

Резервное копирование и восстановление данных в Proxmox VE

 selectel.ru/blog/backups-proxmox-ve

15 марта 2018 г.

Трактат о сущности механизма бэкапов в Proxmox VE



Николай Рубанов Старший технический писатель

15 марта 2018

В статье «Магия виртуализации: вводный курс в Proxmox VE» мы успешно установили на сервер гипервизор, подключили к нему хранилище, позаботились об элементарной безопасности и даже создали первую виртуальную машину. Теперь разберем как реализовать самые базовые задачи, которые приходится выполнять, чтобы всегда иметь возможность восстановить работу сервисов в случае сбоя. Штатные инструменты Proxmox позволяют не только [...]



В статье «Магия виртуализации: вводный курс в Proxmox VE» мы успешно установили на сервер гипервизор, подключили к нему хранилище, позаботились об элементарной безопасности и даже создали первую виртуальную машину. Теперь разберем как реализовать самые базовые задачи, которые приходится выполнять, чтобы всегда иметь возможность восстановить работу сервисов в случае сбоя.

Штатные инструменты Proxmox позволяют не только выполнять резервное копирование данных, но и создавать наборы предварительно настроенных образов операционных систем для быстрого развертывания. Это не только помогает при необходимости создать новый сервер для любого сервиса за несколько секунд, но также и уменьшает время простоя до минимального.

Рассказывать о необходимости создания бэкапов мы не будем, поскольку это очевидно и уже давно является аксиомой. Остановимся на некоторых неочевидных вещах и особенностях.

Сначала рассмотрим каким образом сохраняются данные при процедуре резервного копирования.

Алгоритмы резервного копирования

Начнем с того, что Proxmox имеет неплохой штатный инструментарий для создания резервных копий виртуальных машин. Он позволяет легко сохранить все данные виртуальной машины и поддерживает два механизма сжатия, а также три метода создания этих копий.

Разберем вначале механизмы сжатия:

1. **Сжатие LZO**. Алгоритм сжатия данных без потерь, придуманный еще в середине 90-х годов. Код был написан Маркусом Оберхеймером (реализуется в Proxmox утилитой lzor). Основной особенностью этого алгоритма является очень скоростная распаковка. Следовательно, любая резервная копия, созданная с помощью этого алгоритма, может при необходимости быть развернута за минимальное время.

2. **Сжатие GZIP**. При использовании этого алгоритма резервная копия будет «на лету» сжиматься утилитой GNU Zip, использующей мощный алгоритм Deflate, созданный Филом Кацем. Основной упор делается на максимальное сжатие данных, что позволяет сократить место на диске, занимаемое резервными копиями. Главным отличием от LZO является то, что процедуры компрессии/декомпрессии занимают достаточно большое количество времени.

Режимы архивирования

Proxmox предлагает на выбор системному администратору три метода резервного копирования. С помощью них можно решить требуемую задачу, определив приоритет между необходимостью простоя и надежностью сделанной резервной копии:

1. **Режим Snapshot (Снимок)**. Этот режим можно еще назвать как Live backup, поскольку для его использования не требуется останавливать работу виртуальной машины. Использование этого механизма не прерывает работу VM, но имеет два очень серьезных недостатка — могут возникать проблемы из-за блокировок файлов операционной системой и самая низкая скорость создания. Резервные копии, созданные этим методом, надо всегда проверять в тестовой среде. В противном случае есть риск, что при необходимости экстренного восстановления, они могут дать сбой.

