



Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Amanda Network Backup: корпоративный бэкап Linux и Windows

Как мы разворачиваем Amanda 3.5.4: vtape, storage/policy, S3-vault и учения по восстановлению

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

Суть проблемы

У клиента бэкап обычно — это rsync-скрипты на NAS без каталога, без проверки и без ретеншена: ротация молча затирает нужную точку, а выясняется это в момент шифровальщика или удалённой папки. Мы переводим копирование в управляемую систему: явный disklist, предсказуемый dumpcycle, ретеншен секцией policy и подтверждённое восстановление. Иначе простой считается днями.

Почему это важно бизнесу

- Потеря папки трёхмесячной давности = переделка проектной работы: часы юристов и инженеров, которые никто не оплатит
- Без index yes и каталога восстановление одного файла превращается в разбор всего тома — RTO растёт с часов до суток
- Шифровальщик проходит по SMB-шаре вместе с копией: бэкап без отдельного хранилища умирает вместе с боевыми данными
- Непроверенный бэкап — расход без страховки: платим за диски и обслуживание, а в аварии получаем нули
- Сроки хранения по договорам и налоговым требованиям не подтвердить, если ретеншен живёт в голове администратора



Ключевые параметры реализации

3.5.4

Актуальный релиз Amanda Community: в runtar закрыта инъекция аргументов
CVE-2023-30577

Amanda 3.5.4 release notes

10080/tcp

Единственный порт клиента при auth bsdtcp: amindexd и amidxtaped идут через amandad

amanda-auth(7), Amanda 3.5

7 дней

dumpcycle: полный дамп каждого DLE не реже 7 дней вместо дефолтных 10 в amanda.conf

amanda.conf(5): dumpcycle default 10

tapecycle 15

Дефолт tapecycle — 15 томов; в policy retention-tapes по умолчанию = tapecycle-1

amanda.conf(5): policy section

1280k

device-output-buffer-size по умолчанию; под taper на 10G-линке поднимаем адресно

amanda.conf(5), Amanda 3.5

1.5x

Наш порог: holding disk не меньше 1.5x крупнейшего DLE при chunksize 1 Gb

Наш стандарт + amanda.conf(5): chunksize



Сервер Amanda: vtape-хранилище, storage и расписание

Что настраиваем

Debian 12, выделенная VM или bare-metal: amanda-server 3.5.4, том /backups под chg-disk, holding disk на NVMe

Как мы это делаем

- 1 Ставим amanda-server, amanda-client, amanda-common; конфиг в /etc/amanda/daily (amanda.conf + disklist), состояние и индексы — в /var/lib/amanda/daily
- 2 tapetype с реальной length под слот и blocksize 128k вместо дефолтных 32k; каталоги /backups и holding disk отдаём backup:backup
- 3 Storage-секция daily: tpchanger chg-disk:/backups/vtape/daily с num-slot и auto-create-slot, labelstr ^daily-[0-9]+\$, policy daily
- 4 Планирование: dumpcycle 7, runspercycle 5, runtapes 1, inparallel 4, maxdumps 2; holdingdisk chunksize 1 Gb, reserve снижаем с дефолтных 100 %
- 5 amlabel по слотам, дальше /etc/cron.d/amanda под пользователем backup: amcheck daily в 22:00 и amdump daily в 23:00

РЕЗУЛЬТАТ

Ночное окно предсказуемо: планировщик сам раскладывает полные дампы и инкременты по циклу, не выдавая пиков нагрузки. Оператор утром смотрит одну сводку вместо ручного разбора логов, а amcheck ловит права, метки и недоступных клиентов до старта, а не в три часа ночи.

КЛЮЧЕВОЙ НЮАНС

tapecycle обязан превышать число томов за цикл (runspercycle × runtapes), иначе сервер перезагрузит ещё нужный том. Глобальный tpchanger в 3.5 устарел — ротацию описываем секциями storage и policy.



