КИБЕРПРОТЕКТ

КИБЕР Бэкап

Версия 16

Резервное копирование баз данных PostgreSQL

Редакция: 03.04.2024

Содержание

Заявление об авторских правах

1 Введение

Кибер Бэкап 16 поддерживает резервное копирование баз PostgreSQL, а также баз Postgres, разработанных специально для российского рынка на основе открытой СУБД PostgreSQL.

В этой документации описывается установка и настройка PostgreSQL. За дополнительной информацией обратитесь к пользовательской документации Кибер Бэкап.

1.1 Возможности

1. Кибер Бэкап 16 поддерживает следующие виды резервного копирования:
   - полное резервное копирование;
   - инкрементное резервное копирование.

   Полное резервное копирование означает резервное копирование кластеров с базами данных. На одном сервере может быть несколько кластеров.
2. Кибер Бэкап 16 поддерживает в качестве хранилищ резервных копий:
   - локальные папки;
   - сетевые папки;
   - NFS;
   - узлы хранения;
   - ленты.
3. Кибер Бэкап 16 поддерживает следующие варианты расписания резервного копирования:
   - всегда полное;
   - еженедельно полное, ежедневно инкрементное;
   - другое (пользовательская схема).

2 Поддерживаемые операционные системы

Для резервного копирования баз PostgreSQL вам нужно будет установить агент Кибер Бэкап для операционной системы, которую вы используете (Windows-агент или Linux-агент), а также агент PostgreSQL. Требования к операционным системам, поддерживаемым Windows- и Linux-агентами приведены в документации Кибер Бэкап в разделе "Требования к программному обеспечению".

Однако у агента PostgreSQL более узкие требования к операционным системам. Агент PostgreSQL может работать только на 64-разрядных операционных системах нового поколения. Поэтому для совместной работы Windows- и Linux-агентов с агентом PostgreSQL учитывайте список поддерживаемых операционных систем, приведенный ниже.

2.1 Поддерживаемые операционные системы Windows

- Windows Server 2008 R2 (x64).
- Windows Server 2012 R2 (x64).
- Windows Server 2016.
- Windows Server 2019.
- Windows Server 2022.
- Windows 7 (x64).
- Windows 8 или 8.1 (x64).
- Windows 10 (x64).

2.2 Поддерживаемые операционные системы Linux

Linux с версией ядра от 2.6.23 и выше:

- Red Hat Enterprise Linux 5.x и выше.
- Ubuntu 14.04 и выше.
- Fedora 22 и выше.
- SUSE Linux Enterprise Server 11 и выше.
- Debian 7.0 и выше.
- CentOS 6.x и выше.
- Astra Linux 1.6 и выше.

3 Поддерживаемые версии PostgreSQL

Вы можете выполнять резервное копирование баз PostgreSQL следующих версий:

- PostgreSQL 11, 12, 13, 14, 15.
- Postgres PRO Standard\Enterprise 11, 12, 13, 14, 15.

4 Подготовка к установке программы

4.1 Предварительные требования

Для работы с PostgreSQL у вас должны быть лицензии «Кибер Бэкап Расширенная редакция для PostgreSQL» на каждый экземпляр PostgreSQL, резервное копирование которого вы планируете выполнять. При этом количество лицензий не зависит от количества устанавливаемых агентов PostgreSQL.

4.2 Необходимые компоненты программы

Чтобы защитить данные PostgreSQL, необходимо установить следующие компоненты:

- **Сервер управления** позволяет централизованно управлять несколькими машинами: создавать планы резервного копирования, отслеживать их выполнение, развертывать агенты и выполнять другие действия. Его можно установить на машине с Windows или Linux, которая имеет сетевой доступ ко всем управляемым машинам.
  Чтобы установить сервер управления, выполните действия, описанные в разделе "Установка сервера управления" документации пользователя.
- **Агенты** необходимы для резервного копирования серверов и баз данных.
  - В зависимости от операционной системы сервера, на котором работает PostgreSQL, установите на сервер **Агент для Windows** или **Агент для Linux**.
  - Чтобы защитить физический или виртуальный сервер, на котором работает PostgreSQL, установите **агент для PostgreSQL**.

  Чтобы установить агенты, выполните действия, описанные в разделе "Локальная установка агентов" документации пользователя.

Агент PostgreSQL может быть установлен как на сервер, на котором находятся базы PostgreSQL, так и на другую машину.

