Acronis

Acronis Инфраструктура 4.0

Backup Gateway Quick Start Guide for Amazon S3 and EC2

5 ноября 2020 г.

Заявление об авторских правах

Оглавление

ГЛАВА 1

Об этом руководстве

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

Все эти шаги описываются в следующих главах.

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

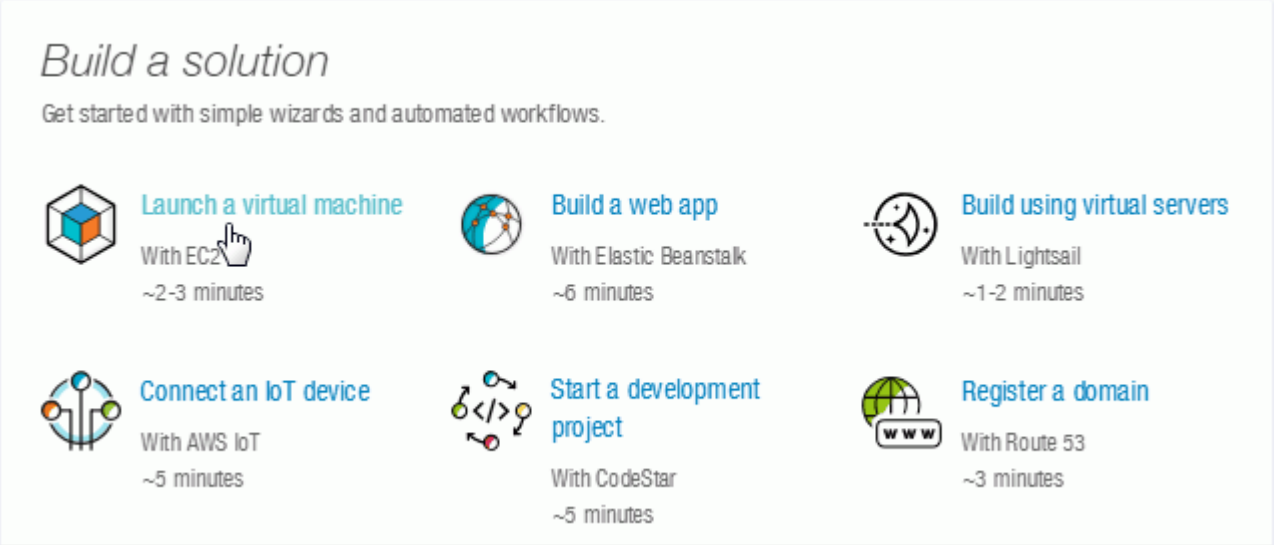
- Connecting to public cloud storage via Backup Gateway
- Migrating backups from older solutions
- Monitoring Backup Gateway
- Releasing nodes from Backup Gateway

