WHITE PAPER

РЕКОМЕНДАЦИИ ПО ОПТИМИЗАЦИИ И ИНТЕГРАЦИИ TATLIN.BACKUP.M С RUBACKUP

Головин А. Ю.

О WHITE PAPERS

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 и носит рекомендательный характер.
Конкретные результаты и эффективность конечных решений зависят от множества факторов, которые могут различаться в зависимости от особенностей инфраструктуры и условий эксплуатации.

ОГЛАВЛЕНИЕ

ОБ АВТОРЕ 4
ВВЕДЕНИЕ 5
ОБЩИЕ РЕКОМЕНДАЦИИ ПО КОНФИГУРАЦИИ TATLIN.BACKUP.M 6
ТЕКУЩИЕ ЛИМИТЫ TATLIN.BACKUP.M 7
АРХИТЕКТУРА RUBACKUP 7
КОМПОНЕНТЫ СИСТЕМЫ 7
РЕКОМЕНДАЦИИ ПО КОНФИГУРАЦИИ RUBACKUP 8
ОБЩИЕ РЕКОМЕНДАЦИИ ПО КОНФИГУРАЦИИ RUBACKUP 8
НАСТРОЙКИ TATLIN.BACKUP.M 9
СОЗДАНИЕ ФАЙЛОВЫХ СИСТЕМ 9
СОЗДАНИЕ ФАЙЛОВЫХ РЕСУРСОВ NFS 10
СОЗДАНИЕ ФАЙЛОВЫХ РЕСУРСОВ CIFS/SMB 10
СОЗДАНИЕ ТОЧКИ МОНТИРОВАНИЯ NFS НА UNIX-КЛИЕНТЕ 11
НАСТРОЙКИ RUBACKUP 11
ЗАПИСЬ РЕЗЕРВНЫХ КОПИЙ НА ОБЩИЕ РЕСУРСЫ, СОЗДАННЫЕ НА TATLIN.BACKUP.M 11
РЕЗЕРВНОЕ КОПИРОВАНИЕ С ИСПОЛЬЗОВАНИЕМ ПЕРЕДАЧИ ДАННЫХ РЕЗЕРВНЫХ КОПИЙ ПО ПРОТОКОЛУ T-BOOST С МЕДИАСЕРВЕРА RUBACKUP 14
РЕЗЕРВНОЕ КОПИРОВАНИЕ С ИСПОЛЬЗОВАНИЕМ ПЕРЕДАЧИ ДАННЫХ РЕЗЕРВНЫХ КОПИЙ ПО ПРОТОКОЛУ T-BOOST НАПРЯМУЮ С АГЕНТА RUBACKUP 14

ОБ АВТОРЕ

Алексей Головин — специалист с 15-летним опытом работы в IT, включая опыт в таких компаниях, как Dell EMC и системных интеграторах. В 2022 году присоединился к команде YADRO в должности ведущего специалиста по интеграционным решениям. В YADRO 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, Dell EMC и других компаний-производителей.

ВВЕДЕНИЕ

Данный документ предназначен для ИТ-специалистов и администраторов, ответственных за внедрение и поддержку системы хранения данных TATLIN.BACKUP.M (далее — TATLIN.BACKUP.M, СХД). Документ содержит рекомендации по настройке и оптимизации TATLIN.BACKUP.M, а также по интеграции с системой резервного копирования RuBackup (далее — RuBackup, СРК) 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 их восстановлению.

