WHITE PAPER

РЕКОМЕНДАЦИИ ПО ОПТИМИЗАЦИИ И ИНТЕГРАЦИИ TATLIN.BACKUP.M С КИБЕР БЭКАП

О WHITE PAPER

Данный документ описывает архитектурные принципы и подходы, а также рекомендации по их применению при построении корпоративных решений на основе продуктов производства компании YADRO.

Документ предназначен для широкой аудитории, но также может включать материалы, требующие специальной профессиональной подготовки, ориентированные на системных архитекторов, администраторов, сервисных инженеров и других IT-специалистов, участвующих в планировании, проектировании и внедрении комплексных решений.

! Представленная информация основана на результатах исследований, а также экспертизе специалистов YADRO. Документ носит не предписывающий, а информационный характер, целью которого является информирование получателей документа о предмете произведенного исследования и о его результатах. При этом конкретные результаты и эффективность конечных решений зависят от множества факторов, которые могут различаться в зависимости от особенностей инфраструктуры и условий эксплуатации. Ни при каких обстоятельствах YADRO не несет ответственность за последствия применения получателем документа рекомендаций, инструкций, подходов и решений, указанных в документе.

Запрещается копировать, воспроизводить, изменять, публиковать, передавать, распространять, продавать информацию (часть информации), содержащуюся в документе, или создавать производные работы на основе содержания документа без предварительного письменного разрешения YADRO.

Любая информация или утверждения относительно возможностей, емкости, производительности или других характеристик продукции, указанной в документе, предоставляются исключительно на условиях «как есть» и приведена исключительно в целях описания произведенного исследования. YADRO оставляет за собой право вносить изменения/обновлять информация в документе без уведомления.

«YADRO» является зарегистрированным товарным знаком ООО «КНС ГРУПП». Другие названия продуктов и компаний, упомянутые здесь, могут быть товарными знаками или торговыми наименованиями их соответствующих владельцев.

Актуальные версии документации публикуются на информационном ресурсе YADRO по адресу service.yadro.com.

ОГЛАВЛЕНИЕ

1. ОБ ЭКСПЕРТАХ 4
2. ВВЕДЕНИЕ 5
3. ОБЩИЕ РЕКОМЕНДАЦИИ ПО КОНФИГУРАЦИИ TATLIN.BACKUP.M 6
4. ТЕКУЩИЕ ЛИМИТЫ TATLIN.BACKUP.M 8
5. АРХИТЕКТУРА КИБЕР БЭКАП 9
   5.1. Основные элементы архитектуры 9
6. РЕКОМЕНДАЦИИ ПО КОНФИГУРАЦИИ СИСТЕМЫ КИБЕРБЭКАП 10
   6.1. Общие рекомендации 10
   6.2. SMB/CIFS 10
   6.3. NFS 10
7. СЦЕНАРИИ ИНТЕГРАЦИИ СРК КИБЕР БЭКАП С TATLIN.BACKUP M 10
   7.1. Оптимизация трафика на агенте 10
   7.2. Экономия ресурсов продуктивной среды 11
   7.3. Гибридное решение по оптимизации 11
8. НАСТРОЙКА ХРАНИЛИЩ РЕЗЕРВНЫХ КОПИЙ НА СЕРВЕРЕ УПРАВЛЕНИЯ 12
   8.1. Вход в консоль сервера управления 12
   8.2. Добавление неуправляемых хранилищ 12
   8.3. Добавление управляемых хранилищ 13
   8.4. Добавление папки NFS 14
   8.5. Добавление в качестве локальной папки NFS-экспорта или виртуальной файловой системы, экспортированной по протоколу T-BOOST 15
   8.6. Создание планов резервного копирования 16
   8.7. Первое задание (SMB) 16
9. ПРИЛОЖЕНИЕ 1. ДИАГНОСТИКА ПОДКЛЮЧЕНИЯ ПО ПРОТОКОЛУ SMB 18
   9.1. Первое задание (SMB) 19
   9.2. Жесткое указание версии протокола SMB для агента 19
   9.3. Агент Virtual Appliance 20
10. ПРИЛОЖЕНИЕ 2. ОШИБКА FAILED TO LOCK THE FILE ПРИ РЕЗЕРВНОМ КОПИРОВАНИИ НА NFS-ХРАНИЛИЩЕ 21
    10.1. Отключение блокировок NFS (агент для Linux) 21
    10.2. Резервное копирование и репликация резервных копий на общие ресурсы NFS 22

ОБ ЭКСПЕРТАХ

Алексей Головин — специалист с 15-летним опытом работы в сфере ИТ, включая опыт в таких компаниях, как Dell EMC и системных интеграторах. В команде YADRO занимает позицию ведущего специалиста по интеграционным решениям. Алексей поддерживает сложную инфраструктуру корпоративных клиентов.

Занимается настройкой, оптимизацией и обслуживанием хранилищ данных и инфраструктуры резервного копирования. Специализируется на диагностике и устранении неисправностей систем YADRO, DellEMC, Cisco, Brocade, Pivotal и других производителей..

ВВЕДЕНИЕ

Данный документ предназначен для ИТ-специалистов и администраторов, ответственных за внедрение и поддержку системы резервного копирования TATLIN.BACKUP M. Документ содержит рекомендации по настройке и оптимизации TATLIN.BACKUP M, а также по интеграции с платформой защиты данных Кибер Бэкап для достижения максимальной производительности, отказоустойчивости и безопасности данных.

Целевая аудитория включает технических специалистов, инженеров по безопасности данных и администраторов систем хранения, которым требуется обеспечить эффективную работу инфраструктуры резервного копирования с учетом современных требований к управлению данными и восстановлениям.

	ВЕРСИИ ИСПОЛЬЗУЕМОГО ПО
TATLIN.BACKUP.M	1.1
Кибер Бэкап	1.7 / 1.8

ОБЩИЕ РЕКОМЕНДАЦИИ ПО КОНФИГУРАЦИИ TATLIN.BACKUP.M

- Максимальная скорость чтения/записи достигается при использовании двух и более дисковых модулей расширения. В минимальной конфигурации с одним дисковым модулем расширения скорость первого резервного копирования может быть ниже.
- Для оптимальной работы T-RAID (для оптимального распределения дисков по группам аллокации) рекомендуется производить увеличение дисковой емкости целыми дисковыми модулями.
- На TATLIN.BACKUP.M рекомендуется создать несколько виртуальных файловых систем, поскольку параллельная запись в несколько файловых систем позволяет достичь более высокой скорости.
- Рекомендуется создать 4-16 виртуальных файловых систем, каждая из которых должна обрабатывать по 4-16 потоков данных.
- В целях повышения отказоустойчивости при передаче данных по Ethernet-соединениям рекомендуется использовать технологию агрегации каналов LACP.
- Если к СХД подключаются более одного хоста или более чем из одной подсети, рекомендуется использовать две LACP-агрегации с портами из разных сетевых карт (`bond0:data0p0`, `data1p1` и `bond1:data0p1`, `data1p0`).
- Если доступ к TATLIN.BACKUP.M осуществляется через один отказоустойчивый хост, рекомендуется использовать одну LACP-агрегацию (`bond0:data0p0`, `data0p1`, `data1p0`, `data1p1`).
- На сетевых data-интерфейсах рекомендуется использовать jumbo-фреймы с MTU 9000 для эффективного использования каналов.
- При передаче данных по протоколам NFS, Samba (SMB/CIFS) или T-Boost между клиентом и сервером используются свободные порты для установления соединений.
- Эти порты участвуют в выборе сетевого интерфейса при использовании агрегированных соединений (LACP).

