Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Иммутабельный бэкап: MinIO S3 + Veeam против шифровальщиков

Разворачиваем immutable S3-хранилище MinIO с Object Lock как offsite-репозиторий Veeam B&R

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Бэкапы на NAS или сетевой шаре в той же сети и под теми же учётками шифровальщик уничтожает вместе с боевыми данными. Мы выносим копии в отдельное S3-хранилище MinIO с Object Lock: Veeam проставляет каждому объекту retention в режиме COMPLIANCE, и удалить копию до истечения срока не может никто — даже администратор с root-ключами MinIO.

Почему это важно бизнесу

- Атака по RDP с шифрованием и прода, и «бэкапа на шаре» — выбор между выкупом и потерей данных за годы; иммутабельная копия убирает этот выбор.
- Простой офиса 20–50 РМ без 1С и файлового сервера — остановка продаж и бухгалтерии; наша цель RTO — часы, а не недели.
- Object Lock закрывает и человеческий фактор: копию не удалит ни ошибка инженера, ни украденный пароль администратора.
- Своё S3-хранилище на горизонте 3 лет дешевле облака: нет платы за исходящий трафик при восстановлении полного объёма.

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

13.0.2

ветка Veeam B&R, которую ставим; S3 Compatible-репозитории и иммутабельность — из коробки

Veeam KB4738, 2026

EC:3

чётность erasure coding MinIO по умолчанию на 6–7 дисках: переживаем отказ любых трёх

доки MinIO, storage class

30 дней

retention COMPLIANCE: Veeam ставит его каждому объекту галкой Make recent backups immutable

наш стандарт

+10 дней

block generation: Veeam добавляет к сроку лока на S3 Compatible — цепочка истекает разом

доки Veeam v13

14 дней

operational restore window SOBR: свежие точки на локальном extent, старше — offload в MinIO

доки Veeam, capacity tier

РЕАЛИЗАЦИЯ 1 ИЗ 3

Разворачиваем MinIO как immutable S3-target

Что настраиваем

Отдельный сервер Debian 12: 6×SATA под XFS, 32 ГБ RAM, вне продового VLAN и вне домена

Как мы это делаем

1. Собираем MinIO из исходников (go install github.com/minio/minio@latest) — готовых community-бинарников с осени 2025 нет; версию фиксируем у себя
2. Диски — XFS с noatime; в /etc/default/minio задаём MINIO_VOLUMES="/data/disk{1...6}": erasure coding с чётностью EC:3 включается автоматически
3. TLS обязателен для S3-endpoint: кладём public.crt/private.key в каталог certs MinIO, endpoint вида https://backup.local:9000
4. Бакет создаём сразу с локом: mc mb --with-lock office/veeam — Object Lock включается только при создании, к существующему бакету его не добавить
5. Для Veeam — сервисная учётка mc admin user add + политика только на этот бакет (mc admin policy create/attach); root-ключи в Veeam не отдаём

РЕЗУЛЬТАТ

S3-хранилище на десятки ТБ, переживающее отказ до трёх дисков из шести; записанные объекты защищены локом на уровне самого хранилища, а не правами доступа.

КЛЮЧЕВОЙ НЮАНС

Иммутабельность — свойство бакета с первой секунды: имя, лок и политику доступа планируем до первой записи, потому что перевести обычный бакет в режим Object Lock задним числом нельзя.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Подключаем Veeam B&R и включаем иммутабельность

Что настраиваем

Сервер Veeam B&R 13 / 12.3.2; SOBR: локальный RAID — performance tier, MinIO — capacity tier

Как мы это делаем

1. Backup Infrastructure → Add Repository → Object Storage → S3 Compatible: endpoint https://…:9000, ключи сервисной учётки, бакет с Versioning + Object Lock
2. Ставим Make recent backups immutable for 30 days — Veeam сам проставляет per-object lock в режиме COMPLIANCE (Governance не используется)
3. Default retention на бакете НЕ настраиваем и lifecycle-правила не включаем: по докам Veeam это ведёт к сбоям и потере данных — сроками управляет сам Veeam
4. Собираем SOBR: Copy в MinIO сразу после создания точки + Move для цепочек старше 14 дней; offload-сессия отрабатывает каждые 4 часа
5. Проверяем боем: mc stat объекта показывает COMPLIANCE и дату истечения, попытка удаления под root MinIO возвращает Access Denied

РЕЗУЛЬТАТ

Свежие точки восстанавливаются с локального extent за минуты, а при шифровании прода в MinIO гарантированно остаётся целая копия: 30 дней retention + до 10 дней block generation.

КЛЮЧЕВОЙ НЮАНС

Versioning и Object Lock на уже подключённом бакете трогать нельзя, как и включать бакетный default retention: содержимым Veeam-бакета управляет только сам Veeam.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Изолируем бэкап-контур и проверяем восстановление

Что настраиваем

Сетевой периметр MinIO + мониторинг заданий Veeam, регламент DR-прогонов

Как мы это делаем

1. MinIO — в отдельном VLAN за межсетевым экраном: порты 9000/9001 открыты только с IP Veeam-сервера, SMB и RDP на хосте отсутствуют
2. Хост вне AD: локальные учётки, SSH по ключам; root-ключи MinIO — в офлайн-хранилище паролей, в конфигурации Veeam они не фигурируют
3. Метрики /minio/v2/metrics/cluster забираем в мониторинг, живость — /minio/health/live; алерты на деградацию дисков erasure-set
4. Уведомления Veeam о каждой ошибке джоба — на почту и в мессенджер: «молча падающий» бэкап недопустим
5. Раз в квартал поднимаем ВМ из бэкапа в изолированной сети: проверяем, что 1С открывается, а СУБД стартует без ошибок

РЕЗУЛЬТАТ

Даже при полной компрометации домена у злоумышленника нет пути к хранилищу копий, а эксплуатация узнаёт о проблемах бэкапа из алерта, а не в момент попытки восстановиться.

