

RuBackup

Система резервного копирования и восстановления данных

Резервное копирование и восстановление данных FreeIPA



RuBackup

Версия 1.4

2020 г.

Содержание

Введение.....	3
Установка клиента RuBackup.....	4
Подготовка хоста FreeIPA.....	5
Резервное копирование FreeIPA.....	7
Мастер-ключ.....	9
Защитное преобразование резервных копий.....	10
Локальные списки ограничений.....	12
Менеджер Администратора RuBackup (RBM).....	13
Правила глобального расписания RuBackup.....	19
Менеджер Клиента RuBackup (RBC).....	20
Утилиты командной строки клиента RuBackup.....	24

Введение

Система резервного копирования RuBackup позволяет выполнять полное резервное копирование данных FreeIPA в ОС Linux.

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

FreeIPA является интегрированной системой проверки подлинности и авторизации в сетевой среде Linux. FreeIPA сервер обеспечивает централизованную проверку подлинности, авторизацию и контроль аккаунтов пользователей, сохраняя сведения о пользователе, группах, узлах и других объектах, необходимых для обеспечения сетевой безопасности. Это комплексное решение по управлению безопасностью Linux-систем, 389 Directory Server, MIT Kerberos, NTP, DNS и Dogtag. FreeIPA поддерживает веб-интерфейс и интерфейс командной строки.

Для выполнения резервного копирования данных FreeIPA на клиенте RuBackup должен быть установлен модуль RuBackup **rb_module_freeipa**. Работа этого модуля на клиенте возможна только в том случае, если на нём установлены необходимые пакеты FreeIPA, и активна служба `ipa.service`.

Резервное копирование выполняется по заранее заданным правилам в глобальном расписании RuBackup. Также клиенту доступно срочное резервное копирование данных FreeIPA.

Восстановление данных из архива возможно по инициативе клиента. Для восстановления данных пользователь должен ввести пароль, позволяющий выполнить восстановление. Резервное копирование может быть выполнено с применением сжатия на стороне клиента или на стороне сервера RuBackup. При необходимости, возможно выполнить защитное преобразование резервной копии выбранным алгоритмом (см. раздел «Защитное преобразование резервных копий»).

Установка клиента RuBackup

Для осуществления резервного копирования и восстановления данных FreeIPA при помощи RuBackup на хост должен быть установлен клиент RuBackup со всеми необходимыми модулями. Клиент RuBackup представляет собой фоновое системное приложение (демон или сервис), обеспечивающее взаимодействие с серверной группировкой RuBackup. Для выполнения резервного копирования ресурсов FreeIPA клиент RuBackup должен работать от имени суперпользователя (root в Linux и Unix). Подробно процедуру установки клиента RuBackup см. «Руководство по установке RuBackup».

Подготовка хоста FreeIPA

Чтобы подготовить хост с установленным FreeIPA для выполнения резервного копирования и восстановления данных средствами RuBackup необходимо выполнить следующее:

1. Установить модуль RuBackup **rb_module_freeipa**. В зависимости от используемой в ОС системы управления пакетами следует выполнить команду:

```
# sudo dpkg -i ./gubackup-freeipa.deb
```

Либо:

```
# sudo rpm -I ./gubackup-freeipa.rpm
```

Внимание! Для работы модуля rb_module_freeipa требуется Python версии 3.6 или выше.

2. Очистить каталог `/var/lib/ipa/backup`.

Перед использованием модуля необходимо убедиться, что каталог `/var/lib/ipa/backup` пуст. Если до того, как модуль был установлен, в этом каталоге присутствуют резервные копии, рекомендуется перенести их в другое место во избежание ошибок.

3. Подготовить файл конфигурации модуля `/opt/gubackup/etc/rb_module_freeipa.conf`. Это файл содержит два поля:

- `password` - поле для ввода пароля администратора FreeIPA;

- `direct_restore` - значение этого поля указывает, нужно ли просто распаковать резервную копию в определённый каталог (значение `no`) или выполнить восстановление резервной копии (значение `yes`).

Пример содержания файла:

```
password:123456789
direct_restore:yes
```

Если в файле конфигурации модуля поле `password` содержит пароль, а поле `direct_restore` было оставлено пустым, то по умолчанию будет произведено восстановление полной резервной копии.

Файл `rb_module_freeipa.conf` используется только при восстановлении резервной копии, поэтому после восстановления данных рекомендуется оставлять его пустым во избежание утечки пароля.

Внимание! Если конфигурационный файл отсутствует, то резервная копия будет распакована в заданную директорию.

