RuBackup

Система резервного копирования и восстановления данных

Резервное копирование и восстановление виртуальных машин KVM

Версия 1.3.1 2020

Оглавление

Введение

Система резервного копирования RuBackup позволяет выполнять полное, инкрементальное или дифференциальное резервное копирование виртуальных машин KVM без их остановки.

Полное резервное копирование – это создание резервной копии всех данных из исходного набора, независимо от того, изменялись данные или нет с момента выполнения последней полной резервной копии.

Дифференциальное резервное копирование сохраняет только данные, изменённые со времени выполнения предыдущего полного резервного копирования.

Инкрементальное резервное копирование сохраняет только данные, изменённые со времени выполнения предыдущей инкрементальной резервной копии, а если такой нет, то со времени выполнения последней полной резервной копии.

Для выполнения резервного копирования виртуальных машин на хост, где установлен KVM, требуется установить клиента RuBackup и модуль kvm для клиента RuBackup. В виртуальные машины, для которых предполагается выполнение резервного копирования средствами RuBackup, должен быть установлен qemu-guest-agent и в их конфигурацию должен быть добавлен Channel Device org.qemu.guest_agent.0.

Резервное копирование выполняется по заранее заданным правилам в глобальном расписании RuBackup. Клиенту доступно срочное резервное копирование виртуальных машин KVM, но в этом случае выполняется полное резервное копирование выбранного ресурса.

Восстановление резервной копии возможно по инициативе клиента. Для восстановления данных пользователь должен ввести пароль, позволяющий выполнить восстановление.

Полное резервное копирование может быть выполнено с применением сжатия на стороне клиента или на стороне сервера RuBackup, возможно преобразовать резервную копии выбранным алгоритмом (см. раздел “Защитное преобразование резервных копий”).

RuBackup может выполнять резервное копирование виртуальных машин KVM с дисками следующих типов: file, block, network (в том случае, когда диски виртуальной машины располагаются в хранилище Ceph в виде rados block device).

Резервное копирование поддерживается для raw, lvm, qcow2. Количество дисков в виртуальной машине может быть больше одного, в этом случае резервное копирование выполняется для всех дисков.

В ходе выполнения резервного копирования используется технология создания моментальных снимков виртуальной машины. Перед созданием снимка и сразу после создания снимка, внутри виртуальной машины может быть выполнен скрипт, который обеспечит консистентность данных приложения, функционирующего в виртуальной машине.

Установка клиента RuBackup

Для возможности резервного копирования виртуальных машин KVM при помощи RuBackup на сервер должен быть установлен клиент RuBackup. Подробно процедура установки клиента описана в «Руководстве по установке» RuBackup.

Клиент RuBackup представляет собой фоновое системное приложение (демон или сервис), обеспечивающее взаимодействие с серверной группировкой RuBackup. Для выполнения резервного копирование виртуальных машин KVM клиент RuBackup должен работать от имени суперпользователя (root для Linux и Unix).

Подготовка хоста KVM для выполнения резервного копирования средствами RuBackup

1. Установка модуля KVM RuBackup для возможности выполнения резервного копирования и восстановления виртуальных машин KVM

В зависимости от типа операционной системы:

sudo dpkg -i ./rubackup-kvm.deb

или

sudo rpm -I ./rubackup-kvm.rpm

2. Каталог для создания резервных копий и хранения временных файлов

Для создания резервных копий виртуальных машин и хранения временных файлов, которые создаются при их восстановлении, требуется определённое пространство. Рекомендуется выделить для этой цели отдельный диск или устройство хранения достаточного размера и примонтировать к /kvm-backup (либо к иной удобной точке монтирования), во избежание переполнения системного диска. Необходимо определить этот каталог как значение параметра use-local-backup-directory в конфигурационном файле /opt/rubackup/etc/config.file и перезагрузить клиент RuBackup.

В исключительных случаях допустимо использование возможности сервера RuBackup предоставить клиенту NFS каталог для создания резервной копии. Для этого нужно определить значение параметра nfs-share-mountpoint, который определяет в какую точку файловой системы будет примонтирован NFS каталог. Параметр use-local-backup-directory в этом случае должен быть отключён, а на сервере RuBackup произведены соответствующие настройки для определения разделяемого каталога. Более подробно см. «Руководство системного администратора RuBackup».

3. Настройка AppArmor для резервного копирования виртуальных машин, которые содержат несколько дисков

В некоторых случаях apparmor может блокировать выполнение резервного копирования вирутальных машин. На это может указывать следующая ошибка:

(error: internal error: unable to execute QEMU command 'transaction': Could not create file: Permission denied)

и сообщения о блокировании операций AppArmor в журнале системы.

Для того, чтобы это преодолеть, необходимо:

sudo apt-get install apparmor-utils

sudo aa-complain /usr/sbin/libvirtd

sudo aa-complain /etc/apparmor.d/libvirt/libvirt-7d2b303d-8c14-4a1d-9cbd-9020460b2f4e (подобные файлы)