Клиенты Linux/Windows, шифрование и согласованность

Что настраиваем

Файловые серверы, 1С/СУБД и почта; на Linux amanda-client, на Windows — Zmanda Windows Client как служба с VSS

Как мы это делаем

- 1 auth bsdtcp по всему парку: на Debian .amandahosts — это /etc/amandahosts (симлинк из /var/backups), владелец backup, права 600
- 2 На клиенте строка «<сервер> backup amdump», на сервере — «<клиент> backup amindexd amidxtaped»; прямая и обратная DNS обязаны сходиться
- 3 amgtar: ONE-FILE-SYSTEM и SPARSE по умолчанию YES, ATIME-PRESERVE требует GNU tar 1.15.90+; свои EXCLUDE-LIST под кэши, temp и своп
- 4 Шифрование на клиенте: encrypt client + client-encrypt /usr/sbin/amcrypt-oss1, парольная фраза в /var/lib/amanda/.am_passphrase с правами 600
- 5 СУБД снимаем pre/post-скриптами в консистентный дамп, а не с живых файлов; Windows-тома — через VSS-снимок клиента

РЕЗУЛЬТАТ

Данные уходят с клиента уже зашифрованными: компрометация бэкап-сервера или объектного хранилища не даёт доступа к содержимому. Согласованные снимоты убирают класс отказов «восстановили, а база битая» — подъём СУБД перестаёт быть лотереей.

КЛЮЧЕВОЙ НЮАНС

Парольная фраза amcrypt-oss1 и .amandahosts — две точки, где ошибка ломает восстановление молча. Копию /var/lib/amanda/.am_passphrase держим вне самого бэкапа, иначе расшифровывать будет нечем.



Вторая копия, ретеншен и учения по восстановлению

Что настраиваем

Storage-секции Amanda 3.5: локальный vtape плюс S3-совместимое объектное хранилище на отдельной площадке

Как мы это делаем

- 1 Второе storage: `tpchanger chg-multi:s3:bucket/prefix-{001..060}` и `device-property S3_HOST, S3_SERVICE_PATH, S3_SSL yes, STORAGE_API, NB_THREADS_BACKUP`
- 2 `vault-storage «s3»` в глобальной секции: `amdump` после основной записи сам дописывает дампы во вторую копию; параметр `vault` в `storage` задаёт задержку в днях
- 3 Свой `policy` на каждое storage: `retention-tapes, retention-days, retention-full` — правила хранения описаны конфигом, а не памятью админа
- 4 Ежеквартальные учения: `amcheckdump` по последнему прогону, затем `amfetchdump/amrecover` случайного DLE на изолированную машину с замером RTO
- 5 `set-no-reuse yes` в storage месячных и квартальных томов (дефолт `no`), чтобы автоматика не пустила их в оборот раньше срока

РЕЗУЛЬТАТ

Копия физически вне периметра клиента, ротация описана декларативно и проверяется через `amadmin`. Ежеквартальный замер даёт честные цифры RPO и RTO для регламента вместо оценки «за ночь как-нибудь поднимем».

КЛЮЧЕВОЙ НЮАНС

Vault идёт после дампа и тянет тот же канал: без `MAX_SEND_SPEED` и разумного `NB_THREADS_BACKUP` выгрузка в S3 выедает полосу уже в рабочее время.



Подводные камни

✗ **amcheck не запускается перед amdump**

Права, метки и недоступный клиент всплывают ночью и рвут прогон. Ставим amcheck отдельной строкой cron за час до amdump и вешаем алерт.

✗ **tapecycle меньше числа томов за цикл**

Томов за цикл = runspercycle × runtapes; при заниженном tapecycle сервер затирает том, который ещё нужен для восстановления цепочки.

✗ **Holding disk «на остатках» диска**

Меньше 1.5x крупнейшего DLE — и дампы идут мимо holding disk прямо в taper, скорость падает до последовательной записи. Считаем по факту.

✗ **Расхождение прямой и обратной DNS**

bsdtcp сверяет reverse DNS с forward; при несовпадении клиент отваливается с невнятной ошибкой. Проверяем PTR до установки.

✗ **index оставлен по умолчанию**

index по умолчанию no: без каталога в indexdir amrecover не покажет дерево файлов, и точечное восстановление превращается в разбор всего тома.

✗ **Windows-клиент без VSS**

Копия живых файлов БД и открытых документов даёт битый архив. Включаем VSS-снимок, а pagefile.sys и temp выносим в EXCLUDE-LIST.

