RuBackup

Система резервного копирования
и восстановления данных

ОСНОВНЫЕ СВЕДЕНИЯ

ВЕРСИЯ 2.9.0.0.0

Содержание

Система резервного копирования RuBackup — клиент-серверное приложение, которое:

- автоматически выполняет резервное копирование СУБД, виртуальных машин, почтовых систем, файловых систем, подсистемы Linux и службы каталогов;
- восстанавливает данные из резервных копий по запросу.

Полностью российская разработка с возможностью гибкой адаптации под требования заказчика.

Для быстрого создания системы обеспечения сохранности данных используйте программный комплекс RuBackup OneClick. Продукт ориентирован на малый, средний бизнес и территориально распределенные организации.

Поддерживаемые продукты

СУБД	Системы виртуализации (безагентный способ)	Почтовые системы
Tantor Special Edition (с использованием модуля PostgreSQL) Arenadata Greenplum Microsoft SQL Server MySQL Oracle Database PostgreSQL + в кластере Patroni Postgres Pro SAP HANA YandexDB РЕД База Данных	**ПК СВ «Брест»** **VMmanager** Альт Виртуализация (с использованием модуля Proxmox VE) АЭРОДИСК vAir Р-Виртуализация РУСТЭК Basis Dynamix Enterprise KVM Microsoft Hyper-V OpenStack oVirt/zVirt/REDVirt Proxmox VE ROSA Space VM Tionix VMware vSphere	**RuPost** CommuniGate Pro Mailion VK Workmail Microsoft Exchange

Файловые системы	Подсистема Linux
Linux (Ext4, Ext3, Ext2, XFS, ZFS, BTRFS) Windows (NTFS)	LVM Linux

Службы каталогов	Хранилища
ALD Pro **FreeIPA** Microsoft Active Directory	Файловые хранилища Блочные устройства Облачные хранилища Ленточные библиотеки Клиентские хранилища

Преимущества

- Лучшая производительность среди российских решений
- Сертификат соответствия ФСТЭК России №4879
- Единственное решение с многопоточностью — на всех этапах позволяет выполнять самые жесткие требования к срокам RPO и RTO
- Широкие возможности интеграции — полнофункциональный REST API, толстый клиент и Web, CLI, документация для интеграторов и клиентов
- Надежность и масштабируемость — встроенные алгоритмы кластеризации и балансировки нагрузки между узлами СРК, резервирование собственных компонентов СРК
- Глубокая интеграция с Postgres — поддержка инкрементальных и дифференциальных копий (PTRACK, DELTA, PAGE), использование механизмов работы с томами (LVM и аппаратные снэпшоты)

Быстрый старт

Начните работу в корпоративной среде

Глава 1. Функции

1.1. Надежность и производительность

- Полное, инкрементальное и дифференциальное резервное копирование
- Хранение резервных копий в СХД, ленточных библиотеках, облаке S3
- Автоматическая верификация резервных копий (размер файлов, md5sum, электронная подпись)
- Сжатие резервных копий на клиенте СРК или на сервере
- Срочное резервное копирование по инициативе клиента СРК или администратора
- Параллелизм — количество одновременных сессий ограничено только аппаратными характеристиками сервера. Параллельные сессии доступны как для СРК в целом, так и для отдельного клиента

1.2. Автоматизация

- Аналитика — построение плана резервного копирования с прогнозированием требуемых ресурсов
- Экономия дискового пространства — автоматическое перемещение резервных копий на другие носители и удаление устаревших копий
- Балансировка нагрузки — распределение копий по разным хранилищам в зависимости от выбранной политики
- Глобальное расписание — автоматическое создание резервных копий клиентских устройств
- Локальное расписание — клиенты могут управлять резервным копированием самостоятельно
- Стратегии резервного копирования — автоматические групповые операции с клиентами СРК

1.3. Управляемость

- Полноценное управление СРК из командной строки (CLI)
- Графические приложения для клиента и для администратора СРК
- Веб-приложение для администратора СРК, адаптированное под мобильные устройства
- Взаимодействие с СРК через REST API

1.4. Безопасность

- Многопользовательская модель администрирования
- Локальный лист запретов (с regexp) для каждого клиента, ограничивающий доступную для копирования информацию
- Защитное преобразование резервных копий по алгоритмам ГОСТ 34-12-2015 (Kuznyechik), Anubis, ARIA, CAST6, Camellia, Kalyna, MARS, AES, Serpent, Simon, SM4, Speck, Treefish, Twofish
- Интеграция с хранилищем секретов
- Рассылка уведомлений пользователям о событиях в СРК
- Протоколирование всех действий администратора и пользователей в базе данных и системном журнале

Глава 2. Ключевые понятия

Серверная группировка RuBackup состоит из основного сервера, необязательного резервного сервера и медиасерверов. В простейшем случае медиасервером является основной сервер резервного копирования (а также резервный сервер, при наличии).

Клиент системы резервного копирования — это отдельный сервер, компьютер или виртуальная машина, на которой установлено клиентское ПО RuBackup для выполнения резервного копирования. Для удобства клиенты могут быть объединены в **группы клиентов**.

На программном уровне сервером RuBackup называется также фоновый процесс (сервис) на сервере СРК, а клиентом RuBackup — фоновое клиентское ПО.

Хранение данных резервных копий (архивов) реализовано в виде хранилищ (storage). Каждое **хранилище** входит в определенный **пул**. Пул — это логическое объединение однотипных устройств хранения резервных копий. Каждый **пул** принадлежит определенному **медиасерверу**. Таким образом, организация хранения данных резервных копий имеет следующую структуру:

```
Медиасервер → Пул → Хранилище
```

Метаданные резервных копий хранятся в **репозитории**. Непосредственно **резервные копии** располагаются в **хранилищах** резервных копий, которые ассоциированы с **пулами** хранения резервных копий. Хранилища бывают пяти типов:

1. файловая система;
2. ленточная библиотека;
3. облако;
4. блочные устройства;
5. определяемые клиентом.

Все действия СРК реализованы в виде **задач**, которые объединены в **очереди задач**, в зависимости от типа.

Периодические задания резервного копирования и восстановления данных реализованы в виде **правил глобального расписания**, которые входят в **глобальное расписание** резервного копирования (Рисунок 1).

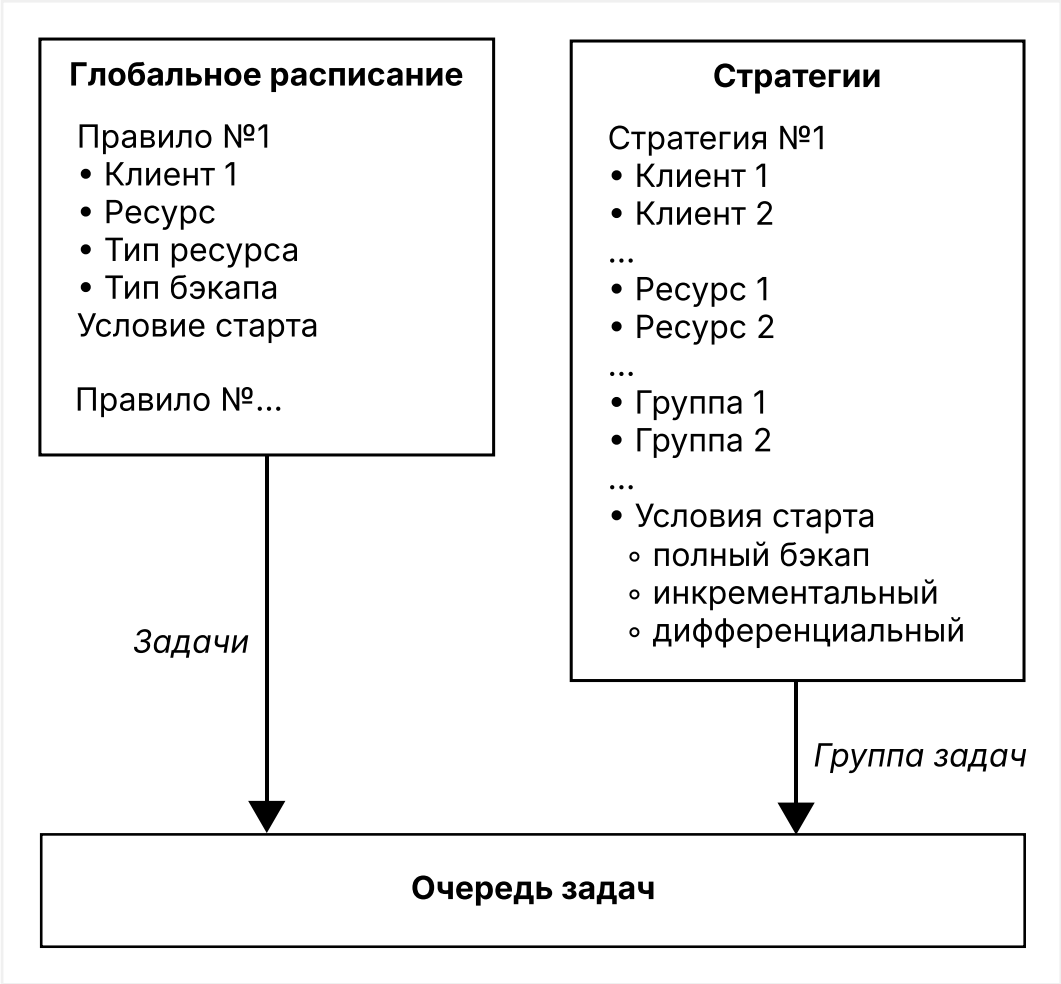


Рисунок 1. Глобальное расписание, стратегии и очередь задач

Одновременные действия над группами ресурсов реализованы в виде **стратегий**, которые создают **задачи** резервного копирования в соответствии с **расписаниями** для всех ресурсов и клиентов, которые их касаются.