Какой именно файл блокируется можно выяснить командой:

sudo cat /var/log/syslog | grep "apparmor" | grep "DENIED" | grep libvirt

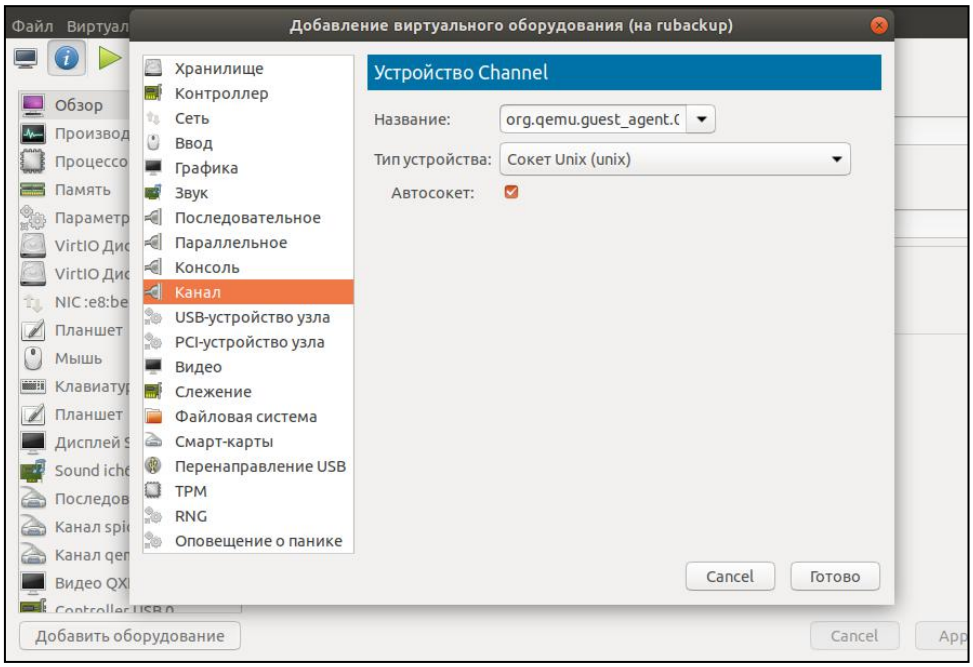
В том случае, когда у виртуальной машины несколько дисков, при создании снэпшота может возникнуть блокировка, инициированная apparmor.

Чтобы избежать подобных ситуаций, необходимо внести информацию о каталоге для создания резервных копий и хранения временных файлов в шаблон /etc/apparmor.d/libvirt/TEMPLATE.qemu:

```
profile LIBVIRT_TEMPLATE flags=(attach_disconnected) {
  #include <abstractions/libvirt-qemu>
  /kvm-backup/** rw,
}
```

Подготовка виртуальной машины KVM для выполнения резервного копирования средствами RuBackup

Установить для виртуальной машины оборудование chanell device org.qemu.guest_agent.0. Это можно сделать при помощи virt-manager:



Linux

В операционной системе виртуальной машины необходимо установить пакет qemu-guest-agent.

 # apt-get install qemu-guest-agent

или

 # yum install qemu-guest-agent

Windows

Для windows с диска virtio-win необходимо установить пакет qemu-ga из папки guest-agent, которая находится в корне диска.

Для Astra Linux Смоленск:

Необходимо использовать диск разработки и добавить соответствующий iso image в операционную систему как виртуальный CDROM. После этого:

 # sudo apt-cdrom add

 # sudo apt update

 # sudo apt install qemu-guest-agent

Защитное преобразование резервных копий

При необходимости ваши резервные копии могут быть преобразованы на клиенте сразу после выполнения резервного копирования. Таким образом, критичные данные будут недоступны для администратора RuBackup или для иных лиц, которые могли бы получить доступ к резервной копии (например, во внешнем хранилище картриджей ленточной библиотеки или на площадке провайдера облачного хранилища для ваших резервных копий).

Ключ для преобразования резервных копий располагается на клиенте в файле /opt/rubackup/keys/master-key. Пользователь сам должен задать ключ длиной 256 бит (32 байта).

Преобразование осуществляется специальной утилитой преобразования rbcrypt. Автоматическое защитное преобразование и обратное преобразование резервных копий клиентом RuBackup возможны при помощи ключей длиной 256 бит, однако утилита rbcryt поддерживает ключи длиной 128, 256, 512 и 1024 бита (в зависимости от выбранного алгоритма). Если необходимо для правила глобального расписания выбрать особый режим преобразования, с длиной ключа, отличной от 256 бит и с ключом, располагающемся в другом месте, то вы можете воспользоваться возможностью сделать это при помощи скрипта, выполняющегося после выполнения резервного копирования (определяется в правиле глобального расписания администратором RuBackup). При этом необходимо, чтобы имя преобразованного файла осталось таким же, как и ранее, иначе задача завершится с ошибкой. Выполнить обратное преобразование такого файла после восстановления его из резервной копии следует вручную при помощи утилиты преобразования. При таком режиме работы нет необходимости указывать алгоритм преобразования в правиле резервного копирования, либо архив будет преобразован ещё раз автоматически с использованием мастер-ключа.

Для выполнения преобразования доступны следующие алгоритмы:

Наименование алгоритма	**Поддерживаемая rbcrypt длина ключа, бит**	**Примечание**
Anubis	128, 256	
Aria	128, 256	
CAST6	128, 256	
Camellia	128, 256	
Kalyna	128, 256, 512	Украинский национальный стандарт ДСТУ 7624:2014
Kuznyechik	256	Российский национальный стандарт ГОСТ Р 34.12-2015
MARS	128, 256	
Rijndael	128, 256	Advanced Encryption Standard (AES)
Serpent	128, 256	
Simon	128	
SM4	128	Chinese national standard for Wireless LAN
Speck	128, 256	
Threefish	256, 512, 1024	
Twofish	128, 256	

Локальный лист ограничений

В том случае, если какие-либо конкретные ресурсы клиента не должны попасть в резервную копию, их можно включить в локальный лист ограничений на клиенте. Лист ограничений располагаются в каталоге /opt/rubackup/etc/rubackup_restriction.list.kvm

Наименование ресурса, для которого нет необходимости выполнять резервное копирование, должно быть указано в отдельной строке листа ограничений.