Если вы устанавливаете агент PostgreSQL на другую машину:

1. Убедитесь, что машина с агентом и сервер PostgreSQL смогут обмениваться данными по сети. Откройте необходимые порты, настройте соединение, если требуется - настройте прокси-сервер.
2. На сервере PostgreSQL разрешите локальные входящие соединения типа replication.

4.3 Настройка аутентификации в PostgreSQL

Чтобы настроить соединение между Кибер Бэкап и PostgreSQL, укажите параметры аутентификации в конфигурационном файле pg_hba.conf, расположенном в каталоге с данными кластера базы данных. (HBA расшифровывается как host-based authentication – аутентификация по имени узла.) Файл pg_hba.conf со стандартным содержимым создаётся командой initdb при инициализации каталога с данными.

Обычный формат файла pg_hba.conf представляет собой набор записей, по одной в строке. Пустые строки игнорируются, как и любой текст комментария после знака **#**. Записи не продолжаются на следующей строке. Записи состоят из некоторого количества полей, разделённых между собой пробелом и/или **tabs**. В полях могут быть использованы пробелы, если они взяты в кавычки. Если в кавычки берётся какое-либо зарезервированное слово в поле базы данных, пользователя или адресации (например, all или replication), то слово теряет своё особое значение и просто обозначает базу данных, пользователя или сервер с данным именем.

Каждая запись обозначает тип соединения, диапазон IP-адресов клиента (если он соотносится с типом соединения), имя базы данных, имя пользователя и способ аутентификации, который будет использован для соединения в соответствии с этими параметрами. Первая запись с соответствующим типом соединения, адресом клиента, указанной базой данных и именем пользователя применяется для аутентификации. Процедур fall-through или backup не предусмотрено: если выбрана запись и аутентификация не прошла, последующие записи не рассматриваются. Если же ни одна из записей не подошла, в доступе будет отказано.

Укажите параметры в следующем формате:

```
# TYPE  DATABASE        USER            ADDRESS                 METHOD

# "local" is for Unix domain socket connections only
local   all             all                                     peer
# IPv4 local connections:
host    all             all             127.0.0.1/32            ident
host    all             all             0.0.0.0/0               md5
# IPv6 local connections:
host    all             all             ::1/128                 ident
# Allow replication connections from localhost, by a user with the
# replication privilege.
local   replication     all                                     peer
host    replication     all             127.0.0.1/32            md5
host    replication     all             ::1/128                 ident
host    replication     all             0.0.0.0/0               md5
```

Значения полей описаны ниже:

TYPE

Тип подключения. Значение local управляет подключениями через Unix-сокеты. Без подобной записи подключения через Unix-сокеты невозможны. Значение **host** управляет подключениями, устанавливаемыми по TCP/IP.

DATABASE

Определяет, каким именам баз данных соответствует эта запись. Значение all определяет, что подходят все базы данных. Значение replication показывает, что запись соответствует, если запрашивается подключение для физической репликации (имейте в виду, что для таких подключений не выбирается какая-то конкретная база данных). Несколько имён баз данных

можно указать, разделяя их запятыми. Файл, содержащий имена баз данных, можно указать, поставив знак @ в начале его имени.

USER

Указывает, какому имени (или именам) пользователя базы данных соответствует эта запись. Значение all показывает, что запись соответствует всем пользователям. Несколько имён пользователей можно указать, разделяя их запятыми. Файл, содержащий имена пользователей, можно указать, поставив знак @ в начале его имени.

ADDRESS

Указывает адрес (или адреса) клиентской машины, которым соответствует данная запись. Это поле может содержать или имя компьютера, или диапазон IP-адресов, или одно из нижеупомянутых ключевых слов.

Диапазон IP-адресов указывается в виде начального адреса диапазона, дополненного косой чертой (/) и длиной маски CIDR. Длина маски задаёт количество старших битов клиентского IP-адреса, которые должны совпадать с битами IP-адреса диапазона. Биты, находящиеся правее, в указанном IP-адресе должны быть нулевыми. Между IP-адресом, знаком / и длиной маски CIDR не должно быть пробельных символов.

Типичные примеры диапазонов адресов IPv4, указанных таким образом: 172.20.143.89/32 для одного компьютера, 172.20.143.0/24 для небольшой и 10.6.0.0/16 для крупной сети. Диапазон адресов IPv6 может выглядеть как ::1/128 для одного компьютера (это адрес замыкания IPv6) или как fe80::7a31:c1ff:0000:0000/96 для небольшой сети. 0.0.0.0/0 представляет все адреса IPv4, а ::0/0 – все адреса IPv6. Чтобы указать один компьютер, используйте длину маски 32 для IPv4 или 128 для IPv6. Опускать замыкающие нули в сетевом адресе нельзя.