Система уведомлений RuBackup использует **пользователей** и **группы пользователей** RuBackup для уведомления о событиях системы резервного копирования.

Автономный режим работы клиента — использование клиента СРК RuBackup без сервера резервного копирования. При этом сохраняется возможность использования некоторых клиентских функциональных модулей для создания резервных копий. Чтобы узнать, поддерживается ли использование модуля в автономном режиме, запустите исполняемый файл модуля с опцией `--autonomous` и проверьте код возврата.

Пример 1. Команда проверки поддержки автономного режима для модуля `rb_module_filesystem`

```
sudo /opt/rubackup/modules/rb_module_filesystem --autonomous
```

Пример 2. Команда проверки кода возврата

```
echo $?
```

Код возврата `0` говорит о том, что модуль поддерживает автономный режим. Другие коды возврата говорят о том, что автономный режим не поддерживается.

Неинтерактивный режим работы — режим для сценариев массового развертывания, например при использовании Ansible.

Резервный сервер и медиасервер не функционируют с тестовой лицензией!

Глава 3. Архитектура и инфраструктура

Архитектура системы резервного копирования (СРК) — программные компоненты СРК и их связи между собой.

Инфраструктура СРК — физические или виртуальные машины (узлы), на каждом из которых может быть установлен один или более программных компонентов СРК, и связи между ними.

Элементы инфраструктуры СРК:

- обязательные:
  - основной сервер;
  - служебная база данных.
- опциональные:
  - клиент резервного копирования (клиент РК);
  - резервный сервер;
  - медиасервер.

На одном узле может быть установлено более одного программного компонента СРК (один узел может выполнять функции нескольких элементов инфраструктуры СРК). Если в инфраструктуре СРК более одного узла, между этими узлами должна быть обеспечена связь по протоколу TCP.

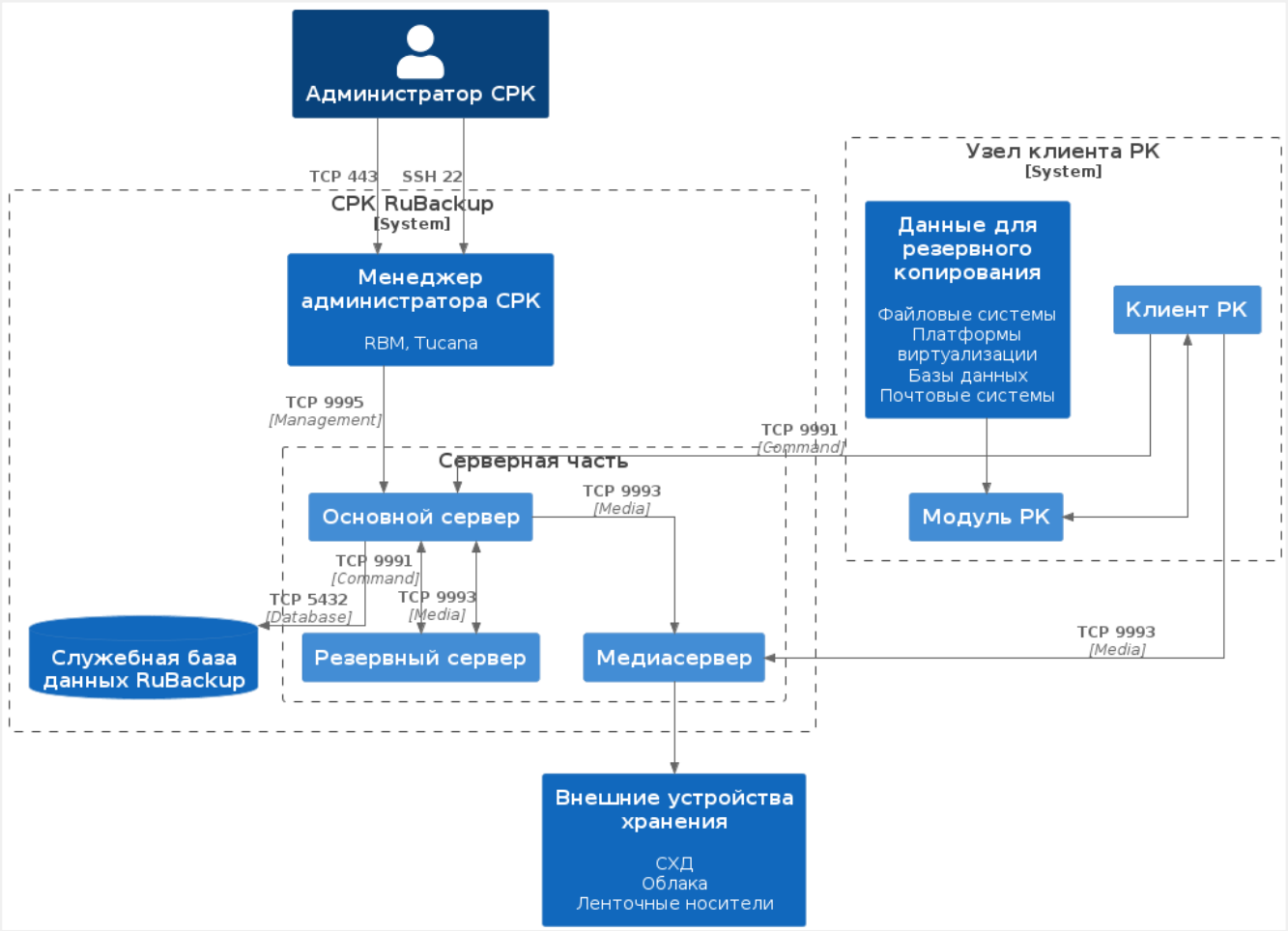


Рисунок 2. Условная схема инфраструктуры СРК *RuBackup*

3.1. Элементы инфраструктуры СРК

Клиент резервного копирования

Клиент РК — узел, на котором

- доступен ресурс, для которого выполняется резервное копирование;
- установлен пакет `rubackup-client`;
- обеспечен сетевой доступ к серверу;
- обеспечен сетевой доступ к медиасерверу (при наличии).

У клиента РК есть *модули*. Модуль клиента РК — подключаемый программный компонент, который отвечает за резервное копирование и восстановление ресурса определенного типа (например, блочных устройств или базы данных) и упаковку резервных копий.

Модули, устанавливаемые по умолчанию вместе с программным компонентом `rubackup-client`, позволяют резервировать Резервное копирование и восстановление файловых систем Linux и Резервное копирование и восстановление логических томов Linux.

Клиент РК отвечает за взаимодействие с сервером *RuBackup* с одной стороны, и с модулями резервного копирования и восстановления — с другой.

API модулей резервного копирования является открытым и может быть использован для разработки модулей третьими лицами.

Клиенты РК могут быть объединены в группы.

Взаимодействие в системе резервного копирования обеспечивает основной сервер резервного копирования либо резервный сервер, если он функционирует в режиме замещения основного сервера.

Основной сервер

Основной сервер — узел, на котором

- установлены пакеты `rubackup-server` и `rubackup-client`;
- обеспечен сетевой доступ к клиенту РК;
- обеспечен сетевой доступ к медиасерверу (при наличии).

Основной сервер — главный управляющий сервер, обеспечивающий взаимодействие элементов СРК. Основной сервер хранит информацию о том, *что* и *куда* сохранено, а также *как* восстановить информацию.

Основной и резервный серверы включают в себя функции медиасервера.

Основной сервер выполняет функцию медиасервера при установке способом «Всё в одном», в процессе которой все программные компоненты СРК *RuBackup* устанавливаются на одном узле.

Резервный сервер

При обслуживании высококритичных сервисов система резервного копирования может быть дополнена резервным сервером.

Резервный сервер — узел, на котором

- установлены пакеты `rubackup-server` и `rubackup-client`;
- обеспечен сетевой доступ к клиенту РК;
- обеспечен сетевой доступ к медиасерверу (при наличии).

Резервный сервер выполняет функции основного сервера, если основной сервер становится недоступен. В случае отказа основного сервера клиенты РК автоматически подключатся к резервному серверу. После восстановления функционирования основного сервера клиенты РК вернутся к работе с основным сервером.

Решение об использовании резервного сервера принимается *клиентом РК* немед-

ленно, если основной сервер не отвечает на запрос *при выполнении операции*.

Если клиент РК не выполняет операций, требующих ответа сервера, он не получит информации об отказе основного сервера.

При недоступности основного сервера подключите Менеджер администратора RuBackup (RBM) или Tucana к резервному серверу.

В графических интерфейсах управления недоступный сервер будет отмечен знаком в разделе **Серверы RuBackup**.

Медиасервер

Медиасервер — узел, обеспечивающий хранение резервных копий в доступных ему хранилищах, на котором

- установлены пакеты `rubackup-server` и `rubackup-client`;
- обеспечен сетевой доступ к *клиенту РК*.

