

Установка и настройка Proxmox Backup Server

 interface31.ru/tech_it/2022/01/ustanovka-i-nastroyka-proxmox-backup-server.html

Записки IT специалиста

Технический блог специалистов ООО "Интерфейс"

- [Главная](#)
- Установка и настройка Proxmox Backup Server

Виртуализация плотно вошла в нашу жизнь, предоставляя широкие возможности даже небольшим организациям, вместе с тем появляются и новые сложности, одна из них - эффективное резервное копирование виртуальной инфраструктуры. А так как количество копируемых данных только растет также остро встает вопрос эффективного использования пространства хранения и нагрузки на каналы связи. Многие из этих вопросов позволяет решить новый продукт от компании Proxmox - Backup Server, который прекрасно дополняет собственные решения по виртуализации.



Почему именно Backup Server, что такого, чего нет в существующих решениях предоставляет данная разработка? Proxmox Virtual Environment имеет собственные средства резервного копирования, построенные на базе **vzdump**. Они просты и надежны, но все их достоинства на этом заканчиваются. По сути, штатные средства умеют только создавать дампы в выбранное хранилище, в том числе и сетевое, но остальное - это уже отдельная забота системного администратора. Если нод или кластеров несколько, то каждый из них имеет собственные настройки резервного копирования, собственные хранилища и т.д. и т.п. Нет никакой общей точки управления бекапами.

Proxmox Backup Server такую общую точку предоставляет, теперь вы можете видеть все свои резервные копии в одном месте и централизованно управлять ими. Но централизация - важное, но не единственное преимущество нового продукта. Так **vzdump** не умеет создавать инкрементные копии, каждый раз создавая полный образ виртуальной машины или контейнера. Даже если у вас достаточно места на устройствах хранения, то все равно остается вопрос нагрузки на каналы связи, особенно если резервные копии нужно делать в рабочее время или технологическое окно невелико.

Proxmox Backup Server использует собственный формат резервных копий и полностью поддерживает инкрементное копирование, теперь по сети будут передаваться только измененные данные виртуальной машины, что позволяет не только снизить трафик, но и ускорить сам процесс копирования. Теперь копии можно делать чаще и быстрее, что только положительно скажется на надежности инфраструктуры.

Вторая существенная проблема современных информационных систем - постоянно растущий объем данных и виртуализация только подливает масла в огонь. Вместо одной системы с множеством сервисов мы получаем множество систем с индивидуальным сервисом в каждой, каждая из которых нуждается в резервном копировании и содержит пересекающиеся с другими системами данные - системные файлы и библиотеки, которые одинаковы в однотипных машинах. Решение этой проблемы придумано достаточно давно - дедупликация и Proxmox Backup Server ее поддерживает.

Только этих двух возможностей уже достаточно, чтобы задуматься о внедрении, но это далеко не всё, мы не будем пересказывать документацию полностью, но коснемся каких-то из них в данной статье, а что-то оставим за кадром, так как их рассмотрение предмет отдельного материала.

Установка Proxmox Backup Server

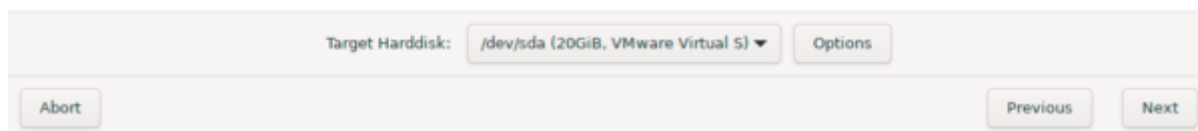
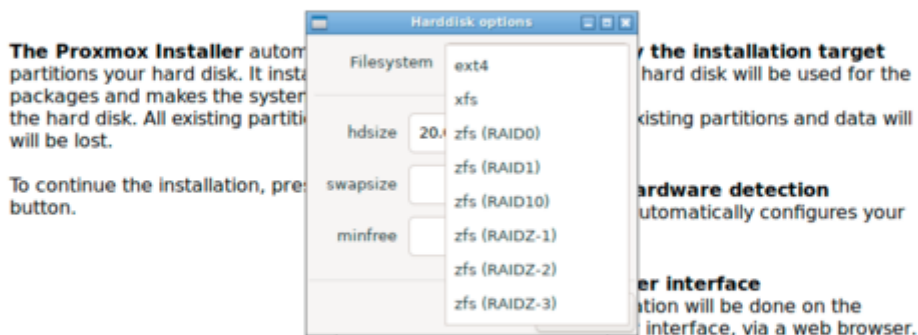
Установка Proxmox Backup Server не представляет особой сложности, продукт имеет фирменный инсталлятор, прекрасно знакомый любому, кто работал с Proxmox.



Запутаться там решительно негде, все что вам понадобится - это указать ряд параметров: имя системы, сетевые настройки, часовой пояс. Отдельное внимание следует уделить настройке дисковой подсистемы, тонких настроек инсталлятор не предоставляет, поэтому мы советуем выполнить установку в минимальной дисковой конфигурации - на одиночный диск или зеркало, а систему хранения сконфигурировать уже после установки. Поддерживаются ext4, XFS и ZFS, но мы не советуем использовать XFS без веских на то оснований, так как эта файловая система имеет ряд существенных недостатков: невозможность уменьшить размер файловой системы и трудности с восстановлением данных.



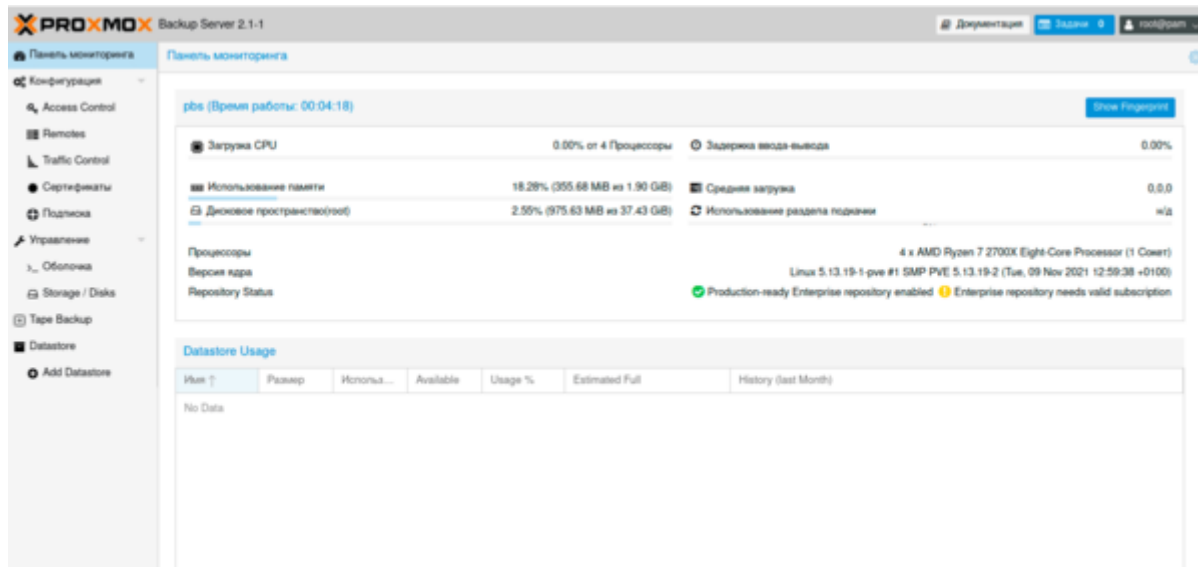
Proxmox Backup Server (PBS)



Общие рекомендации по организации системы хранения дать сложно, но чаще всего имеет смысл разделять систему, вынося ее на отдельные высокоскоростные диски (NVMe, SSD), и собственно хранилище, собранное из дисков подходящей емкости. Для системы мы предпочитаем использовать ext4, как наиболее простую и понятную файловую систему, а для хранилища ZFS.