Запись, сделанная в формате IPv4, подойдёт только для подключений по IPv4, а запись в формате IPv6 подойдёт только для подключений по IPv6, даже если представленный адрес находится в диапазоне IPv4-в-IPv6. Имейте в виду, что записи в формате IPv6 не будут приниматься, если системная библиотека C не поддерживает адреса IPv6.

Вы также можете прописать значение all, чтобы указать любой IP-адрес, samehost, чтобы указать любые IP-адреса данного сервера, или samenet, чтобы указать любой адрес любой подсети, к которой сервер подключён напрямую.

Если определено имя компьютера (всё, что не является диапазоном IP-адресов или специальным ключевым словом, воспринимается как имя компьютера), то оно сравнивается с результатом обратного преобразования IP-адреса клиента (например, обратного DNS-запроса, если используется DNS). При сравнении имён компьютеров регистр не учитывается. Если имена совпали, выполняется прямое преобразование имени (например, прямой DNS-запрос) для проверки, относится ли клиентский IP-адрес к адресам, соответствующим имени. Если двусторонняя проверка пройдена, запись считается соответствующей компьютеру. (В качестве имени узла в файле pg_hba.conf должно указываться то, что возвращается при преобразовании IP-адреса клиента в имя, иначе строка не будет соответствовать узлу. Некоторые базы данных имён

позволяют связать с одним IP-адресом несколько имён узлов, но операционная система при попытке разрешить IP-адрес возвращает только одно имя.)

Указание имени, начинающееся с точки (.), соответствует суффиксу актуального имени узла. Так, .example.com будет соответствовать for.example.com (а не только example.com).

Когда в pg_hba.conf указываются имена узлов, следует добиться, чтобы разрешение имён выполнялось достаточно быстро. Для этого может быть полезен локальный кеш разрешения имён, например, nscd. Вы также можете включить конфигурационный параметр log_hostname, чтобы видеть в журналах имя компьютера клиента вместо IP-адреса.

METHOD

Метод-аутентификации.

Чтобы к PostgreSQL можно было подключаться с логином и паролем, укажите значение md5. PostgreSQL проверит пароль пользователя, производя аутентификацию SCRAM-SHA-256 или MD5.

Значение ident получает имя пользователя операционной системы клиента, связываясь с сервером Ident, и проверяет, соответствует ли оно имени пользователя базы данных. Аутентификация ident может использоваться только для подключений по TCP/IP. Для локальных подключений применяется аутентификация peer.

Значение peer получает имя пользователя операционной системы клиента из операционной системы и проверяет, соответствует ли оно имени пользователя запрашиваемой базы данных. Доступно только для локальных подключений.

Внимание
Для настройки аутентификации при переходе с версии Кибер Бэкап 15 Обновление 2.6 или Кибер Бэкап Обновление 2.7 на Кибер Бэкап 16 обратитесь к разделу Известные проблемы и их решения.

5 Установка и настройка программы

Выполняйте действия по установке и настройке программы в следующем порядке:

1. Подготовьте сервер PostgreSQL. Обратите внимание на поддерживаемые версии PostgreSQL.
2. Если вы устанавливаете агент PostgreSQL не на сервере PostgreSQL, подготовьте соединение.
3. Настройте параметры аутентификации на сервере PostgreSQL.
4. Установите программу Кибер Бэкап, в состав которой входит агент PostgreSQL. Подробнее в разделе пользовательской документации об установке программы.
   В процессе установки вам будет предложено выбрать агенты, которые вы хотите установить. Выберите **агент PostgreSQL** и **агент Windows** (или **агент Linux**). Они устанавливаются вместе.
5. После установки программы через веб-консоль Кибер Бэкап добавьте лицензии «Кибер Бэкап Расширенная редакция для PostgreSQL» для каждого экземпляра PostgreSQL, резервное копирование которого вы планируете выполнять. Подробнее см. в разделе пользовательской документации об управлении лицензиями.
6. Через веб-консоль Кибер Бэкап добавьте устройства PostgreSQL:
   a. Щелкните **Все устройства** > **Добавить**.
   b. В списке **Приложения** выберите **PostgreSQL**.

