



SberCloud

Cloud Backup and Recovery

Часто задаваемые вопросы (FAQ)

ВЕРСИЯ 1.0

ОТ 18 ЯНВАРЯ 2020 Г



Оглавление

ТОВАРНЫЕ ЗНАКИ	4
ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ	5
ОБЩИЕ ВОПРОСЫ	6
Что собой представляет услуга резервного копирования?	6
Что такое полное резервное копирование и инкрементное резервное копирование?	6
В чем разница между резервным копированием и аварийным восстановлением?	7
В чем разница между резервным копированием и снимками?	8
Нужно ли остановить сервер, чтобы выполнить резервное копирование?	9
Как можно определить, каким образом было произведено копирование: вручную или автоматически?	9
Можно ли сделать резервную копию определенной части диска?	9
Можно ли сделать резервную копию нужного диска?	10
Где хранятся созданные копии?	10
Можно ли экспортировать резервную копию на другой сервер?	10
Можно ли скачать резервную копию диска или сервера на локальный компьютер?	10
ВОССТАНОВЛЕНИЕ ДАННЫХ	11
Нужно ли останавливать сервер для восстановления данных?	11
Можно ли использовать резервную копию системного диска для восстановления ECS?	11
Нужно ли останавливать сервер перед восстановлением данных?	11
Можно ли восстановить сервер, после того как он был изменен?	12
Можно ли восстановить диск, если емкость была увеличена?	12
Есть ли ограничения в количестве резервных копий?	12
Сколько стоит услуга резервного копирования?	12
ПОЛИТИКА РЕЗЕРВНОГО КОПИРОВАНИЯ	13
Как можно настроить автоматическое копирование сервера или диска?	13
Как можно сделать резервную копию нескольких серверов за один раз?	13
Почему правило хранения резервных копий не вступает в действие сразу после изменений?	14
ТАРИФИКАЦИЯ	16
Из чего складывается стоимость сервиса CRB?	16



Как отключить сервис резервного копирования?	16
ТЕХНИЧЕСКАЯ ПОДДЕРЖКА.....	17
ОТЗЫВЫ И ПОЖЕЛАНИЯ.....	18



ТОВАРНЫЕ ЗНАКИ

Linux® – товарный знак Linus Torvalds.

Windows®, Excel® – товарные знаки Microsoft Corporation.

CentOS® – товарный знак Red Hat, Inc.

CoreOS® – товарный знак CoreOS, Inc.

Debian® – товарный знак Software in the Public Interest, Inc.

EulerOS® – товарный знак Huawei Technologies Co., Ltd.

Fedora® – товарный знак Red Hat, Inc.

OpenSUSE® – товарный знак Suse Ltd.

Ubuntu® – товарный знак Canonical Ltd.

Red Hat® – товарный знак Red Hat, Inc.

Mac® – товарный знак Apple Inc.



ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

Термин/сокращение	Определение
ECS	Облачный Сервер (<i>Elastic Cloud Server</i>)
VM	Виртуальная Машина
vCPU	Виртуальный Процессор (<i>Virtual Central Processor Unit</i>)
OS	Операционная Система
VPC	Облачная выделенная сеть (<i>Virtual Private Cloud</i>)
Security Group	Группа Безопасности
EIP	Внешний IP (<i>Elastic IP</i>)
NIC	Сетевой Адаптер (<i>Network Interface Controller</i>)
Bandwidth	Пропускная способность
Key Pair	Ключевая Пара
Instance	Синоним слова «виртуальная машина»
Outbound traffic	Исходящий трафик
Inbound traffic	Входящий трафик
Default security group	Группа безопасности по умолчанию
AZ	Зона доступности (<i>Availability Zone</i>)
Subnet	Подсеть
ELB	Балансировщик нагрузки (<i>Elastic Load Balancer</i>)
VPN	Виртуальная частная сеть (<i>Virtual Private Network</i>)
ЦОД	Центр обработки данных (<i>Data Center</i>)
CBR	Сервис для резервного копирования и восстановления данных (<i>Cloud Backup and Recovery</i>)
Backup Vault	Хранилище для резервных копий
Retention rule	Правило хранения резервных копий



ОБЩИЕ ВОПРОСЫ

Что собой представляет услуга резервного копирования?

Услуга резервного копирования предоставляется сервисом Cloud Backup and Recovery (CBR). CBR позволяет выполнить резервное копирование облачных дисков и серверов. Это предотвращает потерю данных при вирусных атаках, случайных удалениях информации, а также при программном или аппаратном сбое.

Сервис включает в себя:

- **резервные копии** (*backups*) – обеспечивают сохранность данных серверов и дисков на основе технологии снимков (*snapshots*);
- **хранилища** (*vaults*) – CBR использует хранилища для агрегирования резервных копий;
- **политику резервного копирования** (*backup policies*) – применяется для выполнения автоматического копирования в определенные временные интервалы, также содержит правила хранения созданных копий.