Первоначальная настройка Proxmox Backup Server

После установки вам будет доступен веб-интерфейс сервера резервного копирования по адресу **https://<адрес_сервера>:8007**, в качестве адреса можно использовать как IP-адрес, так и FQDN имя. Обратите внимание, что в отличие от Proxmox VE, который использует порт 8006, Backup Server использует порт **8007**. Русский язык присутствует, но перевод выполнен частично. Сам интерфейс реализован в привычном ключе и не должен вызвать затруднений в работе.



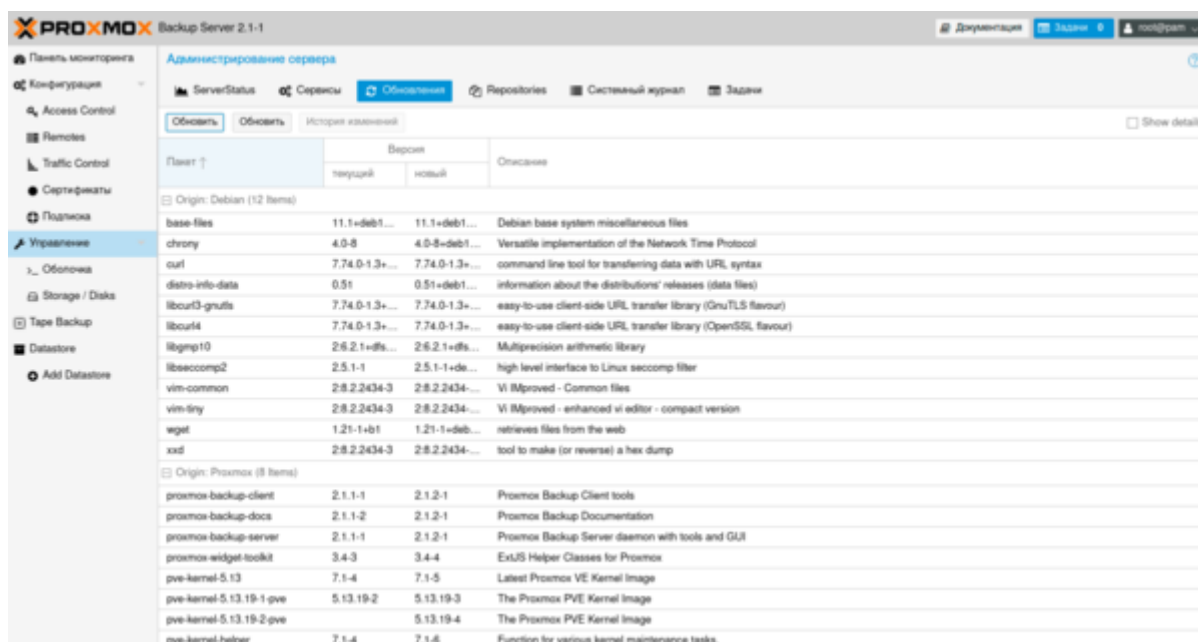
Но перед тем, как начинать настройку сервера нужно выполнить некоторые подготовительные действия, прежде всего нужно отключить коммерческий репозиторий Проксмах и подключить репозиторий без подписки. Для отключения удалим файл репозитория из источников адресов apt:

```
rm -f /etc/apt/sources.list.d/pbs-enterprise.list
```

И создадим новый файл с адресом некоммерческого репозитория:

```
echo "deb http://download.proxmox.com/debian/pbs bullseye pbs-no-subscription" > /etc/apt/sources.list.d/pbs-no-subscription.list
```

Теперь получим список пакетов и обновим систему, это можно сделать как в консоли, так и в графической оболочке. В этом случае, если вы используете русский язык, у вас будет две кнопки **Обновить**, которые выполняют различные действия: первая обновляет список пакетов (Update), вторая обновляет систему (Upgrade), эти действия нужно выполнить последовательно.

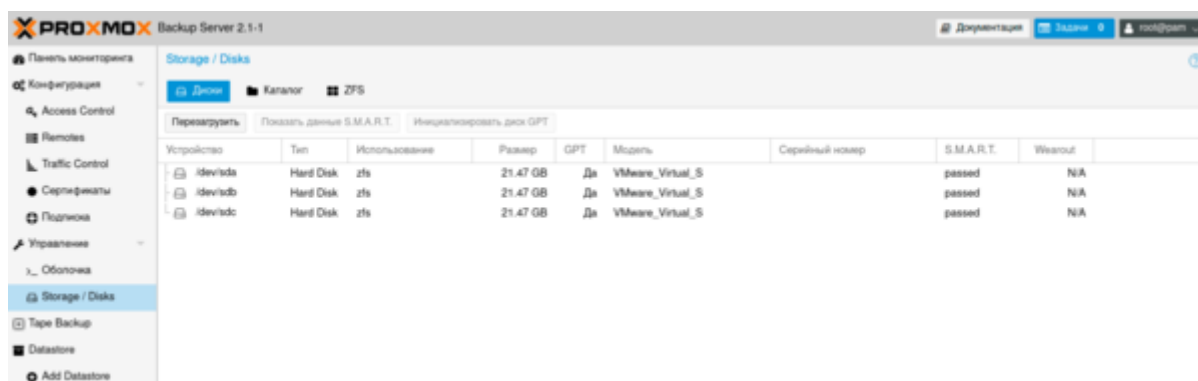


Либо откройте консоль и выполните:

```
apt update  
apt full-upgrade
```

После обновления систему следует перезагрузить.

Следующим шагом следует настроить хранилище, для этого перейдите в раздел **Administration - Storage / Disks** где будут показаны все ваши физические диски на которых вы можете создать различные конфигурации системы хранения. Раздел **Directory** предназначен для управления файловыми системами ext4 и XFS, но наиболее гибко управлять хранилищем и создавать отказоустойчивые конфигурации можно только посредством ZFS, и мы не видим причин делать иначе.



Конкретные рекомендации по организации системы хранения дать сложно, все зависит от типа, объема и количества используемых дисков, а также предполагаемой нагрузки и объема хранимых данных. Но в любом случае мы бы советовали присмотреться к **RAIDZ**, это оригинальная реализация RAID-массива от ZFS, продолжающая заложенные в RAID-5 идеи, но избавленная от многих его недостатков. В данном случае RAIDZ массивы являются наиболее оптимальными по сочетанию производительности и надежности хранения, цифра в наименовании массива показывает отказ какого количества дисков одновременно он способен выдержать. Так RAIDZ-1 допускает выход одного жесткого диска, а RAIDZ-3 - сразу трех.

Управление хранилищами данных

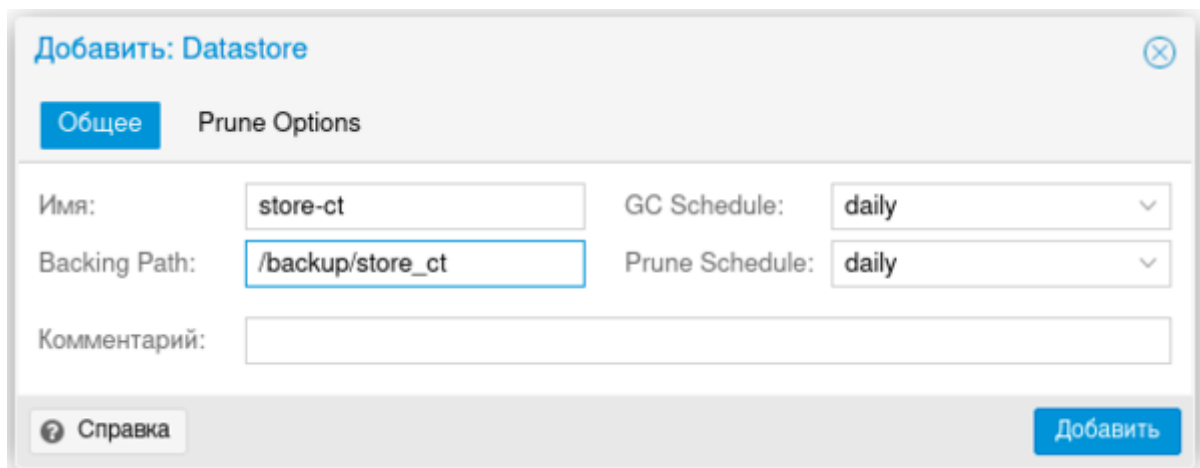
Для размещения резервных копий Proxmox Backup Server использует **хранилища данных (Datastore)** - это дополнительный уровень абстракции, представляющий собой особым образом организованную директорию в пределах существующей файловой системы. Каждое хранилище имеет собственные настройки глубины хранения, очистки, дедупликации, наборы прав доступа и т.д. Количество хранилищ не ограничено, но вы должны создать как минимум одно.