ВЕРСИИ ИСПОЛЬЗУЕМОГО ПО

ПО	ВЕРСИЯ
TATLIN.BACKUP	1.1
RuBackup	2.5

ОБЩИЕ РЕКОМЕНДАЦИИ ПО КОНФИГУРАЦИИ TATLIN.BACKUP.M

1. 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.
2. Для оптимальной работы T-RAID (для оптимального распределения дисков по группам аллокации) рекомендуется производить увеличение дисковой емкости целыми модулями.
3. На СХД 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.
4. В целях повышения отказоустойчивости при передаче данных по Ethernet-соединениям рекомендуется использовать технологию агрегации каналов LACP.
5. 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`).
6. Если доступ к СХД осуществляется через один отказоустойчивый хост, рекомендуется использовать одну LACP-агрегацию (`bond0:data0p0, data0p1`, `data1p0`, `data1p1`).
7. На сетевых data-интерфейсах рекомендуется использовать jumbo-фреймы с MTU 9000 для эффективного использования каналов.
8. Рекомендации по настройке LACP в файловых системах:
   - Выбор метода балансировки (Transmit Hash Policy)
     - **Layer2+3 (MAC + IP)** — рекомендуется при использовании нескольких IP-адресов на агрегированном интерфейсе. Метод обеспечивает равномерное распределение трафика.
     - **Layer3+4 (IP + TCP/UDP Port)** — используется при динамическом распределении нагрузки, но не гарантирует равномерного распределения.
   - Настройка LACP для файловых систем
     - **NFS**
       - **Layer2+3** предпочтителен с несколькими IP-адресами.
       - **Layer3+4** применим с **nconnect=<N>** для увеличения числа соединений.
     - **CIFS/SMB**
       - **Layer2+3** обеспечивает стабильное распределение трафика.
       - **Layer3+4** допустим при отсутствии дополнительных IP-адресов.
     - **T-BOOST**
       - **Layer2+3** предпочтителен при работе с несколькими виртуальными файловыми системами.
9. Рекомендуется выбирать версию протокола NFS в зависимости от поддерживаемой версии на хосте или в ПО системы резервного копирования (далее — СРК). При наличии поддержки NFSv4 предпочтительно использовать именно ее.
10. При монтировании по NFS рекомендуем использовать следующие опции:
    - Использовать mount-опцию `-o write=eager`.
    - Не использовать `direct` при записи.
    - Убедиться, что NFS примонтирован с `rsize/wsize 1 Mb` (1048576 байт) .
11. Для достижения большей скорости обмена данными с TATLIN.BACKUP.M рекомендуется отдавать предпочтение I/O со следующими характеристиками:
    - Разделение по направлению передачи данных (`read` или `write`, не смешанный `read/write`).
    - Большой блок данных: 1–4 МиБ.
    - Последовательное выполнение операций.
    - Несколько I/O потоков на виртуальной файловой системе: 4–16 I/O потоков в каждую из 4–16 виртуальных файловых систем.
12. Оптимальная производительность СХД достигается при совершении операций в 32 потока, равномерно распределенных по виртуальной файловой системе.
13. Для эффективного использования механизма дедупликации рекомендуется отключить механизм дедупликации на уровне ПО СРК.

ТЕКУЩИЕ ЛИМИТЫ TATLIN.BACKUP.M

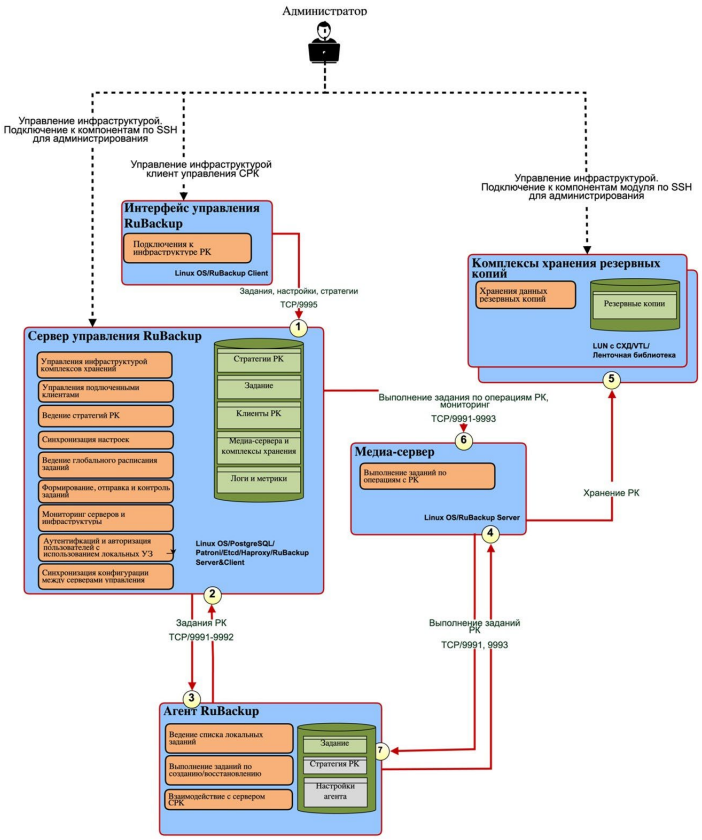
ПАРАМЕТРЫ	ОГРАНИЧЕНИЯ
Максимальный размер файла	16 ТБ
Максимальный размер файловой системы	693.3 ТБ / 630.6 ТиБ
Максимальное количество виртуальных файловых систем на СХД	64 виртуальных файловых системы/ресурса с общим доступом
Максимальное количество пользователей	59 000
Максимальное число файлов на 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 RUBACKUP