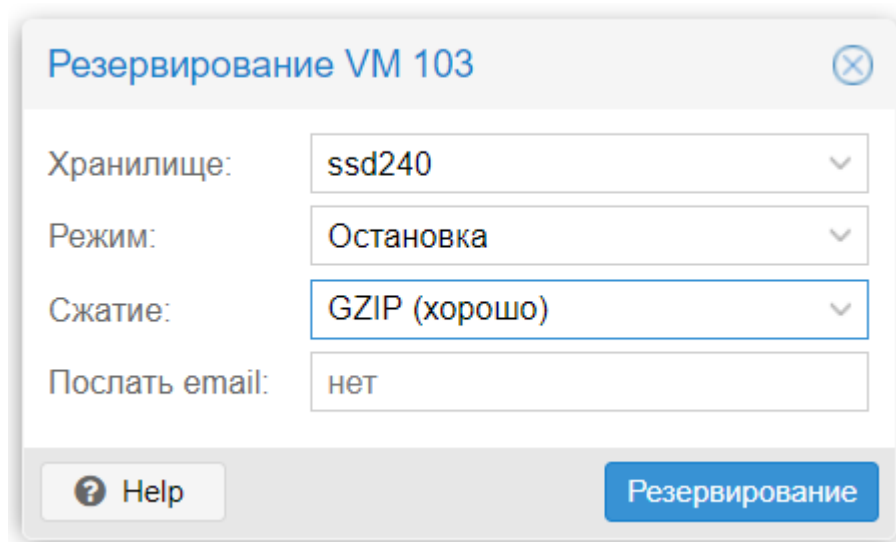
2. **Режим Suspend (Приостановка)**. Виртуальная машина временно «замораживает» свое состояние, до окончания процесса резервного копирования. Содержимое оперативной памяти не стирается, что позволяет продолжить работу ровно с той точки, на которой работа была приостановлена. Разумеется, это вызывает простой сервера на время копирования информации, зато нет необходимости выключения/включения виртуальной машины, что достаточно критично для некоторых сервисов. Особенно, если запуск части сервисов не является автоматическим. Тем не менее такие резервные копии также следует разворачивать в тестовой среде для проверки.

3. **Режим Stop (Остановка)**. Самый надежный способ резервного копирования, но требующий полного выключения виртуальной машины. Отправляется команда на штатное выключение, после остановки выполняется резервное копирование и затем отдается команда на включение виртуальной машины. Количество ошибок при таком подходе минимально и чаще всего сводится к нулю. Резервные копии, созданные таким способом, практически всегда разворачиваются корректно.

Выполнение процедуры резервирования

Для создания резервной копии:

1. Переходим на нужную виртуальную машину.
2. Выбираем пункт **Резервирование**.
3. Нажимаем кнопку **Резервировать сейчас**. Откроется окно, в котором можно будет выбрать параметры будущей резервной копии.