Резервное копирование FreeIPA

Система резервного копирования RuBackup позволяет выполнять полное резервное копирование сервера FreeIPA либо резервное копирование только данных FreeIPA. Подробно процедура настройки описана в разделе «Менеджер администратора RuBackup (RBM)» на стр. **Error! Bookmark not defined.**

Полное резервное копирование сервера FreeIPA

Полное резервное копирование сервера FreeIPA создаёт копию всех файлов сервера FreeIPA, а также данных LDAP. FreeIPA затрагивает сотни файлов и каталогов, а также конфигурации и файлы журналов, которые относятся непосредственно к IPA или к различным его службам.

Модуль RuBackup **rb_module_freeipa** производит резервное копирование при помощи утилиты `ipa-backup`.

При выполнении полного резервного копирования утилита `ipa-backup` останавливает все службы FreeIPA, чтобы обеспечить безопасный ход процесса резервного копирования.

Резервное копирование производится в каталог `/var/lib/ipa/backup/`.

Восстановление полной резервной копии из файла происходит при помощи утилиты `ipa-restore`, которая имеет следующий синтаксис:

```
# ipa-restore path_to_backup -U --password=password [ --data [ --  
online ] ]
```

Значение *path_to_backup* задаёт путь к файлу резервной копии. Значение *password* содержит пароль администратора хоста. Параметр `--data` позволяет задать восстановление только данных из полной резервной копии сервера FreeIPA. При восстановлении только данных параметр `--online` позволяет выполнить восстановление без остановки служб FreeIPA.

Резервное копирование только данных FreeIPA

Резервная копия только данных FreeIPA создаёт копию данных LDAP и журнала изменений. Этот тип резервного копирования также поддерживает запись содержимого LDAP, хранящегося в LDIF.

Модуль RuBackup **rb_module_freeipa** производит резервное копирование модуль производит при помощи утилиты `ipa-backup`. Вызов:

```
# ipa-backup --data [ --online ]
```

Резервная копия данных может выполняться как в режиме онлайн (без остановки служб FreeIPA), так и в автономном режиме.

Резервное копирование производится в каталог `/var/lib/ipa/backup/`.

Восстановление резервной копии данных из файла происходит при помощи утилиты `ipa-restore`, которая имеет следующий синтаксис:

```
# ipa-restore path_to_backup -U --password=password [ --data [ --online ] ]
```

Значение *path_to_backup* задаёт путь к файлу резервной копии. Значение *password* содержит пароль администратора хоста. Параметр `--data` позволяет задать восстановление только данных из полной резервной копии сервера FreeIPA. При восстановлении только данных параметр `--online` позволяет выполнить восстановление без остановки служб FreeIPA.

Мастер-ключ

В ходе установки клиента RuBackup будет создан мастер-ключ для защитного преобразования резервных копий, а также ключи для электронной подписи, если предполагается использовать электронную подпись.

Внимание! При утере ключа вы не сможете восстановить данные из резервной копии, если она была преобразована с помощью защитных алгоритмов.

Важно! Ключи рекомендуется после создания скопировать на внешний носитель, а также распечатать бумажную копию и убрать эти копии в надёжное место.

Мастер-ключ рекомендуется распечатать при помощи утилиты hexdump, так как он может содержать неотображаемые на экране символы:

```
$ hexdump /opt/rubackup/keys/master-key
00000000 79d1 4749 7335 e387 9f74 c67e 55a7 20ff
00000100 6284 54as 83a3 2053 4818 e183 1528 a343
00000200
```

Защитное преобразование резервных копий

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

Защитное преобразование осуществляется входящей в состав RuBackup утилитой `gbscrypt`. Ключ для защитного преобразования резервных копий располагается на хосте клиента в файле `/opt/rubackup/keys/master-key`. Защитное преобразование данных при помощи `gbscrypt` возможно с длиной ключа 256 бит (по умолчанию), а также 128, 512 или 1024 бита в зависимости от выбранного алгоритма преобразования.

Если для правила глобального расписания необходимо выбрать особый режим защитного преобразования с длиной ключа, отличной от 256 бит, и с ключом, расположенным в другом месте, то вы можете 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. Провести обратное преобразование такого файла после восстановления его из архива следует вручную при помощи утилиты `gbscrypt`. При таком режиме работы нет необходимости указывать алгоритм преобразования в правиле резервного копирования, иначе архив будет повторно преобразован с использованием мастер-ключа.

Алгоритмы защитного преобразования

Для выполнения защитного преобразования доступны следующие алгоритмы:

Таблица 1. Алгоритмы защитного преобразования, доступные в утилите gbscrypt.

Алгоритм	Длина ключа, бит	Примечание
Anubis	128, 256	
Aria	128, 256	
CAST6	128, 256	
Camellia	128, 256	
Kalyna	128, 256, 512	Украинский национальный стандарт <u>ДСТУ 7624:2014</u>
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	Китайский национальный стандарт для беспроводных сетей
Speck	128, 256	
Threefish	256, 512, 1024	
Twofish	128, 256	

Локальные списки ограничений

При работе модуля **rb_module_freeipa** локальные списки ограничений не применяются.