КОМПОНЕНТЫ СИСТЕМЫ

Архитектура RuBackup включает в себя следующие компоненты:

- Основной сервер, включающий систему управления базами данных (далее — СУБД) для хранения метаданных резервных копий и конфигурационных параметров.
- Медиасервер — серверы, на которых подключены устройства хранения резервных копий.
- Агент СРК, осуществляющий сбор данных на клиенте, формирование и передачу резервной копии.



Управление RuBackup может осуществляться с помощью:

- веб-интерфейса Tucana;
- графического интерфейса;
- утилиты командной строки;
- программного интерфейса REST API.

RuBackup поддерживает одновременную установку всех компонентов на один сервер при выполнении консолидированных аппаратных требований, предъявляемых компонентами к серверу, на который производится установка. Этот способ установки называется «Все в одном».

RuBackup поддерживает работу в режиме высокой доступности, включая:

- конфигурацию СУБД с применением решения Patroni, развернутом на отдельно стоящих серверах;
- использование резервного сервера в дополнение к основному. В случае отказа основного сервера резервный сервер возьмет на себя функции основного сервера RuBackup, а агенты RuBackup подключатся к резервному серверу. После восстановления функционирования основного сервера агенты RuBackup подключатся к основному серверу.

Пакеты для развертывания RuBackup могут быть установлены из дополнительного публичного репозитория или из **облачного диска** компании «Группа Астра».

Публичные репозитории доступны для таких ОС, как:

- Astra Linux 1.8;
- Astra Linux 1.7;
- Astra Linux 1.6;
- Debian 10;
- Ubuntu 20.04;
- Ubuntu 1 8.04.

Документация на RuBackup доступна на **официальном сайте RuBackup**.

РЕКОМЕНДАЦИИ ПО КОНФИГУРАЦИИ RUBACKUP

Сценарии использования TATLIN.BACKUP.M для хранения и передачи резервных копий RuBackup:

- Запись резервных копий на общие ресурсы, созданные на TATLIN.BACKUP.M:
  - NFS (v3 и v4) для высокопроизводительной передачи данных между серверами.
  - SMB/CIFS.
- Передача резервных копий с использованием T-BOOST для увеличения производительности резервного копирования с функцией дедупликации:
  - Передача данных резервных копий с медиасервера RuBackup на TATLIN.BACKUP.M.
  - Передача данных резервных копий напрямую с агента RuBackup на TATLIN.BACKUP.M.

ОБЩИЕ РЕКОМЕНДАЦИИ ПО КОНФИГУРАЦИИ RUBACKUP

Ниже приведены общие рекомендации для обеспечения оптимальной работы TATLIN.BACKUP.M в среде резервного копирования RuBackup.

Размер блока при записи

- Для NFS: используйте блок записи объемом 1 МБ.
- Для SMB: предпочтительно использовать блок записи объемом 4 МБ.

Оптимизация данных

- Вместо записи множества мелких файлов рекомендуется объединять файлы в один крупный архив для более эффективной обработки и хранения.
- При записи первой резервной копии рекомендуется выбирать источники с максимальным количеством уникальных блоков данных, чтобы оптимизировать дедупликацию.

