КИБЕРПРОТЕКТ

cyberprotect.ru

Кибер Инфраструктура

4.7

Руководство по быстрому старту Backup Gateway для Amazon S3 и EC2

РЕДАКЦИЯ: 11.04.2022

Заявление об авторских правах

С ПО или Услугой может быть предоставлен исходный код сторонних производителей. Лицензии этих сторонних производителей подробно описаны в файле license.txt, находящемся в корневом каталоге установки.

Оглавление

1 О кратком руководстве BackupGateway для Amazon

В этом руководстве объясняется, как настроить Backup Gateway для хранения резервных копий в облаке Amazon.

В общих чертах потребуется выполнить следующие действия.

1. Развернуть экземпляр с продуктом Кибер Инфраструктура из образа Amazon Machine Image (AMI) в Amazon EC2.
2. Получить пароль и выполнить вход на панель администрирования Кибер Инфраструктура.
3. Настроить Backup Gateway для работы с облаком Amazon.

Все эти шаги описываются в следующих главах.

Замечание

Общие задачи, связанные с Backup Gateway, описаны в следующих разделах руководства по быстрому старту Backup Gateway:

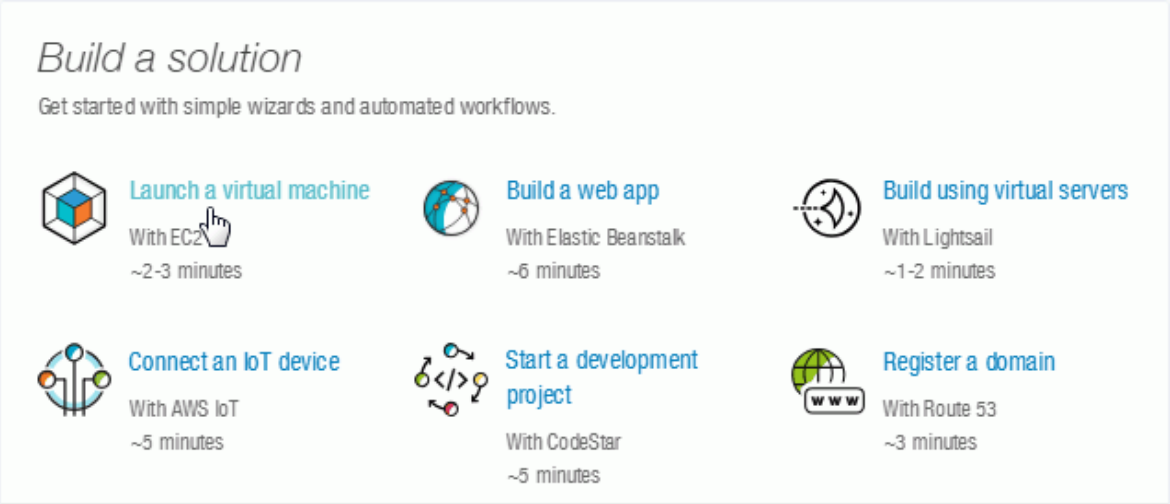
- Подключение к публичному облачному хранилищу через Backup Gateway
- Изменение схемы избыточности для Backup Gateway
- Мониторинг шлюза Backup Gateway
- Освобождение серверов от Backup Gateway

---

2 Запуск экземпляра

Сначала необходимо создать и запустить экземпляр с продуктом Кибер Инфраструктура. Выполните следующие действия.

1. На главной странице консоли AWS нажмите **Launch a virtual machine** (Запустить виртуальную машину) и выполните поиск «Кибер Инфраструктура» в каталоге AWS Marketplace.



2. Нажмите **Select** (Выбрать) рядом с найденным образом AMI.
3. На шаге 2 выберите для экземпляра тип **t2.large**.

Step 2: Choose an Instance Type

	Family	Type	vCPUs	Physical Processor	Memory (GiB)
☐	General purpose	t2.nano	1	Intel Xeon Family	0.5
☐	General purpose	t2.micro Free tier eligible	1	Intel Xeon Family	1
☐	General purpose	t2.small	1	Intel Xeon Family	2
☐	General purpose	t2.medium	2	Intel Broadwell E5-2686v4	4
☑	General purpose	t2.large	2	Intel Broadwell E5-2686v4	8

