



Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

MinIO S3 в офисе: 20 ТБ бэкапов и архива на объектнике

Наша схема: erasure coding на JBOD, Object Lock под Veeam,
репликация на вторую площадку

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

Суть проблемы

Архив и бэкапы на 20 ТБ живут на iSCSI-полке и SMB-шарах: место кончилось, восстановление идёт часами, а шифровальщик, добравшийся до сервера бэкапов, удаляет копии вместе с боевыми данными — шара смонтирована под учёткой, права снимаются. Мы переводим объём на свой S3-объектник MinIO: один HTTPS-эндпоинт для Veeam, WAL-G, Nextcloud и архива, неизменяемость на уровне протокола.

Почему это важно бизнесу

- Одна атака на файловый сервер обнуляет и данные, и бэкапы: шара доступна той же учётке, что и боевые каталоги
- Облачный S3 на 20 ТБ — постоянный ежемесячный платёж плюс плата за исходящий трафик при каждом восстановлении
- Простой без архива дел, почты и баз считается днями: суд, ФНС и контрагенты сроков не сдвигают
- Хранение документов и переписки 5–7 лет требуется законом, а неизменность на обычной шаре доказать нечем
- Каждый новый сервис просит свою шару и свои права; один S3-эндпоинт убирает зоопарк доступов



Ключевые параметры реализации

EC:4

Дефолт для набора от 8 дисков;
MINIO_STORAGE_CLASS_STANDARD
задаём явно, а не молчанием
по докам MinIO, storage class

50 %

Потолок parity — половина erasure
set: на 16 дисках выше EC:8 задать
нельзя
по докам MinIO, erasure coding

XFS + JBOD

Диск = отдельный том XFS,
контроллер в HBA: RAID, LVM и
сетевые ФС доки не рекомендуют
по докам MinIO, storage requirements

2025-10-15

Последняя community-сборка
RELEASE.2025-10-15T17-29-55Z;
репозиторий с апреля 2026
архивный
офиц. релизы сервера MinIO

1-999 дн.

Диапазон иммутабельности
объектного репозитория Veeam;
ставим 30 суток на суточные копии
по докам Veeam B&R 13

30 сут

Наш дефолт GOVERNANCE на
бакете бэкапов: перекрывает окно
обнаружения инцидента
наш стандарт



Узел хранения: диски, файловая система, служба

Что настраиваем

Один физический сервер, Debian 12, режим Single-Node Multi-Drive: 8 HDD в JBOD, NVMe-зеркало под ОС, служба под systemd

Как мы это делаем

- 1 Контроллер переводим в HBA/passthrough: MinIO ждёт прямые диски, все тома одной ёмкости и модели — разнокалиберный пул доки запрещают
- 2 Каждый диск размечаем в XFS, монтируем по UUID в /mnt/disk1..8, в MINIO_VOLUMES задаём шаблон /mnt/disk{1...8} — фигурные скобки разворачивает сервер
- 3 Фиксируем MINIO_STORAGE_CLASS_STANDARD=EC:4 в /etc/default/minio; MINIO_ROOT_USER и MINIO_ROOT_PASSWORD — там же, файл 0640, владелец minio-user
- 4 TLS-пару public.crt/private.key кладём в certs-каталог службы (\${HOME}/.minio/certs); наружу — только S3-порт, --console-address и SSH из служебной подсети
- 5 Приёмка: mc admin info, тестовый PUT/GET, /minio/health/live; управление ведём через mc admin — веб-консоли управления в community-сборке нет

РЕЗУЛЬТАТ

Набор из 8 дисков с EC:4 переживает отказ четырёх: объекты читаются, для записи нужно 5 живых томов — устойчивость выше RAID-6 и без RAID-контроллера. Ёмкость возвращается фоновым хилингом, без суточного ребилда массива и окна обслуживания.