Для того, чтобы листы ограничений имели силу, необходимо включить эту возможность для клиента в конфигурации RuBackup (см. Руководство системного администратора RuBackup).

Использование менеджера администратора RuBackup для резервного копирования виртуальных машин KVM

Оконное приложение “Менеджер администратора RuBackup” (RBM) предназначено для общего администрирования серверной группировки RuBackup, управления клиентами резервного копирования, глобальным расписанием резервного копирования, хранилищами резервных копий и пр. RBM может быть запущено администратором на основном сервере резервного копирования RuBackup.

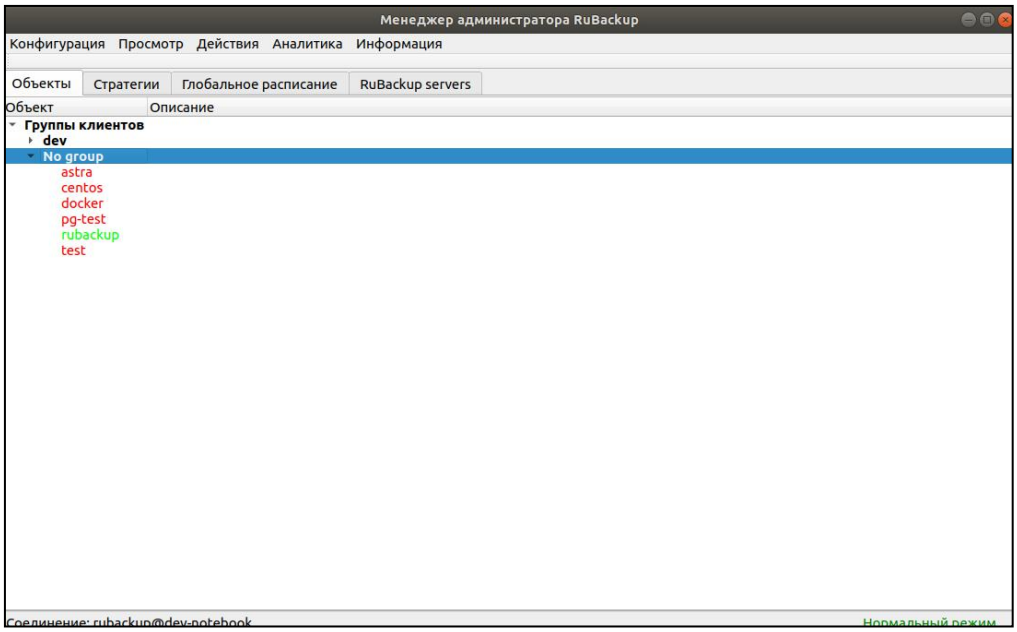
Запуск менеджера администратора RBM:

Вариант 1:

```
# sudo LD_LIBRARY_PATH=/opt/rubackup/lib /opt/rubackup/bin/rbm
```

Вариант 2:

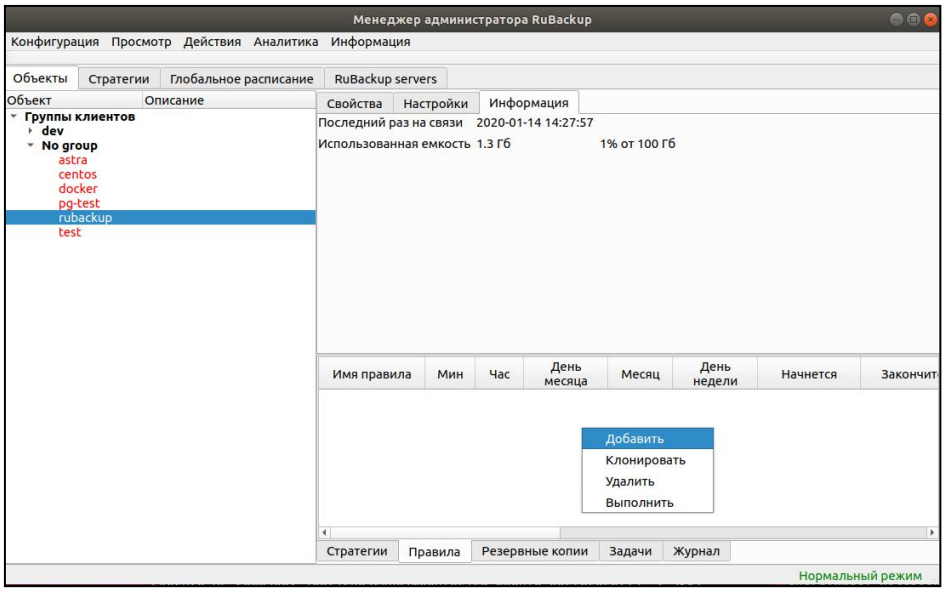
```
# ssh -X you_rubackup_server
# sudo LD_LIBRARY_PATH=/opt/rubackup/lib /opt/rubackup/bin/rbm
```