Менеджер Администратора RuBackup (RBM)

Оконное приложение Менеджер Администратора RuBackup (RBM) предназначено для администрирования серверной группировки RuBackup, включая управление клиентами, глобальным расписанием, хранилищами резервных копий и другими параметрами RuBackup. Системный администратор RuBackup может запустить RBM на основном сервере резервного копирования RuBackup.

Для запуска RBM следует выполнить команду:

```
# ssh -X user@rubackup_server  
# /opt/rubackup/bin/rbm&
```

Пользователь, запускающий RBM, должен входить в группу rubackup.

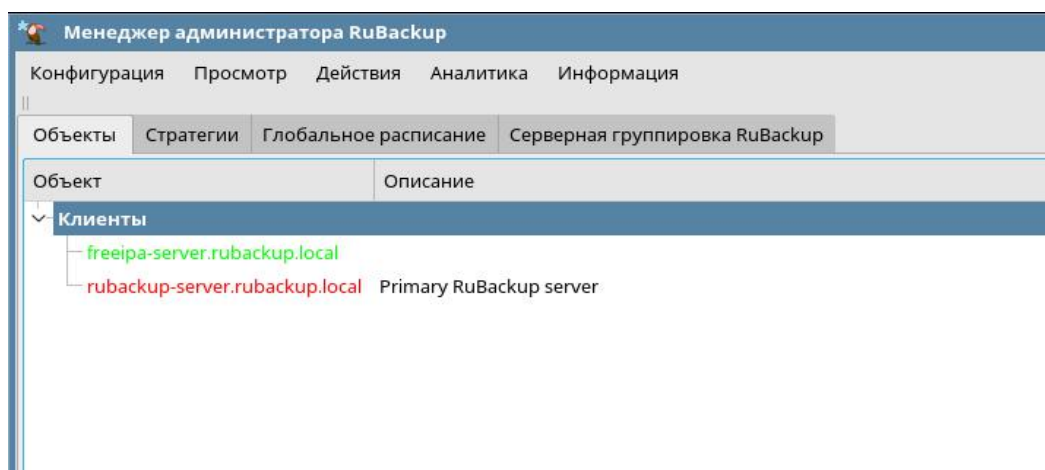


Рис. 1. Менеджер администратора RuBackup.

Для резервного копирования данных FreeIPA на хосте должен быть установлен клиент RuBackup и необходимые модули. Клиент должен быть авторизован администратором RuBackup.

Если клиент RuBackup установлен, но не авторизован, в нижней части окна RBM появится сообщение о том, что найдены неавторизованные клиенты. Все новые клиенты должны быть авторизованы в системе резервного копирования RuBackup.

Для авторизации неавторизованного клиента в RBM выполните следующие действия:

1. Откройте меню «Действия» > «Клиенты» > «Авторизовать клиентов».

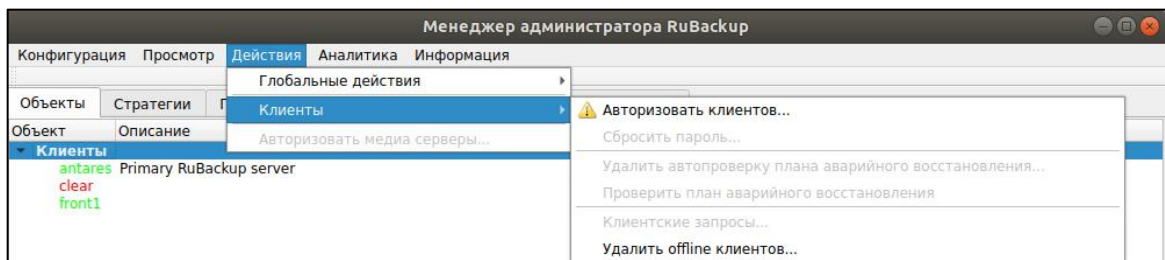


Рис. 2. Меню авторизации клиентов.

2. Выберите нужного неавторизованного клиента и нажмите «Авторизовать».

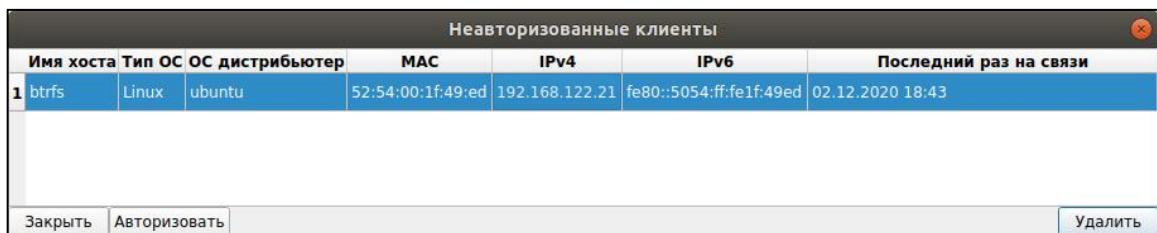


Рис. 3. Список неавторизованных клиентов в RBM.