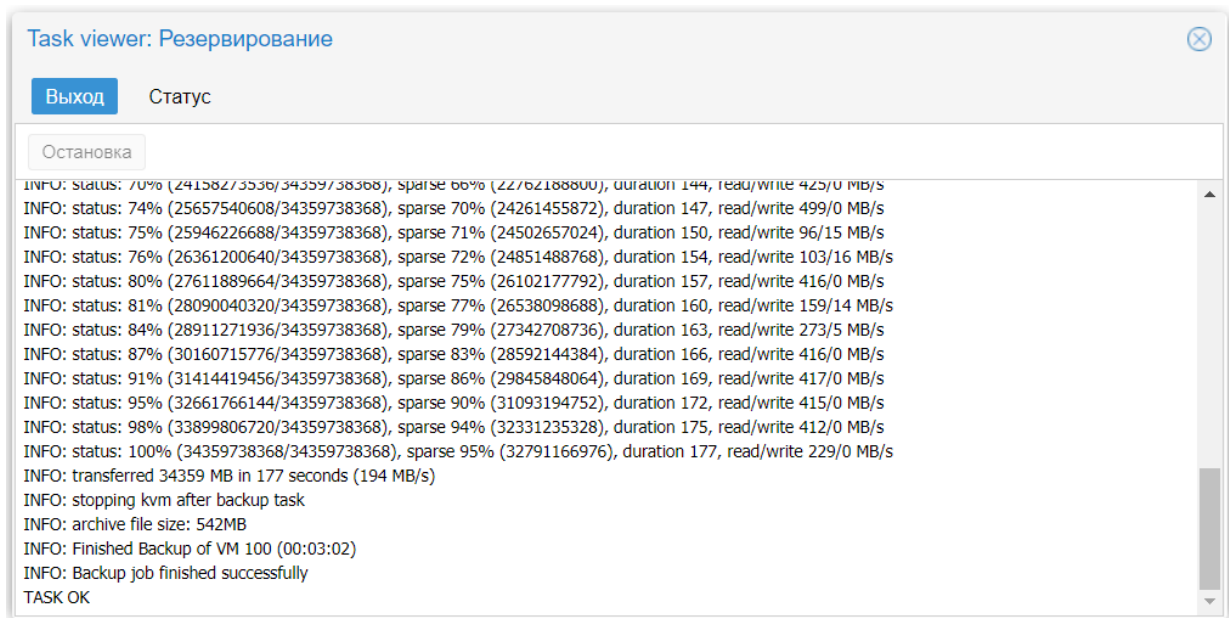


Резервирование VM 103

Хранилище:	ssd240
Режим:	Остановка
Сжатие:	GZIP (хорошо)
Послать email:	нет

? Help Резервирование

4. В качестве хранилища указываем то, которое мы подключаем в предыдущей части.
5. После выбора параметров нажимаем кнопку **Резервирование** и ждем, пока резервная копия будет создана. Об этом будет говорить надпись **TASK OK**.



Теперь созданные архивы с резервными копиями виртуальных машин станут доступны для скачивания с сервера. Самым простым и банальным способом копирования является SFTP. Для этого воспользуйтесь популярным кроссплатформенным FTP-клиентом FileZilla, который умеет работать по SFTP-протоколу.

1. В поле **Хост** вводим IP-адрес нашего сервера виртуализации, в поле **Имя пользователя** вводим root, в поле **Пароль** — тот, который был выбран при установке, а в поле **Порт** указываем «22» (либо любой другой порт, который был задан для SSH-подключений).
2. Нажимаем кнопку **Быстрое соединение** и, если все данные были введены правильно, то в активной панели Вы увидите все файлы, расположенные на сервере.
3. Переходим в директорию **/mnt/storage**. Все создаваемые резервные копии будут лежать в поддиректории **«dump»**. Они будут иметь вид:
 - **vzdump-qemu-номер_машины-дата-время.vma.gz** в случае выбора метода сжатия GZIP;
 - **vzdump-qemu-номер_машины-дата-время.vma.lzo** для использования метода LZO.

Резервные копии рекомендуется сразу скачивать с сервера и сохранять в надежном месте, например, в нашем облачном хранилище. Если распаковать файл с разрешением **vma**, одноименной утилитой, идущей в комплекте с Proxmox, то внутри будут файлы с расширениями **raw**, **conf** и **fw**. В этих файлах содержится следующее:

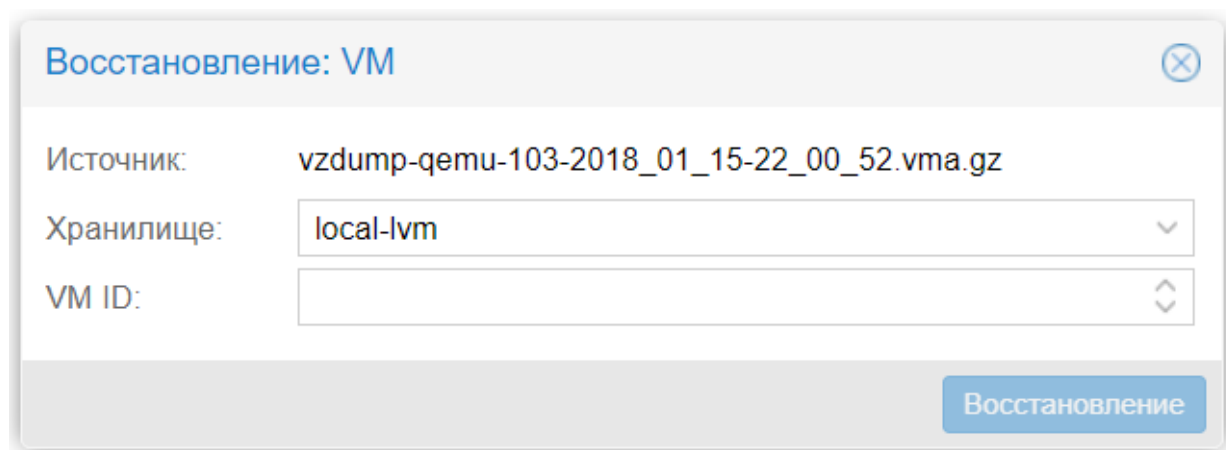
- **raw** — образ диска;
- **conf** — конфигурация VM;