Что такое полное резервное копирование и инкрементное резервное копирование?

После первого полного резервного копирования система будет производить инкрементное резервное копирование по умолчанию:

- Первое полное резервное копирование охватит только используемое пространство диска. Например, если из 100 Гб дискового пространства занято только 40 Гб, то первая резервная копия займет 40 Гб.



- Следующие копии будут инкрементными, т. е. записываться будут только изменения с момента последней резервной копии. Например, если с момента последнего резервного копирования изменилось 5 Гб данных, то ровно столько данных и будет изменено.

В чем разница между резервным копированием и аварийным восстановлением?

Основные различия между резервным копированием и аварийным восстановлением перечислены в Таблице 1.

Таблица 1. Разница между резервным копированием и аварийным восстановлением

Вопрос	Резервное копирование	Аварийное восстановление
Назначение	Для предотвращения потери данных. Использует техники снимков (<i>snapshots</i>) или резервного копирования для создания резервных копий, которые могут быть использованы для восстановления данных	Для обеспечения непрерывности работы системы. Использует технику репликации (<i>replication</i>) для создания данных, которые будут использованы в случае неисправности
Сценарий использования	Защита от случайного удаления, программных и аппаратных сбоев, восстановление после вирусных атак	Позволяет быстро восстанавливать сервис после программных и аппаратных сбоев, а также стихийных бедствий
Стоимость	От 1 до 2 % от стоимости содержания основной системы	От 20 до 100 % от стоимости содержания основной системы



В чем разница между резервным копированием и снимками?

Основные различия между резервным копированием и снимками перечислены в Таблице 2.

Таблица 2. Разница между резервным копированием и снимками

Вопрос	Хранение	Синхронизация данных	Восстановление
Резервное копирование	Резервные копии хранятся в объектном хранилище (в сервисе OBS), а не на EVS дисках. Это обеспечивает восстановление данных при потере или повреждениях на диске	Резервное копирование – это копия данных на определенный момент времени. CBR поддерживает автоматическое копирование, которое определяется политикой копирования. При удалении диска данные резервного копирования сохраняются	Данные резервного копирования используют для восстановления исходного диска или для создания нового
Снимки	Снимки хранятся на EVS дисках (блочное хранилище). Создание снимков занимает немного времени	Снимок – это состояние диска на определенный момент времени. При удалении диска снимки удаляются	Снимки используют для восстановления исходного диска или чтобы создать диск для восстановления данных



Нужно ли остановить сервер, чтобы выполнить резервное копирование?

Нет, не нужно. Сервис CBR позволяет проводить резервное копирование на работающем сервере. Если в это время производятся изменения, то вновь созданные данные хранятся в памяти сервера в виде кэша (*cache*). Кэш не будет записан в резервную копию и, таким образом, будет разница между данными на сервере и резервными данными.

Чтобы обеспечить целостность данных, рекомендуется создавать резервную копию сервера в нерабочее время. При необходимости включите функцию автоматического резервного копирования базы данных.

Как можно определить, каким образом было произведено копирование: вручную или автоматически?

Это можно определить по префиксу:

- Автоматическое резервное копирование: ***autobk_xxxx***;
- Ручное резервное копирование: ***manualbk_xxxx*** или *имя, указанное пользователем*.

Можно ли сделать резервную копию определенной части диска?

Нет, нельзя.



Можно ли сделать резервную копию нужного диска?

Да, в сервисе CBR есть такая функция.

Где хранятся созданные копии?

Копии хранятся в объектном хранилище – Object Storage Service (OBS).

Можно ли экспортировать резервную копию на другой сервер?

Да, можно. Для этого создайте новый диск используя резервную копию, после чего прикрепите данный диск к нужному серверу.

Можно ли скачать резервную копию диска или сервера на локальный компьютер?

Нет, нельзя.



ВОССТАНОВЛЕНИЕ ДАННЫХ

Нужно ли останавливать сервер для восстановления данных?

Перед восстановлением данных сервер будет автоматически остановлен, а затем, после завершения восстановления, запущен.

Если деактивировать чек-бокс **Start the server immediately after restoration**, то, после завершения процедуры восстановления, сервер нужно будет запустить вручную.

Можно ли использовать резервную копию системного диска для восстановления ECS?

Да, можно. Однако, перед восстановлением, нужно открепить системный диск от ECS.

Можно также использовать резервную копию системного диска для создания новых дисков, но диски, созданные таким образом, нельзя использовать как системные.

Нужно ли останавливать сервер перед восстановлением данных?

Да, нужно. Сделайте следующее:

1. Остановите сервер (статус **Stopped**).
2. Открепите диск от сервера.
3. После восстановления данных прикрепите диск к серверу.
4. Запустите сервер (статус **Running**).