После авторизации новый клиент будет виден в главном окне RBM:

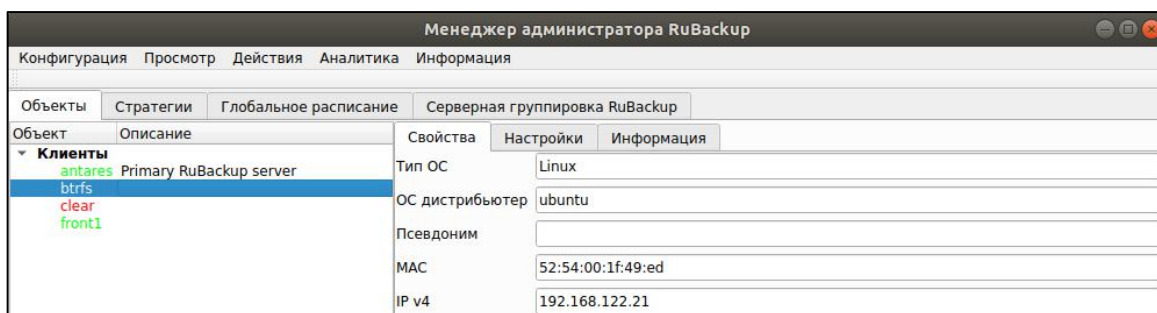


Рис. 4. Авторизованный клиент в RBM.

Чтобы выполнять регулярное резервное копирование данных FreeIPA, необходимо создать правило в глобальном расписании. Для этого выполните следующие действия:

1. Выберите хост клиента, на котором установлено FreeIPA, и добавьте правило резервного копирования.

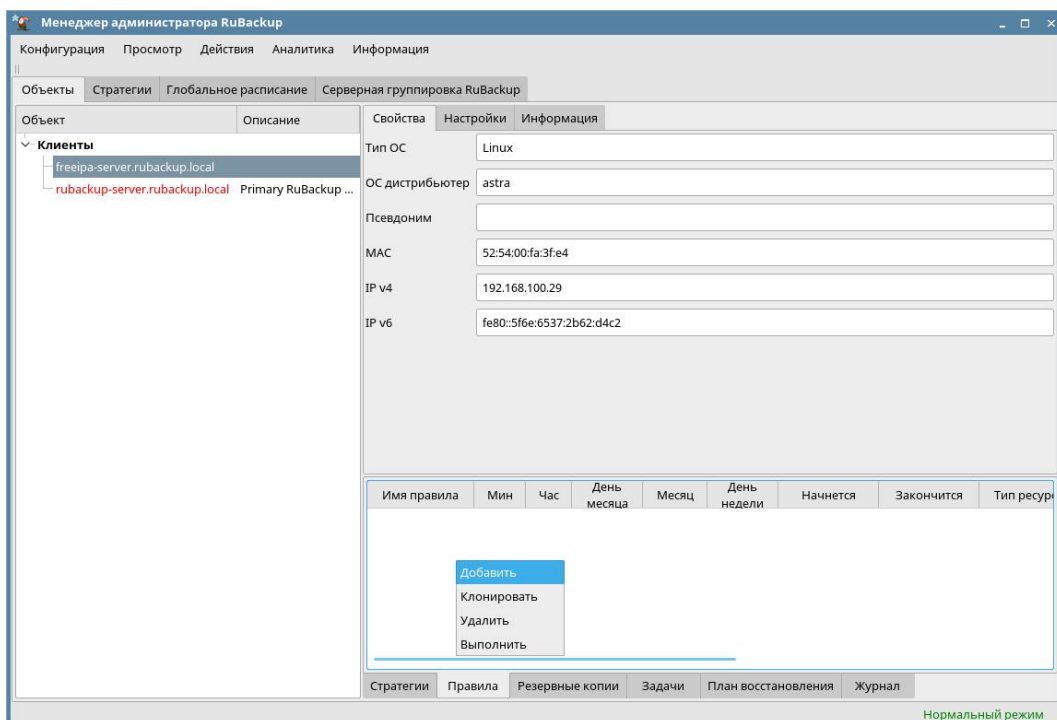


Рис. 5. Добавление правила резервного копирования.

2. Выберите тип ресурса “Free IPA”.