- **fw** — настройки файервола.

Восстановление из резервной копии

Рассмотрим ситуацию, когда виртуальную машину случайно удалили и требуется ее экстренное восстановление из резервной копии:

1. Открываем хранилище, на котором лежит резервная копия.
2. Переходим на вкладку **Содержимое**.
3. Выбираем нужную копию и нажимаем кнопку **Восстановление**.



Восстановление: VM

Источник: vzdump-qemu-103-2018_01_15-22_00_52.vma.gz

Хранилище: local-lvm

VM ID:

Восстановление

4. Указываем целевое хранилище и ID, который будет присвоен машине, после завершения процесса.
5. Нажимаем кнопку **Восстановление**.

Как только восстановление завершится, VM появится в списке доступных.

Клонирование виртуальной машины

Для примера, предположим, что в компании требуется внести изменения в какой-либо критичный сервис. Такое изменение реализуется через внесение множества правок в конфигурационные файлы. Результат при этом непредсказуем и любая ошибка способна вызвать сбой сервиса. Чтобы подобный эксперимент не затронул работающий сервер, рекомендуется выполнить клонирование виртуальной машины.

Механизм клонирования создаст точную копию виртуального сервера, с которой допустимо проводить любые изменения, при этом не затрагивая работу основного сервиса. Затем, если изменения будут успешно применены, новая VM запускается в работу, а старая выключается. В этом процессе есть особенность, о которой всегда следует помнить. На клонированной машине IP-адрес будет точно таким же, как и у исходной VM, то есть при ее запуске возникнет конфликт адресов.

Расскажем, как избежать такой ситуации. Непосредственно перед выполнением клонирования, следует внести изменения в конфигурацию сети. Для этого необходимо временно изменить IP-адрес, но не перезапускать сетевой сервис.

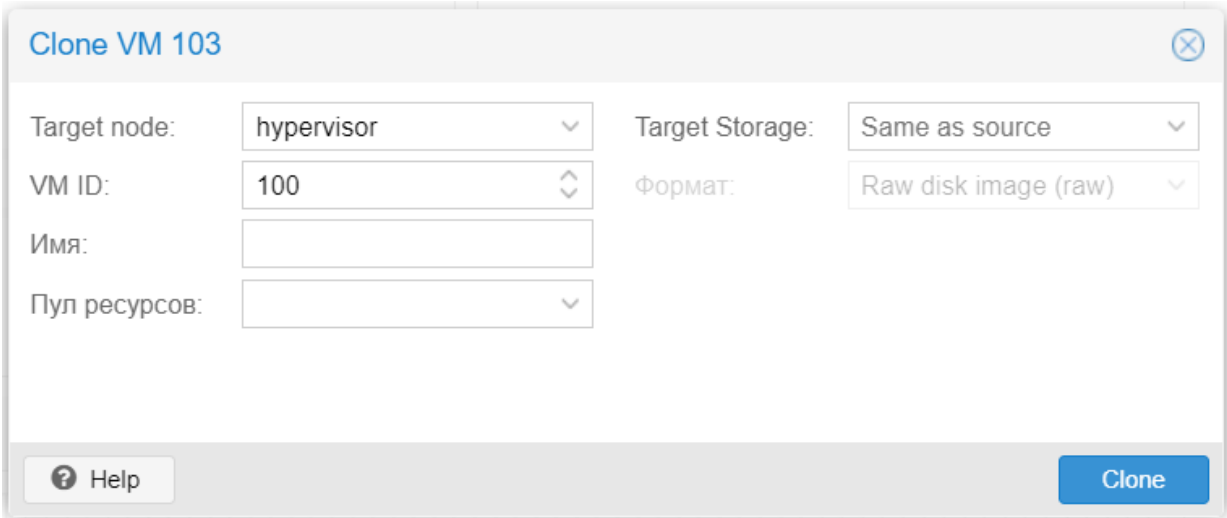
После выполнения клонирования на основной машине следует вернуть настройки обратно, а на клонированной машине задать любой другой IP-адрес. Тем самым мы получим две копии одного и того же сервера на разных адресах. Это позволит быстро ввести новый сервис в работу.