ГЛАВА 2

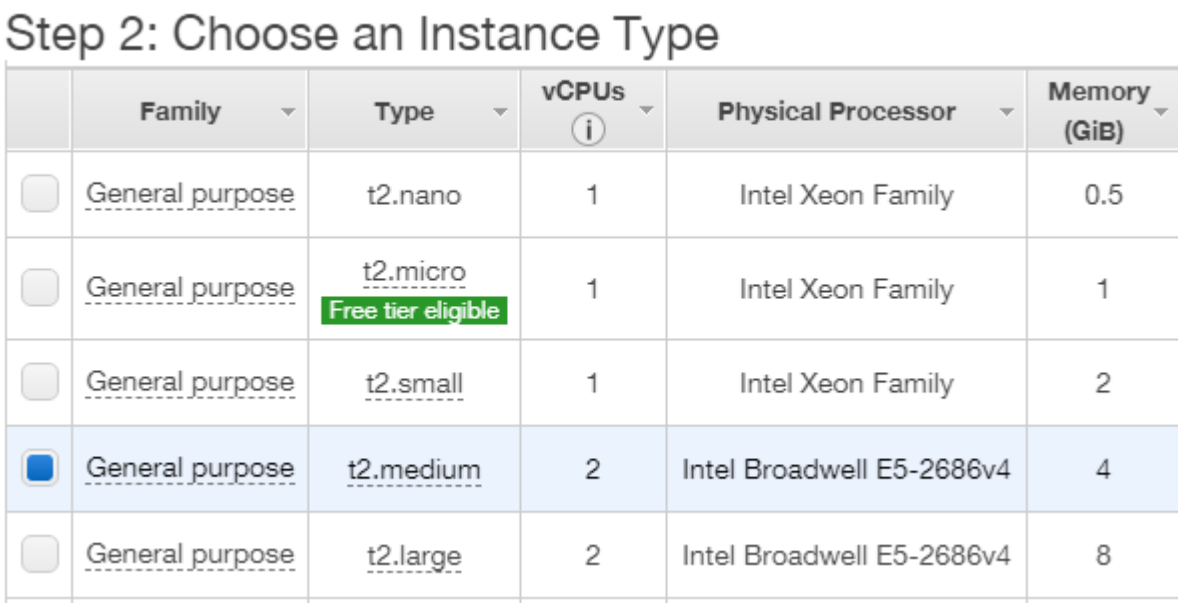
Запуск экземпляра

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

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



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

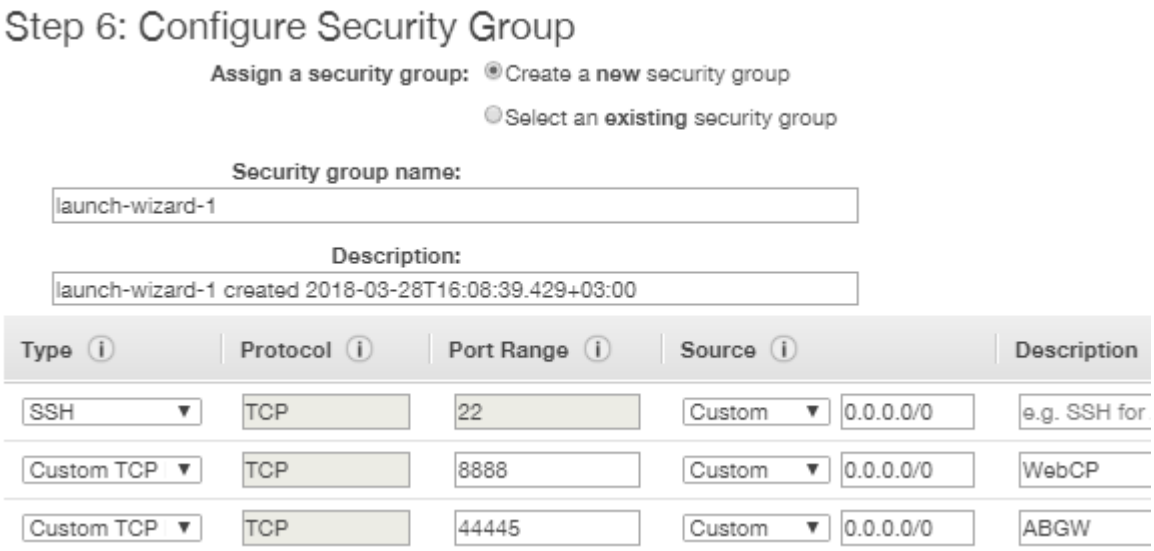


4. Шаги 3–5 — **Configure Instance Details** (Настройка сведений об инстансе), **Add Storage** (Добавление хранилища) и **Add Tags** (Добавление тегов) — не являются обязательными. Их можно пропустить, нажав **Next** (Далее).

   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 Connecting to public cloud storage via Backup Gateway.