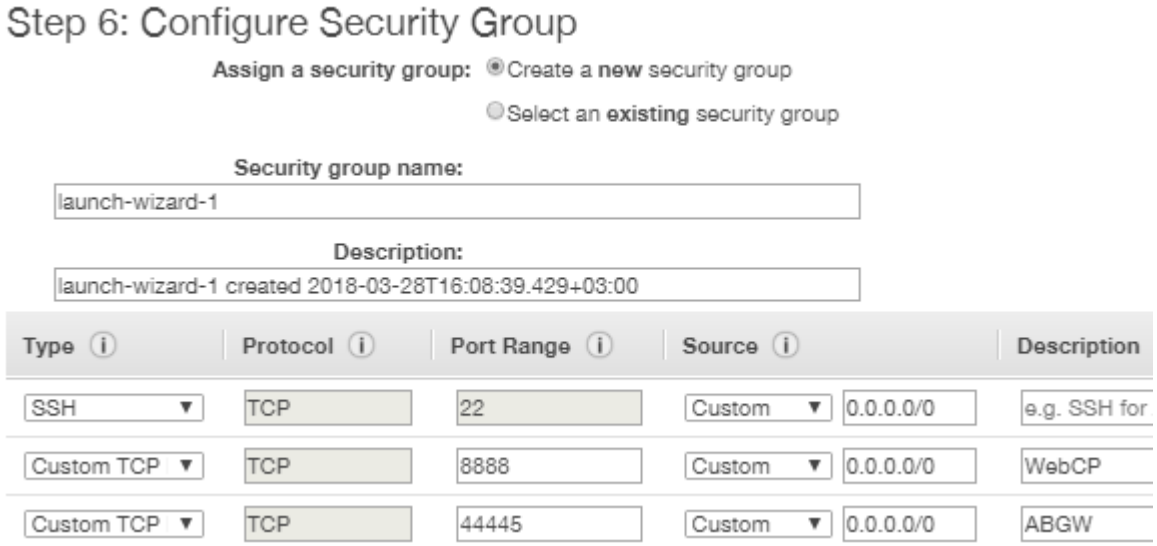
4. Шаги 3-5 – **Configure Instance Details** (Настройка сведений об экземпляре), **Add Storage** (Добавление хранилища) и **Add Tags** (Добавление тегов) – не являются обязательными. Их можно пропустить, нажав **Next** (Далее).

   Однако убедитесь, что в кластере хранилища, развернутом на экземпляре, достаточно логического пространства для промежуточного копирования (локального сохранения резервных копий перед отправкой в облако). Например, при ежедневном резервном

копировании обеспечьте достаточно места для резервных копий как минимум за 1,5 дня. Дополнительные сведения см. в разделе «Создание хранилища резервных копий в общедоступном облаке» руководства администратора.

5. На шаге 6 добавьте в новую группу безопасности два правила для открытия портов 8888 и 44445 в дополнение к порту 22, открытому по умолчанию. Порты 22 (SSH) и 8888 (панель администрирования) требуются для управления экземпляром и в целях безопасности должны быть открыты только узкому диапазону IP-адресов, с которых администратор будет обращаться к экземпляру. Порт 44445 необходим для получения трафика резервного копирования и подключения к облачной консоли управления, поэтому он должен быть открыт для всех IP-адресов.

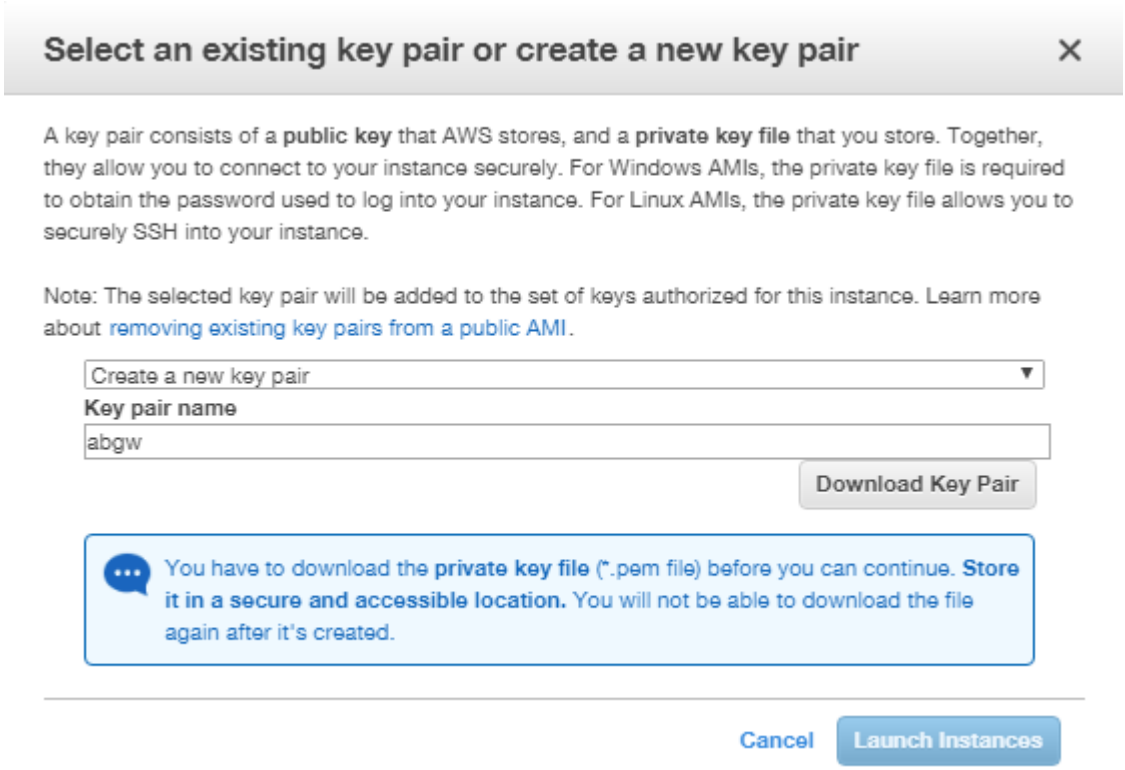
   Добавив правила, нажмите **Review and Launch** (Просмотреть и запустить).