Медиасервер:

- получает резервные копии от клиентов РК;
- хранит резервные копии;
- передает клиентам РК резервные копии по запросу.

Основной и резервный серверы включают в себя функции медиасервера.

При увеличении количества клиентов РК, а также при увеличении количества ресурсов, на которых предполагается хранить резервные копии, могут возникнуть задачи распределения нагрузки. В этом случае в серверную группировку могут быть добавлены медиасерверы, с помощью которых можно перераспределить задачи резервного копирования на несколько серверов резервного копирования или построить иерархическую систему хранения резервных копий.

Служебная база данных

В служебной базе данных хранится информация о:

- глобальных настройках резервного копирования;
- клиентах РК;
- глобальном расписании;
- стратегиях;
- репозитории резервных копий и пр.

Служебная БД хранится в СУБД PostgreSQL или Tantor с именем по умолчанию

`rubackup`.

Служебная база данных может находиться как на одном узле с сервером, так и на отдельном узле (машине).

Для изменения большинства параметров конфигурации СРК не требуется останавливать СРК и редактировать файлы настроек. Изменения производятся с помощью штатных средств администрирования *RuBackup*.

3.2. Минимальная конфигурация

В минимальной конфигурации СРК *RuBackup* состоит из:

- одного сервера;
- одного клиента РК, установленного на том же узле, на котором работает сервер резервного копирования.

В минимальной конфигурации единственный сервер резервного копирования взаимодействует с клиентом РК, координирует задания СРК и хранит резервные копии на доступных ему (как медиасерверу) ресурсах: файловых системах, картриджах ленточных библиотек и облачных сервисах.

Развертывание СРК *RuBackup* в этой конфигурации описано в разделе Быстрый старт.

Для использования *RuBackup* в продуктивных окружениях среднего и промышленного масштаба, а также для проведения нагрузочных испытаний, рекомендуем разворачивать *RuBackup,* включая служебную базу данных *RuBackup,* на отдельных машинах с рекомендуемой конфигурацией (Системные требования). Это позволит достичь максимальных показателей производительности и выполнить резервное копирование, восстановление и удаленную репликацию данных в кратчайшие сроки.

3.3. Управление хранением

Система резервного копирования может быть настроена таким образом, что резервные копии будут перемещаться на другие устройства хранения (например с дискового устройства хранения на картридж ленточной библиотеки) по достижении определенного срока хранения.

Общий объем резервных копий, хранящихся в системе резервного копирования, может быть ограничен для клиента РК, для правила резервного копирования, а также для стратегии резервного копирования.

Устаревшие резервные копии могут быть удалены из СРК автоматически. Сообщение о том, что устаревшие копии следует удалить, может быть отправлено

администраторам СРК.

Глава 4. Зависимости пакетов RuBackup

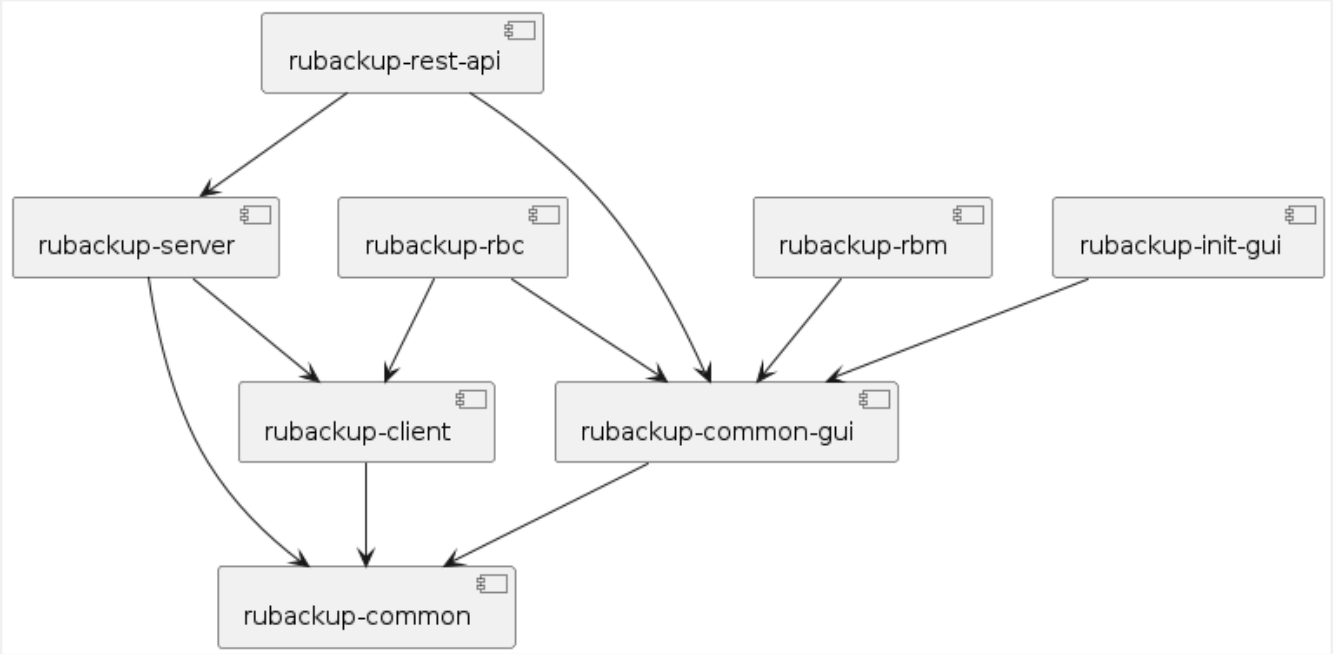


Рисунок 3. Зависимости пакетов RuBackup

Глава 5. Способы установки

Способы установки СРК:

- локальная;
- распределённая.

5.1. Локальная установка

Локальная установка означает, что все компоненты СРК развёртываются на одном узле (сервере, компьютере или виртуальной машине).

Сервер, база данных, клиент РК и модули работают в рамках одного узла.

Преимущества

- Простота развёртывания. Не требует настройки сети и настройки компонентов на каждом узле.
- Автономность.
- Подходит для тестирования или небольших систем.

Недостатки

- Масштабируемость. Резервируемые источники данных в пределах одного узла. При высокой нагрузке ресурсы одного медиасервера могут быть недостаточны.
- Отказоусточивость. Выход из строя основного сервера приводит к полной недоступности СРК.

5.2. Распределённая установка

Распредёленная установка — развёртывание компонентов СРК на нескольких узлах, связанных между собой через сеть.

Каждый узел выполняет свою функцию. Примеры:

- служебная база данных;
- основной сервер;
- резервный сервер;
- медиасервер;
- клиент РК 1;
- клиент РК 2;

- АРМ администратора.

Преимущества

- Масштабируемость. Можно добавлять новые узлы для обработки растущей нагрузки (горизонтальное масштабирование).
- Отказоустойчивость. Если основной сервер выйдет из строя, то его функции продолжит выполнять резервный сервер.
- Гибкость. Можно резервировать разные данные.
- Оптимизация ресурсов. Каждый сервер специализируется на своей задаче (например, хранение данных).

Недостатки

- Сложность настройки. Необходимы настройка каждого компонента на узлах, сетевые настройки, синхронизация данных;
- Усложнённое управление. Необходимо мониторить все узлы, обеспечивая безопасность, балансировать нагрузку.

5.3. Сравнение способов установки

Таблица 1. Сравнение способов установки СРК RuBackup

Критерий	Локальная установка	Распределённая установка
Масштабируемость	Ограничена ресурсами одного сервера	Масштабируется добавлением узлов
Отказоустойчивость	Низкая (единая точка отказа)	Высокая (дублирование)
Производительность	Зависит от одного клиента РК	Распределение нагрузки между узлами
Сложность	Простота развёртывания	Требует настройки сети и координации

5.4. Как выбрать?

Когда лучше выбрать распределённую установку?

- Высокие нагрузки (разнообразие резервируемых ресурсов).
- Критическая отказоустойчивость.
- Гибкость архитектуры.

Когда лучше выбрать локальную установку?

- Тестирование, разработка.
- Небольшие проекты с низкой нагрузкой.
- Быстрое развёртывание без сложной архитектуры.

Глава 6. Способы управления

Возможные способы управления:

- локальное;
- централизованное.

6.1. Локальное управление

Локальное управление резервным копированием и восстановлением данных выполняется на клиенте РК одним из инструментов, установленным на этом же узле:

- Менеджер администратора RuBackup (RBM);
- Менеджер клиента RuBackup (RBC);
- Утилиты командной строки.

6.2. Централизованное управление

Централизованное управление резервным копированием и восстановлением данных клиента РК выполняется на любом удалённом узле, имеющем сетевой доступ к узлам компонентов СРК:

- Tucana;
- Утилиты командной строки;
- Менеджер администратора RuBackup (RBM).

Рекомендуем включить функцию централизованного восстановления на клиенте РК. Это позволит управлять восстановлением данных на клиенте удаленно через приложение Менеджер администратора RuBackup (RBM).