Группировка данных для дедупликации

- Рекомендуется объединять однотипные виды данных.
- Рекомендуется настраивать задания для разных типов данных так, чтобы их создание не происходило одновременно.

Шифрование и защита данных
Рекомендуется отключить защитное преобразование резервных копий, поскольку это может затруднить дедупликацию
.

Дедупликация блоков
В настройках создания резервной копии на устройства TATLIN.BACKUP.M в разделе Общие настройки модуля выключите опцию deduplication (дедупликацию блоков), которая выполняется до записи в хранилище.

Глубина хранения и частота резервных копий
Чем чаще создаются резервные копии и выше глубина хранения, тем эффективнее использование TATLIN.BACKUP.M.

Разделение критичных данных
Разделяйте различные типы критичных данных по отдельным устройствам хранения, а также создавайте реплики копий на другие типы хранилищ для дополнительной безопасности.

Методы резервного копирования
TATLIN.BACKUP.M не поддерживает метод резервного копирования с обратной инкрементной копией.

Профиль набора данных
TATLIN.BACKUP.M эффективно поддерживает до 100 миллионов файлов. При превышении этого лимита производительность системы может значительно снизиться. При планировании системы, на которой будут размещаться как резервные копии, так и архивы, учитывайте это ограничение.

Планирование резервного копирования и репликации
Настройте выполнение операций резервного копирования и репликации до начала рабочего дня, чтобы избежать нарушений доступа пользователей к системе TATLIN.BACKUP.M.

Политики резервного копирования
Учитывайте фоновую нагрузку от операций при настройке политик резервного копирования и планировании других задач.

Регулярная очистка данных
Настройте регулярную очистку данных на ежедневной, еженедельной или ежемесячной основе, особенно если объем данных составляет миллионы файлов. Это позволит поддерживать оптимальную производительность хранилища.

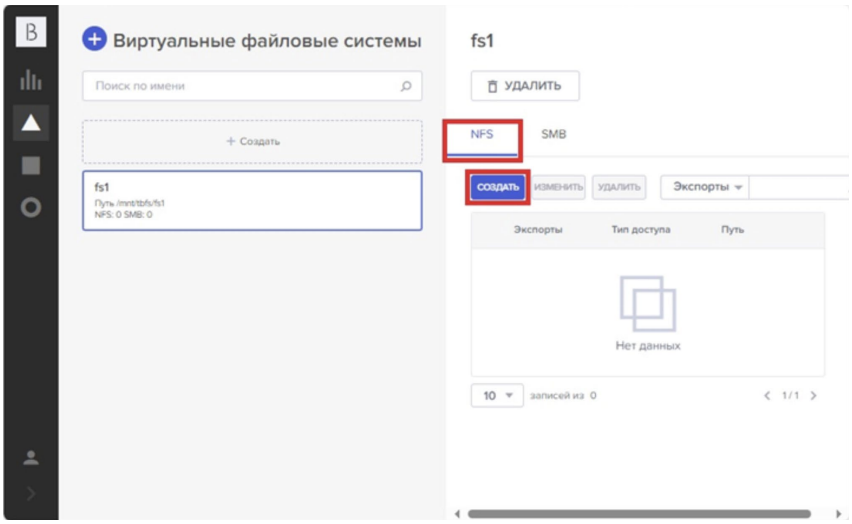
НАСТРОЙКИ TATLIN.BACKUP.M

СОЗДАНИЕ ФАЙЛОВЫХ СИСТЕМ

1. Перейдите в **Хранилище**.
2. Создайте виртуальную файловую систему:
   - Нажмите **Создать** или значок в верхнем левом углу экрана.
   - Введите имя файловой системы. Например, **fs1**.
   - Нажмите **Создать**.
3. Убедитесь, что в **Хранилище** в списке файловых систем для созданной файловой системы отображается путь `/mnt/tbfs/fs1`.
   Если путь отображается, файловая система успешно создана и примонтирована.
4. Повторите шаги 2-3 для создания второй файловой системы, например, **fs2**.