6. На шаге 7 сформируйте новую пару ключей для доступа к экземпляру по SSH. Загрузите файл с парой ключей.

Важно

Сохраните ключ в безопасном месте: присвойте файлу ключ, который будет читаться только вами (например, chmod 400 <key_file> в Linux или Mac), и поместите его в каталог, к которому есть доступ только у вас (например, chmod 700 <dir> в Linux или Mac).



7. Нажмите **Launch Instance** (Запустить экземпляр).
8. Привяжите к экземпляру эластичный IP-адрес, как описано в Документации Amazon AWS. Это сделает экземпляр доступным из Интернета.

После запуска экземпляра доступ к нему можно получить по имени хоста, указанному в сведениях об экземпляре, например https://ec2-18-197-117-93.eu-central-1.compute.amazonaws.com.

3 Получение пароля и вход в продукт Кибер Инфраструктура

После запуска экземпляра необходимо получить пароль по умолчанию для панели администрирования продукта Кибер Инфраструктура, который хранится внутри экземпляра в каталоге /.initial-admin-password.

Чтобы получить доступ к файлу пароля на машине Linux или Mac

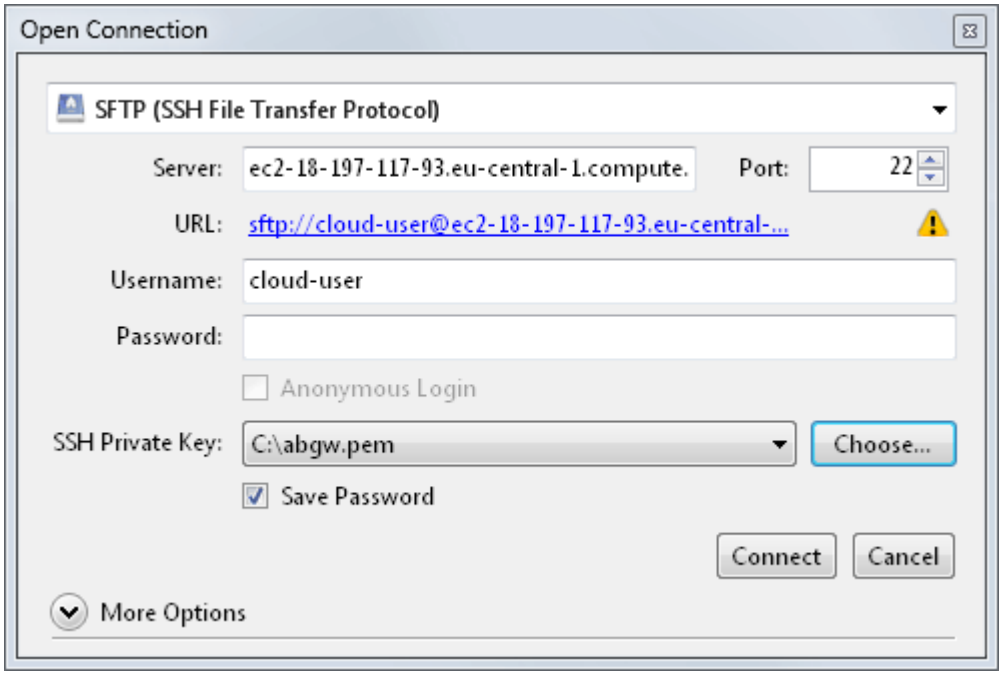
Используйте ранее созданный ключ, например:

```
# chmod 400 astor-23.pem
# ssh -i astor-23.pem cloud-user@ec2-18-197-117-93.\
eu-central-1.compute.amazonaws.com
# cat /.initial-admin-password
```