Если этим сервисом является веб-сервер, то достаточно только изменить А-запись у Вашего DNS-провайдера, после чего запросы клиентов по этому доменному имени будут направляться уже на адрес клонированной виртуальной машины.

Кстати, Selectel предоставляет всем своим клиентам услугу размещения любого количества доменов на NS-серверах бесплатно. Управление записями осуществляется как с помощью нашей панели управления, так и с помощью специального API. Подробнее об этом читайте [в нашей базе знаний](#).

Клонирование VM в Proxmox является очень простой задачей. Для ее выполнения необходимо выполнить следующие действия:

1. Перейти на нужную нам машину.
2. Выбрать из меню **More** пункт **Clone**.
3. В открывшемся окне заполнить параметр **Имя**.



4. Выполнить клонирование нажатием кнопки **Clone**.

Этот инструмент позволяет сделать копию виртуальной машины не только на локальном сервере. Если несколько серверов виртуализации объединить в кластер, то с помощью этого инструмента можно сразу переместить созданную копию на нужный физический сервер. Полезной функцией является выбор дискового хранилища (параметр **Target Storage**), что очень удобно при перемещении виртуальной машины с одного физического носителя на другой.

Форматы виртуальных накопителей

Расскажем подробнее об используемых в Proxmox форматах накопителей:

1. **RAW**. Самый понятный и простой формат. Это файл с данными жесткого диска «байт в байт» без сжатия или оптимизации. Это очень удобный формат, поскольку его легко смонтировать стандартной командой `mount` в любой linux-системе. Более того это самый быстрый «тип» накопителя, так как гипервизору не нужно его никак обрабатывать.

Серьезным недостатком этого формата является то, что сколько Вы выделили места для виртуальной машины, ровно столько места на жестком диске и будет занимать файл в формате RAW (вне зависимости от реально занятого места внутри виртуальной машины).

2. **QEMU image format (qcow2)**. Пожалуй, самый универсальный формат для выполнения любых задач. Его преимущество в том, что файл с данными будет содержать только реально занятое место внутри виртуальной машины. Например, если было выделено 40 Гб места, а реально было занято только 2 Гб, то все остальное место будет доступно для других VM. Это очень актуально в условиях экономии дискового пространства.

Небольшим минусом работы с этим форматом является следующее: чтобы примонтировать такой образ в любой другой системе, потребуется вначале загрузить особый драйвер nbd, а также использовать утилиту **qemu-nbd**, которая позволит операционной системе обращаться к файлу как к обычному блочному устройству. После этого образ станет доступен для монтирования, разбиения на разделы, осуществления проверки файловой системы и прочих операций.

Следует помнить, что все операции ввода-вывода при использовании этого формата программно обрабатываются, что влечет за собой замедление при активной работе с дисковой подсистемой. Если стоит задача развернуть на сервере базу данных, то лучше выбрать формат RAW.

3. **VMware image format (vmdk)**. Этот формат является «родным» для гипервизора VMware vSphere и был включен в Proxmox для совместимости. Он позволяет выполнить миграцию виртуальной машины VMware в инфраструктуру Proxmox.