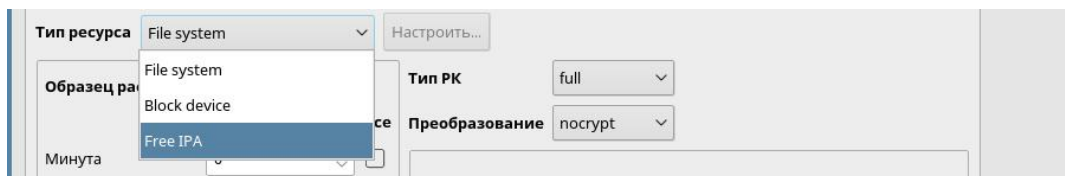


Рис. 6. Выбор типа ресурса для правила резервного копирования.

3. Выберите ресурс, для которого будет выполняться правило.



Рис. 7. Выбор ресурса для правила резервного копирования.

4. Установите настройки правила: название правила, пул хранения данных, максимальный объём для резервных копий правила (в ГБ), тип резервного копирования, расписание резервного копирования, срок хранения и необязательный временной промежуток проверки резервной копии.

Добавить правило в глобальное расписание

Основное | Уведомления | Дополнительно

Имя: Astra freeipa

Клиент: freeipa-server.rubackup.local

Пул: Default

Максимальный объем РК правила: 1 Гб, для данного клиента 10

Ресурс: FreeIPA 4.6.4

Тип ресурса: Free IPA

Образец расписания:

Минута	0	<input type="checkbox"/>
Час	0	<input type="checkbox"/>
День месяца	1	<input type="checkbox"/>
Месяц	January	<input type="checkbox"/>
День недели	Monday	<input type="checkbox"/>

Тип РК: full

Преобразование: nocrypt

Период действия правила:

Начало	16.11.2020 15:34
Окончание	16.11.2021 15:34

Проверять РК через 1 month

Срок хранения РК: 1 year

Да

Отмена

Рис. 8. Настройки правила резервного копирования.

- Нажмите кнопку «Настроить» и настройте дополнительные параметры ресурса Free IPA.

Free IPA settings for client: freeipa-server.rubackup.local

Parameter	Data type	Value
1 online_backup	boolean	false
2 only_data_backup	boolean	false

Да

Отмена

Рис. 9. Настройки ресурса FreeIPA.

Установка значения `true` для настройки `online_backup` добавляет в команду параметр `--online`, который позволяет выполнить резервное копирование в режиме онлайн, без остановки служб FreeIPA.

Установка значения `true` для настройки `only_data_backup` добавляет в команду параметр `--data`, который позволяет выполнить резервное копирование только данных FreeIPA.

Включение настройки `online_backup` автоматически подразумевает использование параметра `only_data_backup`, и при срабатывании правила будет произведено резервное копирование только данных в режиме онлайн.

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

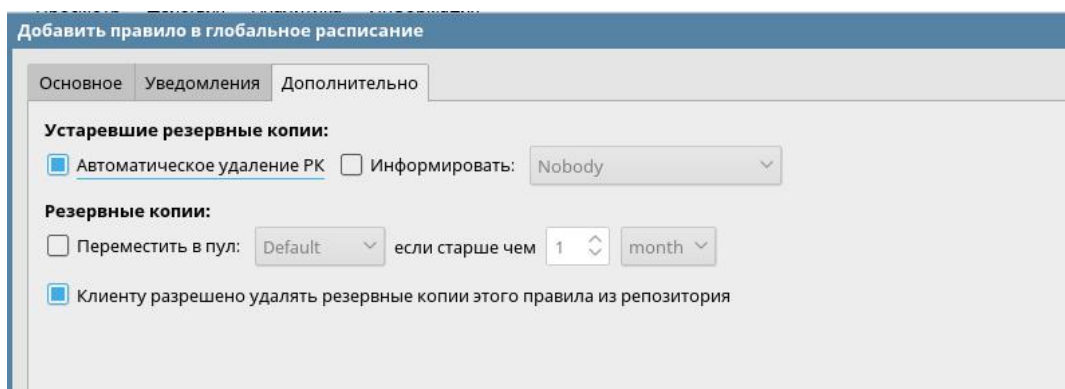


Рис. 10. Дополнительные параметры правила резервного копирования.

Вновь созданное правило будет иметь статус `wait`. Это означает, что оно не будет порождать задач на выполнение резервного копирования, пока администратор RuBackup не запустит его (тогда его статус сменится на `run`). При необходимости, администратор может приостановить работу правила или немедленно запустить его (т.е. инициировать немедленное создание задачи при статусе правила `wait`).