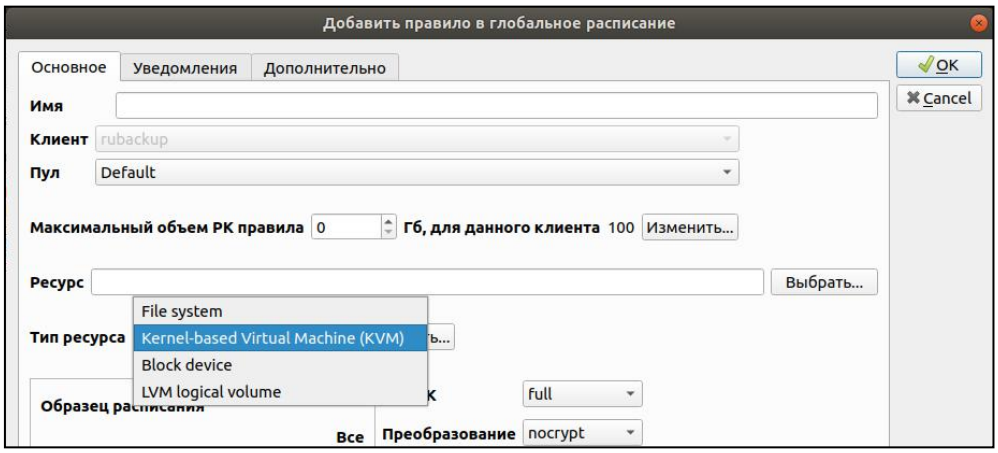
Для резервного копирования виртуальных машин KVM на хосте, где функционирует KVM, должен быть установлен клиент RuBackup и модуль, обеспечивающий резервное копирование KVM. Клиент должен быть авторизован администратором RuBackup (см.раздел “Клиенты” менеджера администратора RuBackup).

При помощи менеджера администратора RuBackup можно создать в глобальном расписании одно или несколько правил резервного копирования виртуальных машин гипервизора KVM.

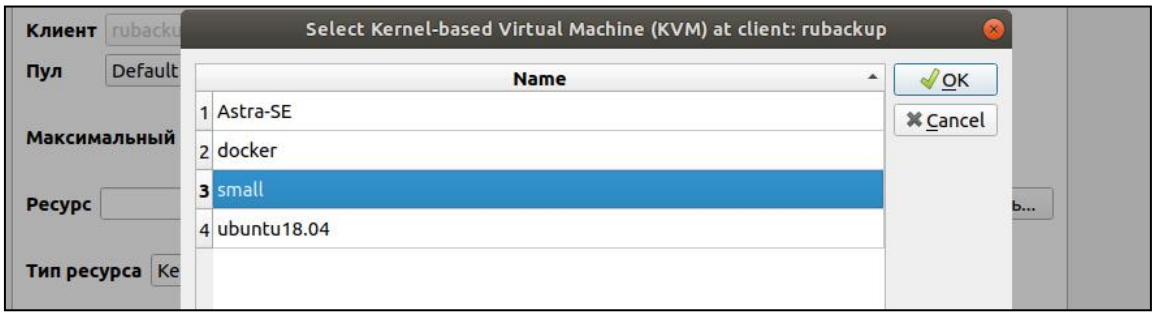
Выбираем клиентский хост, на котором установлен KVM и добавляем правило резервного копирования:



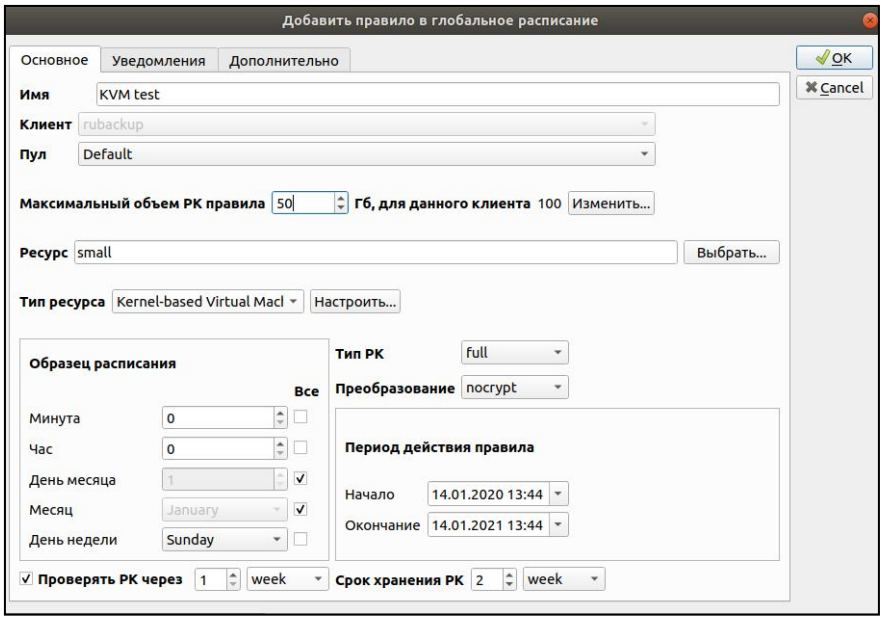
Выбираем тип ресурса «Kernel-based Virtual Machine (KVM)»:



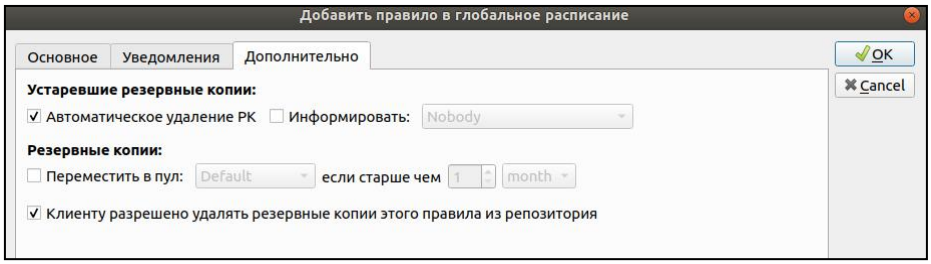
Выбираем ресурс, для которого будет выполняться правило:



Устанавливаем прочие настройки: тип резервного копирования (Full), максимальный объем для резервных копий данного правила (50Гб), срок хранения (2 недели), через какой промежуток времени требуется выполнить проверку резервной копии:



На вкладке «Дополнительно» можно установить разрешение для клиента удалять резервные копии, установить автоматическое удаление устаревших резервных копий или определить условие их перемещения в другой пул.



