

КИБЕРПРОТЕКТ



КИБЕР Бэкап

Версия 16.5

Содержание

1 Введение	4
1.1 Возможности	4
2 Поддерживаемые операционные системы	5
2.1 Поддерживаемые операционные системы Windows	5
2.2 Поддерживаемые операционные системы Linux	5
3 Поддерживаемые версии PostgreSQL	6
4 Подготовка к установке программы	7
4.1 Предварительные требования	7
4.2 Необходимые компоненты программы	7
4.3 Настройка аутентификации в PostgreSQL	8
5 Установка и настройка программы	12
6 Резервное копирование PostgreSQL	13
7 Подключение экземпляра PostgreSQL из архива	15
7.1 Предварительные требования	15
8 Восстановление баз данных PostgreSQL	17
8.1 Гранулярное восстановление отдельных баз данных PostgreSQL	17
8.1.1 Предварительные требования	17
9 Ограничения	20
10 Известные проблемы и их решения	21
10.1 Настройка аутентификации	21
10.2 Слоты репликации	21
10.3 Подключение экземпляра PostgreSQL из архива в ОС Astra Linux Special Edition	22
Указатель	24

Заявление об авторских правах

Все права защищены.

Все остальные упоминаемые товарные знаки могут быть зарегистрированными товарными знаками соответствующих владельцев.

Распространение существенно измененных версий данного руководства запрещено без явного разрешения владельца авторских прав.

Распространение настоящих или переработанных материалов, входящих в данное руководство, в виде печатного издания (книги) запрещено без письменного разрешения их владельца.

ДОКУМЕНТАЦИЯ ПОСТАВЛЯЕТСЯ «КАК ЕСТЬ». НЕ СУЩЕСТВУЕТ НИКАКИХ ЯВНО ВЫРАЖЕННЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ ОБЯЗАТЕЛЬСТВ, ПОДТВЕРЖДЕНИЙ ИЛИ ГАРАНТИЙ, В ТОМ ЧИСЛЕ И СВЯЗАННЫХ С ТОВАРНОСТЬЮ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ИЛИ ПРИГОДНОСТЬЮ ЕГО ДЛЯ ИСПОЛЬЗОВАНИЯ В ОПРЕДЕЛЕННЫХ ЦЕЛЯХ, НАСКОЛЬКО ТАКАЯ ОГРАНИЧЕННОСТЬ ОТВЕТСТВЕННОСТИ ДОПУСКАЕТСЯ ЗАКОНОМ.

1 Введение

В этом документе описывается настройка резервного копирования баз PostgreSQL. За дополнительной информацией обратитесь к [пользовательской документации Кибер Бэкап](#).

Кибер Бэкап поддерживает резервное копирование баз PostgreSQL, Postgres Pro, а также кластера PostgreSQL на базе Patroni.

1.1 Возможности

1. Кибер Бэкап 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 поддерживает в качестве хранилищ резервных копий:

- локальные папки;
- сетевые папки;
- NFS;
- узлы хранения;
- ленты.

3. Кибер Бэкап поддерживает следующие варианты расписания резервного копирования:

- всегда полное;
- еженедельно полное, ежедневно инкрементное;
- другое (пользовательская схема).

2 Поддерживаемые операционные системы

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

У агента PostgreSQL более узкие требования к операционным системам, поэтому 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 3.0 и выше:

- Astra Linux 1.6 и выше
- РЕД ОС 7.2, 7.3
- РОСА «КОБАЛЬТ» 7.9
- Альт Сервер 10
- Red Hat Enterprise Linux 7.x и выше
- Ubuntu 18.04 LTS, 20.04 LTS, 22.04 LTS
- SUSE Linux Enterprise Server 12 и выше
- Debian 10 и выше
- CentOS 7.x и выше

3 Поддерживаемые версии PostgreSQL

Вы можете выполнять резервное копирование баз PostgreSQL следующих версий:

- PostgreSQL 11, 12, 13, 14, 15, 16
- Postgres Pro Standard 11, 12, 13, 14, 15, 16
- Postgres Pro Enterprise 11, 12, 13, 14, 15
- Patroni 3.0-3.2.1

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.

Создайте учетную запись пользователя на сервере PostgreSQL, с помощью которой будет происходить соединение с программой Кибер Бэкап.

Учетная запись должна обладать привилегией SUPERUSER.

Например, можно использовать команду:

```
CREATE USER <replicator> SUPERUSER PASSWORD <password>
```

Где:

- <replicator> – имя учетной записи;
- <password> – пароль учетной записи.