КЛЮЧЕВОЙ НЮАНС

Parity задаём числом, а не молчанием: дефолт зависит от размера erasure set (EC:2 до 5 дисков, EC:3 на 6–7, EC:4 от 8), и при расширении пула эффективная ёмкость меняется незаметно.



Иммутабельные бэкапы: Object Lock под Veeam

Что настраиваем

Бакет `veeam-backups` как S3 Compatible репозиторий Veeam B&R; отдельный сервисный ключ, сетевой доступ только с сервера бэкапа

Как мы это делаем

- 1 Бакет создаём сразу командой `mc mb --with-lock: Object Lock` включается только при создании, задним числом его не накинута
- 2 Дефолтная политика: `mc retention set --default GOVERNANCE 30d alias/veeam-backups;` для юридического архива тот же механизм, но режим COMPLIANCE
- 3 В Veeam ставим флаг иммутабельности репозитория: бакету нужны и `versioning`, и `object lock`, иначе мастер добавления S3 его отклонит
- 4 Lifecycle-правила на бакет Veeam не вешаем — ретеншеном по докам управляет только Veeam, ILM ломает цепочки бэкапа и восстановления
- 5 Сервисному ключу выдаём политику без `s3:BypassGovernanceRetention` и без `s3>DeleteBucket`: снять GOVERNANCE-замок скомпрометированной учёткой нельзя

РЕЗУЛЬТАТ

Даже при полном захвате сервера бэкапа копии в пределах срока ретеншена нельзя ни удалить, ни перезаписать: под COMPLIANCE это запрещено всем, включая `root`-учётку хранилища. Ежедневная точка восстановления перестаёт зависеть от целостности одной Windows-машины.

КЛЮЧЕВОЙ НЮАНС

GOVERNANCE — управляемая иммутабельность: её снимает обладатель права обхода. Если ключ бэкапа получил `s3:BypassGovernanceRetention` «на всякий случай», защита от шифровальщика становится декорацией.



Вторая площадка, репликация и жизненный цикл

Что настраиваем

Второй узел MinIO в удалённом офисе; асинхронно реплицируем archive-docs, mail-archive и pg-wal-g через приватный туннель

Как мы это делаем

- 1 Versioning включаем на обеих сторонах до первой записи: без него репликация бакета не поднимется, а маркеры удаления поедут некорректно
- 2 mc replicate add с флагами delete, delete-marker и existing-objects — исторические объекты не уедут, пока existing-objects не указан явно
- 3 mc admin replicate add поднимаем только на чистой второй площадке: по докам данные при старте могут быть лишь на одном узле связи
- 4 Первичный сид 20 ТБ по узкому каналу не гоним: снимаем офлайн-копию, увозим носитель, дельту догоняем репликацией
- 5 ILM: mc ilm rule add с --expire-days и --noncurrent-expire-days отдельно, чтобы старые версии не съели ёмкость молча

РЕЗУЛЬТАТ

Критичные бакеты живут в двух зданиях с задержкой в десятки секунд, а рост ёмкости становится управляемым: неактуальные версии и просроченные объекты уходят по правилу, а не по звонку про заканчивающееся место.

КЛЮЧЕВОЙ НЮАНС

Репликация не заменяет ретеншен: удаление, размноженное на вторую площадку, — это тоже репликация. Иммутабельность и вторая копия решают разные задачи и нужны обе.



Подводные камни

✗ Object Lock «включим потом»

Замок задаётся при создании бакета; на существующем включается только versioning. Бакет бэкапов заводим сразу через `mc mb --with-lock`.

✗ ILM поверх бакета Veeam

Lifecycle-правила конфликтуют с ретеншеном Veeam и рвут цепочки восстановления. Автоочистку оставляем только на архивных бакетах.

✗ MinIO поверх RAID, LVM или NAS

Erasure coding уже даёт избыточность, второй слой съедает ёмкость и предсказуемость. Отдаём диски напрямую, XFS на каждый том.

✗ Ключ бэкапа с правом обхода

`s3:BypassGovernanceRetention` у сервисного ключа обнуляет смысл WORM. Право оставляем только выделенной админ-учётке хранилища.