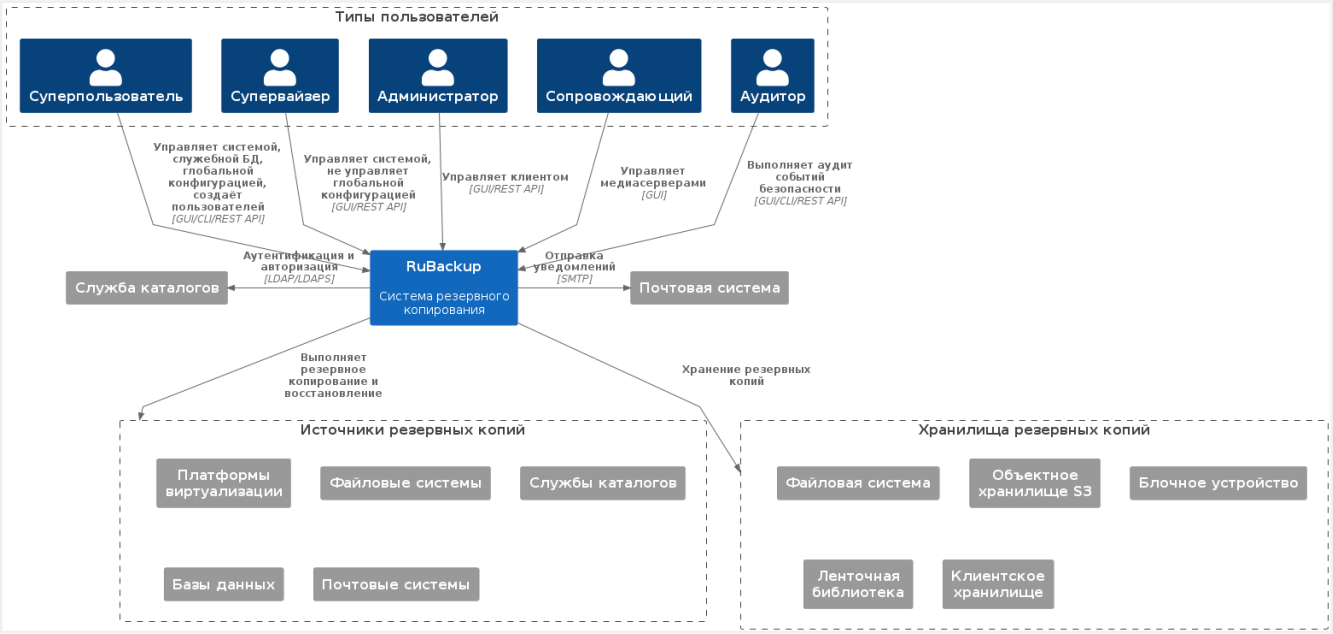
1. Откройте конфигурационный файл клиента РК `/opt/rubackup/etc/config.file` (Linux) или `C:\RuBackup-win-client\etc\config.file.txt` (Windows).
2. Установите значение `yes` параметра `centralized-recovery`. Сохраните изменения.
3. Перезапустите клиент РК.

Глава 7. Многопользовательская модель

В СРК RuBackup реализован многопользовательский режим работы, т.е. назначение типа пользователя и предоставление ему набора полномочий для выполнения определенных рабочих задач в соответствии с его ролью.

В СРК RuBackup предусмотрены следующие типы пользователей:

- суперпользователь (владелец базы данных RuBackup);
- супервайзер;
- сопровождающий;
- администратор;
- аудитор.



7.1. Суперпользователь

Суперпользователь является привилегированным администратором, которому позволены любые действия в СРК. Суперпользователь создаётся при конфигурации основного сервера. Имя суперпользователя и пароль задаются также при настройке. Чтобы поменять пароль суперпользователя в конфигурационном файле сервера, используйте команду:

```
rb_init --passwd
```

```
root@rbs:~# rb_init --passwd
RuBackup initialization utility
```

```
Copyright 2018-2022: LLC "RUBACKUP"
Исключительные права принадлежат ООО "РУБЭКАП"
Author is Andrey Kuznetsov
Version: 2.0 Build: 48024de
password found in /opt/rubackup/etc/config.file

Please enter old password:
Enter new password:
Repeat password:
  Copy old config file to: /opt/rubackup/etc/config.file.old.2024-Jan-18H16-
05-32
Password was changed successfully
root@rbs:~#
```

Для смены пароля в служебной базе данных `rubackup`:

1. Подключитесь к базе данных, используя пользователя `rubackup` или `postgres`, с помощью команды:

   ```
   sudo -u rubackup psql
   ```

   или

   ```
   sudo -u postgres psql
   ```

2. Выполните команду:

   ```
   sql ALTER USER rubackup PASSWORD '<new-password>';
   ```

Суперпользователь создается одновременно с базой данных `rubackup` и является владельцем этой базы данных. В списке пользователей СРК пользователя `Супер-пользователь` увидеть нельзя. Нельзя создать нового пользователя с тем же именем.

Суперпользователь может:

- добавлять новых пользователей в систему. Выбранная группа создаваемого пользователя влияет только на задачи уведомления. Чтобы пользователь мог получить административные привилегии в СРК, его нужно добавить в супервайзеры, сопровождающие или администраторы;
- менять пароль для других пользователей с помощью RBM.

7.2. Супервайзер

Супервайзер может выполнять действия, доступные Суперпользователю, за исключением:

- любых действий с пользователями кроме назначения ролей Сопровождающего и Администратора;
- изменения глобальной конфигурации СРК.

7.3. Сопровождающий

Сопровождающий отвечает за медиасервер и может управлять устройствами хранения на этом медиасервере.

7.4. Администратор

Администратор отвечает за группу клиентов и может выполнять их настройки и действия, связанные с клиентами, входящими в группу.

Администратор в дереве объектов видит только «своих» клиентов, и имеет доступ к правилам глобального расписания, резервным копиям и задачам только «своих» клиентов.

7.5. Аудитор

Аудитор — роль, предназначенная для сотрудников информационной безопасности. Аудитору доступен просмотр всех настроек и информации в СРК (кроме настроек глобальной конфигурации) без возможности редактирования. Аудитору также доступны для просмотра все журналы, включая «Журнал событий ИБ».

Глава 8. Пулы

В СРК RuBackup пул — это логическое объединение однотипных устройств хранения резервных копий. Пулы принадлежат медиасерверам.

8.1. Типы пулов

Файловая система (*File system*)

Пул каталогов файловых систем.

Ленточная библиотека (*Tape library, LTFS* и *Tape library, Native*)

Пул картриджей ленточной библиотеки (в пул типа *Tape library, Native* добавляются картриджи с собственным форматом хранения). При форматировании в пул типа *Tape library, LTFS* записывается файловая система LTFS.

Картриджи одной ленточной библиотеки запрещено добавлять в пулы разных типов.

Облако (*Cloud*)

Пул облачных хранилищ.

Клиентский (*Client defined*)

Пул клиентских хранилищ. Пул позволяет хранить резервные копии в папке или в облаке, доступ к которым задается на стороне клиента. Один пул может содержать в себе несколько клиентских хранилищ, при этом резервные копии одного клиента не могут быть сохранены в хранилище другого клиента.

Блочное устройство (*Block device* и *Block device, gen.2*)

Пул дедуплицированных блочных устройств. Пул типа *Block device, gen.2* отличается использованием алгоритма FastCDC при дедупликации и возможностью хранить метаданные дедуплицированной резервной копии на блочном устройстве данного пула.

По умолчанию при развертывании СРК RuBackup создается пул типа *File system*, принадлежащий основному серверу резервного копирования.

Если пул не содержит никаких устройств хранения, то задачи резервного копирования, для которых пул назначен как место хранения резервных копий, не будут выполнены.

8.2. Сценарии копирования и перемещения РК

С помощью механизма копирования и перемещения РК между пулами возможно перемещение РК как в рамках одного медиасервера, так и в рамках нескольких

медиасерверов одной инсталляции СРК.

Таблица 2. Сценарии копирования РК

	Файловая система	Блочное устройство	Облако	Ленточная библиотека, LTFS	Ленточная библиотека, Native	Клиентский пул
Файловая система	✓	✓	✓	✓	✓	✗
Блочное устройство	✓	✓	✗	✓	✓	✗
Облако	✓	✗	✓	✓	✓	✗
Ленточная библиотека, LTFS	✓	✓	✓	✓	✓	✗
Ленточная библиотека, Native	✓	✓	✓	✓	✗	✗
Клиентский пул	✗	✗	✗	✗	✗	✗

Таблица 3. Сценарии перемещения РК

	Файловая система	Блочное устройство	Облако	Ленточная библиотека, LTFS	Ленточная библиотека, Native	Клиентский пул
Файловая система	✓	✓	✓	✓	✓	✗
Блочное устройство	✓	✓	✗	✓	✓	✗
Облако	✓	✗	✓	✓	✓	✗
Ленточная библиотека, LTFS	✗	✗	✗	✗	✗	✗
Ленточная библиотека, Native	✗	✗	✗	✗	✗	✗
Клиентский пул	✗	✗	✗	✗	✗	✗

Ограничения копирования и перемещения РК:

1. Для копирования или перемещения РК из пула типа *Файловая система* в пул типа *Блочное устройство* у пулов должны совпадать размер блока, хеш-функция и длина хеша.
2. Копирование или перемещение РК из пула типа *Блочное устройство* в пул типа *Файловая система* происходит без сохранения ЭЦП (см. Электронная цифровая подпись). Если исходная РК была подписана ЭЦП, то у конечной РК ЭЦП не будет.
3. Копирование РК из пула типа *Блочное устройство* в пул типа *Ленточная библиотека, LTFS* и *Ленточная библиотека, Native* происходит без сохранения ЭЦП.
4. Перемещение РК невозможно из пулов типа *Ленточная библиотека, LTFS* и *Ленточная библиотека, Native*, так как картриджи ленточной библиотеки могут

располагаться вне ленточной библиотеки.