Если планируется работать с кластером PostgreSQL, то на всех узлах кластера должна быть создана учетная запись с одинаковым именем и паролем.

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.

Для учетной записи пользователя PostgreSQL, с помощью которой происходит соединение с программой Кибер Бэкап (см. раздел "Предварительные требования" (стр. 7)), укажите метод аутентификации `trust`.

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		replicator	127.0.0.1/32	trust
host	all		all	0.0.0.0/0	md5
host	all		all	127.0.0.1/32	ident
# 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		replicator	127.0.0.1/32	trust
host	replication		all	0.0.0.0/0	md5
host	replication		all	127.0.0.1/32	md5
host	replication		all	:::1/128	ident

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. Щелкните **Все устройства > Добавить** и выберите приложение:
 - а. Если необходимо добавить сервер PostgreSQL, в списке **Приложения** выберите **PostgreSQL**.
 - б. Если необходимо добавить кластер PostgreSQL, в списке **Приложения** выберите **Кластер PostgreSQL Patroni**.
7. Укажите настройки соединения с PostgreSQL:
Введите имя хоста или IP-адрес сервера PostgreSQL и порт подключения (по умолчанию для сервера PostgreSQL используется порт 5432, для кластера PostgreSQL - порт 8008), имя пользователя и пароль учетной записи для подключения к PostgreSQL и нажмите кнопку **Добавить**.
Убедитесь, что при настройке [параметров аутентификации](#) вы настроили метод аутентификации trust.

В списке устройств отобразится раздел PostgreSQL с добавленным сервером или кластером.

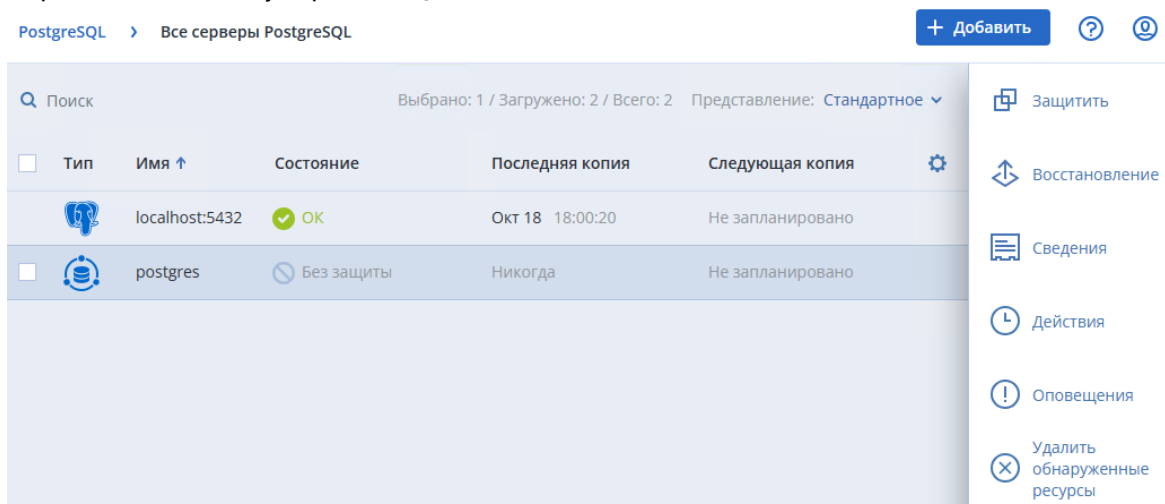
Для кластера PostgreSQL в разделе **Сведения** отобразится информация об IP-адресах/именах узлов, доступность (Online/Offline) и статусы узлов (Leader/Replica).

Настройте резервное копирование баз PostgreSQL. Подробнее см. в разделе "Резервное копирование PostgreSQL" (стр. 13).

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 деления 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.
 - Способ резервного копирования кластера [Только для резервного копирования кластера].
Подробнее см. в разделе "Резервное копирование > Способ резервного копирования кластера" руководства пользователя.
 - Управление лентами. Укажите порядок записи резервных копий на ленточные устройства.
 - Уровень сжатия. Укажите уровень сжатия данных при резервном копировании.

Параметры резервного копирования



 Поиск по имени	Выберите метод разбиения резервных копий на меньшие по размеру фрагменты
Деление	<input checked="" type="radio"/> Автоматически
Имя файла резервной копии	Резервная копия будет разделена только в том случае, если она не помещается на съёмный носитель, отправляется на FTP-сервер или её размер превышает максимальный размер файла, который поддерживается в файловой системе.
Обработка ошибок	<input type="radio"/> Постоянный размер
Способ резервного копирования кластера	
Управление лентами	
Уровень сжатия	

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.