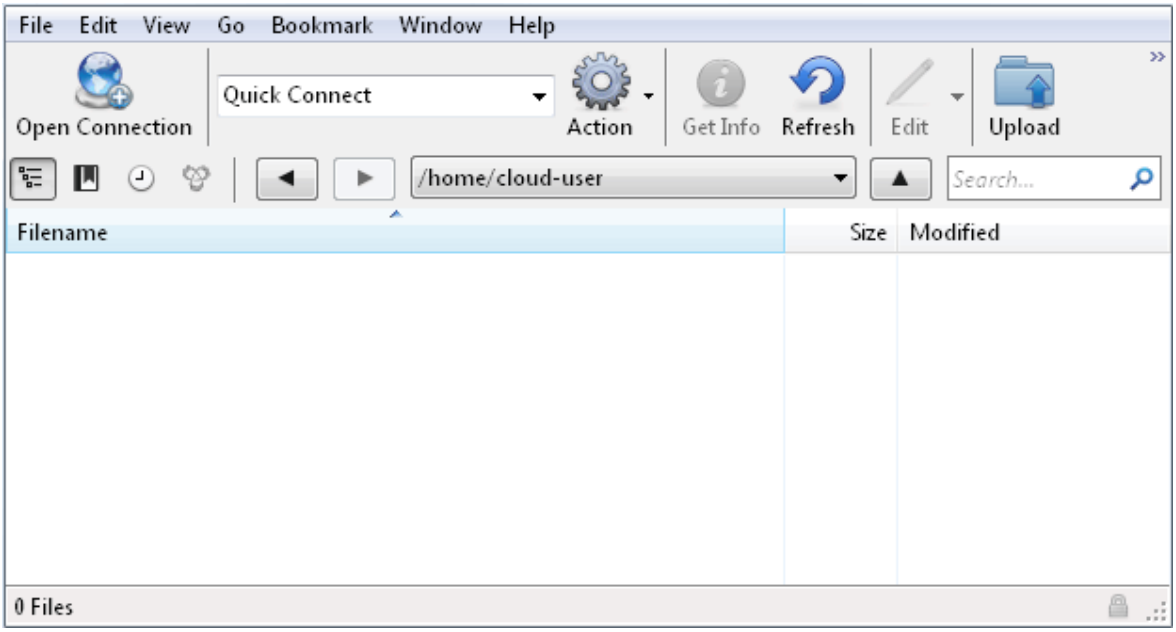
Чтобы получить доступ к файлу пароля на машине Windows или Mac

Используйте программу CyberDuck, например:

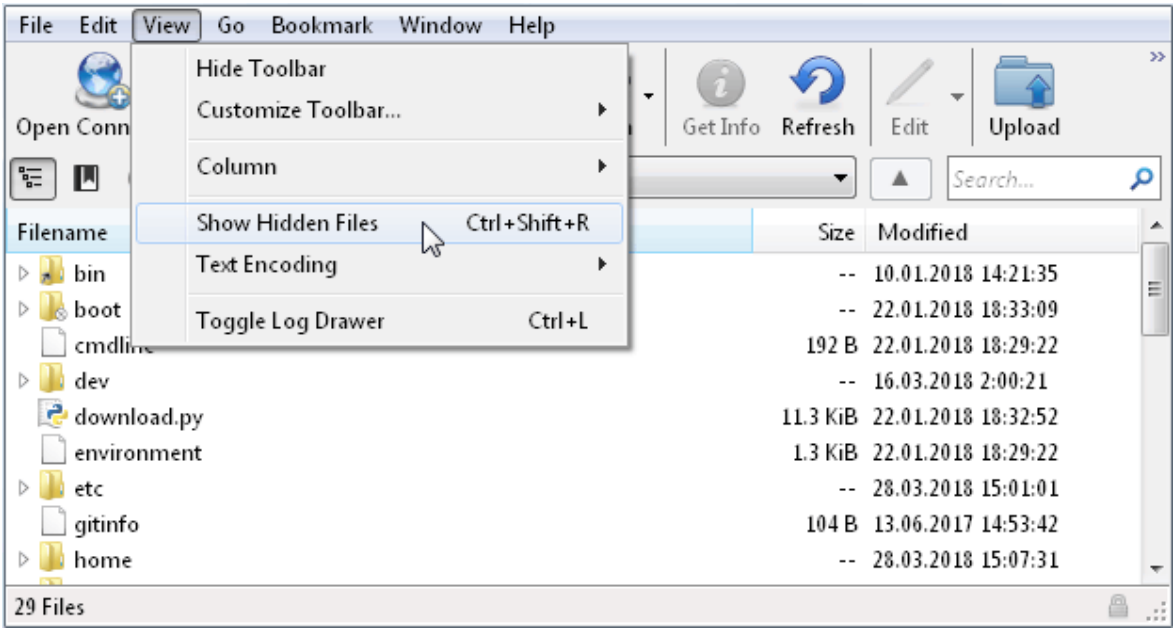
1. Нажмите **Новое подключение**.
2. Заполните сведения о подключении: выберите протокол **SFTP**, вставьте скопированное имя хоста экземпляра, введите имя пользователя **cloud-user**, а затем укажите созданный ранее ключ.