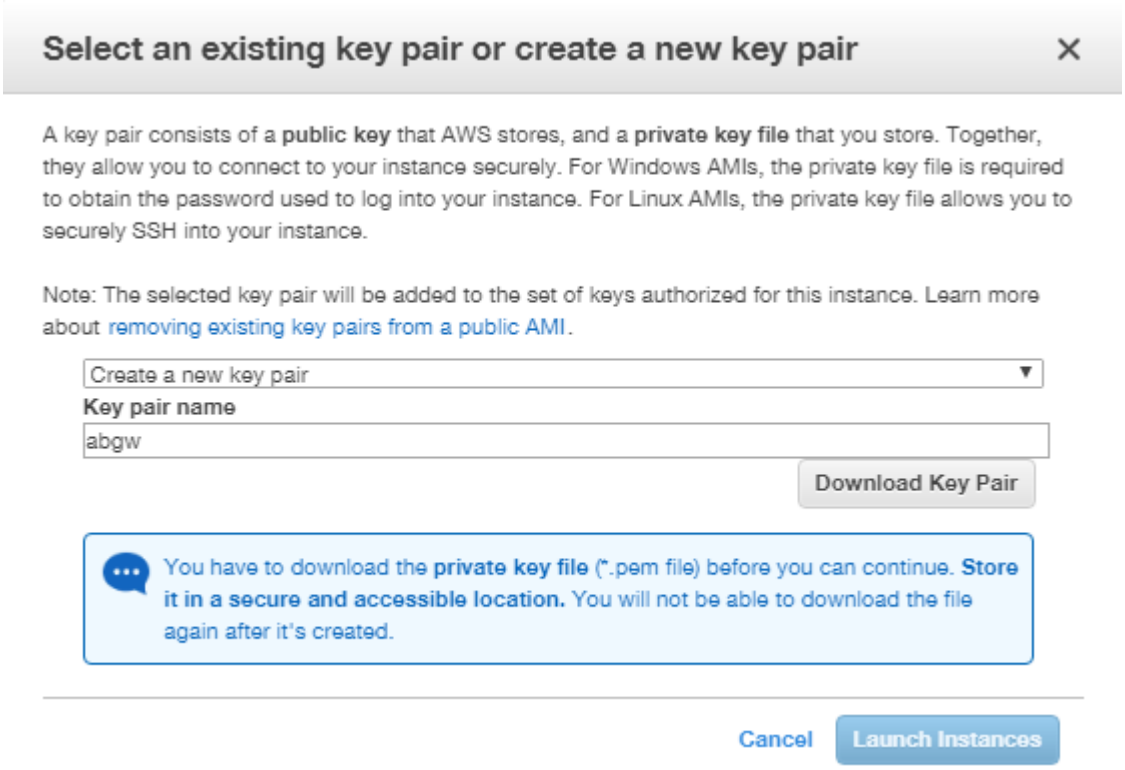
5. На шаге 6 добавьте в новую группу безопасности два правила для открытия портов 8888 и 44445 в дополнение к порту 22, открытому по умолчанию. Порты 22 (SSH) и 8888 (панель администрирования) требуются для управления экземпляром и в целях безопасности должны быть открыты только узкому диапазону IP-адресов, 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. Скачайте файл с парой ключей.

Важно: Сохраните ключ в безопасном месте: сделайте файл с ключом читаемым только для вас (например, `chmod 400 <key_file>` в Linux или Mac) и поместите его в каталог, к которому только у вас есть доступ (например, `chmod 700 <dir>` в Linux или Mac).



7. Нажмите **Launch Instance** (Запустить инстанс).
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.

ГЛАВА 3

Получение пароля и вход в продукт Acronis Инфраструктура

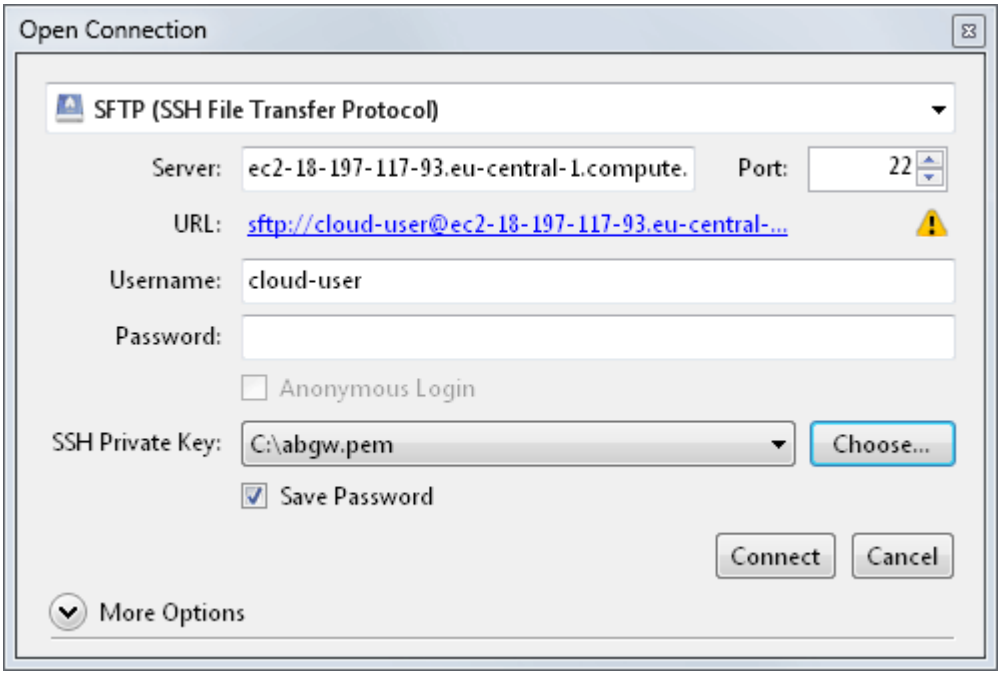
После запуска экземпляра необходимо получить пароль по умолчанию для панели администрирования продукта Acronis Инфраструктура, который хранится внутри экземпляра в каталоге `/.initial-admin-password`.