Хранилища отвечают за логическую структуру хранения данных и поэтому подходить к их организации следует ответственно. Не стоит сваливать все в одну кучу, лучше всего грамотно разделить однотипные объекты по различным

хранилищам, не забывая при этом о разграничении прав доступа, если такой вопрос актуален.

Допустим у нас есть два хранилища в каждом из которых мы храним виртуальную машину и контейнер. Будет ли работать дедупликация? Практически нет, потому что одинаковые данные расположены в различных хранилищах, а вот если мы в одном хранилище будем держать однотипные VM, а во втором - контейнеры, то сразу получим преимущества от дедупликации, плюс получим более стройную и упорядоченную логически систему хранения.

В нашем случае мы создадим два хранилища: одно для контейнеров с Linux, второе для виртуальных машин с Mikrotik CHR. Для того чтобы добавить хранилище выберем **Add Datastore** и заполним ряд необходимых полей: **Name** - имя хранилища, может быть произвольным, но желательно чтобы оно отражало содержимое хранилища, в дальнейшем имя будет использоваться как идентификатор хранилища, **Backing Path** - абсолютный путь к каталогу, в котором вы хотите создать хранилище, если путь не существует, то он будет создан. **GC Schedule** - периодичность выполнения сборки мусора, фактически выполняет задачу дедупликации, **Prune Schedule** - периодичность очистки хранилища от устаревших резервных копий.



Отдельное внимание следует уделить опциям очистки устаревших копий - **Prune Options**, их можно настроить как сразу, так и потом, либо изменить в любое удобное время. Опций немного, но необходимо четко понимать механизм их действия, чтобы избегать разных неожиданностей. Как видим нам доступны опции, в которых мы можем указать количество последних копий за различные периоды и общее их количество. Каким образом эти настройки сочетаются?

Все просто, задание очистки обрабатывает их последовательно, в порядке перечисления, уже обработанные копии из дальнейшей обработки исключаются:

- **Keep Last <N>** - Хранить последние <N> снимки резервных копий.
- **Keep Hourly <N>** - Хранить резервные копии за последние <N> часов
- **Keep Daily <N>** - Хранить резервные копии за последние <N> дней.

- **Keep Weekly <N>** - Хранить резервные копии за последние <N> недель. Недели начинаются в понедельник и заканчиваются в воскресенье.
- **Keep Monthly <N>** - Хранить резервные копии за последние <N> месяцев.
- **Keep Yearly <N>** - Хранить резервные копии за последние <N> лет.

Если за один период создается более одной резервной копии, сохраняется только последняя.

Для того, чтобы лучше понять принцип действия алгоритма рекомендуем воспользоваться Симулятором очистки, давайте зададим следующие параметры: хранить 4 последних копии, копии за последние 4 часа, последние 2 дня и последнюю неделю. Периодичность копирования - один раз в шесть часов. Теперь внимательно изучим результат:

View

Show Calendar: ☒

Show Colors: ☒

Simulated Backup Schedule

Day of week: Monday, Tuesday, Wed

Backup schedule: 0/6:00

Number of weeks: 15

[Update Schedule](#)

Prune Options

keep-last: 4

keep-hourly: 4

keep-daily: 2

keep-weekly: 1

keep-monthly:

keep-yearly:

Backups

| Backup Time ↓ | Keep (reason) |
|---------------------|-----------------------|
| 2022-01-08 18:00:07 | keep (keep-last: 1) |
| 2022-01-08 12:00:07 | keep (keep-last: 2) |
| 2022-01-08 06:00:07 | keep (keep-last: 3) |
| 2022-01-08 00:00:07 | keep (keep-last: 4) |
| 2022-01-07 18:00:07 | keep (keep-hourly: 1) |
| 2022-01-07 12:00:07 | keep (keep-hourly: 2) |
| 2022-01-07 06:00:07 | keep (keep-hourly: 3) |
| 2022-01-07 00:00:07 | keep (keep-hourly: 4) |
| 2022-01-06 18:00:07 | keep (keep-daily: 1) |
| 2022-01-06 12:00:07 | remove |
| 2022-01-06 06:00:07 | remove |
| 2022-01-06 00:00:07 | remove |

Calendar

| Sun, 09 Jan 2022 | Sat, 08 Jan 2022 | Fri, 07 Jan 2022 | Thu, 06 Jan 2022 | Wed, 05 Jan 2022 | Tue, 04 Jan 2022 | Mon, 03 Jan 2022 |
|------------------------|----------------------|------------------------|-----------------------|-----------------------|------------------|------------------|
| | 18:00 (keep-last: 1) | 18:00 (keep-hourly: 1) | 18:00 (keep-daily: 1) | 18:00 (keep-daily: 2) | 18:00 | 18:00 |
| | 12:00 (keep-last: 2) | 12:00 (keep-hourly: 2) | 12:00 | 12:00 | 12:00 | 12:00 |
| | 06:00 (keep-last: 3) | 06:00 (keep-hourly: 3) | 06:00 | 06:00 | 06:00 | 06:00 |
| | 00:00 (keep-last: 4) | 00:00 (keep-hourly: 4) | 00:00 | 00:00 | 00:00 | 00:00 |
| Sun, 02 Jan 2022 | Sat, 01 Jan 2022 | Fri, 31 Dec 2021 | Thu, 30 Dec 2021 | Wed, 29 Dec 2021 | Tue, 28 Dec 2021 | Mon, 27 Dec 2021 |
| 18:00 (keep-weekly: 1) | 18:00 | 18:00 | 18:00 | 18:00 | 18:00 | 18:00 |
| 12:00 | 12:00 | 12:00 | 12:00 | 12:00 | 12:00 | 12:00 |
| 06:00 | 06:00 | 06:00 | 06:00 | 06:00 | 06:00 | 06:00 |
| 00:00 | 00:00 | 00:00 | 00:00 | 00:00 | 00:00 | 00:00 |

С первой опцией все понятно - храним 4 последних копии, а вот с последними 4 часами есть тонкость - наши копии делаются раз в шесть часов, т.е. не попадают под условие очистки, точнее наоборот, попадают, возможно все, так как 4-х часовой интервал будет рассчитываться от последней сохраненной по предыдущему правилу копии. Но в этом случае разработчики решили расширить действие правила, и оно также захватит 4 последних копии, хотя фактически это будет 24-х часовой интервал. Далее мы видим две дневные и одну недельную копию. Все ровно так, как мы и задали: 4 - 4 - 2 - 1, т.е. в любом случае сервер будет хранить резервные копии в количестве **не менее указанного**, даже если они выходят за интервал хранения. На наш взгляд - это правильно, лучше иметь резервную копию, нежели не иметь ее.