Для активации LACP применяется параметр Transmit Hash Policy, определяющий метод балансировки трафика между интерфейсами. Использование метода layer3+4 (балансировка на основе IP-адреса и номера порта) упрощает конфигурацию и позволяет обойтись без дополнительных IP-адресов. Однако номера портов выбираются динамически и заранее неизвестны, что исключает возможность предсказуемого распределения нагрузки по интерфейсам. Несмотря на это, такой подход способен повысить эффективность использования агрегированного интерфейса в ряде сценариев.

Рекомендации по выбору метода балансировки

Для передачи данных по протоколам NFS, Samba или T-Boost между клиентом и сервером выполняется установка соединения, при которой используются свободные порты на системе. Номера этих портов могут быть использованы при выборе LACP-интерфейса, по которому будут передаваться данные. Для включения механизма LACP используется настройка **Transmit Hash Policy layer3+4**.

Такой подход облегчает конфигурирование точек монтирования, так как позволяет избавиться от дополнительных IP-адресов. Однако номера портов для установки соединения заранее неизвестны и их выбор зависит от занятости портов на системе. Поэтому нельзя гарантировать равномерное распределение I/O по интерфейсам. Тем не менее, эта схема позволяет добиться большей эффективности при использовании агрегированного интерфейса.

Протокол NFS

TATLIN.BACKUP поддерживает экспорт данных по протоколам NFSv3 и NFSv4. При наличии поддержки со стороны клиента рекомендуется использовать NFSv4.
Для достижения максимальной производительности при монтировании NFS-директорий рекомендуется:

- Использовать параметры rsize=1048576,wsize=1048576 (1 МБ) для чтения и записи;
- Применять опцию write=eager, которая предотвращает агрегацию мелких блоков и эффективна при записи большими блоками (1 МБ и более);
- Использовать nconnect=1. Повышение значения приводит к неоптимальному профилю I/O нагрузки для файловой системы TBFS и может снизить производительность.
- Опция nconnect позволяет клиенту NFS открывать несколько параллельных соединений с сервером. Это может улучшить распределение трафика при использовании layer3+4, но не рекомендуется в системах, использующих файловую систему TBFS.

Протокол Samba (CIFS/SMB)
Для монтирования виртуальных файловых систем с использованием Samba рекомендуется:

- Использовать версии протокола SMB 3.0 и выше;
- Применять параметры rsize=4194304,wsize=4194304 (4 МБ) для повышения производительности;
- Устанавливать cache=strict для обеспечения согласованности данных.

Протокол T-Boost
Протокол T-Boost реализован в двух вариантах: в виде сервиса tboost и отдельного приложения tb_agent.
tb_agent обслуживает только одну виртуальную файловую систему;
tboost способен одновременно обслуживать несколько виртуальных файловых систем.
Эффективное использование агрегированных сетевых интерфейсов через LACP в случае TBoost возможно только при наличии нескольких виртуальных файловых систем, так как клиентская часть протокола создает единственную TCP-пару соединений на каждую из них.
При использовании одной ФС распределение трафика будет ограничено одним интерфейсом, что снижает преимущества от агрегации. Для устойчивой и предсказуемой работы клиентов T-Boost (tb_agent и tboost) в стандартной конфигурации достаточно:

- 8 ГБ оперативной памяти
- 8-ядерного процессора

При необходимости возможно использование пользовательской конфигурации, позволяющей адаптировать поведение клиента T-Boost под специфические требования системы или окружения.
Для tboost путь к конфигурационному файлу указывается в системной единице службы (systemd) или непосредственно в параметрах запуска.

Пример для дистрибутивов семейства Debian:

```
[Unit]
Description=T-Boost service
After=network.target
[Service]
Environment="RUST_LOG=info"
ExecStart=/usr/bin/tboost --config=/etc/tboost/tboost.toml
RuntimeDirectory=tboost
[Install]
WantedBy=multi-user.target
```

Изменение конфигурации может потребоваться в случаях, когда необходимо:

- Ограничить или перераспределить использование системных ресурсов
- Повысить производительность в специализированных сценариях
- Задать строгие параметры масштабирования

Важно: Пользовательская конфигурация может повысить эффективность, но также способна привести к нежелательным последствиям, включая деградацию производительности или нестабильную работу.
Без необходимости изменять конфигурацию не рекомендуется.

open_direct_io_mode
По умолчанию клиент T-Boost функционирует с параметром open_direct_io_mode с установленным значением false . Установка значения true в этом параметре может увеличить производительность от 5 до 15 и более % в зависимости от окружения.

async_threads
В конфигурации по умолчанию установлено ограничение на потребление оперативной памяти T-Boost клиентом. Но загруженность процессора не ограничивается, клиент может использовать все доступные ядра процессора на системе. Если такое поведение нежелательно, можно задать количество потоков, на которых будет выполняться работа T-Boost клиента. Например, чтобы использовать восемь ядер процессора, требуется указать async_threads = 8 в конфигурационном файле tb_agent или tboost.

fuse_parallel_direct_io
Увеличивает эффективность параллельной записи, особенно при множестве одновременных операций.

Для достижения большей скорости обмена данными с СХД рекомендуется отдавать предпочтение I/O со следующими характеристиками:

- Разделение по направлению передачи данных (readили write, не смешанный read/write).
- Большой блок данных: 1-4 МиБ.
- Последовательное выполнение операций.
- Наличие нескольких I/O потоков на виртуальной файловой системе: 4-16 I/O потоков в каждую из 4-16 виртуальных файловых систем.

Оптимальная производительность СХД достигается при совершении операций в 32 потока, равномерно распределенных по виртуальной файловой системе. Для эффективного использования механизма дедупликации рекомендуется отключить механизм дедупликации на уровне ПО СРК.

ТЕКУЩИЕ ЛИМИТЫ TATLIN.BACKUP.M

ПАРАМЕТРЫ	ОГРАНИЧЕНИЯ
Максимальный размер файла	По NFS — 16 ТиБ По SMB — 15.99 ТиБ Tboost — 17 ТиБ
Максимальный размер файловой системы	693,3 ТБ / 630,6 ТиБ
Максимальное количество виртуальных файловых систем на СХД	64 виртуальных файловых системы / ресурса с общим доступом
Максимальное количество пользователей	59 000
Максимальное число файлов на систему	64 виртуальных файловых системы × 500 каталогов × 100 000 файлов в каталоге
Максимальное число файлов на один каталог	100 000
Максимальное число каталогов в файловой системе	500
Максимальное количество потоков на запись	400
Максимальное количество потоков на чтение	200

АРХИТЕКТУРА КИБЕР БЭКАП

Архитектура Кибер Бэкап основана на централизованной системе управления резервными копиями, которая может интегрироваться с хранилищем TATLIN.BACKUP M.