Доступ к экземпляру можно получить по SSH с использованием ранее созданного ключа, например в Linux или Mac.

```
# 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
```

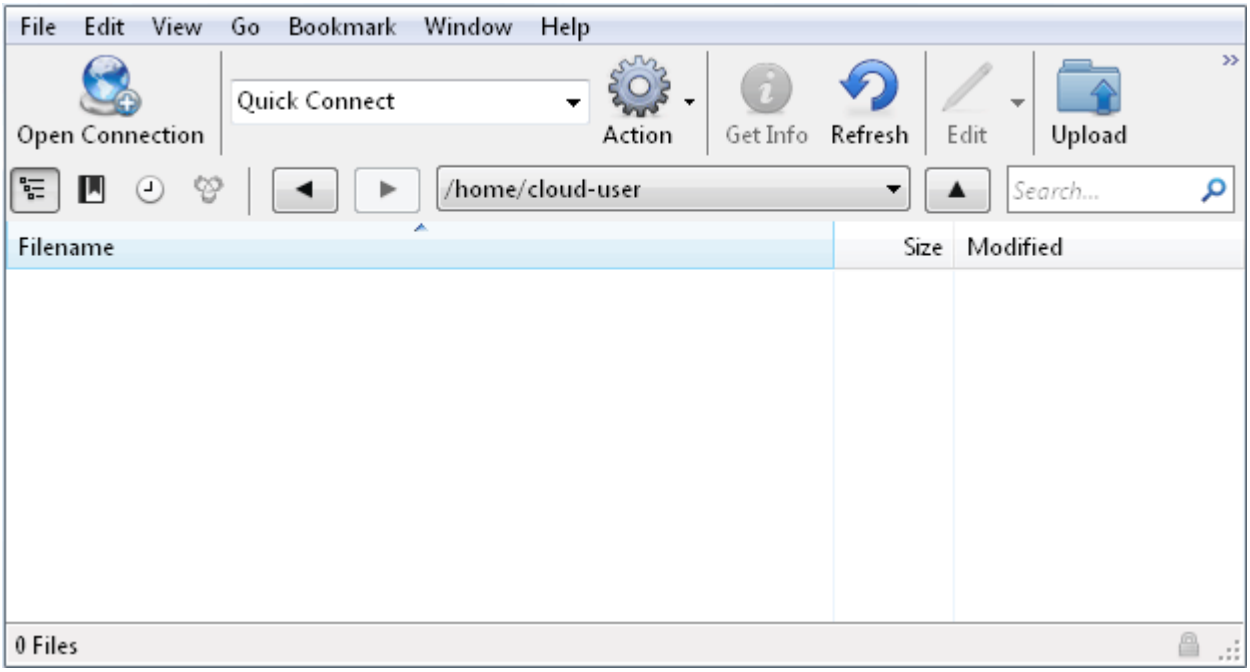
Как вариант, можно получить доступ к файлу пароля по SFTP. Например, в Windows и Mac можно использовать программу CyberDuck.

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.