✗ **vtape-хранилище смонтировано как шара**

Шифровальщик доходит до копии по той же сети. Держим /backups вне доменной шары, доступ — только по протоколу Amanda на 10080/tcp.

✗ **Ретеншен без учений**

Хранить 90 дней и ни разу не восстановить — то же, что не хранить. Раз в квартал amcheckdump плюс реальный подъём случайного DLE.



Как правильно

МИНИМУМ

- Amanda 3.5.4, auth bsdtcp, .amandahosts с правами 600, index yes на всех DLE
- dumpcycle 7 / runspcycle 5 / tapesycle 15 и amcheck перед каждым amdump
- Holding disk не меньше 1.5x крупнейшего DLE, chunksize 1 Gb
- amreport -f на почту, send-amreport-on all, лог прогона в /var/log/amanda

НОРМАЛЬНО

- encrypt client + amcrypt-ossf, .am_passphrase хранится отдельно от бэкапа
- Вторая копия: storage с chg-multi:s3 и S3_SSL yes через vault-storage
- policy с retention-tapes и retention-days вместо голого tapesycle
- amgtar с EXCLUDE-LIST, VSS на Windows, pre/post-скрипты для СУБД

ХОРОШО

- Учения раз в квартал: amcheckdump плюс подъём DLE с замером RTO
- Разделение daily/weekly/monthly/quarterly, у каждого свой policy
- set-no-reuse на долгоживущих томах, MAX_SEND_SPEED на выгрузке в S3
- Сводка в Telegram, факт и длительность прогона под контролем Zabbix



Чек-лист самопроверки

- | | |
|--|--|
| ☐ Знаем ли мы RPO и RTO по каждой системе — и подтверждены ли они замером, а не оценкой? | ☐ Снимаются ли БД и Windows-тома через VSS и pre/post-скрипты, а не с живых файлов? |
| ☐ Запускается ли amcheck отдельным заданием до amdump и приходит ли алерт при ошибке? | ☐ Включён ли index yes на всех DLE, чтобы поднять один файл без разбора всего тома? |
| ☐ Больше ли tapesycle, чем runspercycle x runtapes, и описан ли ретеншен секцией policy? | ☐ Проводили ли мы за последний квартал реальное восстановление случайного DLE? |
| ☐ Есть ли вторая копия вне периметра — S3 или другая площадка — и проверена ли она чтением? | ☐ Ограничен ли доступ к vtape-хранилищу — оно не смонтировано как обычная сетевая шара? |
| ☐ Уходят ли данные с клиента уже зашифрованными и где физически лежит копия .am_passphrase? | ☐ Есть ли письменный регламент: что, куда, на сколько и кто отвечает за проверку? |

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).

- Проектируем схему хранения: disklist, dumpcycle, storage/policy, объём vtape и вторая копия в S3
- Разворачиваем сервер и клиентов Linux/Windows под ключ, включая VSS и шифрование на клиенте
- Настраиваем отчётность: amreport на почту, сводка в Telegram, контроль прогона в Zabbix
- Проводим учения по восстановлению с протоколом и замером RTO раз в квартал
- Держим ваши копии на своей площадке в ЦОД и сопровождаем бэкап на абонентской основе

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** amanda.conf(5) — main configuration file, storage и policy (manpages.debian.org — 3.5.x)
- 02** amanda-auth(7) — методы аутентификации и порты (manpages.debian.org — 3.5.x)
- 03** amanda-devices(7) — свойства S3- и vfs-устройств (manpages.debian.org — 3.5.x)
- 04** amanda-changers(7) — chg-disk, chg-multi, num-slot (manpages.debian.org — 3.5.x)
- 05** amgtar(8) — приложение для GNU tar и его свойства (manpages.debian.org — 3.5.x)
- 06** amcrypt-openssl(8) — шифрование на клиенте, .am_passphrase (manpages.debian.org — 3.5.x)
- 07** Amanda Community 3.5.4 — release notes (zmanda.com — 3.5.4)
- 08** Amanda Community documentation (docs.zmanda.com — 3.5.x)
- 09** Наш шаблон daily/weekly/monthly + протокол учений (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.