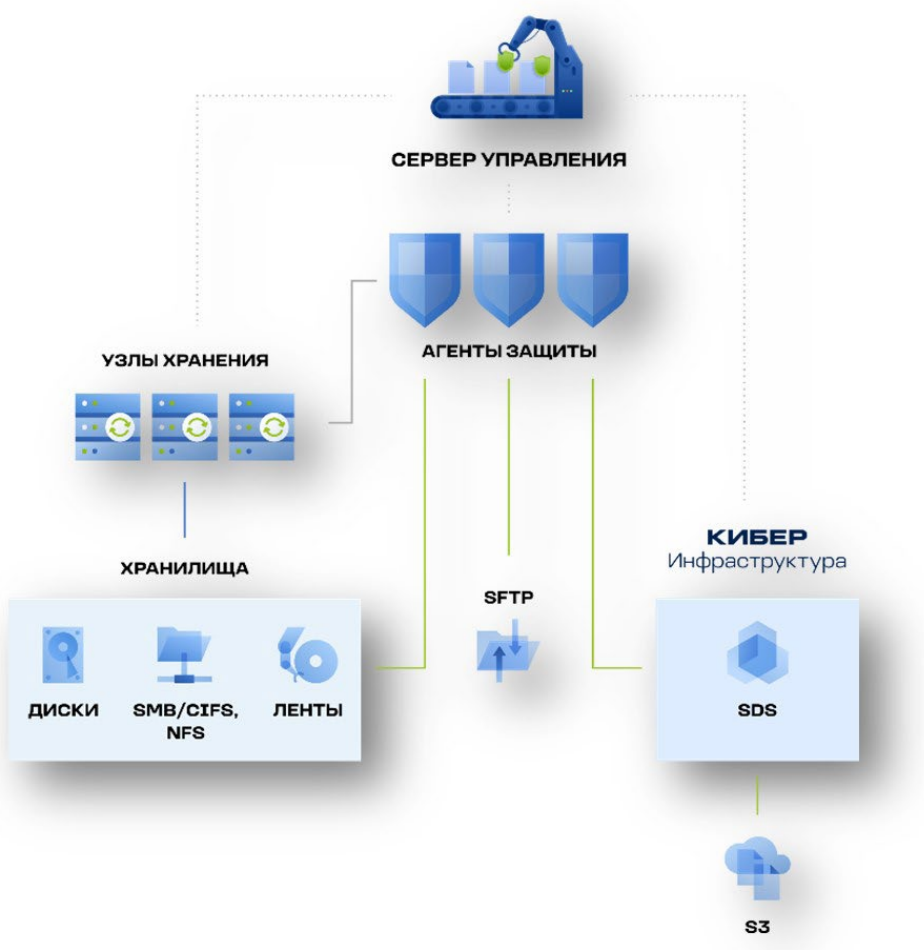
Архитектура системы обеспечивает высокую производительность, отказоустойчивость и масштабируемость для централизованного резервного копирования и восстановления данных. Система включает компоненты, совместимые с 64-разрядными версиями операционных систем Windows и Linux, что делает ее кроссплатформенной и удобной для работы в различных ИТ-средах, включая отечественные ОС.

Основные элементы архитектуры

Сервер управления: главный элемент системы, управляющий процессами резервного копирования, мониторингом, а также конфигурацией и хранением метаданных. Доступ к серверу управления осуществляется через веб-консоль, предоставляя удобный интерфейс для администрирования.

Агенты защиты: устанавливаются на защищаемых системах или рядом с ними, обеспечивая резервное копирование и защиту данных операционных систем, виртуальных платформ и приложений. Агенты работают автономно, минимизируя нагрузку на сервер управления.

Узлы хранения: используются для организации и управления хранилищами, выполняют дедупликацию данных и предоставляют доступ к ленточным и дисковым носителям. Узлы хранения выполняют защиту резервных копий и обеспечивают распределенное хранение в рамках инфраструктуры.



РЕКОМЕНДАЦИИ ПО КОНФИГУРАЦИИ СИСТЕМЫ КИБЕРБЭКАП

Общие рекомендации

Рекомендуется запускать одновременно несколько заданий резервного копирования, так как TATLIN.BACKUP M обеспечивает максимальную производительность именно при параллельной работе с множеством потоков резервного копирования. Для этого в один план добавляйте несколько агентов или виртуальных машин.
Если это задание для безагентного резервного копирования, то регулировать количество потоков (параллельных задний резервного копирования ВМ) можно в параметре – «планирование».
Данная настройка будет действовать для каждого агента виртуализации.

https://docs.cyberprotect.ru/ru-RU/CyberBackup/17.2/user/#scheduling.html

SMB/CIFS

Для оптимальной производительности рекомендуется использовать протокол SMB не ниже 2.1.
Версия используемого протокола зависит от ОС, в которой работает агент Кибер Бэкап, так как все операции монтирования и передачи данных происходят через инструменты ОС.

При возникновении сложностей, можно воспользоваться Приложение 1. Диагностика подключения по протоколу SMB

NFS

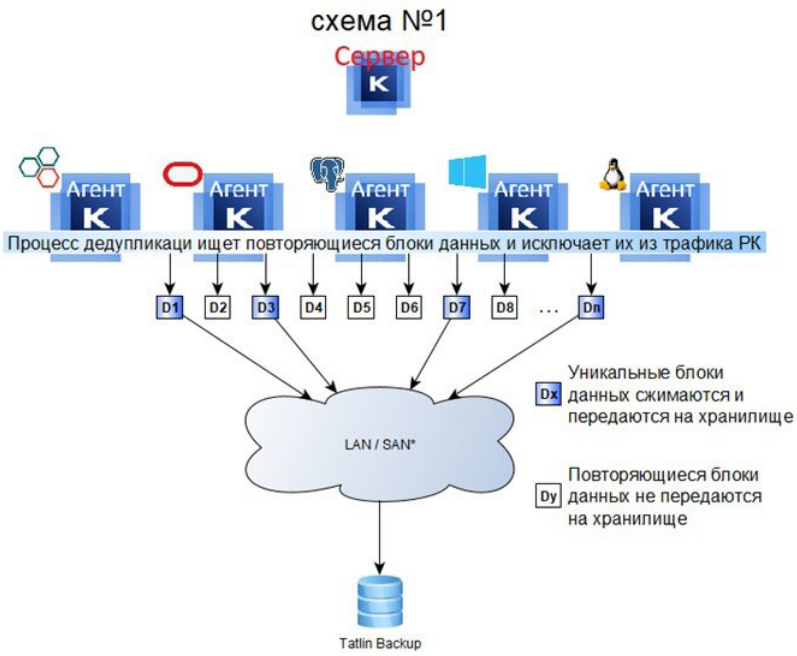
При использовании NFS хранилища необходимо явно отключать для агента использование блокировок файлов резервных копий, так как на стороне хранилища они не поддерживаются.

