-2-1 с ежемесячной проверкой восстановления
- Мониторинг 24/7: место, SMART, RAID, healing — алерты в Telegram, реакция по SLA

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** Erasure Coding — MinIO Documentation (docs.min.io — 2026)
- 02** Erasure Code Settings (MINIO_STORAGE_CLASS_STANDARD) (docs.min.io — 2026)
- 03** mc ilm rule add — Object Lifecycle Management (docs.min.io — 2026)
- 04** Snapshot Replication — Technical Specifications (synology.com — DSM 7.2)
- 05** Hyper Backup — резервное копирование в S3 (kb.synology.com — DSM 7.2)
- 06** Nextcloud Admin Manual: установка и LDAP/AD (docs.nextcloud.com — 34)
- 07** Nextcloud Maintenance and Release Schedule (github.com/nextcloud — 2026)
- 08** Шаблон ITfresh: чек-лист ввода хранилища в строй (itfresh.ru — 2026)