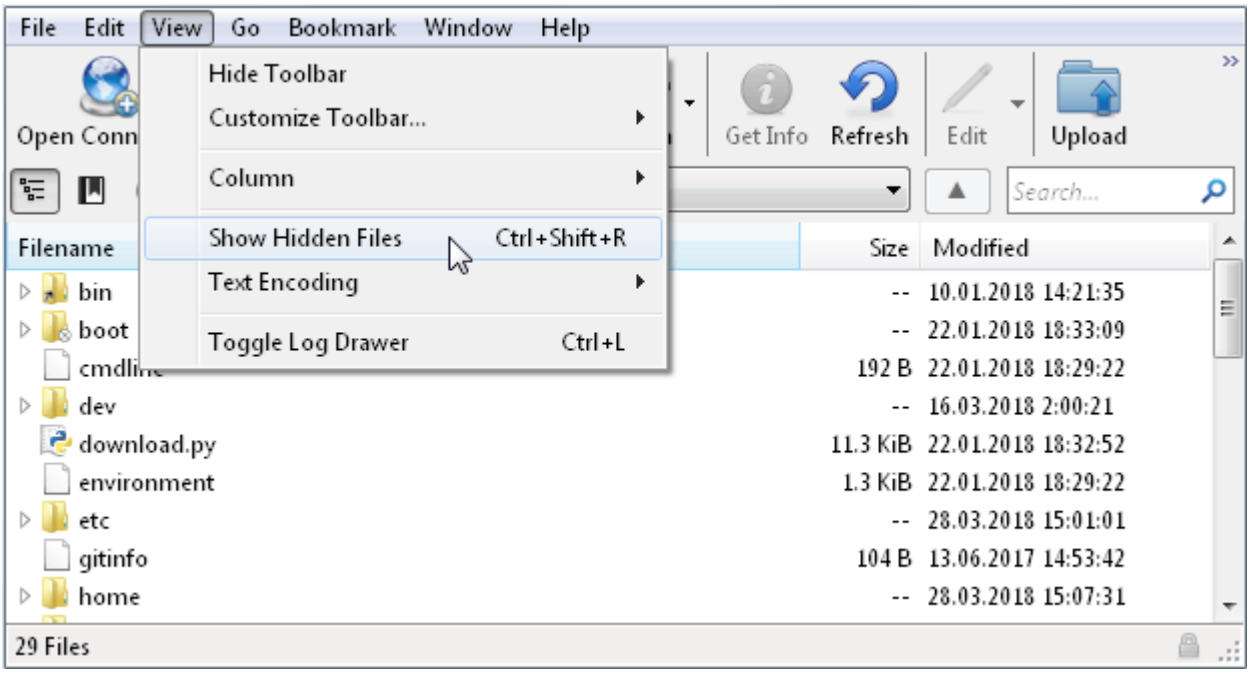


3. Нажмите **Подключиться** и примите отпечаток ключа сервера.

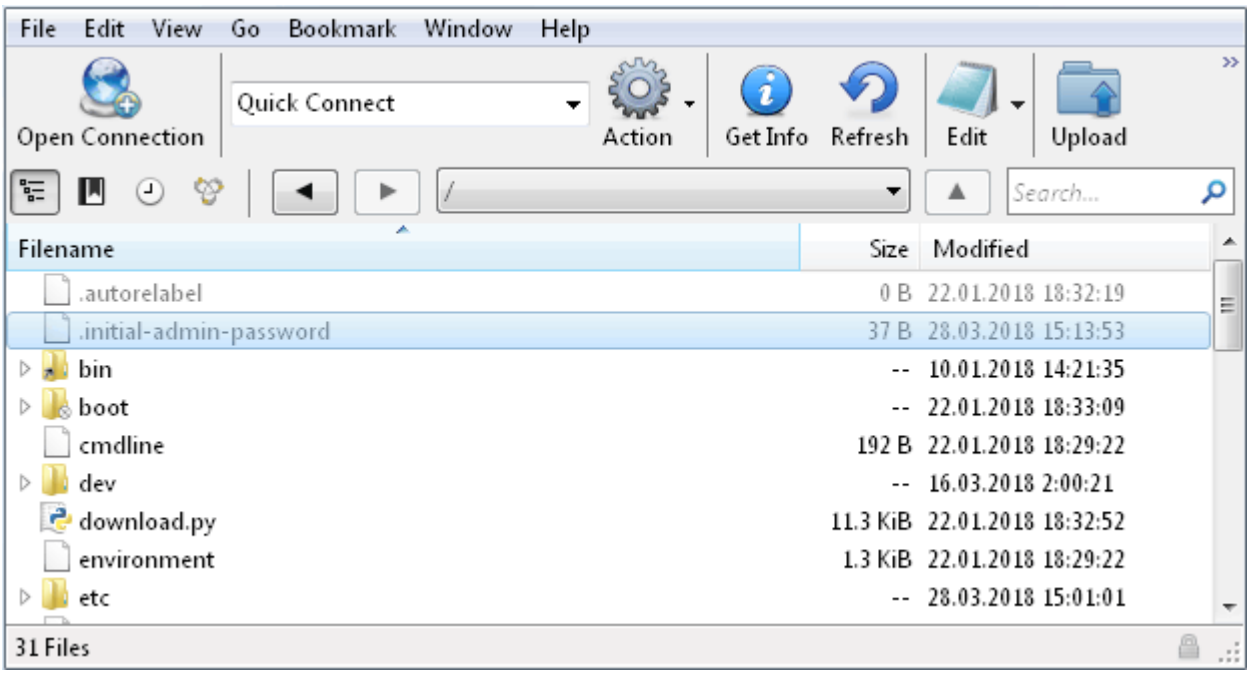
4. Перейдите в домашний каталог, то есть `/home/cloud-user`.