При возникновении сложностей, можно воспользоваться Приложение 2. Ошибка Failed to lock the file при резервном копировании на NFS хранилище

СЦЕНАРИИ ИНТЕГРАЦИИ СРК КИБЕР БЭКАП С TATLIN.BACKUP M

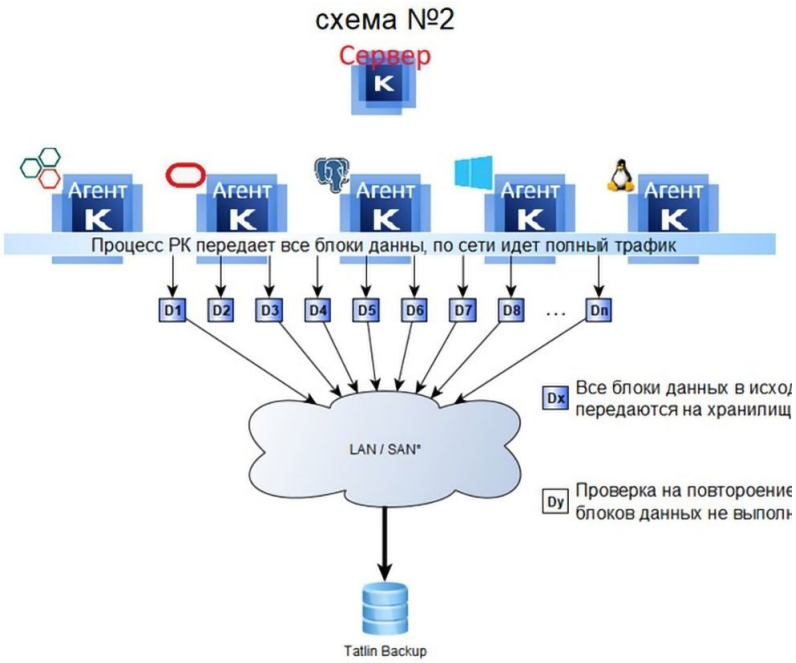
Оптимизация трафика на агенте

Заказчику требуется оптимизировать (уменьшить) трафик резервного копирования на источнике данных перед отправкой его по сети на хранилище резервных копий, поэтому на каждом агенте Кибер Бэкап используется агент T-Boost, который выполняет глобальную дедупликацию уровня TATLIN.BACKUP M - блоки данных, которые ранее уже были записаны на хранилище не передаются, а передаются только метаданные этого блока, которые имеют значительно меньший объем, уникальные блоки сжимаются перед отправкой.



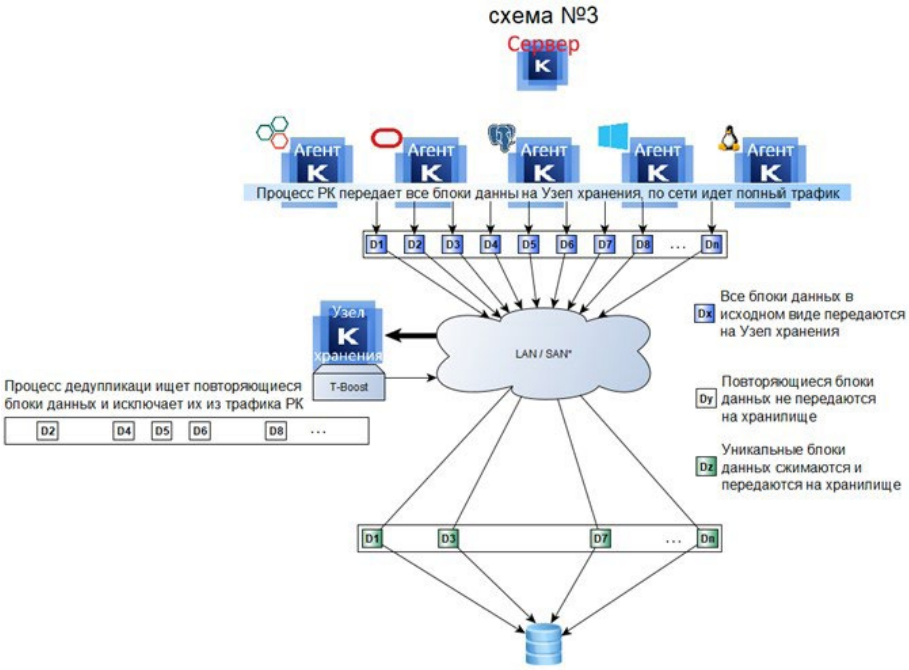
Экономия ресурсов продуктивной среды

Заказчику нельзя тратить процессорные ресурсы и память на глобальную дедупликацию и компрессию уровня TATLIN.BACKUP M на агенте, поэтому он готов всегда посылать все блоки без исключения по сети с использованием протоколов CIFS или NFS, дедупликация и компрессия будет выполняться на хранилище.



Гибридное решение по оптимизации

В случае, если заказчику нельзя тратить процессорные ресурсы и память на глобальную дедупликацию уровня TATLIN.BACKUP M и компрессию на агенте, но требуется передавать Резервные Копии по узкому каналу на TATLIN.BACKUP M, расположенный в удаленном ЦОДе, то трафик в полном объеме нужно передавать на локальный узел хранения (медиа сервер) по протоколу CIFS или NFS, на котором T-Boost агент будет выполнять дедупликацию с компрессией и отправлять данные в оптимизированном формате в удаленный ЦОД по узкому каналу на TATLIN.BACKUP M.



НАСТРОЙКА ХРАНИЛИЩ РЕЗЕРВНЫХ КОПИЙ НА СЕРВЕРЕ УПРАВЛЕНИЯ

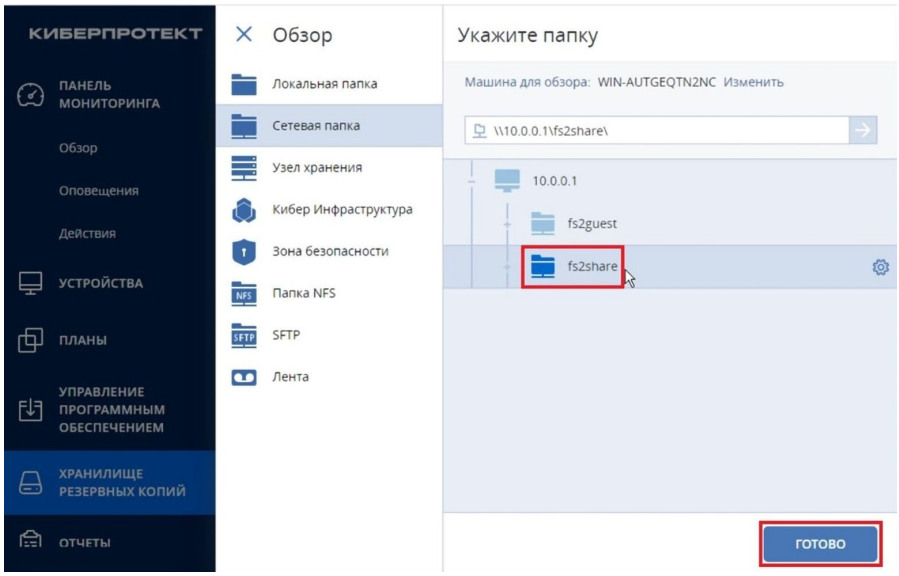
Вход в консоль сервера управления

1. Войдите на сервер управления в браузере по протоколу HTTP/HTTPS, используя URL в формате `http://<IP_ADDRESS>:9877`.
   На рабочем столе машины сервера управления уже будут находиться ярлыки для входа.
2. Для входа в консоль управления необходимо указать учетные данные локального администратора.
3. Активируйте ознакомительный период в разделе **Настройки** — **Лицензии**.