7 Подключение экземпляра PostgreSQL из архива

Подключение экземпляра PostgreSQL из архива может понадобиться для просмотра содержимого резервной копии или других операций с базой данных средствами PostgreSQL.

7.1 Предварительные требования

- На машине с агентом PostgreSQL и на сервере PostgreSQL, которому принадлежит резервная копия, должны совпадать операционная система, версия и редакция PostgreSQL.
- На машине с агентом PostgreSQL в конфигурационном файле `/opt/acronis/var/dsp.database.pg/postgresql-agent.json` в секции `server > recovery_instance > binaries` необходимо указать путь к исполняемым файлам PostgreSQL. Например:

```
"recovery_instance": {  
  "run_as_user": "postgres",  
  "binaries": ["/usr/pgsql-15/bin/postgres"]  
}
```

Далее перезапустите службу агента PostgreSQL:

```
aakore restart
```

Для подключения экземпляра базы данных PostgreSQL из архива:

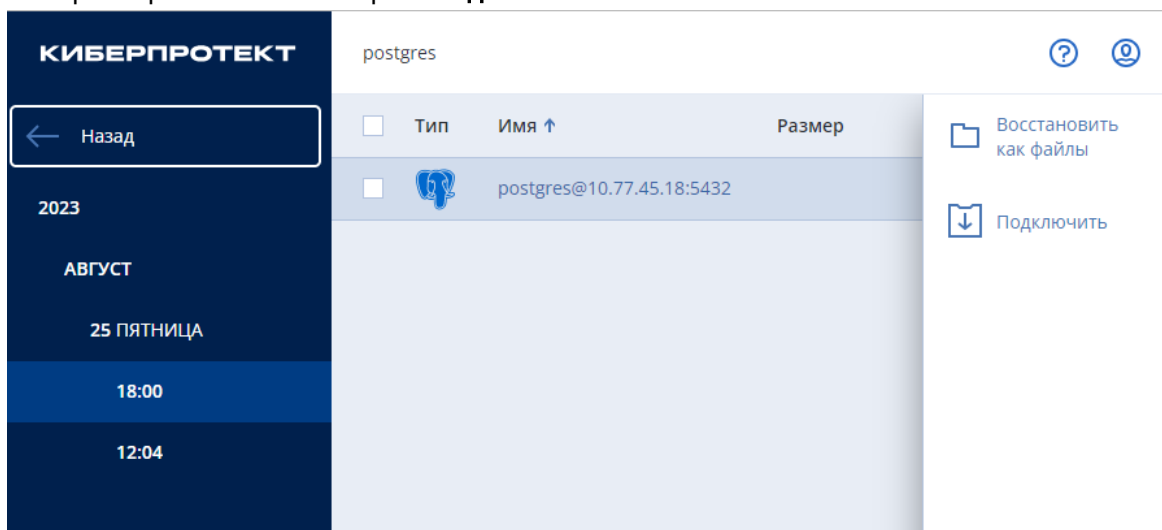
1. Перейдите в **Устройства > PostgreSQL**.
2. Выберите экземпляр PostgreSQL, который нужно подключить.
3. Перейдите на вкладку справа **Восстановление**.

Примечание

Либо перейдите в **Хранилище резервных копий**, выберите необходимое хранилище и перейдите на вкладку справа **Показать резервные копии**.

4. Выберите нужный архив для подключения и нажмите **Восстановить данные PostgreSQL**.

5. Выберите архив и нажмите справа **Подключить**.



6. Проверьте настройки и нажмите **Монтировать**.
7. Подключитесь к восстановленной базе данных и совершите необходимые действия средствами PostgreSQL.
8. Перейдите в **Панель Мониторинга > Действия** и выберите операцию подключения базы данных. Прервите подключение архива базы данных.