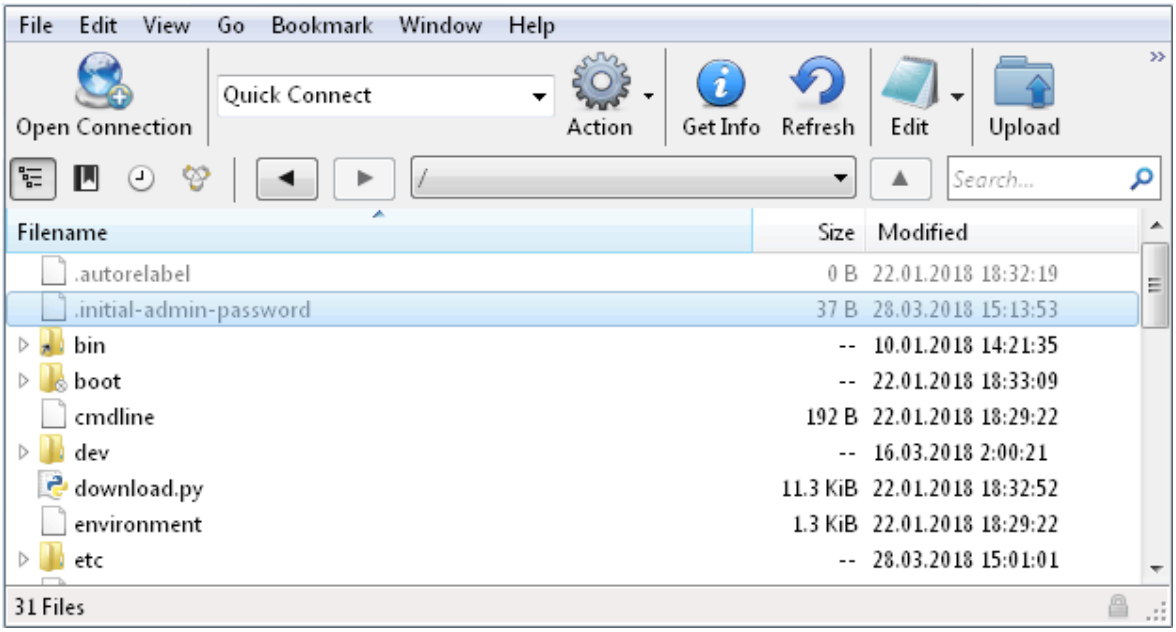
3. Нажмите **Подключиться** и примите отпечаток ключа сервера.
4. Перейдите в домашний каталог, то есть /home/cloud-user.



5. Файл пароля скрыт, поэтому нажмите **Вид** > **Показать скрытые файлы**, чтобы сделать его видимым в клиенте SFTP.



6. Загрузите и откройте файл пароля .initial-admin-password.



Чтобы выполнить вход на панели администрирования Кибер Инфраструктура

1. Найдите имя хоста экземпляра на порте 8888, например https://ec2-18-197-117-93.eu-central-1.compute.amazonaws.com:8888/.
2. Введите имя пользователя **admin** и полученный пароль.
3. Нажмите **Войти**.

Что дальше?

1. Желательно сменить пароль на такой, который вы сможете запомнить, но достаточно сложный, чтобы противостоять атаке методом полного перебора.
2. По умолчанию экземпляр будет использовать самозаверяющий сертификат, поэтому необходимо будет либо принять его в веб-браузере, либо загрузить действительный сертификат, выпущенный доверенным центром.
3. Обычно первым шагом после установки продукта Кибер Инфраструктура является создание кластера хранилища. Однако это делается автоматически при запуске экземпляра с продуктом Кибер Инфраструктура в Amazon EC2, поэтому можно приступать непосредственно к настройке Backup Gateway.

4 Настройка Backup Gateway

Резервные копии представляют собой холодные данные со специфической схемой доступа: к этим данным обращаются редко, но они должны быть немедленно доступны при обращении. Для этого сценария экономичным вариантом будут классы хранилищ, предназначенные для долгосрочного хранения редко используемых данных. Рекомендуемый класс хранилища для Amazon S3 – **Infrequent Access**.

Классы архивных хранилищ, такие как Amazon S3 Glacier, не могут использоваться для резервного копирования, поскольку не предоставляют мгновенного доступа к данным. Большая задержка при доступе (несколько часов) делает технически невозможным просмотр архивов, быстрое восстановление данных и создание инкрементных резервных копий. Хотя архивные хранилища, как правило, очень экономичны, следует учитывать, что существуют различные факторы, определяющие стоимость. В действительности общая стоимость публичного облачного хранилища складывается из платы за хранение данных, операции, трафик, извлечение данных, досрочное удаление и т. д. Например, сервис архивного хранилища может брать полугодовую стоимость хранения всего за одну операцию восстановления данных. Если предполагается более частый доступ к данным, то добавочные расходы значительно повышают общую стоимость хранилища. Чтобы избежать низкой скорости извлечения данных и сократить расходы, рекомендуем использовать Кибер Облачные Сервисы для хранения данных резервного копирования.

Ограничения

- При работе с публичным облаком Backup Gateway использует локальное хранилище для промежуточного копирования, а также для хранения служебной информации. Это означает, что данные, предназначенные для загрузки в публичное облако, сначала сохраняются локально и только после этого отправляются в место назначения. По этой причине для сохранности данных крайне важно, чтобы локальное хранилище было постоянным и избыточным. Использование временных дисков может привести к потере данных.
- Если вы планируете хранить резервные копии в облаке Amazon S3, учтите, что Backup Gateway может иногда блокировать доступ к таким резервным копиям до согласования облака Amazon S3. Это означает, что Amazon S3 может иногда возвращать устаревшие данные, поскольку системе требуется время, чтобы открыть доступ к последней версии данных. Backup Gateway определяет такие задержки и защищает целостность резервной копии, блокируя доступ на время обновления облака.
- Убедитесь, что в локальном кластере хранилища достаточно логического пространства для промежуточного копирования. Например, при ежедневном резервном копировании обеспечьте достаточно места для резервных копий как минимум на 1,5 дня. Если размер ежедневной резервной копии составляет 2 ТБ, необходимо как минимум 3 ТБ логического пространства. Требуемый объем неформатированного пространства будет различаться в зависимости от режима кодирования: 9 ТБ (3 ТБ на сервер) в режиме 1+2, 5 ТБ (1 ТБ на сервер) в режиме 3+2 и т. д.
- Для каждого кластера хранилища резервных копий требуется отдельный контейнер объектов.