СОЗДАНИЕ ФАЙЛОВЫХ РЕСУРСОВ NFS

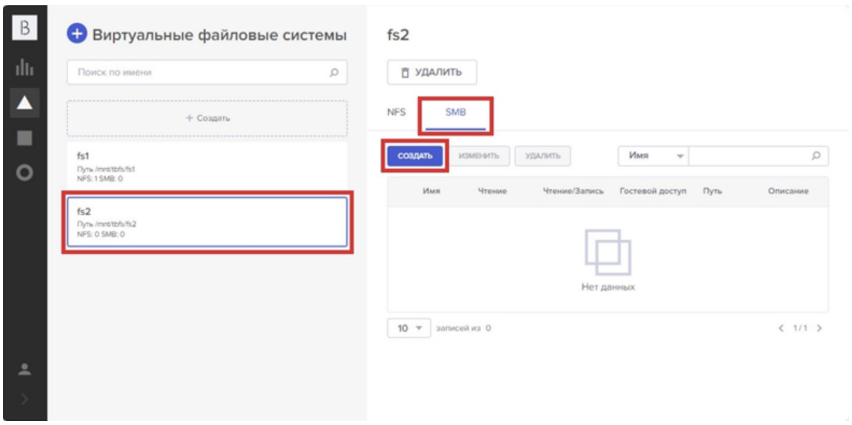
1. В **Хранилище** выберите виртуальную файловую систему fs1.
2. На вкладке NFS нажмите **Создать**.



3. Укажите необходимые значения:
   - В поле **IP-адрес** введите * для предоставления доступа по IP-адресам без ограничений.
   - В поле **Тип доступа** выберите **Чтение/Запись**.
4. Убедитесь, что созданный экспорт появился в списке экспортов NFS.

СОЗДАНИЕ ФАЙЛОВЫХ РЕСУРСОВ CIFS/SMB

1. В **Хранилище** выберите виртуальную файловую систему **fs2**.
2. На вкладке **SMB** нажмите **Создать**.



3. Укажите необходимые значения:
   - В поле **Имя** введите имя ресурса, например, **fs2guest**.
   - В поле **Гостевой доступ** выберите **Чтение/Запись**.
4. Убедитесь, что созданный экспорт появился в списке экспортов SMB.

СОЗДАНИЕ ТОЧКИ МОНТИРОВАНИЯ NFS НА UNIX-КЛИЕНТЕ

Чтобы настроить точку монтирования NFS на UNIX-клиенте для доступа к нужному хранилищу, выполните следующие шаги:

1. Создайте локальную директорию для монтирования.
2. С правами пользователя `root` создайте директорию, в которой будет смонтирован ресурс с общим доступом по протоколу NFS:

```
mkdir /mnt/tb
```

3. Смонтируйте удаленный NFS-ресурс в локальную директорию. Используйте команду mount с указанием нужных опций для используемой ОС.
   Пример команды монтирования NFS-ресурса с TATLIN.BACKUP.M с настройками для оптимальной производительности

```
mount -t nfs -o nolock,hard,intr,vers=3,tcp, rsize=32768,wsize=32768,bg
<TBHOSTNAME>:/data/<VFS> /mnt/tb
```

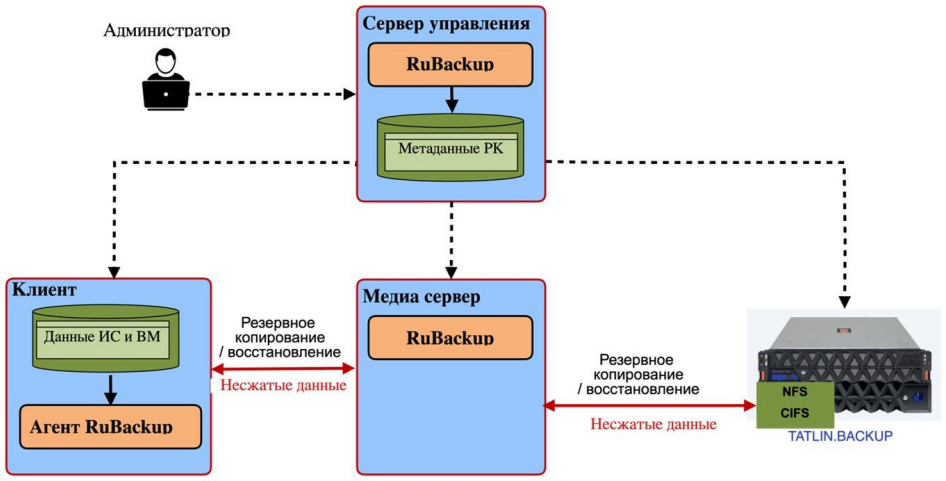
4. Проверьте монтирование:

```
ls -ltr /mnt/tb
```