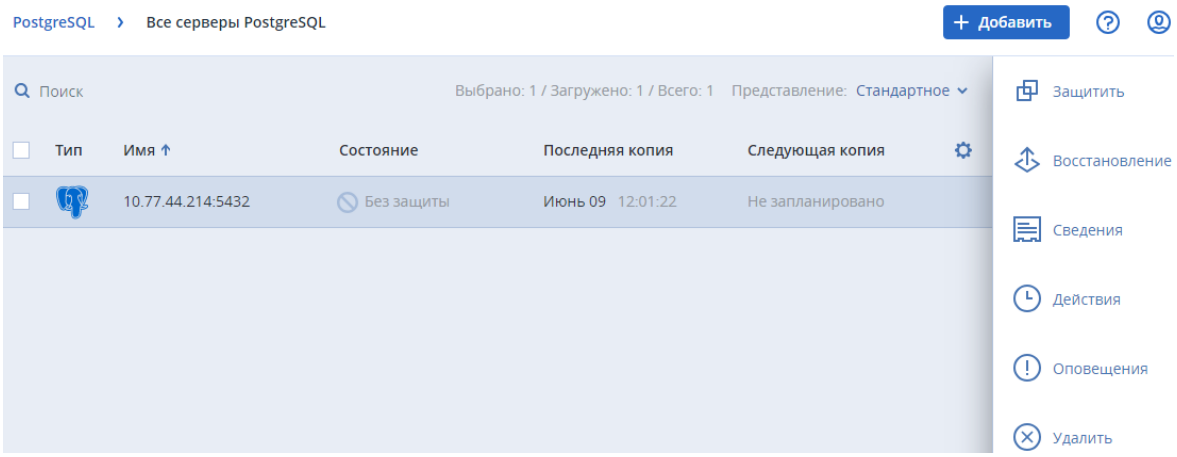
   Подробнее в разделе документации о добавлении машин.
7. Через веб-консоль Кибер Бэкап настройте соединение с PostgreSQL.
   a. Выберите агент PostgreSQL.
   b. Введите имя хоста или IP-адрес сервера PostgreSQL и порт подключения (по умолчанию используется порт 5432), имя пользователя и пароль учетной записи для подключения к PostgreSQL и нажмите кнопку **Добавить**.
      Убедитесь, что при настройке параметров аутентификации вы настроили метод аутентификации md5.

   В списке устройств отобразится раздел PostgreSQL с добавленным сервером.
8. Настройте резервное копирование баз PostgreSQL. Подробнее в разделе "Резервное копирование PostgreSQL" (стр. 12).

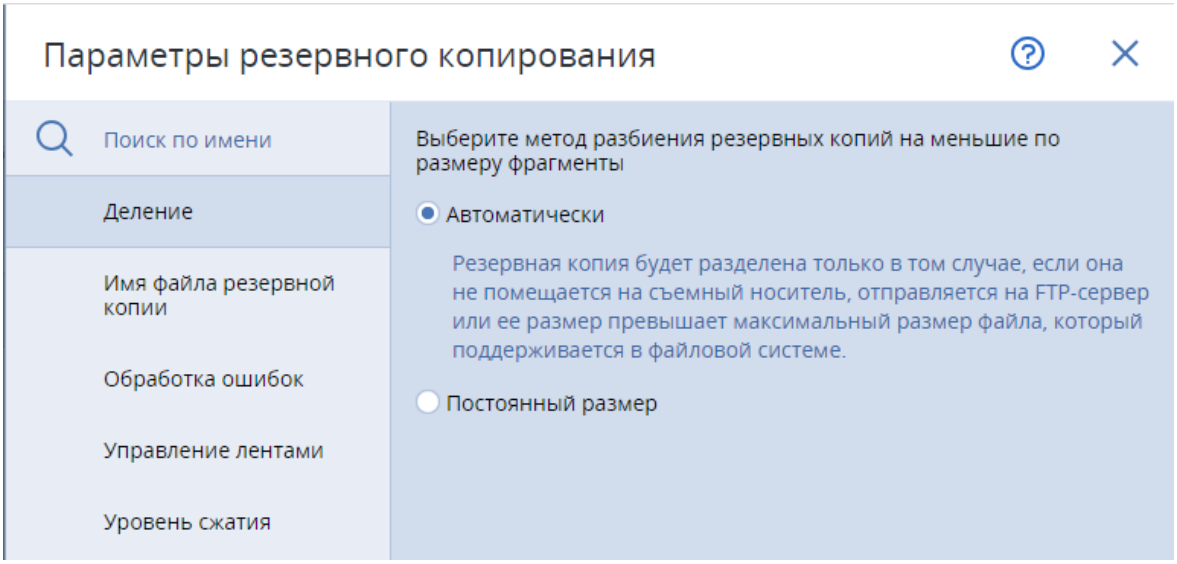
6 Резервное копирование PostgreSQL

Для создания плана защиты выполните следующие действия:

1. Перейдите в **Устройства** > **PostgreSQL**.
2. Выберите сервер PostgreSQL, который вы хотите защитить.
3. Перейдите на вкладку справа **Защитить**.