Вновь созданное правило будет обладать статусом “wait”, это означает что оно не будет порождать задач на выполнение резервного копирования до той поры, пока администратор RuBackup не запустит его и оно изменит свой статус на “run”. При необходимости работу правила можно будет приостановить или запустить в любой момент времени по желанию администратора. Так же администратор может инициировать немедленное создание задачи при статусе правила “wait”.

Правило глобального расписания имеет срок жизни, определяемый при его создании, а так же предусматривает следующие возможности:

1. Выполнить скрипт на клиенте перед началом резервного копирования.

2. Выполнить скрипт на клиенте после успешного окончания резервного копирования.

3. Выполнить скрипт на клиенте после неудачного завершения резервного копирования

4. Для виртуальных машин KVM в дополнительных настройках правила резервного копирования возможно задать выполнение скрипта непосредственно перед созданием снимка виртуальной машины KVM и непосредственно сразу после создания снимка виртуальной машины KVM.

5. Выполнить преобразование резервной копии на клиенте

6. Выполнить сжатие резервной копии на клиенте или на сервере после передачи ему резервной копии

7. Периодически выполнять проверку целостности резервной копии

8. Хранить резервные копии определённый срок, а после его окончания удалять их из хранилища резервных копий и из записей репозитория, либо просто уведомлять пользователей системы резервного копирования об окончании срока хранения.

9. Через определённый срок после создания резервной копии автоматически переместить её в другой пул хранения резервных копий, например на картридж ленточной библиотеки.

10. Уведомлять пользователей системы резервного копирования о результатах выполнения тех или иных операций, связанных с правилом глобального расписания.

При создании задачи RuBackup она появляется в главной очереди задач. Отслеживать исполнение правил может как администратор, с помощью RBM, так клиент при помощи RBC.

После успешного завершения резервного копирования резервная копия будет размещена в хранилище резервных копий, а информация о ней будет размещена в репозитории RuBackup.

Настройки правил глобального расписания RuBackup для резервного копирования виртуальных машин KVM

Для выполнения резервного копирования виртуальной машины KVM необходимо при помощи менеджера администратора RuBackup создать правило в глобальном расписании, в котором указать тип ресурса **Kernel-based Virtual Machine (KVM)**. При создании правила в глобальном расписании администратор RuBackup будет видеть список всех виртуальных машин на хосте гипервизора и может выбрать требуемую виртуальную машину (для этого необходимо, чтобы на клиенте работал клиентский фоновый процесс).

При создании правила резервного копирования можно определить следующие параметры:

- Тип резервного копирования (полный, дифференциальный или инкрементальный)
- Разрешенный максимальный объем для всех резервных копий правила
- Необходимость преобразования резервной копии тем или иным алгоритмом . Преобразование будет выполняться на стороне клиента
- Шаблон времени и даты создания задачи резервного копирования
- Флаг и период автоматической проверки резервной копии
- Срок хранения резервных копий создаваемого правила
- Пул хранения, в котором будут размещены резервные копии
- Необходимость автоматического удаления резервной копии, срок хранения которой истёк
- Перемещение резервной копии в другой пул, при достижении определённого срока с момента её создания

- Возможность для клиента удалять резервные копии из репозитория
- Настройки системы уведомления RuBackup для создаваемого правила. Уведомления могут происходить в следующих случаях:
  - Нормальное исполнение процедуры резервного копирования
  - Исполнение процедуры резервного копирования с ошибками
  - Проверка резервной копии
  - Окончание периода действия создаваемого правила
  - Окончание выделенного объёма для хранения резервных копий правила
  - Окончание срока хранения резервной копии
- Дополнительные настройки правила для выполнения резервного копирования виртуальной машины KVM:
  - Скрипт внутри виртуальной машины, который будет выполнен непосредственно перед созданием снимка состояния виртуальной машины KVM.
  - Скрипт внутри виртуальной машины, который будет выполнен непосредственно после создания снимка состояния виртуальной машины KVM
  - Таймаут в секундах, по истечение которого незавершившийся скрипт внутри виртуальной машины считается завершившимся неудачно
  - Размер блока данных для выполнения копирования информации с raw устройств виртуальной машины
  - Необходимость выполнять резервное копирование, если виртуальная машина находится в выключенном состоянии.

Запуск скрипта внутри виртуальной машины при резервном копировании

В том случае, если дополнительными настройками правила резервного копирования не задан скрипт, который должен быть выполнен внутри виртуальной машины перед и после создания снэпшота, но в виртуальной машине присутствует файл /opt/rubackup/scripts/rubackup-kvm.sh, то он будет выполнен с аргументом before перед созданием снэпшота и с аргументом after - после создания снэпшота. Значение таймаута в этом случае равняется 5 секундам.

Использование клиентского менеджера RuBackup

Принцип взаимодействия клиентского менеджера с системой резервного копирования состоит в том, что пользователь может сформировать ту или иную команду (желаемое действие) и отправить его серверу резервного копирования RuBackup. Взаимодействие пользователя с сервером резервного копирования производится через клиента (фоновый процесс) резервного копирования. Клиентский менеджер отправляет команду пользователя клиенту, клиент отправляет её серверу. В том случае, если действие допустимо, то сервер RuBackup отдаст обратную команду клиенту и/или перенаправит её медиа-серверу RuBackup для дальнейшей обработки. Это означает, что клиентский менеджер обычно не ожидает завершения того или иного действия, но ожидает ответа от клиента, что задание принято. Это позволяет инициировать параллельные запросы клиента к серверу резервного копирования, но требует от пользователя самостоятельно контролировать чтобы не было “встречных” операций, когда происходит восстановление данных, и в этот же момент эти же данные требуются для создания новой резервной копии. После того, как вы отдали ту или иную команду при помощи клиентского менеджера, вы можете просто закрыть приложение, все действия будут выполнены системой резервного копирования (однако стоит дождаться сообщения что задание принято к исполнению и проконтролировать это в закладке “Задачи”).