НАСТРОЙКИ RUBACKUP

ЗАПИСЬ РЕЗЕРВНЫХ КОПИЙ НА ОБЩИЕ РЕСУРСЫ, СОЗДАННЫЕ НА TATLIN.BACKUP.M

Медиасервер RuBackup использует общий ресурс TATLIN.BACKUP.M, если он примонтирован к ОС с установленным компонентом RuBackup в качестве локального агента.



Для настройки RuBackup используется следующая последовательность шагов:

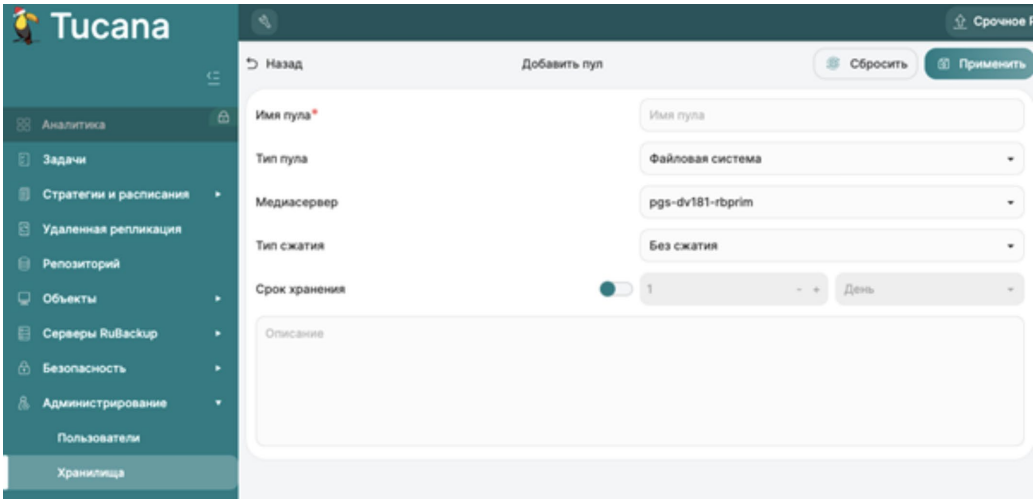
1. Добавление нового пула.
2. Создание локального файлового хранилища.
3. Отключение дедупликации на резервной копии RuBackup.

> **!** Скриншоты в инструкциях ниже иллюстрируют процесс выполнения в веб-интерфейсе Tucana, последовательность шагов в оконном приложении Менеджер Администратора RuBackup (далее — RBM) аналогична.

Добавление нового пула

Для создания нового пула любого типа:

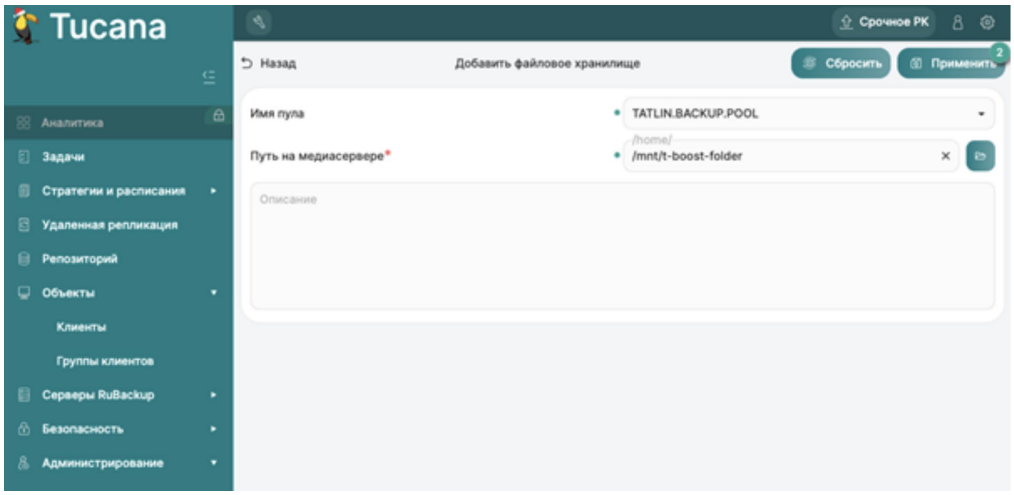
1. Откройте **Администрирование** — **Пулы**.
2. Нажмите **Добавить**.
3. Нажмите **Добавить пул** и заполните следующие поля:
   - **Имя пула** — уникальное имя добавляемого пула.
   - **Тип пула** — тип создаваемого пула: **Файловая система**.
   - **Тип сжатия** — вариант компрессии резервных копий: **Без сжатия**.
   - **Медиасервер** — медиасервер, которому будет принадлежать создаваемый пул.
   - **Срок хранения**.
   - **Описание**.



4. Нажмите **Применить**.

Создание локального файлового хранилища

1. Откройте **Администрирование** — **Локальные файловые хранилища**.
2. Нажмите **Добавить**.
3. Укажите имя пула, созданного на предыдущем этапе.
4. В поле **Путь на медиасервере** укажите путь на медиасервере, которому принадлежит выбранный пул:
   1. Нажмите **Выбрать** (значок).
   2. Укажите каталог на медиасервере. Для этого необходимо, чтобы на медиасервере был запущен клиент резервного копирования. При этом для просмотра будут доступны каталоги только на том медиасервере, которому принадлежит пул.



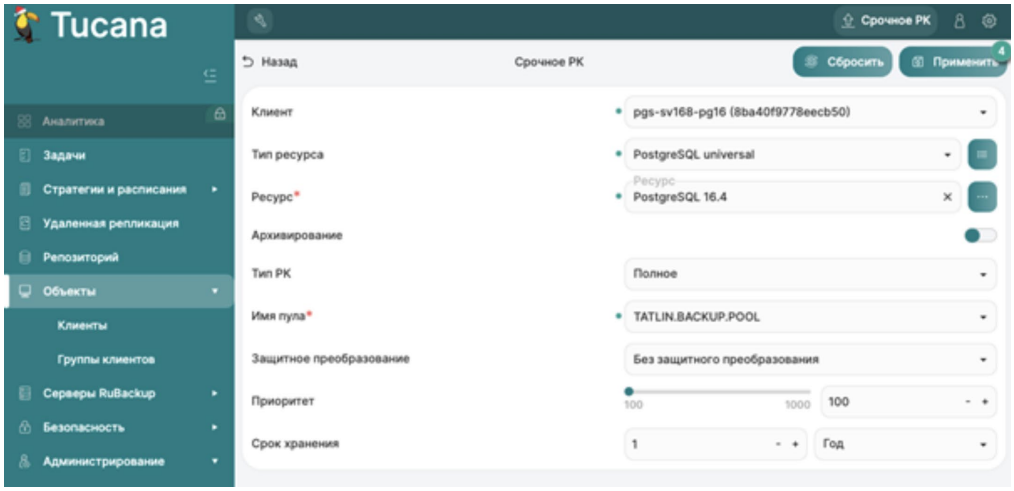
Создание резервной копии, отключение дедупликации

Основными сценариями использования RBM являются:

- Создание срочной резервной копии.
- Создание стратегии.
- Создание глобального расписания.

Создание резервной копии на примере срочной резервной копии:
На странице **Объекты** окно разделено на две части. В левой части окна представлена древовидная структура **Группа клиентов** — **Клиенты** — **Модули клиента**, в правой — табличная информация по выбранной группе клиентов, клиенту или модулю с возможностью переключения вкладок. Клиенты, которые в данный момент находятся online, отмечены зеленым цветом, в состоянии offline — красным.