Добавление неуправляемых хранилищ

1. В разделе Хранилище резервных копий нажмите **Добавить хранилище**.
2. Создайте два хранилища SMB и NFS.

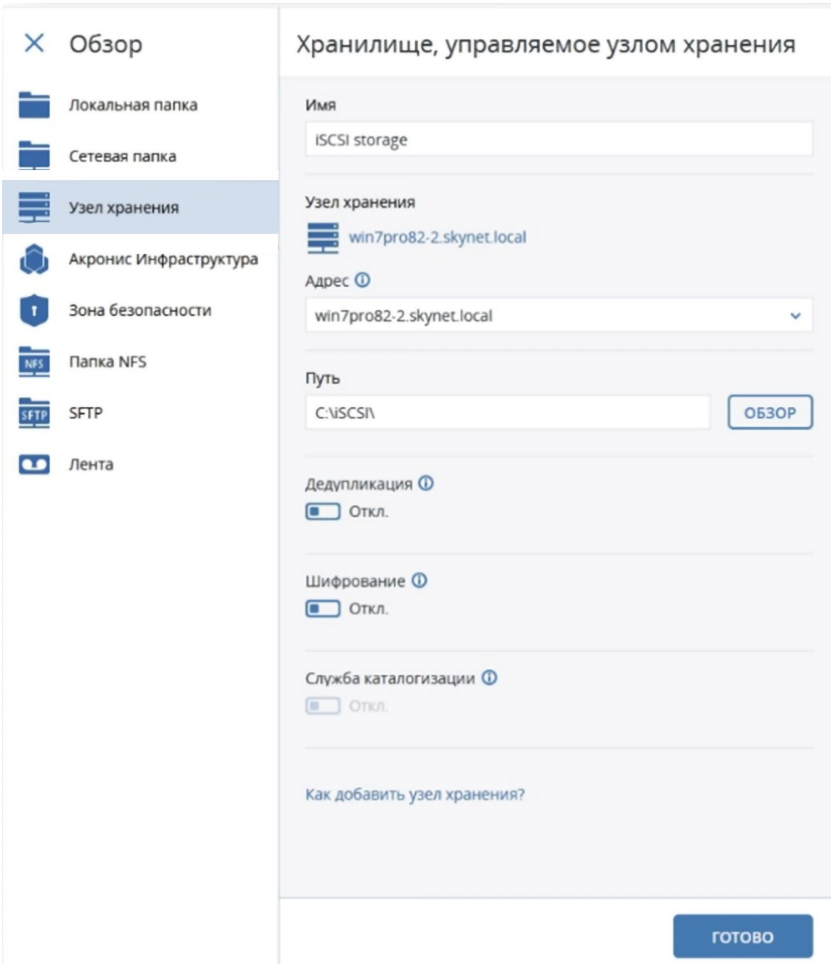
> **!** При создании SMB (сетевой папки) используйте агента, установленного на машине под управлением ОС Windows. При создании NFS (сетевой папки) используйте агента, установленного на машине под управлением ОС Linux. Это происходит из-за ограничения использования NFS агентами Windows.



Добавление управляемых хранилищ

1. В разделе **Хранилище резервных копий** нажмите **Добавить хранилище**.
2. Создайте 2 хранилища (iSCSI-хранилище и FC-хранилище), управляемых узлом хранения:
   1. Выберите узел хранения.
   2. Введите имя хранилища.
   3. Укажите путь до локальной папки, где будет располагаться хранилище.

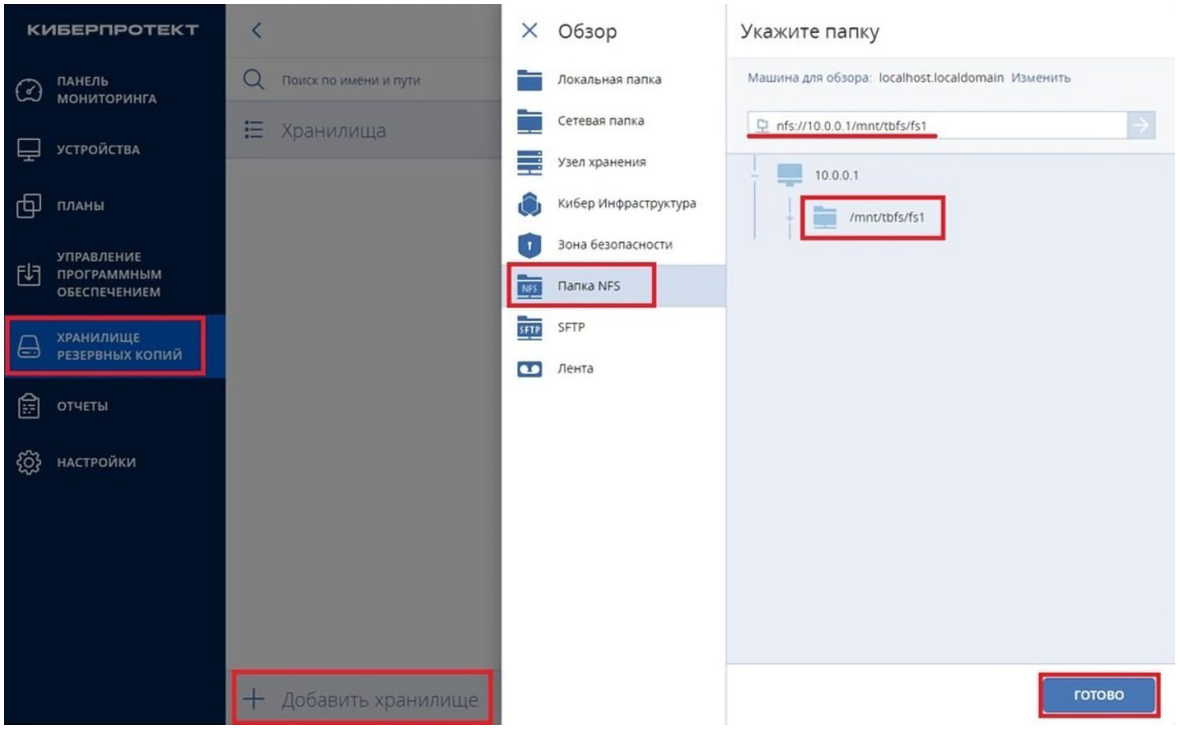
> **!** Хранилища будут находиться в папках D:\iSCSI-storage\ и E:\FC-storage\. При указании расположения хранилища не используйте корневую директорию, а создайте в ней отдельную папку.



Подробнее о создании управляемого хранилища можно прочитать в документации Кибер Бэкап.
В итоге на сервере управления будет создано четыре хранилища, которые можно использовать для хранения резервных копий.