Графический интерфейс клиентского менеджера поддерживает русский и английский языки.

Запуск клиентского менеджера:

Вариант 1:

```
# sudo LD_LIBRARY_PATH=/opt/rubackup/lib /opt/rubackup/bin/rbc
```

Вариант 2:

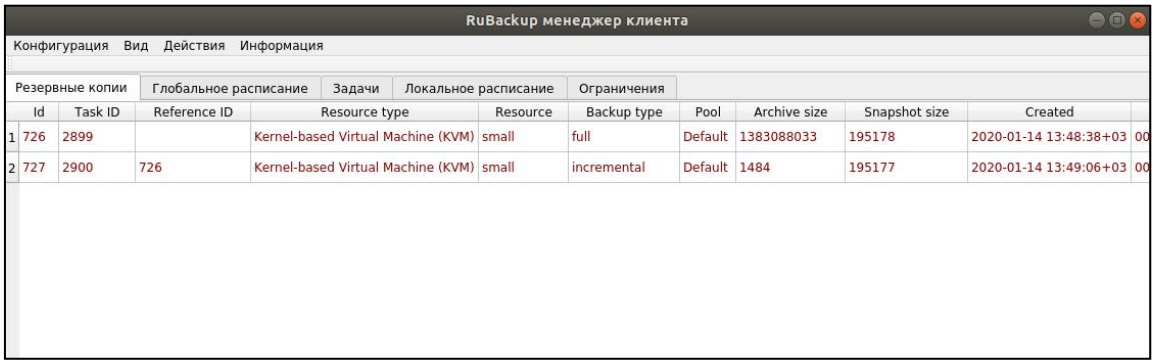
ssh -X you_rubackup_server

sudo LD_LIBRARY_PATH=/opt/rubackup/lib /opt/rubackup/bin/rbc

При первом запуске клиентского менеджера необходимо задать пароль, при помощи которого впоследствии можно будет запросить восстановление резервной копии. Без ввода пароля получить резервную копию для клиента из хранилища невозможно. Хэш пароля восстановления хранится в базе данных RuBackup сервера. При необходимости можно изменить пароль при помощи клиентского менеджера (Меню “Конфигурация” -> “Изменить пароль”).

На главной странице клиентского менеджера расположены переключающиеся закладки, позволяющие управлять резервными копиями, расписанием резервного копирования и просматривать текущие задачи клиента.

Закладка “Резервные копии”



В таблице закладки “Резервные копии” содержится информация обо всех резервных копиях клиента, которые хранятся в репозитории RuBackup. Дифференциальные резервные копии ссылаются на полные резервные копии, инкрементальные резервные копии ссылаются на полные резервные копии или предыдущие инкрементальные, так что при необходимости восстановить данные можно одной командой инициировать восстановление всей цепочки резервных копий.

В закладке “Резервные копии” пользователю доступны следующие действия:

◆ Удалить выбранную резервную копию.

Это действие возможно в том случае, если в правиле глобального расписания есть соответствующее разрешение. Кроме того, при необходимости выполнить удаление резервной копии потребуется вести пароль клиента.

◆ Восстановить цепочку резервных копий

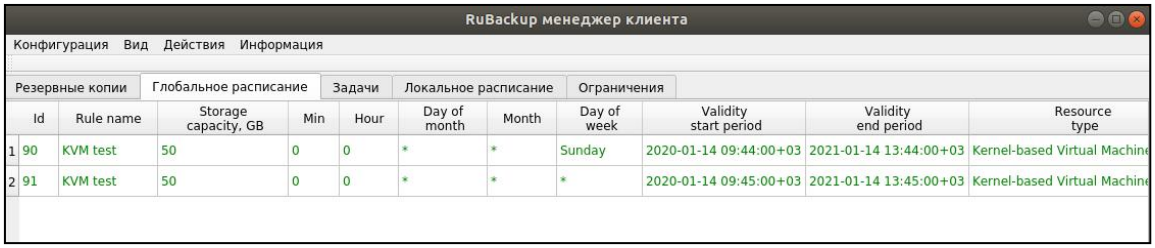
Это действие запускает процесс восстановления цепочки резервных копий на локальной файловой системе клиента. При восстановлении резервной копии или цепочки резервных копий пользователь может выбрать место восстановления резервной копии файлов виртуальной машины KVM.

Клиентский менеджер не ожидает окончания восстановления всех резервных копий, пользователь должен проконтролировать во вкладке “Задачи” что все созданные задачи на восстановление данных завершились успешно (статус задач “Done”). Для успешного выполнения этого действия требуется наличие достаточного свободного места в каталоге, предназначенном для создания и временного хранения резервных копий (см.опцию use-local-backup-directory).

◆ Проверить резервную копию

Это действие инициирует создание задачи проверки резервной копии. В том случае, если резервная копия была подписана цифровой подписью, то будет проверены размер файлов резервной копии, md5 сумма и проверена сама резервная копия. Если резервная копия не была подписана цифровой подписью, то будут проверены размер файлов резервной копии и md5 сумма.