- Чтобы увеличить пространство локального хранилища для Backup Gateway, добавьте один или несколько дисков в виртуальную машину. Не меняйте размер существующих дисков ВМ, поскольку это не будет обнаружено продуктом Кибер Инфраструктура.
- Чтобы можно было зарегистрировать Backup Gateway в Кибер Бэкап Облачный, для вашей партнерской учетной записи должна быть отключена двухфакторная проверка подлинности (2FA).
- Избыточность за счет репликации не поддерживается для хранилищ резервных копий.

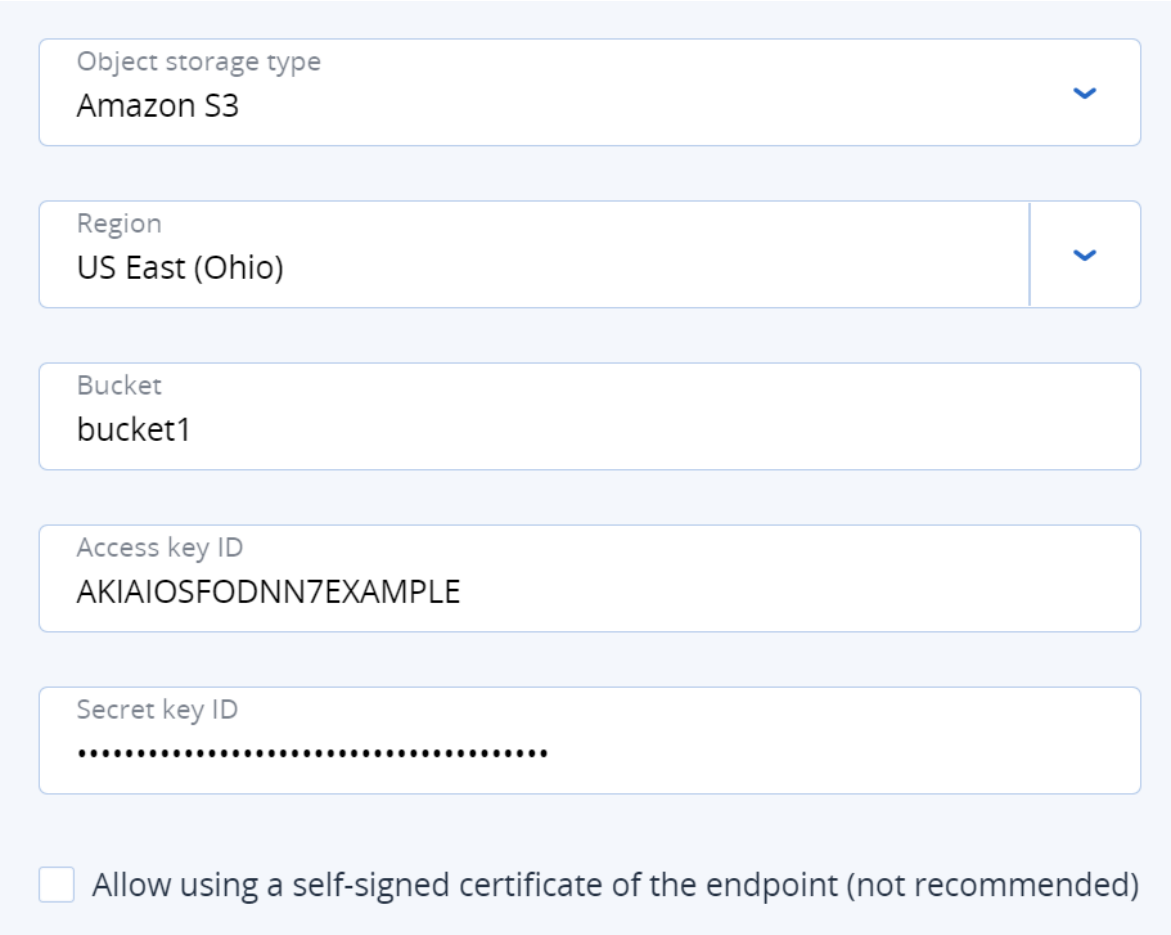
Предварительные требования

- В целевом хранилище достаточно места как для существующих, так и для новых резервных копий.
- Убедитесь, что на каждом сервере, который будет присоединен к кластеру хранилища резервных копий, открыт TCP-порт 44445 для исходящих подключений к Интернету, а также для входящих подключений от продукта Кибер Бэкап.