8.3. Управление пулами

Доступна общая настройка пулов в разделе глобальной конфигурации.

Доступно управление пулами с помощью:

- утилиты командной строки `rb_pools`;
- приложения Менеджер администратора RuBackup (RBM);
- приложения Tucana.

8.4. Режимы работы ленточной библиотеки, мультистриминг и мультиплексинг

8.4.1. Мультистриминг и мультиплексинг

Автоматическая балансировка нагрузки на ленточные библиотеки обеспечивается за счет постоянного мониторинга очередей данных:

- если очередь растет, то подключается либо дополнительный привод, либо приостанавливаются наименее приоритетные задачи в очереди;
- если очередь уменьшается, то часть приводов может быть остановлена.

Для полной утилизации ресурсов ленточных библиотек `Tape library, Native` реализованы алгоритмы мультистриминга и мультиплексинга с возможностью гибкой настройки.

Мультистриминг

Запись одной РК на несколько картриджей ленточной библиотеки одновременно (требует наличия более одного привода).

Запись РК начинается с использования одного привода и одного картриджа. Если при выполнении РК один привод не успевает записывать поступающие данные, то система автоматически выбирает дополнительный картридж из пула и подключает второй привод для выполнения задачи резервного копирования.

РК будет записана на несколько картриджей согласно параметру Количество картриджей на одну РК. Дополнительные картриджи будут подключаться до тех пор, пока ленточная библиотека не начнет справляться с потоком данных.

Для включения функции настройте дополнительные параметры для пулов типа `Tape library, Native`.

Мультиплексинг

Запись нескольких РК одновременно на один картридж ленточной библиотеки.

При создании РК будет производиться попытка задействовать новый свободный привод. Если свободные приводы отсутствуют, то данные РК будут передаваться в очередь текущего рабочего привода.

Если текущий привод успевает записывать поступающую к нему РК, то система может начать передевать ему данные второй и последующих задач резервного копирования.

Одна РК может быть одновременно записана на один картридж, при этом на один картридж может одновременно записываться нескольких РК согласно параметру Количество одновременных РК на картридж.

Для включения функции настройте дополнительные параметры для пулов типа `Tape library, Native`.

8.4.2. Режимы работы ленточной библиотеки

Таблица 4. Режимы работы ленточной библиотеки

Запись РК на несколько картриджей	Количество картриджей на одну РК (мультистриминг)	Количество одновременных РК на картридж (мультиплексинг)	Описание режима работы ленточной библиотеки
Выкл	—	—	Отключена возможность мультистриминга, мультиплексинга и последовательной записи РК на несколько картриджей. Происходит запись одной РК на один картридж, при нехватке места задача завершится с ошибкой.
Вкл	1	1	Включена возможность только последовательной записи РК на более чем один картридж. Происходит запись одной РК на один картридж, но РК может быть последовательно записана на несколько картриджей при нехватке места.
Вкл	>1	1	Мультистриминг
Вкл	1	>1	Мультиплексинг
Вкл	>1	>1	Мультистриминг и Мультиплексинг

Глава 9. Каталог доступных ресурсов и массовое добавление правил стратегии

В крупных организациях число резервируемых ресурсов (файловых систем, виртуальных машин или баз данных) может исчисляться тысячами и даже десятками тысяч. Вручную добавлять к стратегии правила резервного копирования для каждого из таких ресурсов затруднительно.

Для упрощения массового добавления правил в стратегию используется *каталог доступных ресурсов*.

Каталог доступных ресурсов — список «непроницаемых» ресурсов, доступных на узлах клиентов СРК.

«Непроницаемыми» являются ресурсы, просмотр которых в глубину невозможен (напр., таблиц базы данных или содержимого виртуальных машин). Файловые системы, напротив, являются проницаемыми — при создании правила резервного копирования возможен просмотр дерева файловой системы на произвольную глубину.

В каталог доступных ресурсов включаются уникальные сочетания идентификатора клиента, типа резервируемого ресурса и самого ресурса на клиенте. Один и тот же клиент, на котором доступно резервирование двух и более непроницаемых ресурсов, будет включен в каталог доступных ресурсов то же количество раз.

Группы клиентов при формировании каталога доступных ресурсов не учитываются.

Опрос клиентов выполняется сервером последовательно и при большом количестве резервируемых ресурсов формирование каталога может занять до нескольких часов.

Получив список (каталог) доступных ресурсов, любые из них (но только одного типа за одну операцию) можно добавить в выбранную стратегию с заданными настройками или настройками по умолчанию.

Работа с каталогом доступных ресурсов доступна только пользователям СРК с ролью *Суперпользователь* или *Супервайзер* (см. Глава 7).

Глава 10. Удаленная репликация

Удаленная репликация — это синхронизация данных между двумя удаленными узлами.

Система резервного копирования RuBackup поддерживает удаленную репликацию между клиентами СРК. Удаленная репликация реализуется модулями СРК.

Клиенты СРК, которые участвуют в удаленной репликации, делятся на клиентов-источников и клиентов-приемников. Модуль СРК устанавливается на узел с клиентом-источником.

Репликация данных обеспечивает актуальность информации на клиенте-приемнике за счет периодического копирования изменений с клиента-источника по заданному правилу. Например, можно настроить репликацию папки с одного клиента СРК на другой.

Для удаленной репликации на медиасервере необходимо блочное устройство — дедуплицированное хранилище резервных копий. От клиента-источника на клиент-приемник передаются только измененные блоки данных. Минимальное время отставания реплики от клиента-источника составляет 1 минуту.

Удаленная репликация происходит следующим образом:

1. Пользователь создает и запускает правило удаленной репликации.
2. На клиенте-источнике формируется новая резервная копия данных, которая сохраняется на медиасервере в дедуплицированном хранилище с пулом типа *Block device*.
3. Устаревшая резервная копия данных удаляется из хранилища на медиасервере.
4. На клиент-приемник передается реплика, после чего данные автоматически восстанавливаются в предварительно выбранную директорию.

Для выполнения удаленной репликации ресурс на клиенте-приемнике должен существовать и не должен использоваться. Например, если ресурсом являются папки файловой системы, то в процессе репликации в них не должна осуществляться запись; если ресурсом является виртуальная машина, то она должна быть выключена.

10.1. Управление удаленной репликацией

Управление правилами удаленной репликации в СРК RuBackup осуществляется с помощью:

- приложения Tucana (рекомендуемый способ),

- приложения Менеджер администратора RuBackup (RBM),
- утилиты командной строки `rb_remote_replication`.

10.2. Предварительные настройки

Перед созданием правила удаленной репликации выполните предварительные настройки.

1. При первоначальной настройке клиента-приемника включите удаленную репликацию с помощью `rb_init`.

   На настроенном клиенте включите удаленную репликацию в конфигурационном файле (параметр `remote-replication`).

2. На медиасервере СРК настройте пул типа *Block device*, добавьте в него блочное устройство для использования в качестве дедуплицированного хранилища резервных копий.
3. На сервере СРК добавьте клиента-источника и клиента-приемника в одну разделяемую группу.

Глава 11. Интеграция с контроллерами доменов

Контроллер домена (domain controller) — сервер, управляющий доступом к сетевым ресурсам в рамках одного домена (группы сетей или хостов).

Контроллер домена выполняет аутентификацию пользователя в домене (позволяет ему входить в сеть с помощью одной пары логин-пароль с любого компьютера, включенного в домен), и авторизует доступ пользователя к ресурсам в соответствии с политиками доступа.

Интеграция RuBackup с контроллером домена означает, что пользователям, входящим в заданную группу пользователей контроллера домена, при использовании RuBackup может быть присвоена одна из ролей (см. Глава 7). В этом случае пользователи домена могут использовать RuBackup в пределах прав, предоставленных присвоенной ролью.

RuBackup может интегрироваться с контроллерами домена *Microsoft Active Directory* и *ALD Pro*.

11.1. Проверка подключения к контроллеру домена

Для проверки работоспособности подключения к контроллеру домена с сервера RuBackup потребуются:

- `ldapsearch` (`apt install ldap-utils`);
- BindDN — указатель на учётную запись в контроллере домена, имеющую полномочия на подключение к LDAP-серверу и на просмотр содержимого каталога;
- пароль от учётной записи, на которую указывает BindDN;
- BaseDN — база поиска, от которой выполняется запрос.

Запросы к LDAP-каталогу читаются справа налево: от корня каталога к конечному элементу. Например, для домена `rubackup.test` база поиска указывается как `dc=rubackup,dc=test`. Домен не следует путать с FQDN или другим *адресом* хоста.

Запрос BindDN (логин) `uid=bind_user,cn=users,cn=accounts,dc=rubackup,dc=test` означает: домен `rubackup.test` → учётные записи пользователей (`accounts`) → пользователи (`users`) → пользователь с именем `bind_user`.

В примерах предполагается незащищенное соединение (LDAP) с контроллером домена.

Предварительно проверьте доступность контроллера домена (`ping`).