Правила глобального расписания имеют срок жизни, определяемый при создании, а также предоставляют следующие возможности:

- Выполнить скрипт на клиенте перед началом резервного копирования.
- Выполнить скрипт на клиенте после успешного окончания резервного копирования.
- Выполнить скрипт на клиенте после неудачного завершения резервного копирования
- Выполнить защитное преобразование резервной копии на клиенте.
- Выполнить сжатие резервной копии на клиенте или на сервере после передачи ему резервной копии.

- Периодически выполнять проверку целостности резервной копии.
- Хранить резервные копии определённый срок, по окончании которого удалять их из хранилища резервных копий и из записей репозитория, либо уведомлять клиента об окончании срока хранения.
- Через определённый срок после создания резервной копии автоматически переместить её в другой пул хранения резервных копий, например, на картридж ленточной библиотеки.
- Уведомлять пользователей системы резервного копирования о результатах выполнения тех или иных операций, связанных с правилом глобального расписания.
- Установить дополнительные параметры правила резервного копирования (настройки `only_data_backup` и `online_backup` для ресурса FreeIPA).

При создании задачи RuBackup она появляется в главной очереди задач. Отслеживать выполнение правил может как администратор (при помощи RBM или утилит командной строки), так и клиент (при помощи RBC или утилиты командной строки `rb_tasks`).

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

Правила глобального расписания RuBackup

Для выполнения резервного копирования ресурсов FreeIPA необходимо при помощи Менеджера Администратора RuBackup (RBM) создать в глобальном расписании правило для ресурса FreeIPA. При создании правила глобального расписания администратор RuBackup будет видеть список всех ресурсов FreeIPA на клиенте и сможет выбрать необходимый (для этого на клиенте должен работать клиентский фоновый процесс).

При создании правила резервного копирования можно определить следующие параметры:

- Тип резервного копирования (full).
- Разрешённый максимальный объём для всех резервных копий правила.
- Необходимость защитного преобразования резервной заданным алгоритмом. Защитное преобразование выполняется на стороне клиента.
- Шаблон времени и даты создания задачи резервного копирования.
- Включение 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 с истёкшим сроком хранения.
- 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 выполнение процедуры резервного копирования.
 - Выполнение процедуры резервного копирования с ошибками.
 - Проверка резервной копии.
 - Окончание периода действия создаваемого правила.
 - Окончание выделенного объёма для хранения резервных копий.
 - Окончание срока хранения резервной копии.
- Дополнительные настройки правила для выполнения резервного копирования ресурсов FreeIPA.

Менеджер Клиента RuBackup (RBC)

Принцип взаимодействия Менеджера Клиента RuBackup (RBC) с системой резервного копирования состоит в том, что клиент может сформировать ту или иную задачу (желаемое действие) и отправить её серверу резервного копирования RuBackup. Взаимодействие клиента с сервером резервного копирования производится через клиента RuBackup (фоновый процесс). RBC отправляет команду клиенту RuBackup, который отправляет её серверу. Если действие допустимо, сервер RuBackup отдаст команду клиенту RuBackup и, при необходимости, перенаправит её медиа серверу RuBackup для дальнейшей обработки. Это означает, что, как правило, RBC не ожидает завершения того или иного действия, но ожидает ответа от клиента RuBackup о том, что задание принято. Это позволяет инициировать параллельные запросы процесса клиента RuBackup к серверу, но требует от клиента самостоятельно контролировать отсутствие «встречных» операций», при которых происходит восстановление данных, и в этот же момент эти же данные требуются для создания новой резервной копии. После того, как клиент отдал какую-либо команду при помощи RBC, он может просто закрыть приложение, все действия будут выполнены системой резервного копирования (тем не менее, стоит дождаться сообщения о том, что задание принято к исполнению, и проконтролировать это на вкладке «Задачи»).

Графический интерфейс RBC поддерживает русский и английский языки.

Для запуска RBC следует выполнить команду:

```
# ssh -X user@freeipa_host  
# /opt/rubackup/bin/rbc&
```

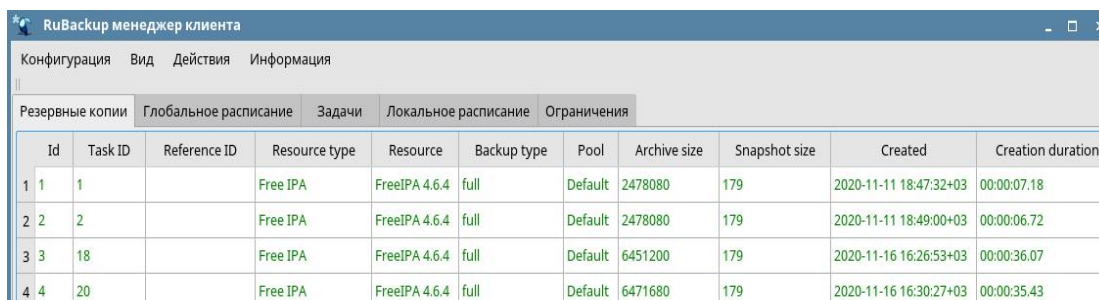
Пользователь, запускающий RBC, должен входить в группу rubackup.