Добавление папки NFS

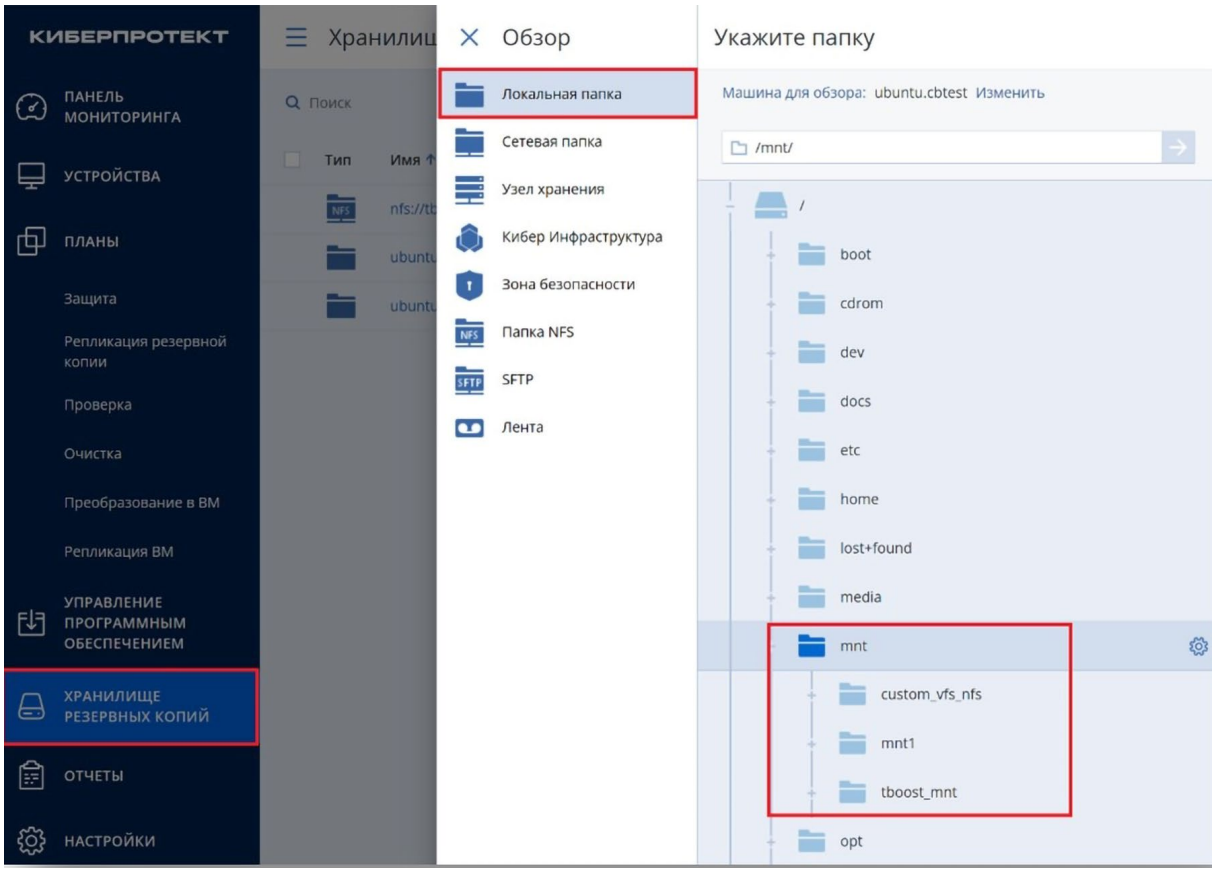
1. В разделе **Хранилище резервных копий** нажмите **Добавить хранилище**.
2. В окне **Создание нового хранилища** выберите тип хранилища — NFS.
3. В поле **Машина для обзора** выберите агента, установленного на машине под управлением ОС Linux, который имеет доступ к NFS-серверу.
4. Настройте подключение к NFS:
   1. В поле **Сетевой путь** укажите путь к каталогу, экспортированному на NFS-сервере. Убедитесь, что агент имеет права доступа на запись в указанную папку.
   2. Нажмите **Сохранить**, чтобы создать хранилище. Система автоматически проверит подключение к NFS-хранилищу.
      Если проверка прошла успешно, NFS-хранилище отобразится в списке доступных для использования.



Добавление в качестве локальной папки NFS-экспорта или виртуальной файловой системы, экспортированной по протоколу T-BOOST

Для добавления локальной папки, в которую смонтирован NFS-экспорт или виртуальная файловая система, экспортированная по протоколу T-BOOST, выполните следующие шаги:

1. Выполните монтирование NFS-экспорта или виртуальной файловой системы, экспортированной с помощью T-BOOST, согласно рекомендациям по конфигурации системы TATLIN.BACKUP.M (стр. 6).
2. Откройте веб-консоль Кибер Бэкап и войдите под учетной записью администратора.
3. Перейдите в раздел **Хранилище резервных копий**.
4. Нажмите **Добавить хранилище**.
5. Выберите тип хранилища — **Локальная папка**.
6. В поле **Путь** укажите локальный путь к папке, в которую смонтирован NFS-экспорт или виртуальная файловая система, экспортированная по протоколу T-BOOST.



7. В поле **Сетевой путь** укажите путь к папке, экспортированной на NFS-сервере. Убедитесь, что агент имеет права доступа на запись в указанную папку.
8. Нажмите **Сохранить**, чтобы создать хранилище. Система автоматически проверит подключение к NFS-хранилищу. Если проверка прошла успешно, NFS-хранилище отобразится в списке доступных для использования.

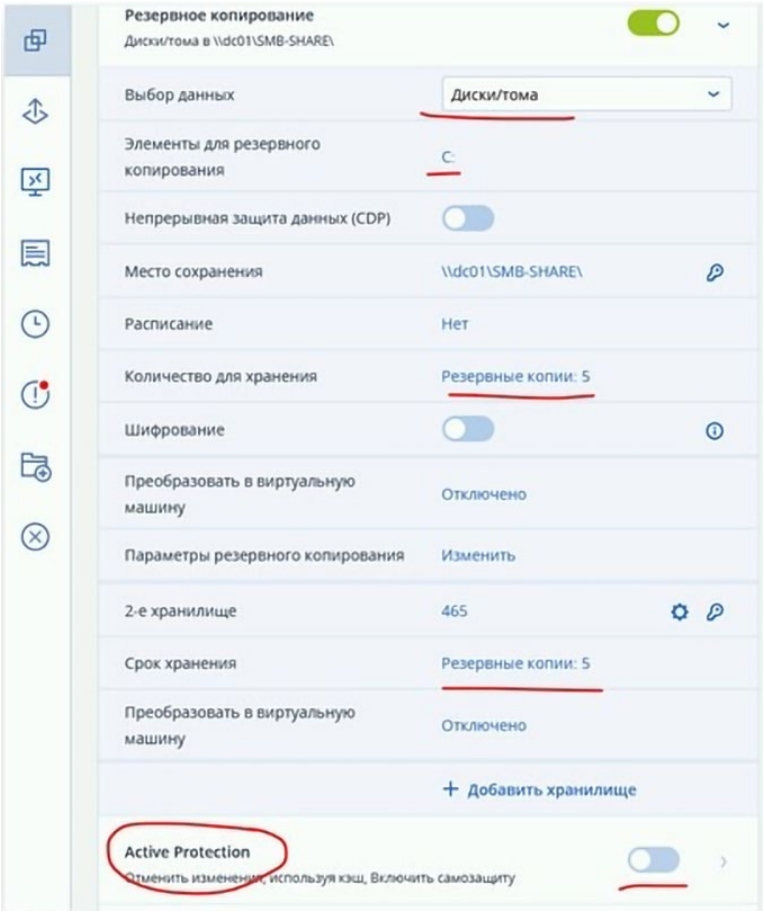
Создание планов резервного копирования

Создайте задания резервного копирования для тестирования сохранения резервных копий в хранилища. Для максимального упрощения создайте два задания, в каждом из которых используйте два хранилища. Реальное резервное копирование будет происходить только в первое хранилище, после чего готовая резервная копия будет реплицироваться во второе хранилище. С учетом нескольких запусков задания и работы правил хранения (удаление старых копий) нагрузка на второе хранилище будет такого же профиля, как и на первое.