Если контроллер домена располагается по адресу `domaincontroller.local` на стандартном порту `389`, то получить сведения (LDIF, LDAP Data Interchange Format), доступные пользователю `bind_user`, можно следующей командой.

Получение всех сведений, доступных пользователю `bind_user`

```
ldapsearch \
  -x \ ❶
  -H 'ldap://domaincontroller.local' \ ❷
  -b 'dc=rubackup,dc=test' \ ❸
  -D 'uid=bind_user,cn=users,cn=accounts,dc=rubackup,dc=test' \ ❹
  -w 'passw0rd' ❺
```

❶ Использование простой аутентификации (BindDN и пароль) вместо SASL.

❷ Адрес контроллера домена с обязательным указанием `ldap://` или `ldaps://`. Опционально указывается порт, если на контроллере домена он отличается от портов по умолчанию — `389` (LDAP) или `636` (LDAPS).

❸ База поиска (BaseDN).

❹ BindDN (логин).

❺ Пароль пользователя, на которого указывает BindDN.

Сведения о пользователях или группах, полученные в результате такого запроса, будут доступны в RuBackup.

Команды ниже приводятся для сведения и не потребуются при настройке RuBackup на работу с контроллером домена.

Запрос сведений о пользователе

```
ldapsearch \
  -x \
  -H 'ldap://domaincontroller.local' \
  -b 'dc=rubackup,dc=test' \
  -D 'uid=bind_user,cn=users,cn=accounts,dc=rubackup,dc=test' \
  -w 'passw0rd' \
  'uid=superv' ❶
```

❶ Поиск пользователя `superv`, выполняемый с учётом базы поиска (`-b`).

Запрос списка групп, доступных пользователю `bind_user`

```
ldapsearch \
  -x \
```

```
  -H 'ldap://domaincontroller.local' \
  -b 'dc=rubackup,dc=test' \
  -D 'uid=bind_user,cn=users,cn=accounts,dc=rubackup,dc=test' \
  -w 'passw0rd' \
  'objectClass=groupofnames' (1)
```

(1) Возвращает объекты каталога типа «группа».

11.2. Настройка подключения к контроллеру домена на ALD Pro

Для подключения RuBackup к контроллеру домена потребуются:

- BindDN — указатель на учётную запись, имеющую полномочия на подключение к LDAP-серверу и на просмотр содержимого каталога;
- пароль от учётной записи, на которую указывает BindDN;
- BaseDN — база поиска, от которой выполняется запрос.

Если используется защищенное соединение с контроллером домена, потребуются сертификаты контроллера домена и корневого хранилища сертификатов в формате PEM.

Обязательные требования к пользователям контроллера домена для RuBackup

1. Только одна из групп в контроллере домена, в которой состоит пользователь, может быть сопоставлена с ролью в RuBackup. Иными словами, если пользователь состоит в двух группах одновременно, нельзя использовать обе группы для присвоения ролей RuBackup.
2. В учётной записи пользователя на контроллере домена обязательно должна быть указана электронная почта.

1. Включите **Сервисный режим**. Перейдите **Администрирование** → **Подключения**.
2. Из списка **Контроллер домена** выберите `ALD Pro`.
3. Из списка **Протокол** выберите `LDAP` или `LDAPS`.
4. (опционально, при использовании LDAPS) В **Путь к сертификату клиента** и **Путь к корневому сертификату** укажите полные пути в файловой системе к сертификатам сервера контроллера домена в формате PEM.
5. В **Адрес сервера** введите адрес контроллера домена.
6. В **Порт** введите порт контроллера домена, соответствующий используемому подключению (LDAP или LDAPS).
7. В **Имя пользователя Bind User** введите через `\` домен и имя пользователя,

который имеет полномочия на подключение к LDAP-серверу и на просмотр содержимого каталога.

Пример 3. Пример ввода имени пользователя

Если домен — `rubackup.test`, а имя пользователя — `bind_user`, введите `rubackup.test\bind_user`.

8. В поле **Пароль пользователя Bind User** укажите пароль пользователя.
9. В **База поиска** укажите корневой элемент домена, от которого будет выполняться поиск пользователей. Для домена `rubackup.test` базой поиска может быть `dc=rubackup,dc=test`.
10. В **База поиска групп** укажите корневой элемент домена, от которого будет выполняться поиск групп. Для домена `rubackup.test` базой поиска групп чаще может быть `dc=rubackup,dc=test`.
11. Нажмите **Подключиться к серверу**.

В случае успешного подключения откроется форма **Ассоциации групп контроллера домена и ролей RuBackup** (**Безопасность** → **Ассоциации ролей**).

11.3. Присвоение ролей группам доменных пользователей

Для присвоения ролей RuBackup группам доменных пользователей потребуются имена групп пользователей контроллера домена, каждой из которых должна быть сопоставлена роль в СРК RuBackup.

Если не выполнены требования, необходимые для функционирования роли, аутентификация пользователя с такой ролью невозможна. Например, роль Администратора требует, чтобы в СРК существовала хотя бы одна группа клиентов.

1. Перейдите к форме **Ассоциации групп контроллера домена и ролей RuBackup** (**Безопасность** → **Ассоциации ролей**).
2. Нажмите **Добавить**.
3. В поле **Группа** введите имя группы пользователей контроллера домена.
4. Выберите из списка **Роль RuBackup** введите роль в СРК, которая будет присвоена пользователям указанной группы контроллера домена.
5. Нажмите **Добавить ассоциацию группы**. Нажмите **Применить**.
6. Перейдите **Администрирование** → **Система** → **Группы клиентов**.
7. Если в списке указана только группа `No Group`, нажмите **Добавить** и введите

имя для новой группы клиентов. Нажмите ✓ **Применить**.

8. Отключите ⓘ **Сервисный режим**.

Теперь пользователь, аутентифицирующийся в СРК через контроллер домена, будет получать указанную роль.

Пользователь контроллера домена с присвоенной ему ролью будет показан в разделе 🔒 **Безопасность** → **Пользователи** → (присвоенная пользователю роль).

11.4. Аутентификация с использованием контроллера домена

1. Запустите Менеджер администратора RuBackup (RBM) или Tucana.
2. Переключите **Тип аутентификации** на `Контроллер домена`.
3. Укажите имя пользователя в формате `domain\username`:`password`.

   Пример 4. Пример ввода имени пользователя

   > Если домен — `rubackup.test`, а имя пользователя — `bind_user`, введите `rubackup.test\bind_user`.

4. Укажите пароль пользователя.
5. Нажмите **Войти**.

11.5. Выбор аутентификации через контроллер домена по умолчанию

11.5.1. Выбор аутентификации по умолчанию в RBM

1. Войдите в СРК через Менеджер администратора RuBackup (RBM).
2. Нажмите ⚙ (**Настройки**) и включите ⓘ **Сервисный режим**.
3. Перейдите ⚙ (**Настройки**) → ☰ **Локальная конфигурация** → **Аутентификация**.
4. Выберите `Контроллер домена` как **Тип аутентификации по умолчанию**.
5. Нажмите ✓ **Применить**.

Теперь на этой машине в окне аутентификации RBM **Тип аутентификации** по умолчанию — `Контроллер домена`.

11.5.2. Выбор аутентификации по умолчанию в Tucana

1. Войдите в СРК через Tucana.

2. Нажмите ⚙ и включите ⓘ.
3. Перейдите 👤 → **Настройки аутентификации**.
4. Выберите `Контроллер домена` как **Тип аутентификации по умолчанию**.
5. Нажмите **Применить**.

Теперь на этой машине в окне аутентификации Tucana **Тип аутентификации** по умолчанию — `Контроллер домена`.

11.6. Устранение неисправностей

11.6.1. Ошибка аутентификации с использованием контроллера домена

Описание

При аутентификации пользователя в СРК с использованием контроллера домена возникает ошибка `LogIn: Bad login or password`.

Возможные причины

- Ошибка в написании домена, имени пользователя или пароля.
- В профиле пользователя на контроллере домена отсутствует адрес электронной почты.
- Не выполнены требования к роли, которая присваивается пользователю при попытке аутентификации.

Диагностика

Ошибка аутентификации с использованием контроллера домена `LogIn: Bad login or password` может возвращаться для широкого спектра неоднородных ошибок.

Разверните окно предупреждения и ознакомьтесь с причиной ошибки.

Решение

- Проверьте правильность ввода логина и пароля.

  Пример 5. Пример ввода имени пользователя

  > Если домен — `rubackup.test`, а имя пользователя — `bind_user`, введите `rubackup.test\bind_user`.

- Установите в профиле пользователя на контроллере домена адрес электронной почты.

- Проверьте, выполнены ли требования СРК к роли, которая должна быть присвоена пользователю при аутентификации.

Глава 12. Хранилища секретов

Хранилище секретов — стороннее хранилище, предназначенное для безопасного хранения конфиденциальных данных и учетных записей.

Аутентификационная информация (секрет) для подключения к резервируемым ресурсам хранится в конфигурационных файлах модулей. Если конфигурационные файлы недостаточно защищены или система скомпрометирована, третьи лица могут получить доступ к ресурсам.

Использование внешнего хранилища позволяет:

1. Хранить секреты в зашифрованном виде.
2. Ограничить доступ к данным только авторизованным пользователям СРК RuBackup с соответствующими правами.
3. Управлять чувствительными настройками[1] в модулях.