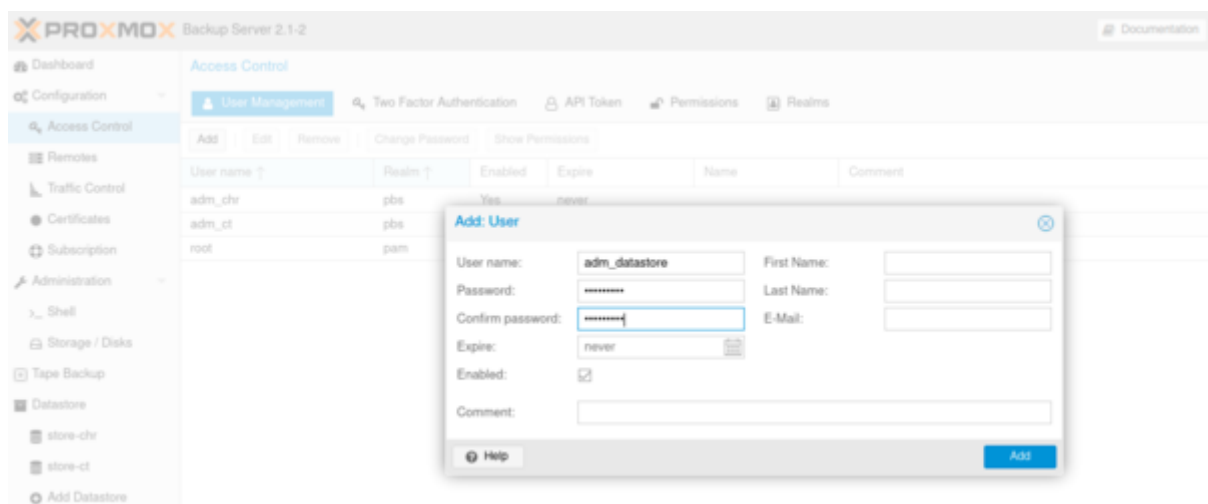
Также обратите внимание, что наличие задания очистки вовсе не обозначает его обязательного соблюдения, так как следует соизмерять заданные в нем интервалы с периодичностью выполнения задания. Скажем, если вы создаете копии каждый час, но выполняете задание только раз в сутки, то реальное количество хранимых копий будет отличаться от расчетного.

Управление пользователями

После установки в системе есть единственный пользователь - root, который также является суперпользователем системы, понятно, что работать от него нежелательно, а тем более указывать его учетные данные на сторонних узлах, которые будут подключаться к серверу резервного копирования. Также может стоять задача разделения доступа к данным, чтобы администраторы одной системы не имели доступа к копиям других систем. Все это важно, так как сервер может хранить самую разную по критичности доступа к данным информацию, а утечка резервной копии ничем не отличается от утечки данных с рабочего сервера.

Поэтому кроме разделения данных по разным хранилищам также следует настроить различные права доступа к ним. Proxmox Backup Server поддерживает две области аутентификации (Realms): стандартную **Linux PAM**, которая включает системных пользователей и **pbs** - область аутентификации Backup Server, этот тип пользователей не регистрируется в системе и не может войти в нее, а существует только в пределах сервера резервного копирования, что обеспечивает более высокую степень безопасности.

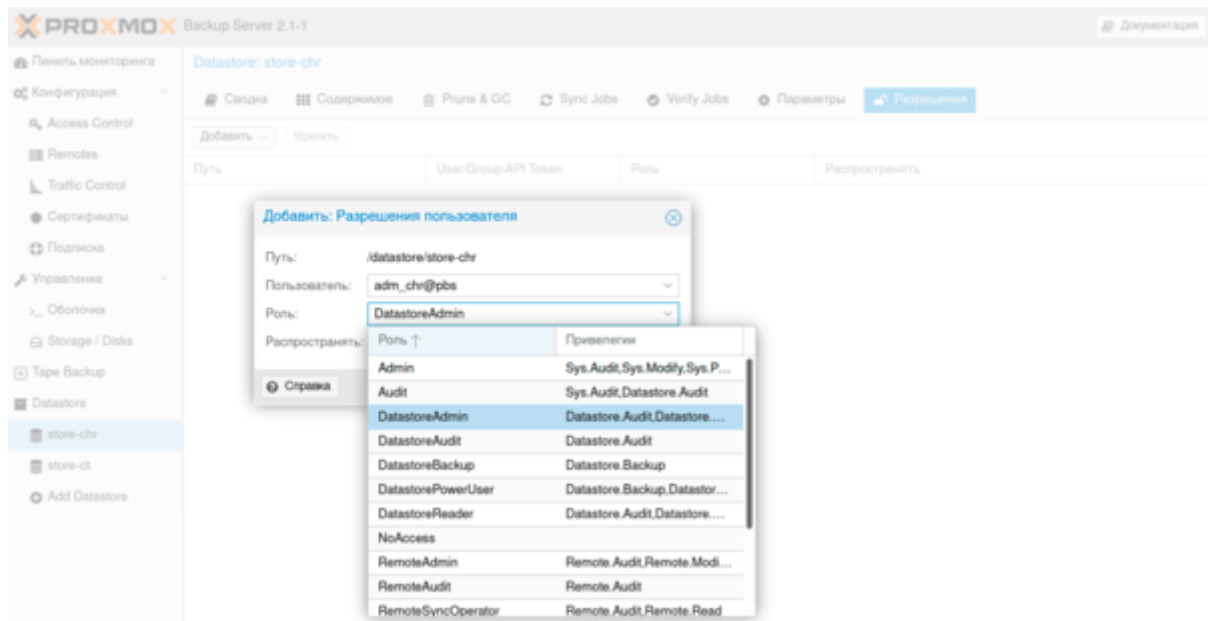
Для создания пользователей следует перейти в **Configuration - Access Control - User Management**, а сам процесс не представляет какой-либо сложности, существует ограничение на длину имени - не менее 5 символов.



Обратите внимание, что все создаваемые при помощи веб-интерфейса пользователи будут включены в область аутентификации **pbs**, если вам нужен пользователь с областью аутентификации **pam** - его следует создать средствами операционной системы. По умолчанию пользователям не назначаются никакие

права, это нужно сделать самостоятельно, для этого можно воспользоваться вкладкой **Permissions**, но если мы хотим задать права доступа к хранилищам, то удобнее пойти другим путем.

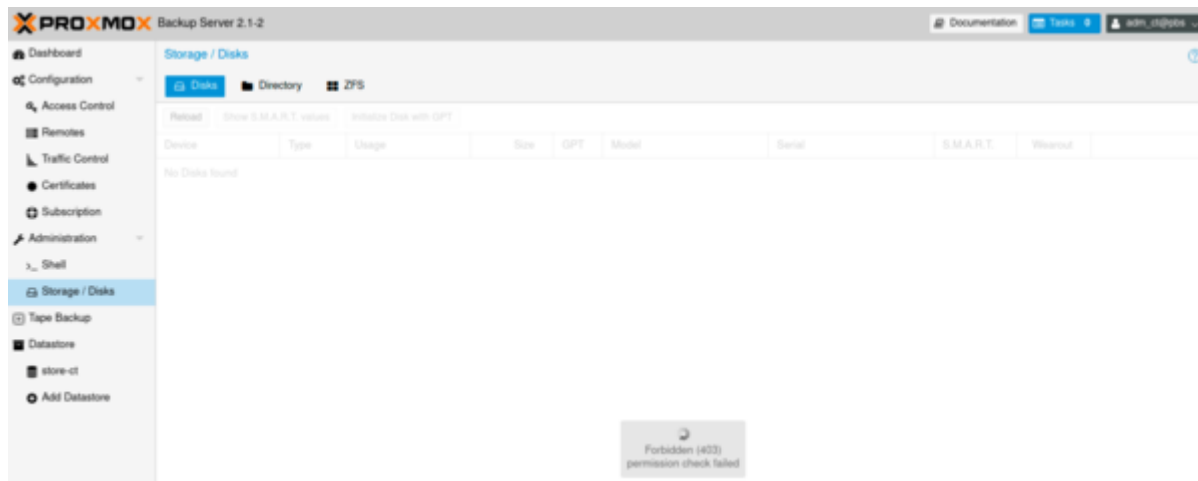
Снова вернемся в **Datastore**, выберем интересующее нас хранилище и в его свойствах перейдем на вкладку **Permissions**, где добавим нужного нам пользователя и укажем назначенный ему уровень прав.