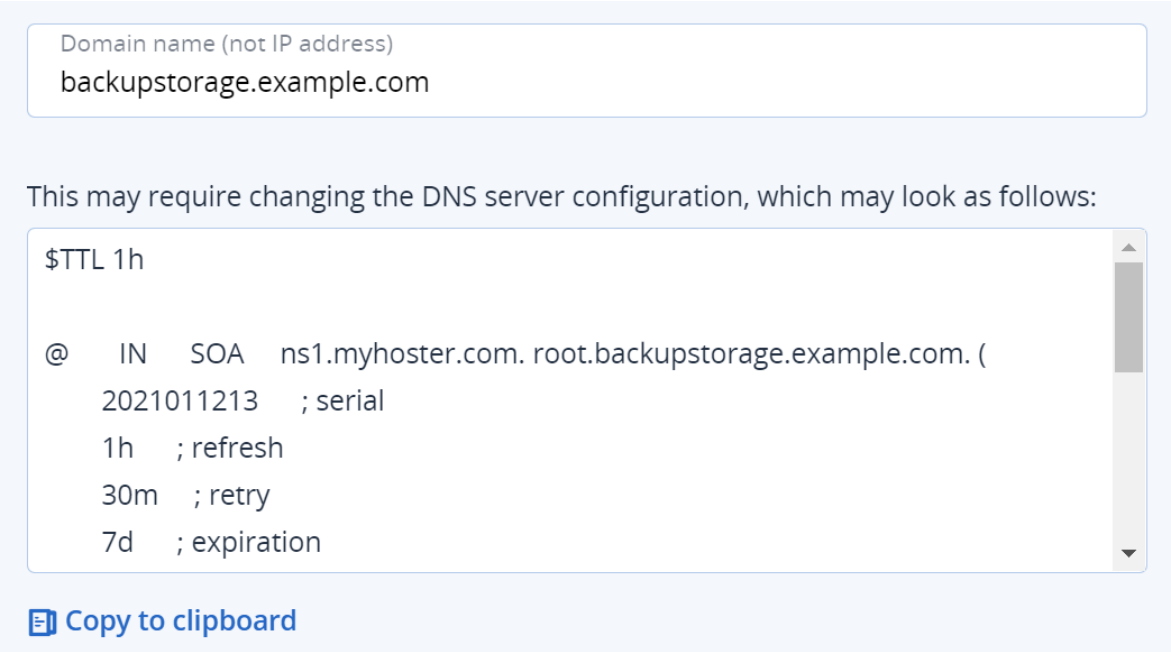
Чтобы настроить Backup Gateway

1. На экране **Инфраструктура** > **Сети** убедитесь, что в сети, которые вы собираетесь использовать, добавлены типы трафика **Резервное копирование (ABGW) внутр.** и **Резервное копирование (ABGW) внешн.**
2. Откройте экран **Сервисы хранения** > **Хранилище резервных копий** и нажмите **Создать хранилище резервных копий**.
3. На шаге **Место назначения резервной копии** выберите **Облачный сервис**.
4. На шаге **Серверы** выберите серверы, которые нужно добавить в кластер хранилища резервных копий, и нажмите **Далее**.
5. На панели **Облачный сервис** выберите **Amazon S3**, нужный регион, а также заполните информацию о ключах и корзине.

Важно
Указанная папка корзины должна быть доступна для записи.



6. На шаге **Политика хранилища** оставьте параметры избыточности без изменений.
7. На шаге **DNS** вставьте скопированное имя хоста экземпляра в поле **Доменное имя**.



8. На шаге **Учетная запись Киберпротект** укажите следующую информацию для вашего продукта Киберпротект:
   - URL-адрес портала управления облаком или имя хоста/IP-адрес и порт локального сервера управления (например, http://192.168.1.2:9877)
   - Данные партнерской учетной записи в облаке или учетные данные администратора организации на локальном сервере управления.
9. На шаге **Сводка** просмотрите конфигурацию и нажмите **Создать**.

После настройки Backup Gateway войдите в Кибер Бэкап Облачный и выполните тестовое резервное копирование в облако Amazon, чтобы убедиться, что все работает правильно.

5 Добавление дискового пространства в продукт Кибер Инфраструктура

Перед созданием новых дисков обратите внимание на следующие рекомендации по выбору размера.

- Если в кластере несколько серверов, они должны быть одинакового размера для эффективного обеспечения избыточности. В этом случае данные будут распределены по серверам более равномерно. Дополнительные сведения см. в разделе «Общие сведения о распределяемом дисковом пространстве» в руководстве администратора по командной строке.
- Одинаковый размер дисков помогает более равномерно распределять нагрузку. Внутри кластера диски используются пропорционально их размеру. Например, если у вас есть диск размером 10 ТБ и диск размером 2 ТБ, при загрузке кластера на 50 % на дисках будет использовано 5 и 1 ТБ соответственно.
- Производительность диска зависит от его объема. Как правило, чем больше емкость диска, тем выше производительность. Однако в некоторых случаях пропускная способность нескольких небольших дисков может превышать пропускную способность одного большого диска. Поэтому следует внимательно рассмотреть свои потребности и рекомендации поставщика облачных сервисов, такие как Типы томов Amazon EBS. Производительность дисков также зависит от типа экземпляра, как описано в разделе Экземпляры, оптимизированные для Amazon EBS.