4. В поле **Место хранения** нажмите **Указать** и выберите место хранения резервных копий. Выберите существующее хранилище или нажмите **Добавить хранилище** и создайте новое.
5. В поле **Расписание** укажите схему и периодичность выполнения резервного копирования. В текущей версии доступны полное резервное копирование и инкрементное резервное копирование.
   Подробнее см. в разделе "Резервное копирование > Расписание" руководства пользователя.
6. В поле **Срок хранения** укажите срок хранения резервных копий и правила очистки хранилища. Подробнее см. в разделе "Резервное копирование > Правила хранения" руководства пользователя.
7. При необходимости защитите резервные копии паролем. Подробнее см. в разделе "Резервное копирование > Защита паролем" руководства пользователя.
8. [Необязательно] В поле **Параметры резервного копирования** нажмите **Изменить** и укажите следующие параметры:
   - Деление. Выберите метод разделения резервных копий на меньшие по размеру фрагменты.
   - Имя файла резервной копии. Укажите шаблон для наименований файлов резервных копий.
   - Обработка ошибок. Укажите порядок обработки ошибок, возникающих при резервном копировании.
   - Управление лентами. Укажите порядок записи резервных копий на ленточные устройства.
   - Уровень сжатия. Укажите уровень сжатия данных при резервном копировании.



Подробнее см. в разделе "Параметры резервного копирования" руководства пользователя.

9. Нажмите **Применить**. Новый план защиты появится в списке планов.

В результате вы сможете:

- Выполнять резервное копирование баз PostgreSQL. Подробнее см. в разделе "Резервное копирование" руководства пользователя.
- Выполнять восстановление баз PostgreSQL из резервных копий. Подробнее см. в разделе "Восстановление" руководства пользователя.

7 Ограничения

- Не поддерживается полное резервное копирование баз данных PostgreSQL в хранилище под управлением узла хранения с включенной дедупликацией резервных копий.
- Не поддерживается резервное копирование баз данных PostgreSQL в защищенное паролем хранилище под управлением узла хранения.

8 Известные проблемы и их решения

8.1 Настройка аутентификации

Если вы выполняли настройку аутентификации PostgreSQL в Кибер Бэкап 15 версий Обновление 2.6 или Обновление 2.7 в соответствии с инструкцией и впоследствии перешли на версию Кибер Бэкап 16, резервное копирование PostgreSQL может завершаться с ошибкой.

```
{"error": "FATAL: no pg_hba.conf entry for host "10.77.242.110", user "postgres", database "template1", no encryption (SQLSTATE 28000)",
"request-id": "bff753db-34f0-4ee9-bbda-d429f45b4ea3",
"service": "PostgreSQL",
"serviceMsg": "FATAL: no pg_hba.conf entry for host "10.77.242.110", user "postgres", database "template1", no encryption (SQLSTATE 28000)"}
```

Решение

В пункте IPv4 local connections файла pg_hba.conf укажите настройки так, как показано в следующем примере:

host all all 127.0.0.1/32 trust

host all all 0.0.0.0/0 md5.

После того, как вы изменили настройки, перезапустите PostgreSQL.

Примечание
Укажите ip-адреса в соответствии со своей конфигурацией.

8.2 Слоты репликации

Резервное копирование по расписанию останавливается с ошибкой после нескольких созданий, запусков по расписанию и удалений планов резервного копирования.

```
ОШИБКА: используются все слоты репликации (SQLSTATE 53400)
ОШИБКА: syntax error (SQLSTATE 42601)
```

Решение

Удалите ненужные слоты репликации вручную, используя следующие команды:

- Получить все слоты:
  select * from pg_replication_slots where slot_name like 'cp%'
- Удалить слот:
  select pg_drop_replication_slot('cp_3odiqs5psps0knx0bgjz3g_dsuqc5akrjsnln9fhr6srg')

Указатель