Можно ли восстановить сервер, после того как он был изменен?

Да, можно. Даже после того, как к серверу подключили новые диски или изменили существующие, сервер можно восстановить.

Если диск был добавлен после резервного копирования, то восстановление данных не изменит информацию на новом диске.

Если диск был удален после резервного копирования, то данные на сервер восстановятся без удаленного диска.

Можно ли восстановить диск, если емкость была увеличена?

Да, можно, но после восстановления данных емкость диска уменьшится до его размеров на момент резервного копирования.

Есть ли ограничения в количестве резервных копий?

Нет. Можно создавать и хранить столько копий, сколько требуется.

Сколько стоит услуга резервного копирования?

Сервис CBR бесплатен. Плата взимается только за дисковое пространство, на котором хранятся созданные копии.



ПОЛИТИКА РЕЗЕРВНОГО КОПИРОВАНИЯ

Как можно настроить автоматическое копирование сервера или диска?

Правила автоматического копирования и хранения данных определяются в политике резервного копирования. Чтобы ее настроить сделайте следующее:

1. Перейдите в сервис CRB: консоль управления > **Storage** > **Cloud Backup and Recovery**.
2. Для серверов: в разделе **Cloud Server Backup** нажмите кнопку **Create Server Backup Vault**. Для дисков: в разделе **Disk Backup** нажмите кнопку **Create Disk Backup Vault**.
3. Прикрепите нужные серверы (или диски) во время или после создания **Backup Vault**.
4. После того, как нужные ресурсы прикреплены, перейдите в пункт меню слева **Policies**. Создайте и настройте политику автоматического копирования.
5. Прикрепите политику копирования к нужному **Backup Vault**. Система будет производить резервное копирование и управление копиями автоматически, в соответствии с настроенной политикой.

Как можно сделать резервную копию нескольких серверов за один раз?

Нужно сделать следующее:

1. Перейдите в сервис CRB: консоль управления > **Storage** > **Cloud Backup and Recovery**.



2. В разделе **Cloud Server Backup** нажмите кнопку **Create Server Backup Vault**. Рекомендуемая емкость хранилища – на 20% больше суммарной емкости всех серверов.
3. Прикрепите нужные сервера.
4. После создания **Backup Vault** в строке с нужным хранилищем нажмите **More > Perform Backup**. Здесь можно выполнить резервное копирование двух и более серверов. Также, для данного хранилища, можно прикрепить политику резервного копирования, чтобы копирование прикрепленных серверов происходило по определенному графику.

Почему правило хранения резервных копий не вступает в действие сразу после изменений?

Правило хранения резервных копий (*retention rule*) может не сразу вступить в силу в следующих ситуациях:

1. Изменилось только количество резервных копий. Правило вступит в силу при выполнении следующего резервного копирования.
2. Правило изменилось с количества сохраняемых копий на время, которое копии должны храниться в системе. Новое правило хранения будет действовать только для новых копий. Резервные копии, созданные при прежней политике, нужно, если требуется, удалить вручную.
3. Правило остается для сохранения копий в определенном временном периоде, но изменяется сам период времени. Новое правило хранения будет действовать только для новых копий. Резервные копии, созданные при прежней политике, нужно, если требуется, удалить вручную.
4. Правило изменилось с времени хранения на количество сохраненных



копий. Новое правило хранения будет действовать только для новых копий. Резервные копии, созданные при прежней политики, нужно, если требуется, удалить вручную.



ТАРИФИКАЦИЯ

Из чего складывается стоимость сервиса CRB?

Стоимость сервиса CBR зависит от объема потребляемого дискового пространства.

Как отключить сервис резервного копирования?

Если резервные копии больше не требуются, то нужно удалить хранилища (vaults), в которых хранятся копии. Для этого сделайте следующее:

1. Перейдите в сервис CRB: консоль управления > **Storage** > **Cloud Backup and Recovery**.
2. Для серверов: в разделе **Cloud Server Backup** нажмите кнопку **Create Server Backup Vault**. Для дисков: в разделе **Disk Backup** нажмите кнопку **Create Disk Backup Vault**.
3. Активируйте чек-боксы тех хранилищ, которые нужно удалить.
4. Нажмите кнопку **Delete**.

Если хранилище не может быть удалено, проверьте использовалась ли резервная копия для создания образа (image), если да – требуется удаление данного образа в сервисе Image Management Service (IMS).



ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Специалисты Контакт-центра круглосуточно готовы ответить на вопросы о работе облачного сервиса от SberCloud.

Контакты:

- e-mail support@sbercloud.ru;
- тел. 8-800-444-24-99 (звонок из России бесплатный).



ОТЗЫВЫ И ПОЖЕЛАНИЯ

Отзывы об услуге и ваши пожелания направляйте на support@sbercloud.ru.



Тел: + 8 800 444-24-99
E-mail: support@sbercloud.ru