Поддержка хранилища реализована для всех типов операций: создание и восстановление полных, инкрементальных и дифференциальных резервных копий.

СРК RuBackup совместим с хранилищами секретов:

- HashiCorp Vault.
- Deckhouse Stronghold.

Взаимодействие СРК RuBackup с хранилищем секретов происходит через основной сервер (при его недоступности — через резервный).

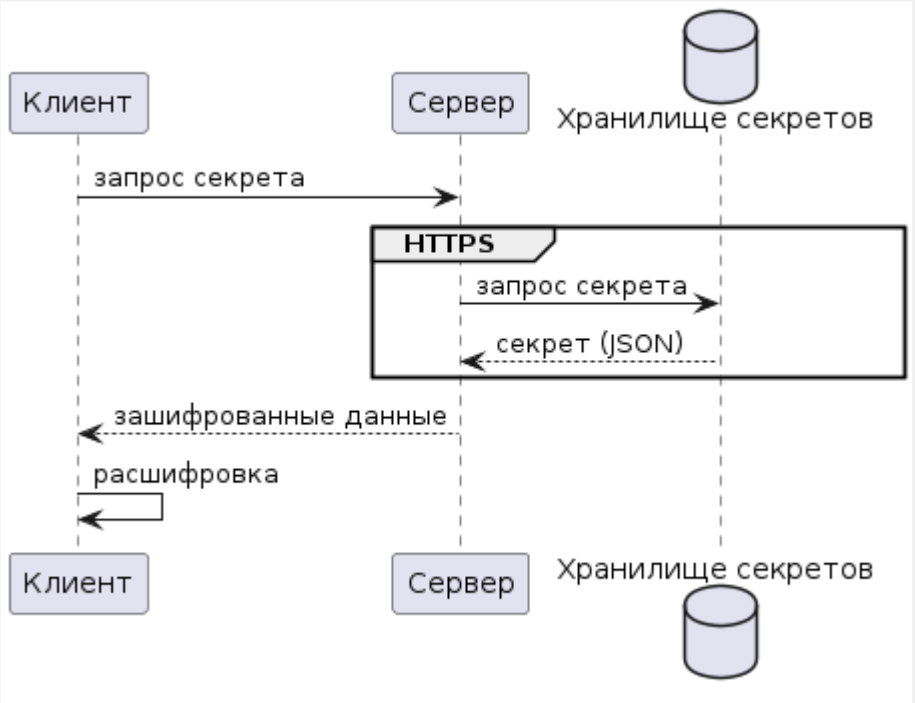


Рисунок 4. Взаимодействие клиента, сервера и хранилища секретов

12.1. Доступ пользователей к методам

Суперпользователь может назначить *Супервайзеру* или *Администратору* доступ к выбранному секрету посредством ассоциации пользователя с методом получения секрета.

Таблица 5. Права доступа пользователей RuBackup к секретам хранилища

Операция	Роль				
	Суперпользователь	Администратор	Аудитор	Сопровождающий	Супервайзер
Редактирование данных хранилища секретов	✓	✗	✗	✗	✗
Добавление данных хранилища секретов	✓	✗	✗	✗	✗
Удаление данных хранилища секретов	✓	✗	✗	✗	✗
Добавление методов получения секретов	✓	✗	✗	✗	✗
Просмотр методов получения секретов	✓	🔑	✗	✗	🔑
Редактирование методов получения секретов	✓	✗	✗	✗	✗
Удаление методов получения секретов	✓	✗	✗	✗	✗
Управление доступом к методам получения секретов	✓	✗	✗	✗	✗

🔑 — доступ на выбранный метод назначает Суперпользователь

12.2. Управление хранилищами секретов

Для работы с хранилищем секретов в приложении Менеджер администратора RuBackup (RBM) смотрите раздел Хранилище секретов.

Для работы с хранилищем секретов в веб-приложении Tucana смотрите раздел 2.9.0.0.0@TucanaGuide:ROOT:page$secret-storages.adoc.

Для работы с хранилищем секретов с помощью Утилит командной строки предназначена утилита `rb_secret_storage`.

[1] Данные, которые требуют особого уровня защиты.

Глава 13. Удаленное логирование

Syslog (System Logging Protocol) — это стандартный протокол для передачи и централизованного сбора сообщений о событиях в компьютерных системах и сетях. Протокол был разработан для унификации процесса логирования в различных устройствах и операционных системах.

Основные компоненты для удаленного логирования включают:

- Syslog-сервер — центральный узел для сбора и хранения логов.
- Syslog-клиенты — устройства, отправляющие сообщения о событиях.
- Форматирование сообщений — стандартизированный формат записи логов.

13.1. Преимущества использования Syslog

Внедрение централизованного логирования через syslog предоставляет ряд существенных преимуществ:

- Централизация данных — все логи собираются в одном месте, что упрощает их анализ и мониторинг.
- Масштабируемость — система легко расширяется для работы с большим количеством устройств.
- Безопасность — возможность шифрования трафика и аутентификации источников.
- Фильтрация и сортировка — гибкие возможности для обработки логов.
- Автоматизация — интеграция с системами мониторинга и оповещения.
- Долгосрочное хранение — централизованное архивирование исторических данных.

13.2. Syslog в СРК RuBackup

RuBackup поддерживает работу с любыми серверами Syslog, поддерживающими протокол TCP и UDP.

Рекомендуется использовать следующие сервера Syslog:

- Раздел 13.4.1.
- Раздел 13.4.2.

Для настройки удаленного логирования в SIEM используйте Раздел 13.3.

13.3. Интеграция с SIEM-системами в СРК RuBackup

SIEM (Security Information and Event Management) представляет собой комплексное решение для обеспечения информационной безопасности, объединяющее управление информацией о безопасности (SIM) и управление событиями безопасности (SEM). Это централизованная система, предназначенная для сбора, анализа и обработки событий безопасности в реальном времени.

Интеграция с SIEM-системами реализована с помощью удаленного логирования Syslog.

Syslog-сервер выступает в роли промежуточного звена между СРК RuBackup и платформой безопасности MaxPatrol SIEM.

СРК RuBackup предоставляет возможность использования SIEM-системы MaxPatrol SIEM.

Для использования SIEM в СРК RuBackup выполните следующие шаги:

1. Установите и настройте один из рекомендуемых syslog-серверов:
   - Раздел 13.4.1.
   - Раздел 13.4.2.
2. Выполните настройку параметров удаленного логирования в одном из интерфейсов:
   - Раздел 13.5.2.
   - Раздел 13.5.1.
3. Выполните Раздел 13.6.

13.4. Установка и настройка

13.4.1. Установка и настройка сервера syslog-ng

Установка

1. Некоторые дистрибутивы Linux уже содержат пакет `syslog-ng`. Проверите наличие пакета:

   ```
   syslog-ng --version
   ```

2. Если сервер не установлен, установите его из репозитория:

   ```
   apt update
   ```

```
apt install syslog-ng
```

3. Запустите сервер:

```
systemctl start syslog-ng.service
```

4. Проверьте статус сервера:

```
systemctl status syslog-ng.service
```

5. Добавьте сервер в автозапуск:

```
systemctl enable syslog-ng.service
```

Настройка

Для приема сообщений от RuBackup сервер `rsyslog` должен быть настроен на прослушивание сетевых сокетов по протоколам TCP и(или) UDP.

Для этого:

1. Откройте файл `/etc/syslog-ng/syslog-ng.conf`:

```
nano /etc/syslog-ng/syslog-ng.conf
```

2. Раскомментируйте и отредактируйте строку:

```
source s_net { tcp(ip(127.0.0.1) port(1000)); };
```

   где:

   - `tcp` — указывает, что сервер будет слушать TCP-порт;
   - `ip(127.0.0.1)` — указывает, что сервер будет слушать локальный адрес (хост) [1];
   - `port(1000)` — указывает, что сервер будет слушать порт 1000 [1].

3. При необходимости использования TLS добавьте еще один источник для прослушивания:

```
source s_tls {
```

```
    network(
        ip(0.0.0.0) (1)
        port(6514) (2)
        transport("tls")
        tls(
            key-file("/etc/syslog-ng/cert.d/server.key")
            cert-file("/etc/syslog-ng/cert.d/server.crt")
            peer-verify(required-untrusted)
            peer-verify(optional-untrusted)
            trusted-dn("CN=rubackup")
        )
    );
};
```

(1) Выполните настройку в соответствии с настройкой основного сервера RuBackup.

(2) Стандартная настройка TLS. Изменение порта недопустимо.

4. (опционально) Для вывода логов RuBackup в отдельный файл добавьте строку в конфигурационный файл:

```
destination d_rubackup { file("/var/log/rubackup.log"); };
```

5. Укажите путь к файлу сбора логов:

```
log { source(s_net); destination(d_rubackup); };
```

6. Если используется TLS, добавьте:

```
log { source(s_tls); destination(d_rubackup); };
```

7. Сохраните конфигурационный файл и проверьте синтаксическую корректность:

```
syslog-ng --syntax-only
```

Команда не должна вернуть никаких ошибок.