При первом запуске RBC необходимо задать пароль, при помощи которого впоследствии можно будет запросить восстановление резервной копии. Без ввода пароля получить резервную копию для клиента из хранилища невозможно. Хеш пароля восстановления хранится в базе данных сервера RuBackup. При необходимости клиент может изменить пароль при помощи RBC (меню «Конфигурация» > «Изменить пароль»).

Главная страница RBC содержит вкладки, которые позволяют управлять резервными копиями и расписанием резервного копирования, а также просматривать текущие задачи клиента, локальное расписание и ограничения.

Вкладка «Резервные копии»

Вкладка «Резервные копии» содержит таблицу с информацией обо всех резервных копиях клиента, которые хранятся в репозитории RuBackup. Инкрементальные резервные копии ссылаются на полные резервные копии или предыдущие инкрементальные. При необходимости восстановить данные можно одной командой инициировать восстановление всей цепочки резервных копий.



RuBackup менеджер клиента											
Конфигурация Вид Действия Информация											
Резервные копии Глобальное расписание Задачи Локальное расписание Ограничения											
	Id	Task ID	Reference ID	Resource type	Resource	Backup type	Pool	Archive size	Snapshot size	Created	Creation duration
1	1	1		Free IPA	FreeIPA 4.6.4	full	Default	2478080	179	2020-11-11 18:47:32+03	00:00:07.18
2	2	2		Free IPA	FreeIPA 4.6.4	full	Default	2478080	179	2020-11-11 18:49:00+03	00:00:06.72
3	3	18		Free IPA	FreeIPA 4.6.4	full	Default	6451200	179	2020-11-16 16:26:53+03	00:00:36.07
4	4	20		Free IPA	FreeIPA 4.6.4	full	Default	6471680	179	2020-11-16 16:30:27+03	00:00:35.43

Рис. 11. Вкладка Резервные копии.

На этой вкладке клиенту доступны следующие действия:

- Удалить выбранную резервную копию. Это действие возможно в том случае, если в правиле глобального расписания есть соответствующее разрешение. При удалении резервной копии потребуются вести пароль клиента.
- Восстановить цепочку резервных копий. Это действие запускает процесс восстановления цепочки резервных копий на системе клиента. RBC не ожидает окончания восстановления всех резервных копий. Клиент должен проконтролировать на вкладке «Задачи» успешное завершение созданных задач на восстановление данных (статус задач Done). Для успешного выполнения этого действия требуется наличие достаточного свободного места в каталоге, предназначенном для создания и временного хранения резервных копий (см. параметр `use-local-backup-directory`).
- Проверить резервную копию. Это действие инициирует создание задачи проверки резервной копии. Если резервная копия была подписана цифровой подписью, то будут 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.

Вкладка «Глобальное расписание»

Вкладка «Глобальное расписание» содержит таблицу с информацией обо всех правилах глобального расписания RuBackup для этого клиента.

Конфигурация Вид Действия Информация												
Резервные копии		Глобальное расписание			Задачи		Локальное расписание		Ограничения			
Id	Rule name	Storage capacity, GB	Min	Hour	Day of month	Month	Day of week	Validity start period	Validity end period	Resource type	Resource	
1	41	1st	10	*	*	*	*	2019-11-05 15:23:00+03	2020-11-05 15:23:00+03	File system	/home/andr	
2	42	2nd	10	*	*	*	*	2019-11-09 19:57:00+03	2020-11-09 19:57:00+03	File system	/home/andr	
3	43	diff	10	0	0	1	January	Monday	2019-11-12 15:29:00+03	2020-11-12 15:29:00+03	File system	/home/andr

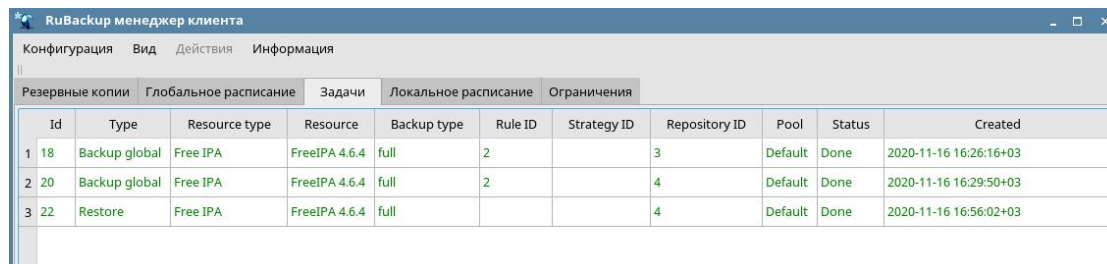
Рис. 12. Вкладка Глобальное расписание.