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



6. Скачайте и откройте файл пароля `.initial-admin-password`.



Используя этот пароль, выполните вход на панель управления Acronis Инфраструктура как пользователь `admin` по имени хоста экземпляра через порт 8888, например https://ec2-18-197-117-93.eu-central-1.compute.amazonaws.com:8888/.

Обратите внимание на следующие моменты.

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.

Обычно первым шагом после установки продукта Acronis Инфраструктура является создание кластера хранилища. Однако это делается автоматически при запуске экземпляра с продуктом Acronis Инфраструктура в Amazon EC2, поэтому можно приступать непосредственно к настройке Backup Gateway.

ГЛАВА 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 Acronis Cyber Cloud для хранения данных резервного копирования.

4.1 Важные требования и 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 облако, сначала сохраняются локально и только после

этого отправляются в место назначения. По этой причине крайне важно, чтобы локальное хранилище было избыточным и постоянным. 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.
- Для каждого кластера Backup Gateway следует использовать 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 Acronis Инфраструктура.
- Чтобы можно было зарегистрировать Backup Gateway в Acronis Cyber Backup Cloud, для вашей партнерской учетной записи должна быть отключена двухфакторная проверка подлинности (2FA).

4.2 Создание шлюза Backup Gateway

Прежде чем приступить, убедитесь, что в целевом хранилище достаточно места для резервных копий.

Для настройки Backup Gateway выполните следующие действия.

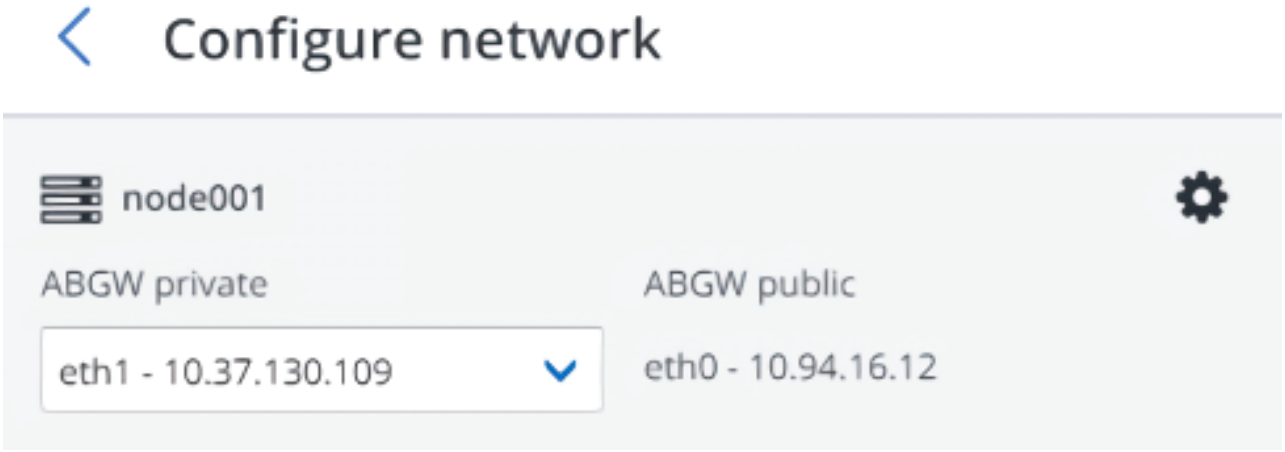
1. На экране **Инфраструктура** > **Сети** убедитесь, что в сети, которые вы собираетесь использовать, добавлены типы трафика **ABGW внутр.** и **ABGW внешн.**
2. В меню слева нажмите **Сервисы хранилища** > **Резервное копирование**.
3. Выберите серверы, на которых будут работать сервисы шлюза, и нажмите **Создать шлюз** на панели справа.