8. Перезапустите `syslog-ng`:

```
systemctl restart syslog-ng.service
```

Проверьте, что сервер слушает указанный сокет:

```
ss -tulpan | grep syslog
```

Пример успешной настройки `syslog-ng` *(состояние портов)*

```
tcp   LISTEN  0   255   0.0.0.0:8181   0.0.0.0:*   users:(("syslog-
ng",pid=4255,fd=12))
```

13.4.2. Установка и настройка сервера rsyslog

Установка

1. Некоторые дистрибутивы Linux уже содержат пакет `rsyslog`. Проверите наличие пакета:

   ```
   rsyslogd -v
   ```

2. Если сервер не установлен, установите его из репозитория:

   ```
   apt update
   apt install rsyslog
   ```

3. Запустите сервер:

   ```
   systemctl start rsyslog
   ```

4. Проверьте статус сервера:

   ```
   systemctl status rsyslog
   ```

5. Добавьте сервер в автозапуск:

   ```
   systemctl enable rsyslog
   ```

Настройка

Для обеспечения приема сообщений от RuBackup сервер rsyslog должен быть настроен на прослушивание сетевых сокетов по протоколам TCP и(или) UDP.

Для этого:

1. Откройте файл `/etc/rsyslog.conf`:

```
nano /etc/rsyslog.conf
```

2. Добавьте строки, в зависимости от того, какой протокол будет использоваться: TCP и(или) UDP:

```
# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")

# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="515")
```

3. Перезапустите `rsyslog`:

```
systemctl restart rsyslog.service
```

Проверьте, что сервер слушает указанные сокеты:

```
ss -tulpan | grep rsyslog
```

Пример успешной настройки `rsyslog` *(состояние портов)*

```
udp   UNCONN 0   0       0.0.0.0:515     0.0.0.0:*
users:(("rsyslogd",pid=1436,fd=5))
udp   UNCONN 0   0          [::]:515        [::]:*
users:(("rsyslogd",pid=1436,fd=6))
tcp   LISTEN 0   25      0.0.0.0:514     0.0.0.0:*
users:(("rsyslogd",pid=1436,fd=7))
tcp   LISTEN 0   25         [::]:514        [::]:*
users:(("rsyslogd",pid=1436,fd=8))
```

13.5. Настройка удаленного логирования в интерфейсе

13.5.1. Настройка логирования в RBM

Для настройки взаимодействия с SIEM системами в Менеджере администратора RuBackup:

1. Перейдите в раздел 🔒 **Безопасность** → **Журналы** → **Настройка внешних журналов** → **Серверы сбора логов**.
2. Нажмите ⊞ **Добавить** для добавления нового сервера сбора логов.
3. Заполните параметры сервера сбора логов:

   ▼ *Параметры сервера сбора логов*

Параметр	Описание
Имя хоста *	Имя хоста Syslog-сервера
Порт *	Порт Syslog-сервера
Тип соединения	TCP или UDP протокол

   При необходимости можно добавить описание сервера сбора логов.

   Нажмите ✓ **Применить** для сохранения настроек.

4. Перейдите в раздел 🔒 **Безопасность** → **Журналы** → **Настройка внешних журналов** → **Цели логирования**.
5. Нажмите ⊞ **Добавить** для создания нового правила сбора Приложение 13.A.
6. Заполните параметры цели логирования:

   ▼ *Параметры цели логирования*

Параметр	Описание
Сервер логирования *	Данные Syslog сервера вида: `<имя_хоста>:<порт> <тип_соединения>`
Протокол логирования *	На данный момент поддерживается только протокол `SysLog`
Формат логирования *	На данный момент поддерживается только формат `CEF`
Использовать TLS	Будет ли использоваться TLS протокол
Путь к сертификату TLS [2]	Полный путь к файлу с сертификатом
Включить логирование	Активирует логирование для этой цели

   При необходимости можно добавить описание цели логирования.

   Нажмите ✓ **Применить** для сохранения настроек.

7. Включите необходимую цель логирования для формата `CEF` переключателем

.

13.5.2. Настройка логирования в Tucana

Для настройки взаимодействия с SIEM системами в Tucana необходимо выполнить следующие шаги:

1. Перейдите в раздел **Безопасность** → **Журналы** → **Серверы сбора логов**.
2. Нажмите ⊞ **Добавить** для добавления нового сервера сбора логов.
3. Заполните параметры сервера сбора логов:

▼ *Параметры сервера сбора логов*

Параметр	Описание
Имя хоста ✱	Имя хоста Syslog-сервера
Порт ✱	Порт Syslog-сервера
Тип соединения	TCP или UDP протокол

При необходимости можно добавить описание сервера сбора логов.

Нажмите 🖫 **Применить** для сохранения настроек.

4. Перейдите в раздел **Безопасность** → **Журналы** → **Точки логирования**.
5. Нажмите ⊞ **Добавить** для добавления правила сбора Приложение 13.A.
6. Заполните параметры цели логирования:

▼ *Параметры цели логирования*

Параметр	Описание
Сервер логирования ✱	Данные Syslog сервера вида: `<имя_хоста>:<порт> <тип_соединения>`
Протокол ✱	На данный момент поддерживается только протокол `SysLog`
Формат ✱	На данный момент поддерживается только формат `CEF`
Использовать TLS	Будет ли использоваться TLS протокол
Путь к сертификату TLS [3]	Полный путь к файлу с сертификатом
Точка логирования	Активирует логирование для этой цели

При необходимости можно добавить описание цели логирования.

Нажмите 🖫 **Применить** для сохранения настроек.

7. Включите необходимую цель логирования для формата `CEF` переключателем .

13.6. Настройка `rb_syslog_reporter`

Утилита представляет собой исполняемый файл `rb_syslog_reporter`, входит в состав пакета `rubackup-server_<версия-пакета>_amd64_signed.deb`. Утилита предназначена для сбора и анализа данных из syslog-файлов и отправки их в syslog-сервер.

Предоставьте права на выполнение:

```
chmod 111 /opt/rubackup/bin/rb_syslog_reporter
```

13.6.1. Настройка конфигурационного файла `rb_siem.conf`

1. Создайте конфигурационный файл с помощью утилиты `rb_syslog_reporter`:

   ```
   /opt/rubackup/bin/rb_syslog_reporter -gen > /opt/rubackup/etc/rb_siem.conf
   ```

2. Откройте Приложение 13.Б и отредактируйте его в соответствии с вашими требованиями.
3. Ограничьте доступ к файлу `rb_siem.conf`:

   ```
   chown root:root rb_siem.conf
   chmod 600 rb_siem.conf
   ```

13.6.2. Настройка планировщика событий Linux

Запуск утилиты осуществляется через планировщик `cron` согласно заданному расписанию. В планировщике необходимо указать интервалы запуска.

Для этого:

1. Откройте планировщик:

   ```
   crontab -e
   ```

2. Добавьте строчку:

   ```
   * * * * * RB_SIEM_CONFIG=/abs/path/to/rb_siem.conf
   /opt/rubackup/bin/rb_syslog_reporter >> /tmp/sync.log 2>>
   /tmp/sync_error.log
   ```

где:

- `/abs/path/to/rb_siem.conf` — абсолютный путь до конфигурационного файла;
- `/opt/rubackup/bin/rb_syslog_reporter` — абсолютный путь к исполняемому файлу `rb_syslog_reporter`;
- `/tmp/sync.log`, `/tmp/sync_error.log` — абсолютные пути до файлов с логами.

Рекомендуется запускать ее каждую минуту.

3. Сохраните изменения.

Приложение А: События информационной безопасности

Таблица 6. Пользовательские сценарии, приводящие к формированию событий в журнале ИБ

Элемент системы	Сценарий
Стратегии	Добавление стратегии
	Редактирование стратегии
	Удаление стратегии
	Включение/выключение стратегии
Правила стратегии	Добавление правила стратегии
	Удаление правила стратегии
Репозиторий	Добавление резервной копии
	Удаление резервной копии
	Перемещение резервной копии
	Копирование резервной копии
	Редактирование срока хранения резервной копии
Клиенты РК	Добавление клиента вручную
	Удаление клиента
Медиасерверы	Добавление медиасервера вручную
	Удаление медиасервера
Пулы	Добавление пула
	Редактирование пула
	Удаление пула
Группы пулов	Добавление группы пулов
	Удаление группы пулов

Элемент системы	Сценарий
Подмена пулов	Добавление правила подмены пулов
	Удаление правила подмены пулов
Очередь задач	Появление новой задачи в очереди задач
	Перезапуск задачи в очереди задач
	Изменение статуса задачи в очереди задач
	Удаление задачи из очереди задач

Приложение Б: Конфигурационный файл `rb_siem.conf`

Таблица 7. Параметры `rb_siem.conf`

Параметр	Описание
`RB_HOST`	IP-адрес сервера RuBackup
`RB_USER`	Логин пользователя RuBackup
`RB_PASSWORD`	Пароль пользователя RuBackup
`DB_HOST`	IP-адрес служебной базы данных RuBackup
`DB_PORT`	Порт, на котором запущена служебная базы данных RuBackup
`DB_NAME`	Имя системной служебной базы данных
`RB_ROOT_CA_CERT`	Путь до корневого сертификата сервера RuBackup
`RB_CLIENT_CERT`	Путь до клиентского сертификата сервера RuBackup
`RB_CLIENT_CERT_KEY`	Путь до ключа клиентского сертификата сервера RuBackup

[1] Выполните настройку в соответствии с настройкой основного сервера RuBackup.

[2] Обязательное поле, если используется TLS.

[3] Обязательное поле, если используется TLS.