Существует достаточно сбалансированная система ролей, начиная от роли **Admin**, которому можно все и заканчивая ролью **Audit**, которая ограничена только чтением настроек и не имеет доступа к реальным данным. Если мы говорим о хранилище, то следует выбрать одну из следующих ролей:

- **DatastoreAdmin** - полный доступ к хранилищу данных.
- **DatastoreAudit** - может просматривать настройки хранилища данных и содержимое. Не разрешено читать фактические данные (восстанавливать данные).
- **DatastoreReader** - может проверять содержимое хранилища и выполнять восстановление.
- **DatastoreBackup** - может создавать резервные копии и восстанавливать собственные резервные копии.
- **DatastorePowerUser** - может создавать резервные копии, восстанавливать и удалять собственные резервные копии.

Для примера выполним вход пользователем, для которого мы указали роль **DatastoreAdmin**, он будет иметь доступ только к собственному хранилищу и будет иметь возможность создать новое хранилище, также для него существует возможность создавать новых пользователей и выдавать им права на те объекты, которые ему доступны. Доступа к настройкам других пользователей или системы он не имеет, а при попытке получить доступ ему будет выведено сообщение об ошибке **403 Forbidden**.

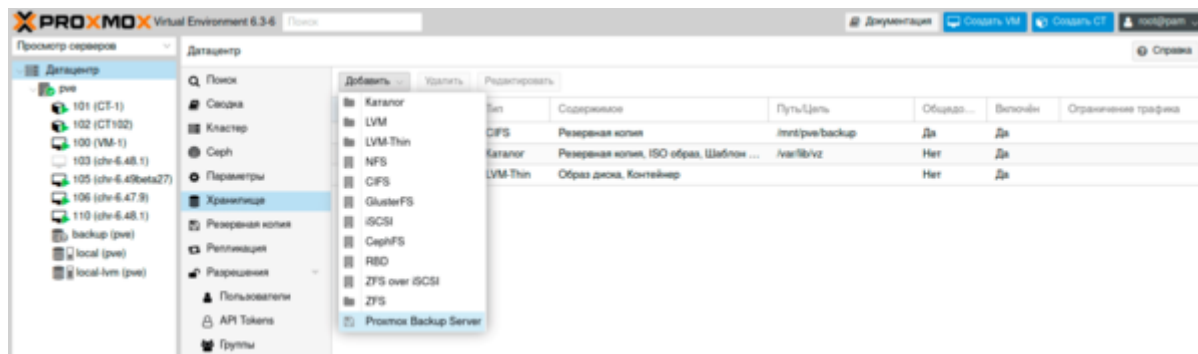


При этом система ролей достаточно гибкая и позволяет назначать одному пользователю несколько ролей, гибко регулируя его возможности в системе. Однако более подробное рассмотрение этой темы выходит за пределы данной статьи.

Подключение Proxmox Backup Server к Virtual Environment

Теперь, когда хранилища настроены и пользователи созданы самое время подключить наш сервер резервного копирования к гипервизору и настроить их совместную работу. Все современные версии Proxmox Virtual Environment поддерживают работу с Backup Server "из коробки", но в любом случае мы советуем обновить пакеты гипервизора до самой последней версии.

Для подключения перейдем на уровень **Датацентр - Хранилища - Добавить** и в выпадающем списке выберем **Proxmox Backup Server**.



Диалог добавления в целом понятен: указываем идентификатор хранилища, его можем выбрать произвольно, но желательно задавать осмысленные имена, адрес сервера можно указать как по IP, так и по FQDN, имя пользователя с обязательным указанием области аутентификации, т.е. **root@pam** или **user_1@pbs**, в поле **Datastore** указываем идентификатор хранилища, к которому подключаемся. Отдельного разговора заслуживает поле **Отпечаток**, о нем ниже.

Добавить: Proxmox Backup Server

Общее
Backup Retention
Encryption

ID:
pbs-chr

Сервер:
192.168.233.147

Имя пользователя:
adm_chr@pbs

Пароль:
.....

Отпечаток:
i3:a3:36:74:c6:be:9b:66:d4:95:e3:15:47:13:05:99:d6:9f:e9:ea:02:11:3d:16:a5:92

Узлы:
pve

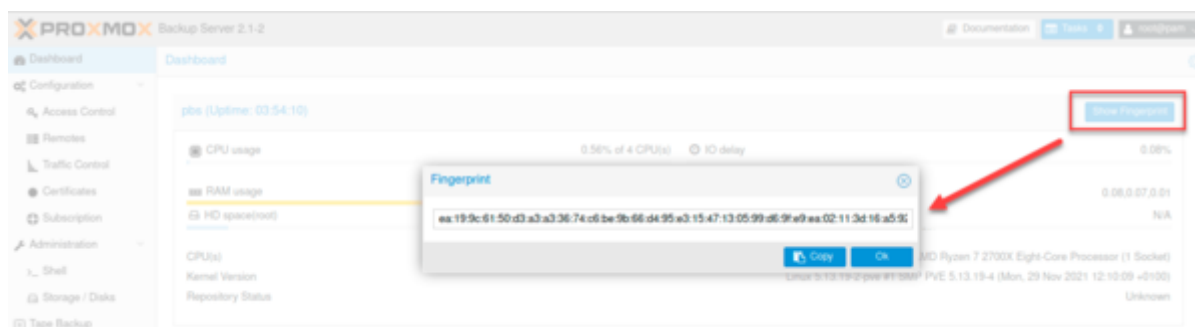
Включить:
☒

Содержимое:
backup

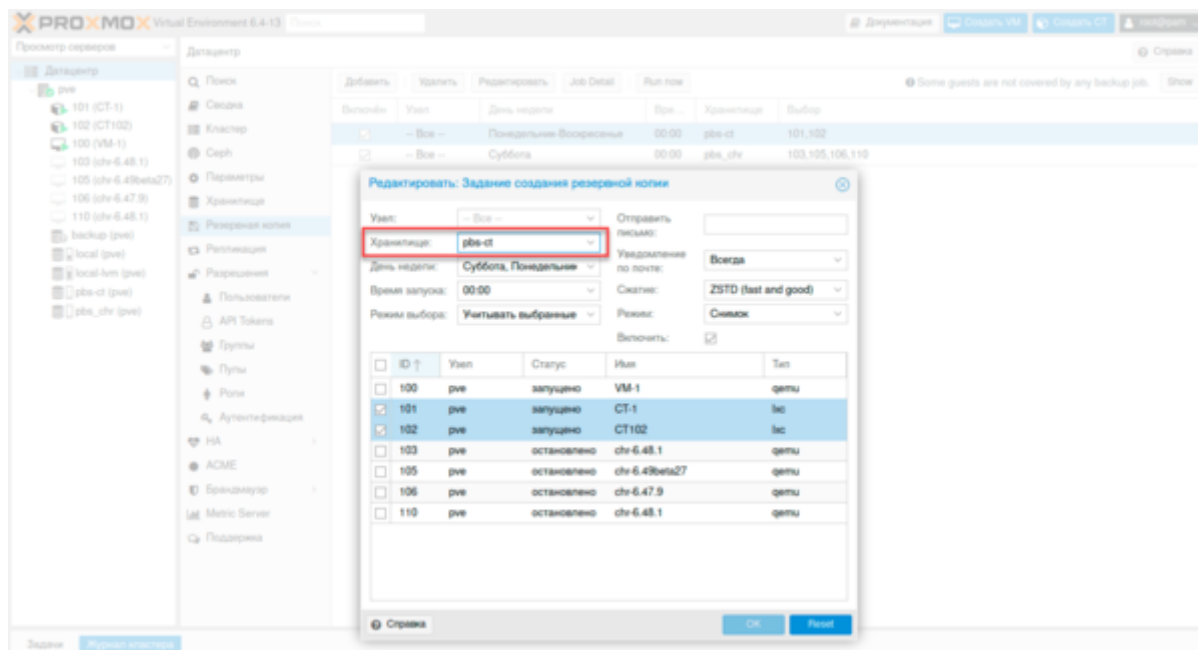
Datastore:
store-chr

? Справка
Добавить

При подключении хранилища мы должны убедиться в подлинности сервера резервного копирования, это можно сделать различными способами, один из них - проверка **отпечатка сертификата**, который остается неизменным на весь период действия последнего и позволяет однозначно подтвердить его подлинность. Получить отпечаток можно перейдя в **Панель мониторинга (Dashboard)** Proxmox Backup Server и нажав в верхнем правом углу кнопку **Show Fingerprint**.