Закладка “Глобальное расписание”



	Id	Rule name	Storage capacity, GB	Min	Hour	Day of month	Month	Day of week	Validity start period	Validity end period	Resource type
1	90	KVM test	50	0	0	*	*	Sunday	2020-01-14 09:44:00+03	2021-01-14 13:44:00+03	Kernel-based Virtual Machine
2	91	KVM test	50	0	0	*	*	*	2020-01-14 09:45:00+03	2021-01-14 13:45:00+03	Kernel-based Virtual Machine

В таблице закладки “Глобальное расписание” содержится информация обо всех правилах в глобальном расписании RuBackup для этого клиента.

В закладке “Глобальное расписание” пользователю доступны следующие действия:

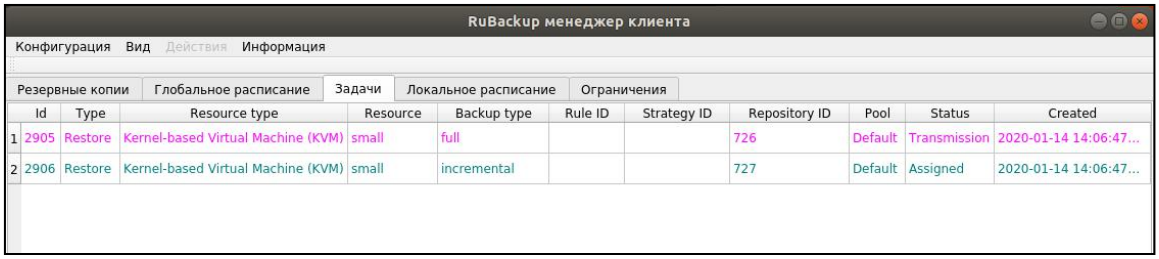
◆ Запросить новое правило

Это действие вызывает диалог подготовки нового правила в глобальном расписании RuBackup для данного клиента. Запрос на добавление правила требует одобрения администратора RuBackup, одобрение может быть сделано в оконном менеджере администратора RuBackup.

◆ Запросить удалить правило из глобального расписания

Это действие формирует запрос к администратору RuBackup об удалении выбранного пользователем правила из глобального расписания RuBackup. Запрос на удаление правила требует одобрения администратора RuBackup, одобрение может быть сделано в оконном менеджере администратора RuBackup.

Закладка “Задачи”



В таблице закладки “Задачи” содержится информация обо всех задачах в главной очереди заданий RuBackup для этого клиента. В зависимости от настроек резервного сервера RuBackup выполненные задачи и задачи, завершившиеся неудачно, через какое-то время могут быть автоматически удалены из главной очереди задач. Информация о выполнении заданий фиксируется в специальном журнале задач сервера RuBackup, при необходимости статус любой задачи, даже удалённой из очереди, можно уточнить у администратора RuBackup.Так же информация о выполнении задач клиента заносится в локальный журнальный файл на клиенте. В клиентском менеджере можно открыть окно отслеживания журнального файла (меню “Информация” -> “Журнальный файл”).

Закладка “Локальное расписание”

В закладке «Локальное расписание» можно определить правила, задаваемые клиентом для тех или иных локальных ресурсов. Для работы локального расписания эта возможность должна быть включена администратором RuBackup для клиента.

Закладка “Ограничения”

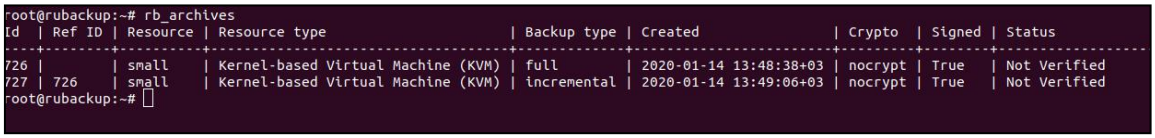
В закладке «Ограничения» могут быть определены локальные ресурсы, резервное копирование которых нежелательно. Для работы локальных ограничений эта возможность должна быть включена администратором RuBackup для клиента.

Утилиты командной строки клиента RuBackup

Для управления RuBackup со стороны клиента, помимо клиентского оконного менеджера, можно воспользоваться утилитами командной строки:

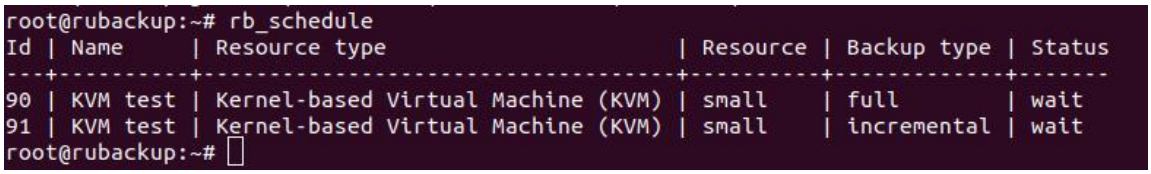
rb_archive

Утилита предназначена для просмотра списка резервных копий клиента в системе резервного копирования, создания срочных резервных копий, их удаления, проверки и восстановления.



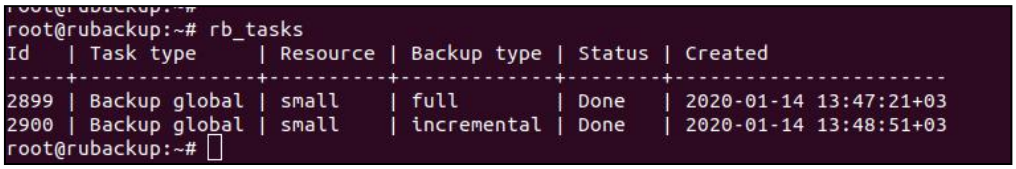
rb_schedule

Утилита презназначена для просмотра имеющихся правил клиента в глобальном расписании резервного копирования.



rb_tasks

Утилита предназначена для просмотра задач клиента, которые присутствуют в главной очереди задач системы резервного копирования.