1. Выберите клиента.
2. Справа от поля поиска выберите **Срочное РК** (срочное резервное копирование).



3. Выберите ресурс, тип ресурса и тип резервной копии, пул, вид защитного преобразования и приоритет срочного резервного копирования.
4. Нажмите **Общие настройки модуля**.
5. Отключите опцию **deduplication**.
6. Выставить количество **worker_parallelism = 1**.

> **!** **ВАЖНО! Необходимо проконтролировать чтобы количество всегда было не больше 1!**
> (на окно / скорость резервного копирования увеличение данного параметра не влияет)

7. После заполнения полей необходимо нажать «Применить». Срочное резервное копирование позволяет единоразово создать резервную копию ресурса выбранного клиента, не назначая правило по расписанию. Срочное резервное копирование позволяет создать полную, инкрементальную или дифференциальную копию.

РЕЗЕРВНОЕ КОПИРОВАНИЕ С ИСПОЛЬЗОВАНИЕМ ПЕРЕДАЧИ ДАННЫХ РЕЗЕРВНЫХ КОПИЙ ПО ПРОТОКОЛУ T-BOOST С МЕДИАСЕРВЕРА RUBACKUP

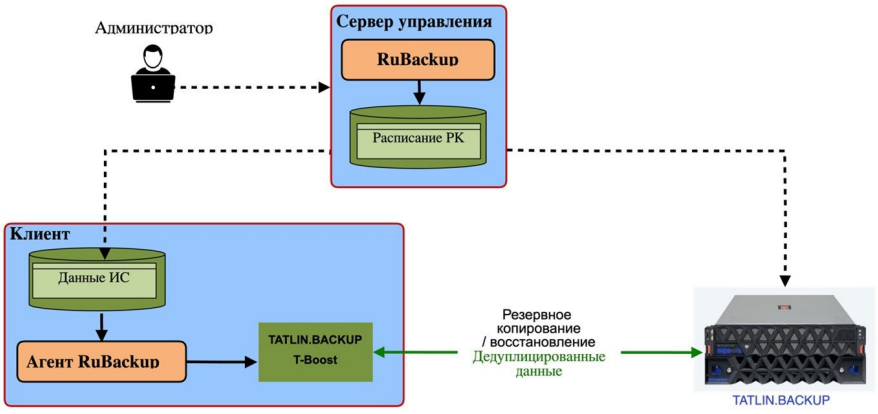
Агент T-BOOST устанавливается на медиасервер RuBackup, где проводит анализ данных на наличие уникальных блоков для создания их резервной копии. Сервер RuBackup сохраняет все возможности по управлению резервными копиями. Недостатком данного способа является передача несжатых данных между агентом и медиасервером RuBackup.



Медиасервер RuBackup использует общий ресурс TATLIN.BACKUP.M, предоставленный локально агентом T-BOOST. Последовательность настройки RuBackup полностью аналогична предыдущему пункту.

РЕЗЕРВНОЕ КОПИРОВАНИЕ С ИСПОЛЬЗОВАНИЕМ ПЕРЕДАЧИ ДАННЫХ РЕЗЕРВНЫХ КОПИЙ ПО ПРОТОКОЛУ T-BOOST НАПРЯМУЮ С АГЕНТА RUBACKUP

Агент T-BOOST устанавливается на клиента, агент RuBackup выполняет резервное копирование непосредственно на TATLIN.BACKUP.M с помощью агента T-BOOST. При таком способе между клиентом, на котором установлен агент RuBackup, и агентом RuBackup будут передаваться дедуплицированные данные. Недостатком данного способа является потеря управления резервными копиями сервером RuBackup, который сохранит возможности отдавать команды резервирования/восстановления и их планирования.



Агент RuBackup использует общий ресурс TATLIN.BACKUP.M, предоставленный локально агентом T-BOOST. Последовательность настройки RuBackup полностью аналогична предыдущему пункту.