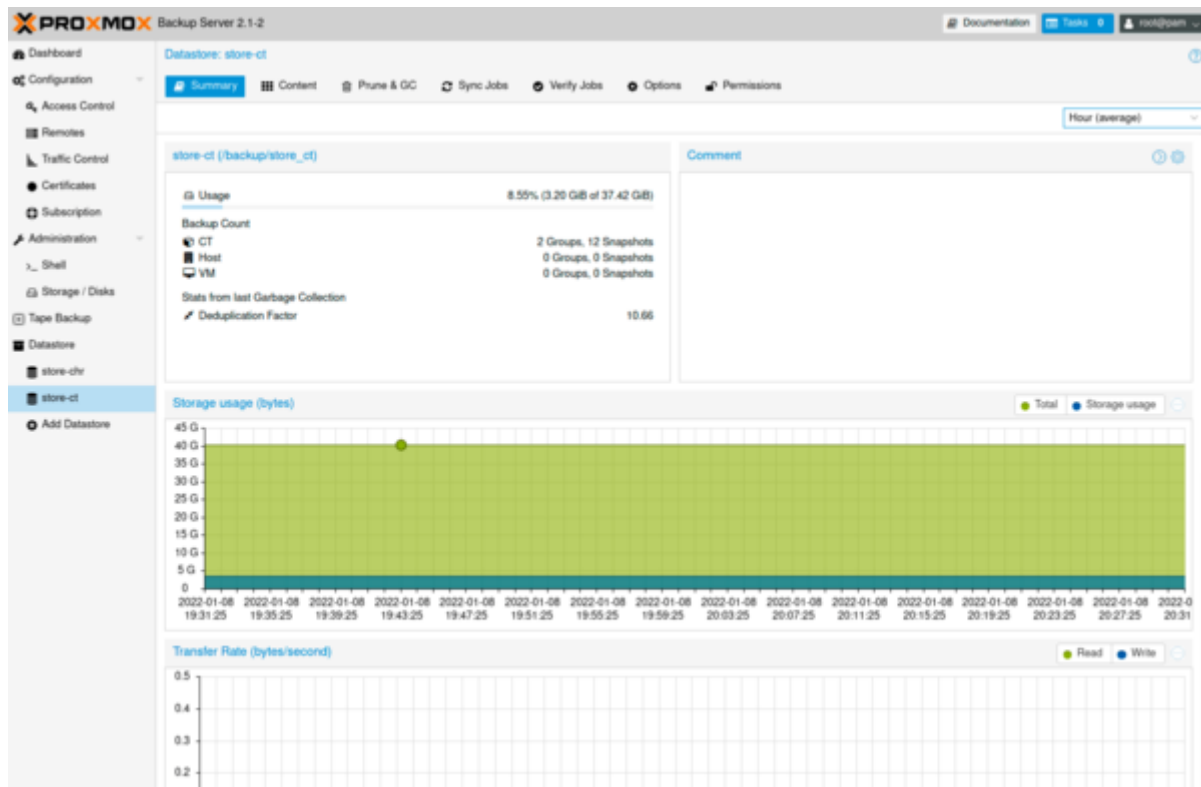
Если все сделано правильно, то хранилище будет добавлено в список доступных для этого датацентра (или отдельной ноды, если при подключении вы указали ограничения в поле **Узлы**) и его можно использовать для настройки резервного копирования штатными средствами. Если у вас есть уже настроенные задания то их можно легко перенаправить на Proxmox Backup Server просто изменив хранилище в настройках.



Как видим, ничего сложного в интеграции Proxmox Backup Server в уже существующую инфраструктуру нет, все максимально просто и прозрачно, все что вам понадобится - это добавить сервер в хранилища датацентра. Сам процесс создания и восстановления резервных копий остается прежним.

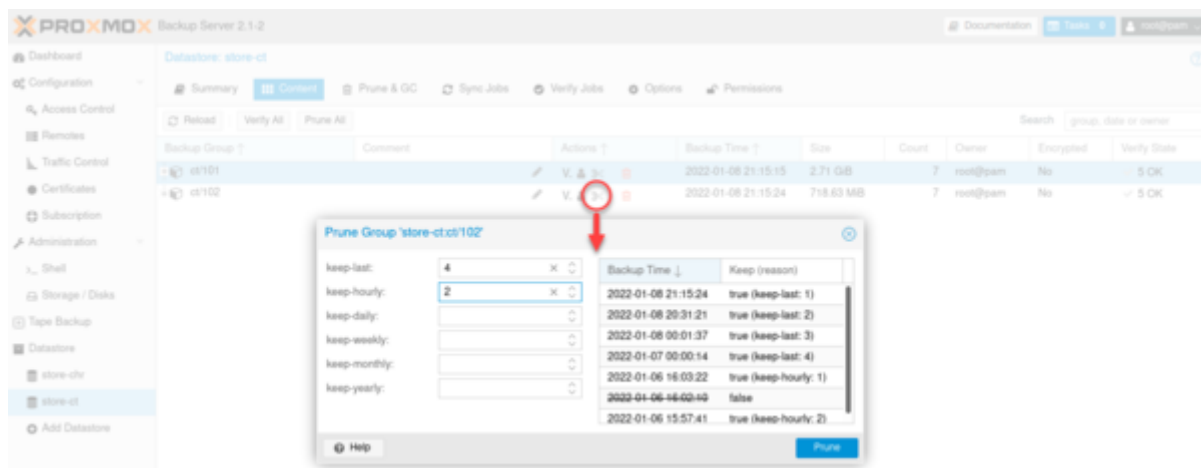
Управление резервными копиями

Теперь, когда мы все настроили и проверили самое время посмотреть какие возможности предоставляет Proxmox Backup Server и ради чего все это затевалось. Начнем со статистики, она ведется для каждого хранилища и показывает не только объем занятого пространства, но и скорости обмена с дисками, количество и задержки операций ввода-вывода, что очень важно, так как позволяет непосредственно контролировать производительность хранилища, понимать и избегать узких мест.

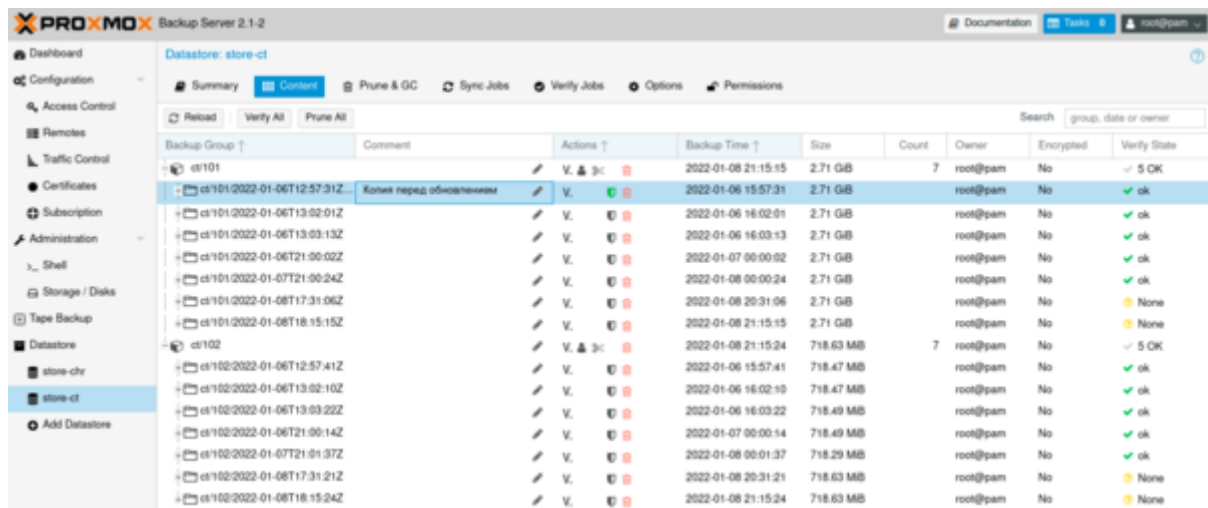


Единственный момент, который следует учитывать - это параметр **Storage usage**, который показывает занятое и доступное свободное место не в хранилище, а в файловой системе, где расположено хранилище и если у вас в пределах одной файловой системы расположено несколько хранилищ, то этот показатель будет везде одинаков.