✗ Версии копятя без правил

Versioning без `--noncurrent-expire-days` тихо удваивает объём на активных бакетах. Ставим правило одновременно с включением версий.

✗ Плавающая версия сервера

Репозиторий community архивирован в апреле 2026, новых сборок нет. Пинуем RELEASE.2025-10-15 и держим план перехода на поддерживаемую сборку.

✗ Диски разной ёмкости в пуле

Набор выравнивается по меньшему диску, лишние терабайты пропадают. Закупаем идентичные модели и держим 1-2 в холодном резерве.

✗ Нет процедуры чтения без сервера

На дисках лежат EC-шарды, отдельный файл руками не собрать. Держим документированный порядок подъёма пустого узла на тех же томах.



Как правильно

МИНИМУМ

- Отдельный узел, XFS на каждом диске, MINIO_VOLUMES по шаблону, служба под systemd
- Versioning и Object Lock на бакете бэкапов включены до первой записи
- Сервисные ключи по бакетам, root-креды приложениям не выдаём
- TLS на S3-эндпоинте, --console-address не смотрит в интернет

НОРМАЛЬНО

- Явный EC-параметр и проверка эффективной ёмкости после каждого расширения
- ILM с --expire-days и --noncurrent-expire-days, аудит правил раз в месяц
- GOVERNANCE 30 суток на бэкапы, политика без BypassGovernanceRetention
- Мониторинг /minio/health/live, SMART и свободной ёмкости с алертами

ХОРОШО

- Вторая площадка с репликацией критичных бакетов через приватный туннель
- COMPLIANCE-ретеншен на юридическом архиве, legal hold по запросу юристов
- Первичный сид офлайн-носителем, по каналу — только дельта
- Ежегодный тест полного восстановления бакета из реплики с протоколом



Чек-лист самопроверки

☐ Знаем фактический объём по шарам и месячный прирост данных?

☐ Диски отданы хранилищу напрямую, без RAID, LVM и сетевых томов?

☐ На бакете бэкапов включены и версионирование, и Object Lock?

☐ Режим и срок ретеншена перекрывают реальное окно обнаружения инцидента?

☐ Сервисный ключ бэкапа лишён права s3:BypassGovernanceRetention?

☐ Есть ILM-правила на текущие и неактуальные версии, кроме бакета Veeam?

☐ Версия сервера зафиксирована, обновление проверяется на стенде?

☐ /minio/health/live, SMART и свободная ёмкость заведены в мониторинг?

☐ Есть копия критичных бакетов вне здания и канал под дельту?

☐ Восстановление из объектника проверяли за последние 12 месяцев?

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).

- Считаем объём и профиль данных, подбираем узел и схему erasure coding под ваш прирост
- Разворачиваем хранилище под systemd с TLS, ключами по бакетам и мониторингом
- Переводим Veeam, WAL-G, Nextcloud и почтовый архив на один S3-эндпоинт
- Настраиваем Object Lock, ILM-политики и репликацию на вторую площадку
- Ведём на абонентке: диски, health, аудит политик, ежегодный тест восстановления

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 Code Settings: MINIO_STORAGE_CLASS_STANDARD, EC:N (docs.min.io — 2026)
- 02** Object Lock и иммутабельность, mc retention set (docs.min.io — 2026)
- 03** Storage Requirements: XFS, JBOD, однотипные диски (docs.min.io — 2026)
- 04** mc ilm rule add, mc replicate add, mc admin replicate (docs.min.io — 2026)
- 05** Object Store (AGPLv3): установка, релизы, site replication (minio.community — 2026)
- 06** Immutability for Object Storage Repositories (helpcenter.veeam.com — v13)
- 07** S3 Compatible Object Storage: Considerations, Limitations (helpcenter.veeam.com — v13)
- 08** Наш шаблон узла хранения и чек-лист приёмки (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.