8 Восстановление баз данных PostgreSQL

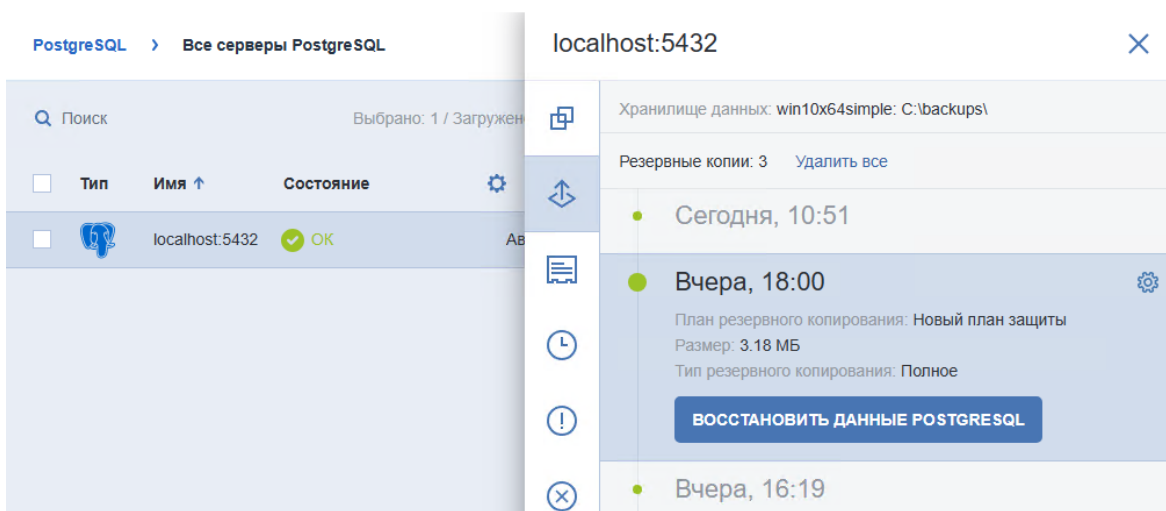
Для восстановления всего экземпляра базы данных PostgreSQL:

1. Перейдите в **Устройства > PostgreSQL**.
2. Выберите экземпляр PostgreSQL, который нужно восстановить.
3. Перейдите на вкладку справа **Восстановление**.

Примечание

Либо перейдите в **Хранилище резервных копий**, выберите необходимое хранилище и перейдите на вкладку справа **Показать резервные копии**.

4. Выберите нужную копию для восстановления и нажмите **Восстановить данные PostgreSQL**.



5. Выберите архив и нажмите справа **Восстановить как файлы**.
6. Выберите место для восстановления файлов, проверьте остальные настройки и нажмите **Начать восстановление**.

Ход выполнения восстановления показан на вкладке **Действия**.

8.1 Гранулярное восстановление отдельных баз данных PostgreSQL

Гранулярное восстановление доступно только для баз данных PostgreSQL, установленных на машинах под управлением ОС Linux. Доступно восстановление отдельных баз данных из единого архива резервной копии.

8.1.1 Предварительные требования

- Для возможности гранулярного восстановления на машину с агентом PostgreSQL необходимо установить [библиотеку libfuse](#).

Для восстановления отдельных баз данных PostgreSQL:




1. Перейдите в **Устройства > PostgreSQL**.
2. Выберите экземпляр PostgreSQL, из которого вы хотите восстановить базы данных.
3. Перейдите на вкладку справа **Восстановление**.



Примечание

Либо перейдите в **Хранилище резервных копий**, выберите необходимое хранилище и перейдите на вкладку справа **Показать резервные копии**.

4. Нажмите на имя резервной копии и выберите необходимые для восстановления базы из архива.

postgres > postgres@10.77.45.18:5432 ? ?

<input type="checkbox"/>	Тип	Имя ↑	Размер
<input checked="" type="checkbox"/>		d1	8.27 МБ
<input checked="" type="checkbox"/>		d1-r1	8.27 МБ
<input type="checkbox"/>		postgres	8.33 МБ

 **Восстановить**
 **Восстановить в dump-файл**

5. Выберите способ восстановления:
 - Если необходимо сразу восстановить выбранные базы из архива, нажмите справа **Восстановить**.
 - Если необходимо сохранить выбранные базы из архива в отдельные dump-файлы, нажмите справа **Восстановить в dump-файл**.
6. [Если выбрано восстановление баз из архива] Укажите следующие настройки:
 - Выберите время восстановления. Можно оставить время создания резервной копии или указать время с момента создания резервной копии.
 - Экземпляр базы данных PostgreSQL, куда будет происходить восстановление.

Примечание

Версия экземпляра PostgreSQL, куда будет происходить восстановление, должна быть не ниже восстанавливаемой. Редакции экземпляров баз данных должны совпадать. Экземпляр базы данных, созданный из кластеризованного экземпляра, можно восстановить на некластеризованный экземпляр и наоборот.

- Для каждой выбранной базы из архива укажите место для восстановления. Возможные варианты: в исходную базу, в новую базу.
7. [Если выбрано сохранение баз данных в dump-файлы] Укажите следующие настройки:
 - Выберите время восстановления. Можно оставить время создания резервной копии или указать время с момента создания резервной копии.