Вкладка **Content** содержит список резервных копий, находящихся в хранилище, он имеет древовидную структуру на уровне виртуальных машин / контейнеров, которые разворачиваются списком копий для этой машины. Для каждой копии доступны персональные действия: создать комментарий, выполнить верификацию, установить защиту, удалить. Для виртуальной машины или контейнера можно сменить владельца или выполнить очистку устаревших копий. При этом можно задать отличные от настроек хранилища параметры и сразу увидеть предполагаемый результат. Данную возможность можно использовать вместо **симулятора очистки** для проверки настроек на реальных данных.



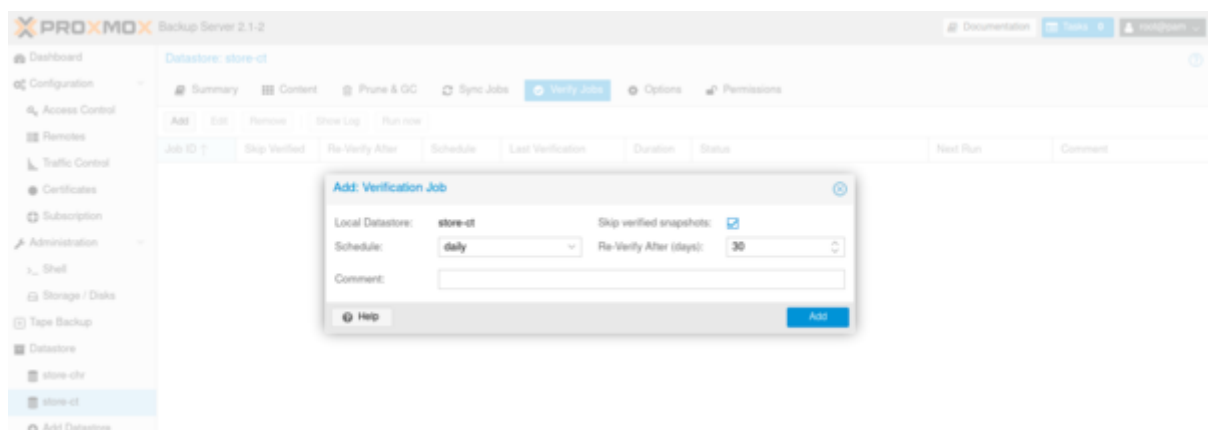
Установка защиты - параметр **Protection** - предотвращает удаление резервной копии при очистке и исключает ее из расчетов количества хранящихся копий, рекомендуется использовать для важных бекапов, скажем перед существенными изменениями, которые можно будет использовать впоследствии как эталон или источник сравнения.



| Backup Group | Comment | Actions | Backup Time | Size | Count | Owner | Encrypted | Verify State |
|----------------------------|-------------------------|------------|---------------------|-----------|-------|----------|-----------|--------------|
| ct101 | | | 2022-01-08 21:15:15 | 2.71 GB | 7 | root@pam | No | ✓ 5 OK |
| ct101/2022-01-06T12:57:31Z | Копия перед обновлением | V, D, S, R | 2022-01-06 15:57:31 | 2.71 GB | | root@pam | No | ✓ ok |
| ct101/2022-01-06T13:02:01Z | | V, D, S, R | 2022-01-06 16:02:01 | 2.71 GB | | root@pam | No | ✓ ok |
| ct101/2022-01-06T13:03:13Z | | V, D, S, R | 2022-01-06 16:03:13 | 2.71 GB | | root@pam | No | ✓ ok |
| ct101/2022-01-06T21:00:02Z | | V, D, S, R | 2022-01-07 00:00:02 | 2.71 GB | | root@pam | No | ✓ ok |
| ct101/2022-01-07T21:00:24Z | | V, D, S, R | 2022-01-08 00:00:24 | 2.71 GB | | root@pam | No | ✓ ok |
| ct101/2022-01-08T17:31:06Z | | V, D, S, R | 2022-01-08 20:31:06 | 2.71 GB | | root@pam | No | None |
| ct101/2022-01-08T18:15:15Z | | V, D, S, R | 2022-01-08 21:15:15 | 2.71 GB | | root@pam | No | None |
| ct102 | | | 2022-01-08 21:15:24 | 718.63 MB | 7 | root@pam | No | ✓ 5 OK |
| ct102/2022-01-06T12:57:41Z | | V, D, S, R | 2022-01-06 15:57:41 | 718.47 MB | | root@pam | No | ✓ ok |
| ct102/2022-01-06T13:02:10Z | | V, D, S, R | 2022-01-06 16:02:10 | 718.47 MB | | root@pam | No | ✓ ok |
| ct102/2022-01-06T13:03:22Z | | V, D, S, R | 2022-01-06 16:03:22 | 718.49 MB | | root@pam | No | ✓ ok |
| ct102/2022-01-06T21:00:14Z | | V, D, S, R | 2022-01-07 00:00:14 | 718.49 MB | | root@pam | No | ✓ ok |
| ct102/2022-01-07T21:01:37Z | | V, D, S, R | 2022-01-08 00:01:37 | 718.29 MB | | root@pam | No | ✓ ok |
| ct102/2022-01-08T17:31:21Z | | V, D, S, R | 2022-01-08 20:31:21 | 718.63 MB | | root@pam | No | None |
| ct102/2022-01-08T18:15:24Z | | V, D, S, R | 2022-01-08 21:15:24 | 718.63 MB | | root@pam | No | None |

Все мы знаем, что резервные копии мало создавать и хранить, нужно еще обеспечивать их целостность и регулярно выполнять такие проверки. Файлы резервной копии могут быть повреждены при передаче, либо может возникнуть ошибка в системе хранения, для "холодных" данных это особенно актуально, так как о возникновении такой ошибки мы узнаем только тогда, когда попробуем прочитать файл.

Proxmox Backup Server позволяет эффективно избегать подобных ситуаций, для этого вместе с каждой резервной копией создается файл-манифест **index.json** который содержит контрольные суммы для каждого файла резервной копии, а процесс **верификации** заново вычисляет контрольные суммы хранящихся файлов и сравнивает их с манифестом, если они совпали - то копия является целостной. Такие проверки следует выполнять регулярно и настроить их можно на вкладке **Verify Jobs**, настройки по умолчанию подразумевают ежедневную верификацию и повторную проверку верифицированных копий раз в месяц, что позволит вовремя выявить проблемы с отказом устройств хранения или возникновения ошибок на них.