Первое задание (SMB)

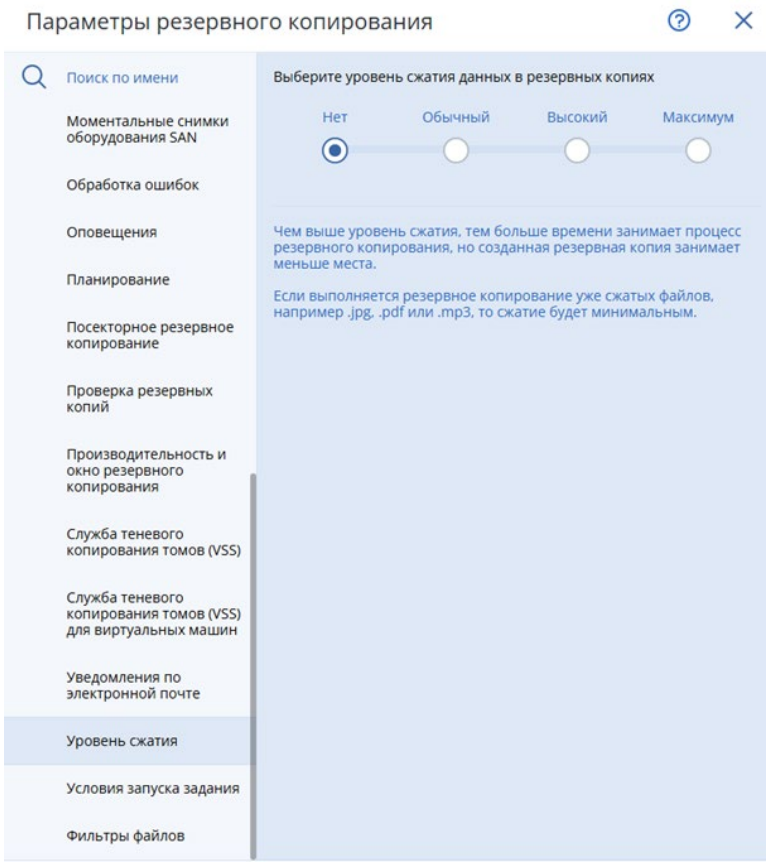
Создайте задание резервного копирования тома системного накопителя 1 на сетевую папку SMB:

1. Перейдите в **Устройства** — **Машины с агентами**.
2. Выберите агента, который является машиной узла хранения.
3. Нажмите **Защитить** и создать новый план:
   - Выбор данных — диски и тома.
   - Элементы резервного копирования — системный накопитель 1.
   - Место сохранения — созданное ранее хранилище — сетевая папка SMB.
   - Расписание — выключено (схема всегда инкрементальная копия).
   - Количество для хранения — 5 копий.
   - Шифрование — отключено.
   - Второе хранилище — iSCSI-хранилище.
   - Срок хранения — 5 копий.
4. Выключите опцию **Active protection** и другие защитные механизмы.



!

При использовании TATLIN.BACKUP в связке с агентом резервного копирования Cyber Backup (например, Acronis), необходимо отключить сжатие на стороне Cyber Backup. Сжатие будет выполняться на стороне агента TBoost, что обеспечивает корректную дедупликацию и максимальную эффективность хранения. Включённое сжатие на стороне Cyber Backup может привести к ухудшению коэффициента дедупликации и увеличению нагрузки на систему.



ПРИЛОЖЕНИЕ 1. ДИАГНОСТИКА ПОДКЛЮЧЕНИЯ ПО ПРОТОКОЛУ SMB

! Оригинальная статья доступна на официальном сайте Киберпротект.

При возникновении сложностей с записью резервных копий в хранилище на сетевой папке SMB рекомендуется смонтировать сетевую папку вручную и записать в нее данные средствами ОС без участия агента.

Linux

1. Создайте папку /mnt/test, в которую монтируется сетевая папка:

```
# sudo mkdir /mnt/test
```

2. Смонтируйте сетевую папку:

```
# mount -t cifs -o username=DOMAIN\Administrator,vers=3.0
//<SERVER_NAME>/<SHARE_NAME> /mnt/test
Password for user_name@//<SERVER_NAME>/<SHARE_NAME>: ********
```

DOMAIN\Administrator
Имя пользователя для доступа к сетевой папке.

vers=3.0
Версия протокола SMB.
Возможные значения: 1, 2.0, 2.1, 3.0, 3.1 и т.д.

//<SERVER_NAME>/<SHARE_NAME>
Адрес сетевой папки для подключения.

/mnt/
Локальная папка, в которую монтируется сетевая папка при подключении.

Если команда завершается ошибкой

1. Создайте случайный файл размером 1 ГБ и запишите его на смонтированную сетевую папку:

```
# dd if=/dev/random of=/mnt/test/test_file bs=1M count=1024 oflag=direct
1024+0 records in
1024+0 records out
1073741824 bytes (1.1 GB, 1.0 GiB) copied, 15.7536 s, 68.2 MB/s
```

В выводе этой команды отображается время копирования файла и средняя скорость, с которой файл был записан в сетевую папку.

Данный профиль записи схож с процессом записи данных агентом при резервном копировании. Поэтому скорость, указанная в тесте, будет близка к реальной скорости записи резервной копии, если исходный накопитель способен передавать данные с достаточной скоростью.

2. По окончании диагностики размонтируйте сетевую папку:

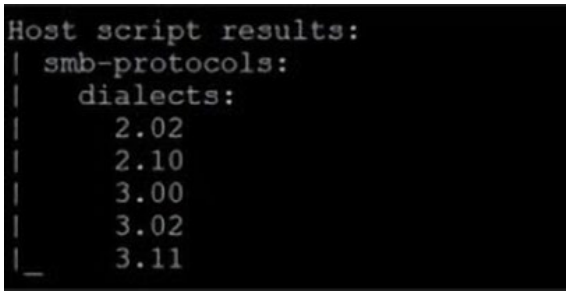
```
# umount /mnt/test
```

Первое задание (SMB)

Если СХД некорректно работает с протоколами SMB версий 2.1-3.0, рекомендуется обновить ПО СХД и настроить вручную протокол SMB версии 2.1 и выше. В качестве альтернативы можно настроить агентов на работу с устаревшими версиями протоколов (1, 2.0).