Использование vmdk на постоянной основе не рекомендуется, данный формат самый медленный в Proxmox, поэтому он годится лишь для выполнения миграции, не более. Вероятно в обозримом будущем этот недостаток будет устранен.

Работа с образами дисков

В комплекте с Proxmox есть очень удобная утилита, под названием **qemu-img**. Одной из ее функций является конвертирование образов виртуальных дисков. Чтобы воспользоваться им, достаточно открыть консоль гипервизора и выполнить команду в формате:

```
qemu-img convert -f vmdk test.vmdk -o qcow2 test.qcow2
```

В приведенном примере, vmdk-образ виртуального накопителя VMware под названием **test** будет преобразован в формат **qcow2**. Это очень полезная команда, когда требуется исправить ошибку при изначальном выборе формата.

Благодаря этой же команде можно принудительно создать нужный образ, используя аргумент **create**:

```
qemu-img create -f raw test.raw 40G
```

Такая команда создаст образ **test** в формате RAW, размером 40 Гб. Теперь он годится для подключения к любой из виртуальных машин.

Изменение размера виртуального диска

И в заключение покажем как увеличить размер образа диска, если по каким-то причинам места на нем перестало хватать. Для этого воспользуемся аргументом **resize**:

```
qemu-img resize -f raw test.raw 80G
```

Теперь наш образ стал размером 80 Гб. Посмотреть подробную информацию об образе можно с помощью аргумента **info**:

```
qemu-img info test.raw
```

Не стоит забывать, что само расширение образа не увеличит размер раздела автоматически — просто добавит доступное свободное пространство. Для увеличения раздела воспользуйтесь командой:

```
resize2fs /dev/sda1
```

где **/dev/sda1** — нужный раздел.

Автоматизация создания резервных копий

Использование ручного способа создания резервных копий — задача весьма трудоемкая и занимает много времени. Поэтому Proxmox VE содержит в себе средство для автоматического резервного копирования по расписанию.

Рассмотрим, как это сделать:

1. Используя веб-интерфейс гипервизора, открываем пункт **Датацентр**.
2. Выбираем пункт **Резервирование**.
3. Нажимаем кнопку **Добавить**.
4. Задаем параметры для планировщика.

Создать: Задания резервирования

Узел:

hypervisor

Хранилище:

ssd240

День недели:

Суббота, Понедельник

Время запуска:

04:00

Выбор режима:

Включая выбранные V

Послать email:

notification@yourcompany.c

Email notification:

Always

Сжатие:

GZIP (хорошо)

Режим:

Остановка

Включить: ☒

<input checked="" type="checkbox"/>	ID ↑	Узел	Статус	Имя	Тип
<input checked="" type="checkbox"/>	103	hypervisor	запущено	VasilisaDB	qemu

Help

Создать

5. Отмечаем галочкой пункт **Включить**.

6. Сохраняем изменения, используя кнопку **Создать**.

Теперь планировщик будет автоматически запускать программу резервного копирования в точно указанное время, исходя из заданного расписания.

Заключение

Нами были рассмотрены штатные способы резервного копирования и восстановления виртуальных машин. Их использование позволяет без особых проблем сохранять все данные и экстренно восстановить их в случае нештатной ситуации.

Конечно, это не единственный возможный способ сохранения важных данных. Существует множество инструментов, например, Duplicity, с помощью которых можно создавать полные и инкрементные копии содержимого виртуальных серверов на базе Linux.

При выполнении процедур резервного копирования всегда следует учитывать, что они активно нагружают дисковую подсистему. В связи с этим выполнять эти процедуры рекомендуется в моменты минимальной нагрузки, чтобы избежать задержек при выполнении операций ввода-вывода внутри машин. Следить за статусом задержек дисковых операций можно непосредственно из веб-интерфейса гипервизора (параметр **IO delay**).

Если у Вас возникли вопросы, то мы будем рады ответить на них в комментариях.