- Место хранения dump-файлов.
8. Нажмите **Начать восстановление**.
 9. [Если выбрано восстановление в исходную базу данных] Укажите порядок восстановления баз данных и нажмите **Начать восстановление**.

Окончательная проверка

Выбранные базы будут восстановлены в Исходный экземпляр (10.77.243.76:5432).

☒ Перезаписать существующие базы

☐ Не перезаписывать существующие базы

Удалить целевую базу до или после восстановления:

☐ Перед восстановлением

☒ После восстановления (рекомендовано) ⓘ

НАЧАТЬ ВОССТАНОВЛЕНИЕ **ОТМЕНА**

Ход выполнения восстановления показан на вкладке **Действия**.

9 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.
- Не поддерживается гранулярное восстановление на машинах под управлением ОС Windows.
- Не поддерживается гранулярное восстановление для резервных копий на ленточных накопителях.

10 Известные проблемы и их решения

10.1 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.

10.2 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_dsuqc5akrjsln9fhr6srg')
```

10.3 Подключение экземпляра PostgreSQL из архива в ОС Astra Linux Special Edition

В ОС Astra Linux Special Edition при подключении экземпляра PostgreSQL из архива могут возникнуть следующие ошибки:

- An error occurred while executing PostgreSQL processes: RunMountedRestore() failed: instance mounter recover PITR at time 0: run postgresql command '/usr/lib/postgresql/11/bin/postgres --single --config-file=/tmp/64c64694-9fa8-64e4-64b0-64204b6403a2/storage/postgresql.conf postgres': exit status 1. The log is available at '/opt/acronis/var/log/dsp.database.pg/postgres.restore.64c64694-9fa8-64e4-64b0-64204b6403a2.log'.
- RunMountedRestore() failed: instance mounter recover PITR at time 0: run postgresql command '/usr/lib/postgresql/11/bin/postgres --single --config-file=/tmp/64c64694-9fa8-64e4-64b0-64204b6403a2/storage/postgresql.conf postgres': exit status 1"
- postgres.recover: postgres does not know where to find the "audit" configuration file.
- postgres.recover: This can be specified as "ac_audit_file" in "/tmp/64c64694-9fa8-64e4-64b0-64204b6403a2/storage/postgresql.conf", or by the -D invocation option, or by the PGDATA environment variable.

При подключении архива на машине с агентом PostgreSQL создается экземпляр PostgreSQL. Для запуска экземпляра используется конфигурационный файл postgresql.conf, создаваемый агентом на основе шаблона. Проблема возникает из-за того, что этот конфигурационный файл не содержит параметров ac_audit_mode и ac_audit_file, которые необходимы для запуска PostgreSQL в ОС Astra Linux Special Edition (в стандартной версии PostgreSQL эти параметры не используются).

Решение

1. Узнайте мажорную версию PostgreSQL, установленную на машине с агентом:
 - а. Просмотрите файл /opt/acronis/var/dsp.database.pg/postgresql-agent.json и из значения параметра server.recovery_instance.binaries получите путь к исполняемому файлу postgres, например:

```
# cat /opt/acronis/var/dsp.database.pg/postgresql-agent.json
{
  "server": {
    "recovery_instance": {
      "run_as_user": "postgres",
      "binaries": ["/usr/lib/postgresql/11/bin/postgres"]
    }
  }
}
```

- b. Узнайте версию PostgreSQL, запустив `postgres` с параметром `--version`, например:

```
# /usr/lib/postgresql/11/bin/postgres --version
(PostgreSQL) 11.21 (Debian 1:11.21-astra.se6+ci1)
```

В этом примере 11 – это мажорная версия PostgreSQL.

2. Добавьте необходимые для запуска PostgreSQL параметры в шаблон `/opt/acronis/etc/dsp.database.pg/postgresql.<major_version>.conf`, который соответствует мажорной версии установленной СУБД PostgreSQL:

```
ac_audit_mode = 'none'
ac_audit_file = "
<...>
```

Указатель

В

Введение 4

Восстановление баз данных PostgreSQL 17

Г

Гранулярное восстановление отдельных баз данных PostgreSQL 17

З

Заявление об авторских правах 3

И

Известные проблемы и их решения 21

Н

Настройка аутентификации в PostgreSQL 8

Необходимые компоненты программы 7

О

Ограничения 20

П

Подготовка к установке программы 7

Поддерживаемые версии PostgreSQL 6

Поддерживаемые операционные системы 5

Подключение экземпляра PostgreSQL из архива 15

Предварительные требования 7, 15, 17

Р

Резервное копирование PostgreSQL 13

У

Установка и настройка программы 12