Ознакомиться с функциями утилит командной строки можно при помощи команды man или в руководстве “Утилиты командной строки RuBackup”.

Действия после восстановления резервной копии виртуальной машины

При восстановлении резервной копии при помощи RBC она будет восстановлена в выбранный пользователем каталог. При использовании утилиты rb_archive (см. опцию -x) она будет восстановлена в локальный каталог, либо же в тот, который был задан опцией -d.

В выбранном пользователем пути будем создан каталог с именем восстанавливаемой виртуальной машины со следующем содержимым:

- конфигурационный файл виртуальной машины в формате xml

- файлы дисков виртуальной машины

Для немедленной проверки восстановленной резервной копии требуется сделать следующее:

A) Файлы дисков виртуальной машины в формате qcow2

1. Необходимо внести изменения в xml файл (предположим, что конфигурационный файл располагается в small.xml):

1.1. Удалить строку с UUID

1.2. Изменить имя домена. Имя домена находится между <name> и </name>, например:

<name>small</name>

```
<domain type='kvm'>
  <name>small-restored</name>
  <memory unit='KiB'>2097152</memory>
  <currentMemory unit='KiB'>2097152</currentMemory>
  <vcpu placement='static'>1</vcpu>
  <os>
    <type arch='x86_64' machine='pc-i440fx-bionic'>hvm</type>
  </os>
```

1.3. Изменить пути доступа к файлам виртуальной машины, например:

<source file='/var/lib/libvirt/images/small.qcow2'/>

```
<disk type='file' device='disk'>
  <driver name='qemu' type='qcow2'/>
  <source file='/var/lib/libvirt/images/small.qcow2'/>
  <target dev='vda' bus='virtio'/>
  <boot order='1'/>
  <address type='pci' domain='0x0000' bus='0x00' slot='0x07' function='0x0'/>
</disk>
```

Требуется изменить на

<source file='/kvm/small.qcow2'/>

```
<disk type='file' device='disk'>
  <driver name='qemu' type='qcow2'/>
  <source file='/kvm/small.qcow2'/>
  <target dev='vda' bus='virtio'/>
  <boot order='1'/>
  <address type='pci' domain='0x0000' bus='0x00' slot='0x07' function='0x0'/>
</disk>
```

если файлы резервной копии были восстановлены в каталог /kvm. При этом необходимо, чтобы данный каталог был разрешён для хранения данных KVM.

2. Запуск виртуальной машины:

virsh create small.xml

```
root@rubackup:/kvm# virsh create small.xml
Domain small-restored created from small.xml

root@rubackup:/kvm#
```

Б) Файлы дисков виртуальной машины в raw формате

В данном случае есть два пути (предположим, что файлы находятся в /kvm/small):

1. Восстановить файлы дисков виртуальной машины в подходящее raw устройство с помощью команды dd, например:

1.1. dd if=/kvm/small/sde1 of=/dev/sde1 bs=5M

1.2. Исправить xml файл: изменить имя домена, удалить строку с UUID, при необходимости изменить пути доступа к raw устройствам.

2. Другой путь - это конвертировать восстановленные файлы raw устройств в qcow2 формат при помощи команды qemu-img convert, например:

2.1. qemu-img convert -f qcow2 -O raw /kvm/small/sde1 /kvm/small/image.qcow2

2.2. Исправить xml файл: изменить имя домена, удалить строку с UUID, при необходимости изменить пути доступа к файлам дисков и их типы.

3. Запуск виртуальной машины:

virsh create small.xml

После проверки функционирования восстановленной виртуальной машины системный администратор должен принять решение о том, куда именно должны быть размещены файлы восстановленной виртуальной машины в рабочую конфигурацию KVM.

Б) Файлы дисков виртуальной машины в raw формате находились в хранилище Ceph в rados block device

В данном случае необходимо внести изменения в xml файл:

1. Изменить <name>restored</name>

2. Удалить <uuid>....</uuid>

3. Секцию <disk> ... </disk> привести к следующему виду, чтобы можно было запустить виртуальную машину с локальным образом:

<disk type='file' device='disk'>

<driver name='qemu' type='raw'/>

<source file='path_to_restored_image'/>

<backingStore/>

4. Удалить секции <auth> ... </auth>

<source protocol='rbd' .... </source>

5. запустить виртуальную машину для проверки:

    # virsh create yourfile.xml

Лицензирование

Система резервного копирования RuBackup имеет следующие типы лицензий:

Простая бесплатная лицензия

Эта лицензия включает в себя возможность выполнять резервное копирование десяти клиентов и десяти виртуальных машин KVM. При необходимости выполнять резервное копирования для большего числа клиентов и большего числа виртуальных машин KVM, необходимо приобретение коммерческой лицензии. Для простой лицензии нет возможности использовать резервный сервер RuBackup и добавлять в конфигурацию дополнительные медиа-серверы.

Коммерческая лицензия

Эта лицензия включает в себя возможность выполнять резервное копирование для того количества клиентов, которые покрываются лицензией. Возможно расширение серверной группировки RuBackup с помощью медиа серверов, построение отказоустойчивой конфигурации путём добавления резервного сервера. Все серверы серверной группировки должны иметь собственные лицензии, одинаковые с точки зрения количества клиентов.

Пробная лицензия

Эта лицензия включает в себя возможность проверить функционал системы резервного копирования. По окончании действия пробной лицензии функционирование системы приостанавливается.

Более подробно о лицензировании RuBackup читайте в соответствующем руководстве.