Примечание: Серверы отображаются с небольшими значками, представляющими их роли внутри кластера. Дополнительные сведения о значках см. в статье https://kb.acronis.com/content/61024.

---

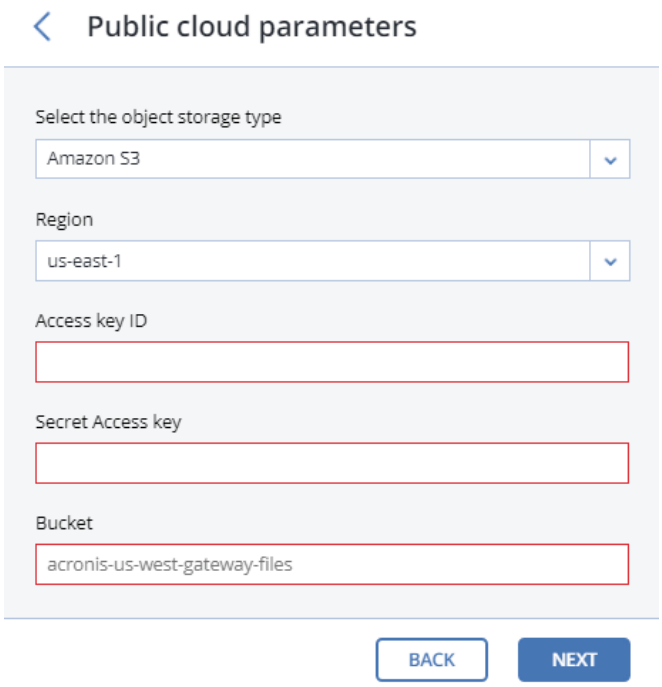
4. Выберите **Облачный сервис** в качестве типа хранилища.
5. Убедитесь, что в раскрывающемся списке выбран правильный сетевой интерфейс. Нажмите кнопку **Далее**.

   При необходимости нажмите значок шестерни и настройте сетевые интерфейсы сервера на экране **Конфигурация сети**.

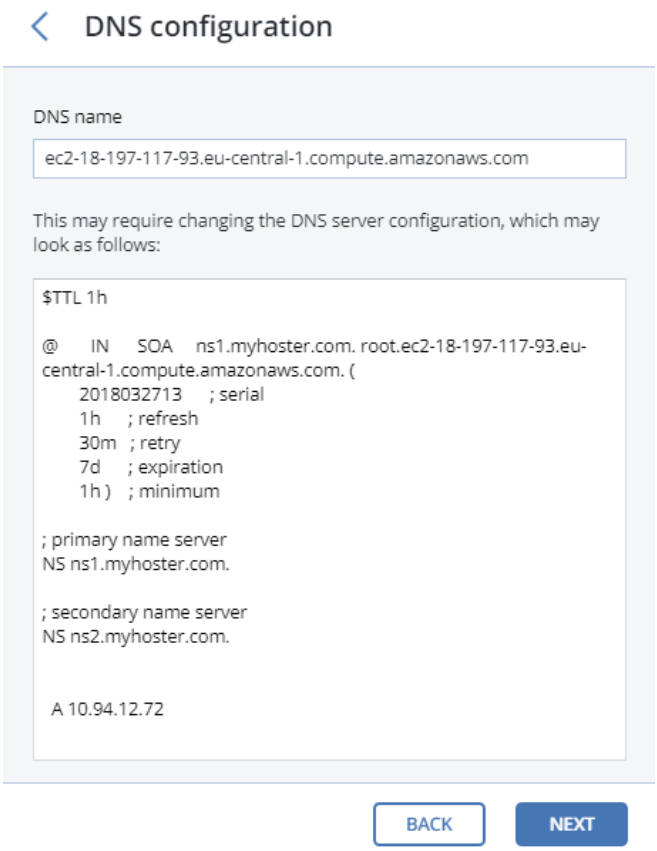


6. На панели **Параметры облачного сервиса** выберите **Amazon S3**, нужный регион, а также заполните информацию о ключах и корзине.