На этой вкладке клиенту доступны следующие действия:

- Запросить новое правило. Это действие вызывает диалог подготовки нового правила в глобальном расписании RuBackup для клиента. Запрос на добавление правила требует одобрения администратора RuBackup, одобрение может быть сделано в RBM.
- Запросить удаление правила из глобального расписания. Это действие формирует запрос к администратору RuBackup об удалении выбранного клиентом правила из глобального расписания RuBackup. Запрос на удаление правила требует одобрения администратора RuBackup, одобрение может быть сделано в RBM.

Вкладка «Задачи»

Вкладка «Задачи» содержит таблицу с информацией обо всех задачах в главной очереди заданий RuBackup для этого клиента.



RuBackup менеджер клиента										
Конфигурация Вид Действия Информация										
Резервные копии		Глобальное расписание			Задачи		Локальное расписание		Ограничения	
Id	Type	Resource type	Resource	Backup type	Rule ID	Strategy ID	Repository ID	Pool	Status	Created
1	18	Backup global	Free IPA	FreeIPA 4.6.4	full	2	3	Default	Done	2020-11-16 16:26:16+03
2	20	Backup global	Free IPA	FreeIPA 4.6.4	full	2	4	Default	Done	2020-11-16 16:29:50+03
3	22	Restore	Free IPA	FreeIPA 4.6.4	full		4	Default	Done	2020-11-16 16:56:02+03

Рис. 13. Вкладка Задачи.

В зависимости от настроек сервера RuBackup выполненные задачи и задачи, завершившиеся неудачно, через какое-то время могут быть автоматически удалены из главной очереди задач. Информация о выполнении задач фиксируется в специальном журнале задач сервера RuBackup. При

необходимости статус любой задачи, даже удалённой из очереди, можно уточнить у администратора RuBackup. Также информация о выполнении задач клиента заносится в локальный файл журнала на хосте клиента. В RBC можно открыть окно отслеживания журнального файла (меню «Информация» > «Журнальный файл»).

Вкладка «Локальное расписание»

На вкладке «Локальное расписание» можно определить правила, задаваемые клиентом для каких-либо локальных ресурсов. Для работы локального расписания эта возможность должна быть включена для клиента администратором RuBackup.

Вкладка «Ограничения»

На вкладке «Ограничения» можно определить локальные ресурсы, резервное копирование которых нежелательно. Для работы локальных ограничений эта возможность должна быть включена для клиента администратором RuBackup.

Утилиты командной строки клиента RuBackup

Для управления RuBackup со стороны клиента, помимо RBC, можно использовать утилиты командной строки.

Пользователь, запускающий утилиты командной строки, должен входить в группу rubebackup.

rb_archives

Эта утилита предназначена для просмотра списка резервных копий клиента в системе резервного копирования, создания срочных резервных копий, их удаления, проверки и восстановления. Ниже представлен пример.

rb_archives

Id	Ref ID	Resource	Resource type	Backup type	Created	Crypto	Signed	Status
1		FreeIPA 4.6.4	Free IPA	full	2020-11-30 12:02:00	threefish	True	Trusted
2		FreeIPA 4.6.4	Free IPA	full	2020-12-01 15:02:08	threefish	True	Trusted
3		FreeIPA 4.6.4	Free IPA	full	2020-12-02 10:00:11	threefish	True	Trusted
4		FreeIPA 4.6.4	Free IPA	full	2020-12-02 11:02:14	threefish	True	Trusted

rb_schedule

Эта утилита предназначена для просмотра имеющихся правил клиента в глобальном расписании резервного копирования. Ниже представлен пример.

#rb_schedule

Id	Name	Resource type	Resource	Backup type	Status
1	Astra freeipa	Free IPA	FreeIPA 4.6.4	full	wait

rb_tasks

Эта утилита предназначена для просмотра задач клиента, которые присутствуют в главной очереди задач системы резервного копирования. Ниже представлен пример выполнения команды.

#rb_tasks

Id	Task type	Resource	Backup type	Status	Created
1	Backup global	FreeIPA 4.6.4	full	Done	2020-12-02 12:01:16+03
2	Backup global	FreeIPA 4.6.4	full	Done	2020-12-02 13:01:53+03
3	Backup global	FreeIPA 4.6.4	full	Done	2020-12-02 14:05:26+03
4	Restore	FreeIPA 4.6.4	full	Error	2020-12-02 15:06:45+03

Ознакомиться с функциями утилит командной строки можно при помощи команды `man` или в руководстве «Утилиты командной строки RuBackup».