Add: Verification Job

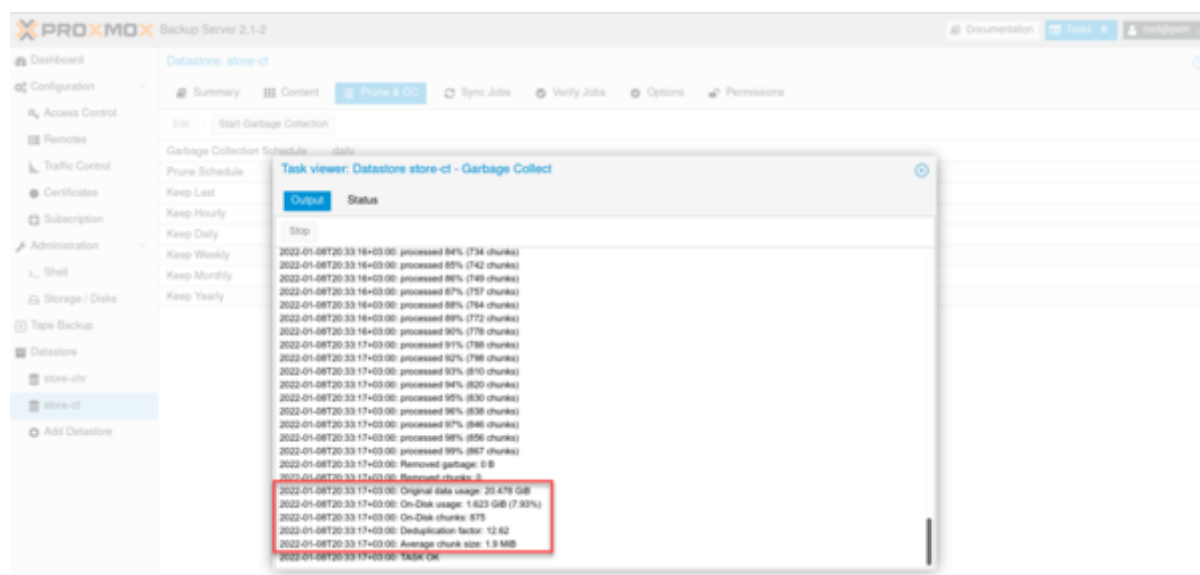
Local Dataset: **store-ct** Skip verified snapshots: ☒

Schedule: **daily** Re-Verify After (days): **30**

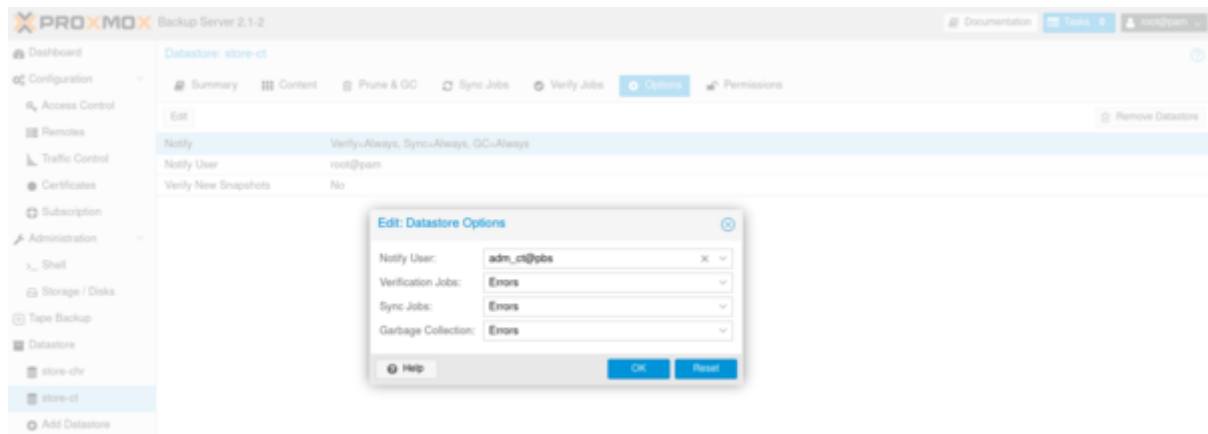
Comment:

Также вы можете выполнить верификацию вручную, не дожидаясь срабатывания задания, выбрав один из вариантов на вкладке **Content**, можно проверить все хранилище, отдельную виртуальную машину / контейнер, либо отдельную копию.

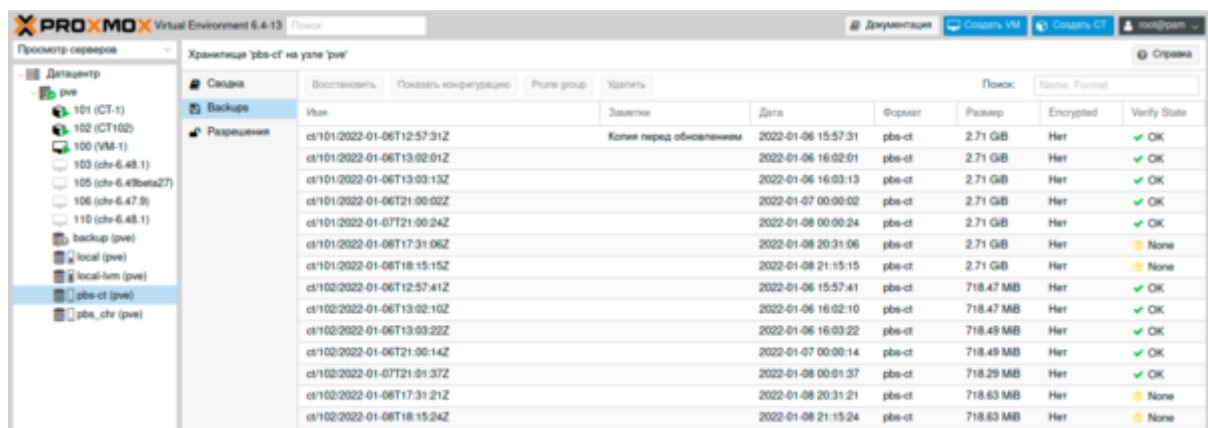
Следующая вкладка **Prune & GC** отвечает за очистку и сборку мусора. Про очистку сказано достаточно, поэтому остановимся на последней операции. Сборка мусора представляет собой процесс дедупликации, в это время анализируется содержимое, общие блоки помещаются в специальное хранилище и заменяются ссылками на них. Процесс достаточно ресурсоемкий, в первую очередь вызывающий большую нагрузку на диски, поэтому следует его выполнять в то время, когда не предполагается активных задач по резервному копированию, по умолчанию он запускается раз в сутки. Также можно запустить данный процесс вручную, вывод задачи также содержит статистику, позволяющую оценить эффективность дедупликации.



Ну и наконец вкладка **Options**, здесь нас интересуют настройки уведомлений. По умолчанию предполагается слать уведомления всегда, но здесь будет уместно вспомнить об одном из правил философии UNIX - *"Не сообщайте пользователю об очевидном"*, либо известную притчу о мальчике и волках, постоянные уведомления со временем притупят внимание и действительно важное событие будет с большой вероятностью пропущено. Поэтому изменим настройки уведомлений таким образом, чтобы они сообщали нам только об ошибках, здесь же можно изменить получателя сообщений, единственное условие - в настройках пользователя должен быть указан действительный адрес электронной почты.



В заключение рассмотрим возможности взаимодействия с сервером резервного копирования в интерфейсе Proxmox Virtual Environment, их немного, но это минимум достаточного. Мы можем восстановить резервную копию в новое расположение, просмотреть конфигурацию виртуальной машины или контейнера, выполнить очистку для группы (под группой подразумевается виртуальная машина / контейнер) или удалить копию, также отсюда мы можем контролировать статус верификации.



Как видим, Proxmox Backup Server представляет собой решение, позволяющее вывести резервное копирование виртуальных машин и контейнеров на новый уровень, предоставляя такие возможности как инкрементное копирование, проверку архивов и дедупликацию. В тоже время он максимально органично встраивается в уже существующую инфраструктуру, позволяя выполнить переход максимально просто и безболезненно. Мы рекомендуем присмотреться к данному продукту всем, кто использует решения виртуализации от этого разработчика.