Важно: Указанная папка корзины должна быть доступна для записи.



7. На панели **Параметры тома** оставьте параметры без изменений.
8. На панели **Настройка DNS** вставьте скопированное имя хоста экземпляра в поле **Доменное имя**.



9. На панели **Регистрация** укажите следующую информацию для вашего продукта Acronis.

Важно: Убедитесь, что для вашей партнерской учетной записи отключена двухфакторная проверка подлинности (2FA). Вы также можете отключить ее для конкретного пользователя при включенной двухфакторной проверке для организации, как описано в документации по Acronis Cyber Cloud, и указать учетные данные этого пользователя.

9.1. В поле **Адрес** укажите адрес портала управления Acronis Cyber Backup Cloud (например, https://cloud.acronis.com/) или имя хоста/IP-адрес и порт сервера управления Acronis Cyber Backup (например, http://192.168.1.2:9877).

9.2. В поле **Аккаунт** укажите данные партнерской учетной записи в облаке или учетной записи администратора организации на локальном сервере управления.

10. Затем нажмите кнопку **Готово**.

После настройки Backup Gateway войдите в Acronis Cyber Backup Cloud и выполните тестовое резервное копирование в облако Amazon, чтобы убедиться, что все работает правильно.

ГЛАВА 5

Добавление дискового пространства в продукт Acronis Инфраструктура

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

1. 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 Understanding allocatable disk space.
2. 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.
3. Производительность диска зависит от его размера. 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.

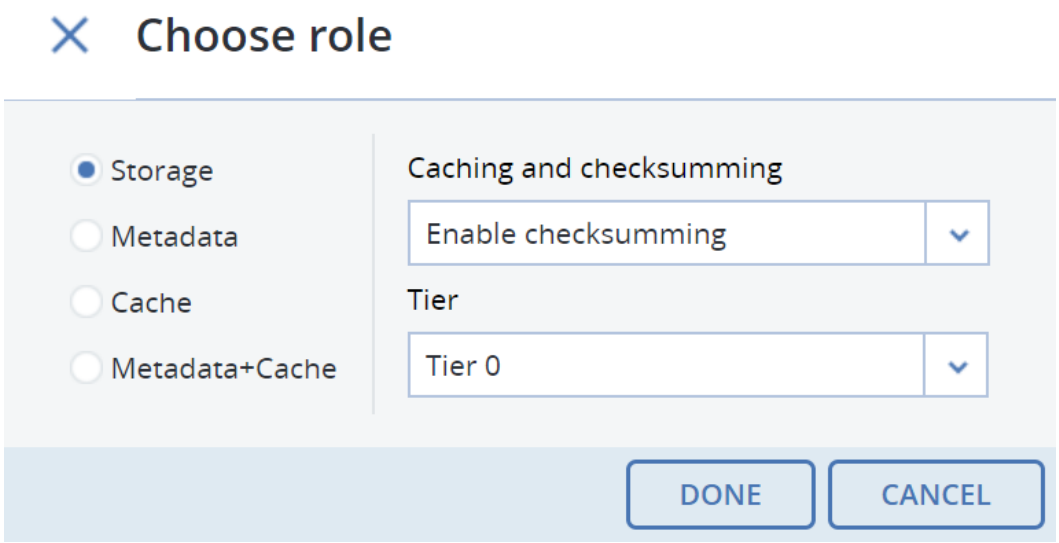
Если вы хотите увеличить физическое пространство в кластере хранилища, необходимо создать и присоединить новые тома Amazon EBS. Не используйте функцию **модификации томов** Amazon EBS на вашем экземпляре Acronis Инфраструктура, поскольку размер файловой системы не будет изменен

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 инстансу. После этого добавленный том будет отображаться в списке дисков сервера на панели администрирования продукта Acronis Инфраструктура.

Выполните эти шаги на панели администрирования, чтобы настроить новый диск.

1. На экране **Инфраструктура** > **Серверы** щелкните имя сервера с созданным диском. Перейдите на вкладку **Диски** для просмотра всех дисков сервера.
2. Созданный ранее диск будет отображаться с ролью **Не назначен**. Выберите его и нажмите **Назначить** на правой панели.
3. На экране **Выбрать роль** выберите роль **Хранилище**, уровень и при необходимости включите проверку контрольных сумм. Дополнительные сведения см. в разделе Assigning disk roles manually.



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