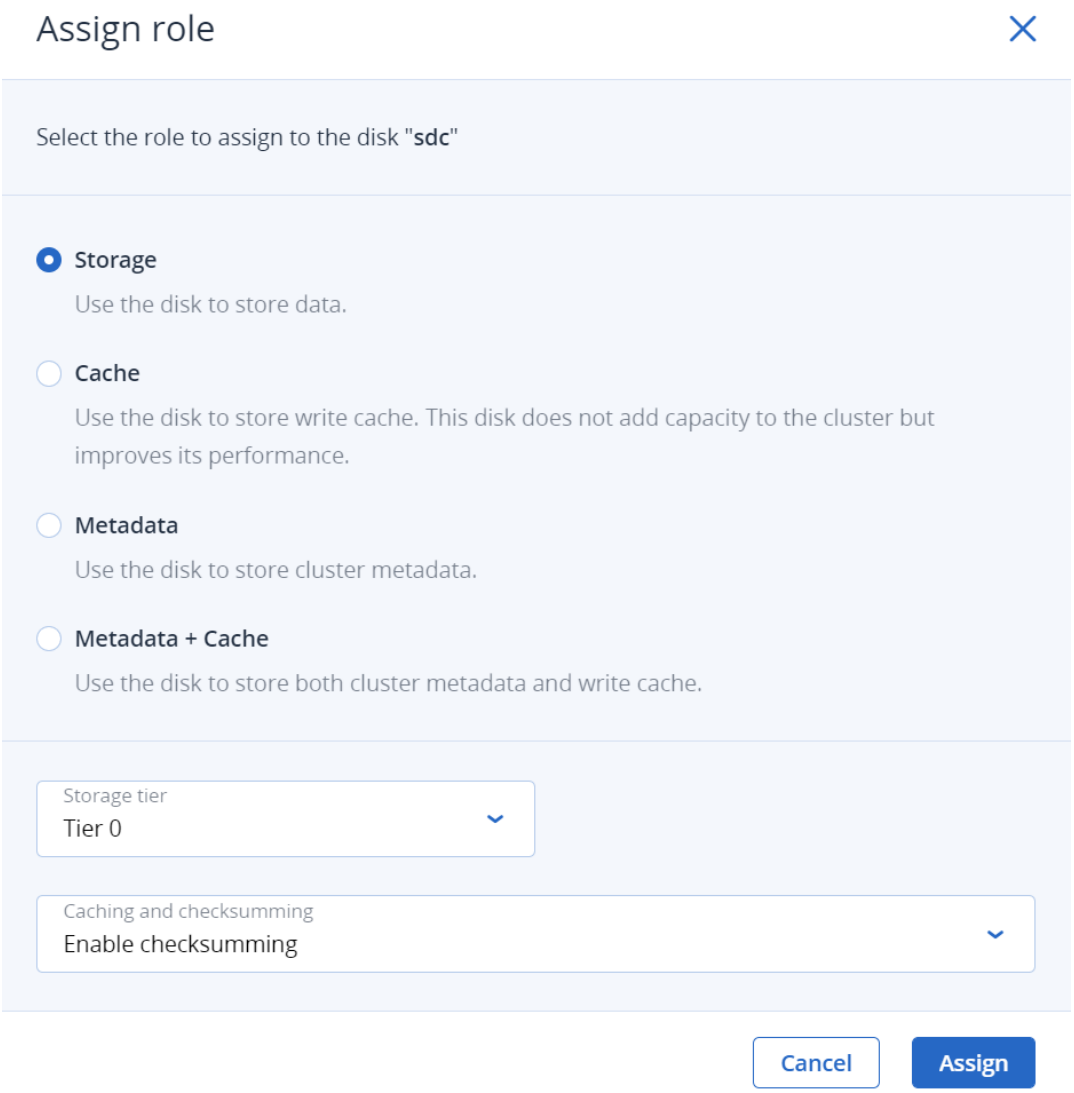
Если вы хотите увеличить физическое пространство в кластере хранилища, необходимо создать и присоединить новые тома Amazon EBS. Не используйте функцию **модификации томов** Amazon EBS на вашем экземпляре Кибер Инфраструктура, поскольку размер файловой системы не будет изменен соответствующим образом. Вместо этого создайте новый том Amazon EBS и присоедините его к экземпляру, как описано ниже.

Создайте пустой том EBS, как показано в разделе Создание тома Amazon EBS. Затем присоедините том к вашему экземпляру, как описано в разделе Присоединение тома Amazon EBS к экземпляру. После этого добавленный том будет отображаться в списке дисков сервера на панели администрирования продукта Кибер Инфраструктура.

Как настроить новый диск на панели администрирования

1. На экране **Инфраструктура** > **Серверы** щелкните по имени сервера с созданным диском. Перейдите на вкладку **Диски** для просмотра всех дисков сервера.
2. Щелкните по диску без роли, созданный ранее.
3. На правой панели диска нажмите **Назначить роль**.
4. В окне **Назначить роль** выберите роль **Хранилище**, укажите уровень хранилища и при необходимости включите проверку контрольных сумм. Дополнительные сведения см. в

разделе «Настройка новых дисков вручную» в руководстве администратора.



Также можно удалить виртуальный диск из виртуальной машины, как описано в разделе Отсоединение тома Amazon EBS от экземпляра.