КЛЮЧЕВОЙ НЮАНС

Иммутабельность не отменяет правило 3-2-1: MinIO закрывает офисные риски, а вторая копия критичных данных в независимом облаке закрывает сценарий физической утраты серверной.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Object Lock на существующем бакете**
  Лок включается только при создании (mc mb --with-lock). Для миграции создаём новый бакет и перегоняем цепочки заново, старый выводим из ротации.

- ✕ **Default retention на бакете под Veeam**
  Бакетный ретеншн конфликтует с per-object локом Veeam: доки прямо предупреждают о непредсказуемом поведении и потере данных. Срок задаём только в Veeam.

- ✕ **Lifecycle-правила в Veeam-бакете**
  Автоудаление и переносы объектов ломают offload и восстановление — Veeam их не поддерживает. Данными в бакете управляет исключительно сам Veeam.

- ✕ **Завышенный срок COMPLIANCE**
  COMPLIANCE не откатывается даже root: лок на 180 дней заморозит ёмкость. Диски считаем как retention + block generation + прирост данных и версии.

- ✕ **wget «свежего» бинарника MinIO**
  Готовые community-сборки не публикуются с осени 2025 — скачанный бинарник без патчей. Собираем из исходников и фиксируем RELEASE в конфигурации.

- ✕ **Ёмкость без учёта версий**
  С Versioning + локом удалённые объекты живут как noncurrent-версии до конца retention: фактическое место больше «размера бэкапа» в консоли Veeam.

- ✕ **Бэкап-хост в домене AD**
  Компрометация домена = компрометация бэкапа: MinIO-сервер держим вне AD, с локальными учётками и SSH по ключам, без RDP и SMB.

- ✕ **Root-ключи MinIO в репозитории Veeam**
  Утечка ключей из конфигурации Veeam отдаёт всё хранилище. Заводим сервисную учётку с политикой на один бакет; лок защитит даже при её утечке.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- MinIO на отдельном хосте вне домена: XFS, TLS, бакет mc mb --with-lock
- Veeam-репозиторий S3 Compatible с immutability 30 дней (COMPLIANCE)
- Алерты Veeam о каждой ошибке джоба на почту / в мессенджер

НОРМАЛЬНО

- SOBR: локальный extent + capacity tier MinIO (Copy сразу, Move 14 дней)
- Отдельный VLAN, порты MinIO открыты только с Veeam-сервера
- Сервисная S3-учётка с политикой на один бакет, root-ключи в сейфе
- Квартальный тест восстановления ВМ в изолированной сети

ХОРОШО

- Вторая копия в независимое облако S3 — полное правило 3-2-1
- Prometheus-мониторинг MinIO: метрики кластера, здоровье дисков
- SureBackup: автоматическая проверка восстанавливаемости точек
- MinIO offsite — другое здание или площадка с гигабитным линком

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Резервные копии недоступны под учётками продовой сети (не SMB-шара, не тот же домен)?
- [ ] Бакет создан с Object Lock и Versioning, а default retention на нём не настроен?
- [ ] В свойствах репозитория Veeam включена галка Make recent backups immutable?
- [ ] Проверяли, что удаление объекта под админом MinIO возвращает Access Denied?
- [ ] Ёмкость дисков посчитана с учётом retention + block generation и noncurrent-версий?
- [ ] Тестовое восстановление 1С и файлового сервера выполнялось за последний квартал?
- [ ] Ошибка бэкап-джоба доходит до ответственного алертом, а не остаётся в логе?
- [ ] Root-ключи MinIO не используются в Veeam и хранятся вне бэкап-контура?

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).

- Аудит текущей схемы бэкапа: находим точки, где шифровальщик дотягивается до копий
- Поставка и настройка сервера MinIO: диски, erasure coding, TLS, Object Lock
- Подключение Veeam B&R 12/13: SOBR, иммутабельность, минимальные сервисные учётки
- Тестовое восстановление, мониторинг и алерты, передача документации по стенду

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 Immutability for Object Storage Repositories (User Guide) (helpcenter.veeam.com — v13)

02 S3 Compatible Object Storage — Considerations and Limitations (helpcenter.veeam.com — v13)

03 Capacity Tier: Moving/Copying Backups (SOBR) (helpcenter.veeam.com — v13)

04 Erasure Coding and Storage Classes (MinIO Server) (min.io — 2025)

05 mc mb --with-lock / mc retention — Object Lock (MinIO Client) (min.io — 2025)

06 Release Information: KB4738 / KB2680 (veeam.com — 2026)

07 Шаблон ITfresh «Immutable S3-target для малого офиса» (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.