Чтобы проверить поддерживаемые версии протокола SMB удаленного сервера, используйте утилиту nmap:

```
# nmap -p445 --script smb-protocols <SERVER_ADDRESS>
```

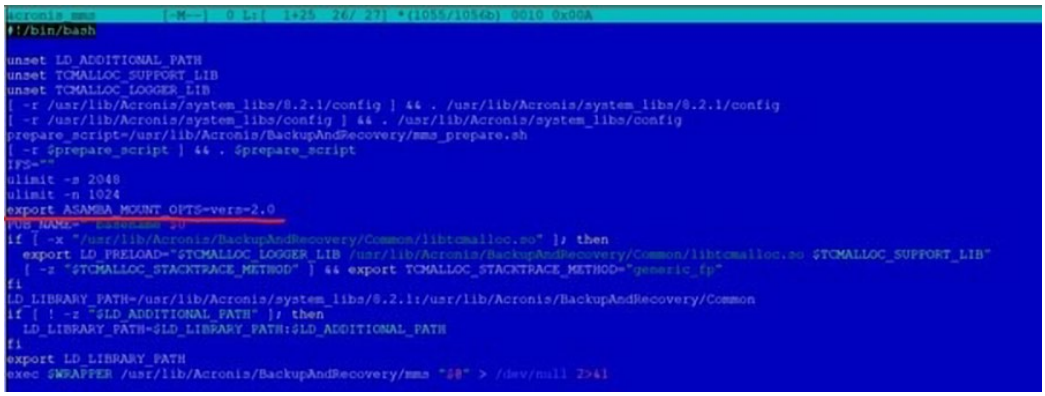


Жесткое указание версии протокола SMB для агента

Агент Linux

1. Отредактируйте файл /usr/sbin/acronis_mms. После строк ulimit добавьте строку xport ASAMBA_MOUNT_OPTS=vers=2.0.

   vers=2.0
   Версия SMB, которую нужно использовать агенту.

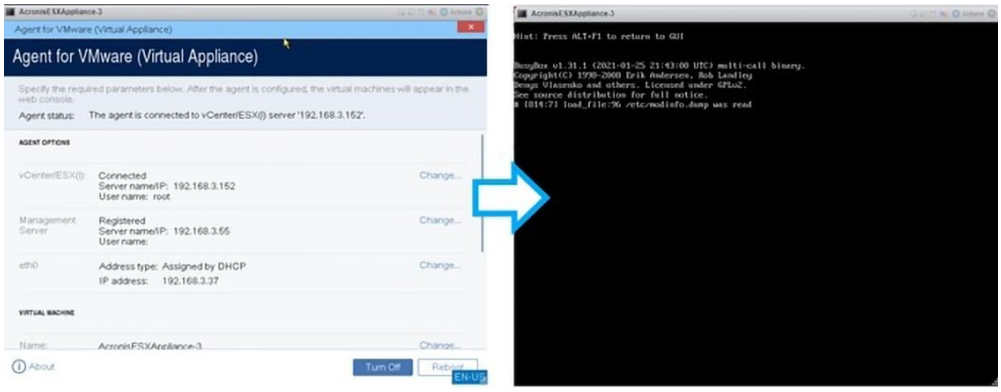


2. Сохраните файл и перезагрузите агента:

```
# systemctl restart acronis_mms
```

Агент Virtual Appliance

1. Подключитесь к консоли Virtual Appliance.
2. В GUI нажмите Ctrl + Shift + F2.



3. Отредактируйте файл `/bin/autostart`. После строк `ulimit` добавьте строку
   `export ASAMBA_- MOUNT_OPTS=vers=2.0`
   Это можно сделать с помощью текстового редактора vi или в консоли Virtual appliance с помощью утилиты WinSCP.
4. Перезагрузите Virtual Appliance:

```
# reboot
```

Дополнительно рекомендуется ознакомится с материалами:

- https://learn.microsoft.com/en-us/windows-server/storage/file-server/file-server-smb-overview>
- https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/storage_administration_guide/mounting_an_smb_share

ПРИЛОЖЕНИЕ 2. ОШИБКА FAILED TO LOCK THE FILE ПРИ РЕЗЕРВНОМ КОПИРОВАНИИ НА NFS-ХРАНИЛИЩЕ

! Оригинальная статья доступна на официальном сайте Киберпротект.

При резервном копировании в неуправляемые хранилища (SMB, NFS, SFTP) агент пытается блокировать файл резервной копии для монопольного доступа на запись.

Если NFS-сервер не поддерживает данные блокировки или они отключены, выводится одна из следующих ошибок:

- Failed to lock the file.
- Failed to replace the volume.
- Object is locked.
- Input/output error.
- Не удалось заблокировать файл.
- Ошибка операционной системы: No locks available.

! Это актуально также и для СХД, которые не поддерживают протокол NFSv4.

Если Сервер NFS не поддерживает работу с блокировками файлов или блокировку диапазонов данных в файлах, рекомендуется:

- Включить блокировки в настройках NFS-сервера или обновить NFS-сервер до версии 4 и выше.
- Выключить на агенте Кибер Бэкап обязательную работу с блокировками.

Отключение блокировок NFS (агент для Linux)

1. Отредактируйте файл конфигурации с помощью редактора vi:

```
vi /usr/sbin/acronis_mms
```

2. Нажмите i и перейдите в режим редактирования.
3. После строки `ulimit -s 2048` добавьте строку `export MOUNT_NFS_NOLOCK=1`.
4. Сохраните файл конфигурации и выйдите из редактора:
   1. Нажмите Esc.
   2. Введите команду:

```
vi /usr/sbin/acronis_mms
```

5. Перезапустите службу агента:

```
systemctl restart acronis_mms restart
```

Резервное копирование и репликация резервных копий на общие ресурсы NFS

Резервное копирование и репликация резервных копий на общие ресурсы NFS могут выполняться с помощью агента для Linux, агента для VMware (виртуального устройства) или загрузочного носителя на базе Linux.

Включите службы Windows для NFS на устройстве, на котором установлен сервер управления Кибер Бэкап при создании централизованного неуправляемого хранилища, или на устройстве, на котором установлен узел хранения Кибер Бэкап при создании централизованного управляемого хранилища:

1. Откройте панель управления.
2. Перейдите в раздел Программы — Программы и компоненты.
3. Нажмите Включение или отключение компонентов Windows.
4. Установите флажок Службы для NFS, а также установите флажки для всех вложенных каталогов.

Общие ресурсы NFS перечислены в файле конфигурации `/etc/exports`.
Для создания резервной копии в общей папке необходимо указать путь вида: `nfs://<SERVER_NAME>/<SHARE>:/`.
Для создания резервной копии во вложенной папке необходимо указать путь вида:
`nfs://<SERVER_-NAME>/<SHARE>:/<SUBFOLDER>`.
Например, файл `/home/tester *(rw,sync,no_subtree_check,no_root_squash)` экспортируется в файл `/etc/exports`.
Для резервного копирования в папку `/home/tester` укажите `nfs://<SERVER_-NAME>/home/tester:/`.
Для резервного копирования в папку `/home/tester/subfolder` укажите `nfs://<SERVER_NAME>/home/tester:/`.