КИБЕРПРОТЕКТ

cyberprotect.ru

Кибер Инфраструктура

4.7

Руководство по быстрому старту Backup Gateway для Microsoft Azure

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 BacupGateway для Microsoft Azure

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

Обычно требуется только создать виртуальную машину (ВМ) с продуктом Кибер Инфраструктура в Azure, указав необходимые сведения, такие как пароль и имя пользователя ВМ, данные партнерской учетной записи в Кибер Бэкап Облачный и т. п. После того как ВМ будет запущена, вы сможете хранить резервные копии в облаке Azure без необходимости входа в продукт Кибер Инфраструктура. Однако при необходимости можно выполнить вход на панель администрирования, используя имя хоста ВМ и порт 8888, например https://backupgateway.azure.com:8888/.

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 Microsoft Azure — **Cool Blob Storage**. Классы архивных хранилищ, такие как Azure Archive Blob, 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.

2 Важные требования и ограничения

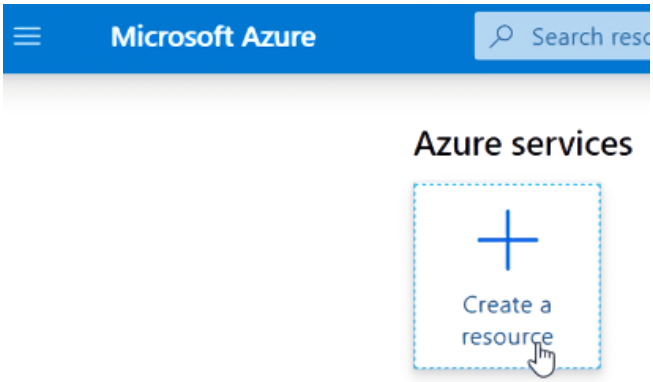
- При работе с публичным облаком Backup Gateway использует локальное хранилище для промежуточного копирования, а также для хранения служебной информации. Это означает, что данные, предназначенные для загрузки в публичное облако, сначала сохраняются локально и только после этого отправляются в место назначения. По этой причине для сохранности данных крайне важно, чтобы локальное хранилище было постоянным и избыточным. Использование временных дисков может привести к потере данных.
- Выберите правильный шаблон диска, который обеспечит нужную производительность резервного копирования (см. пример в следующем абзаце). Учитывайте планы на будущее, поскольку шаблон диска нельзя будет изменить. В этом случае потребуется добавить в ВМ новый диск с правильным шаблоном, добавить новый диск в кластер хранилища, освободить старый диск из кластера и удалить его из ВМ.

  Производительность и размер локального диска ВМ зависят от шаблона. Например, виртуальная машина **STANDARD_DS1** имеет выделенную полосу пропускания 32 МБ/с для трафика дисков хранилища премиум-класса. В свою очередь диск хранилища премиум-класса **P10** может обеспечить пропускную способность 100 МБ/с. Если диск хранилища **P10** присоединен к виртуальной машине **STANDARD_DS1**, его производительность будет ограничена до 32 МБ/с вместо максимальной производительности 100 МБ/с. Дополнительные сведения о хранилище премиум-класса см. в документации Azure.
- 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 Кибер Инфраструктура.
- Чтобы можно было зарегистрировать Backup Gateway в Кибер Бэкап Облачный, для вашей партнерской учетной записи должна быть отключена двухфакторная проверка подлинности (2FA).

3 Создание виртуальной машины Кибер Инфраструктура

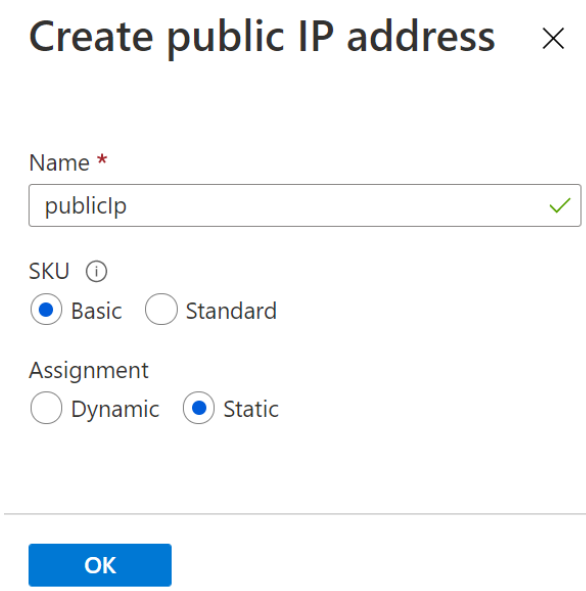
Сначала необходимо создать ВМ с продуктом Кибер Инфраструктура. Выполните следующие действия.

1. На панели мониторинга нажмите **Create a resource** (Создать ресурс).



2. На панели **Home** (Главная) > **Create a resource** (Создать ресурс) найдите и щелкните **Cyber Backup Gateway** в каталоге Azure Marketplace.
3. На панели **Home** (Главная) > **Create a resource** (Создать ресурс) > **Cyber Backup Gateway** нажмите **Create** (Создать).

   Откроется мастер создания ВМ.
4. На вкладке **Basics** (Основные сведения):
   a. В разделе **Project details** (Сведения о проекте) выберите тип подписки и группу ресурсов.
   b. В разделе **Instance details** (Сведения об экземпляре) выберите регион, а затем укажите имя пользователя и пароль для учетной записи администратора ВМ. Пароль не должен содержать специальные символы. Затем задайте политики публичного доступа и укажите пароль для веб-панели продукта Кибер Инфраструктура.
   c. Нажмите **Next: Gateway settings** (Далее: параметры шлюза).
5. На вкладке **Gateway settings** (Параметры шлюза):
   a. В разделе **Virtual machine size** (Размер виртуальной машины) по умолчанию должен быть выбран рекомендуемый размер ВМ **Standard A4 v2**.
   b. В разделе **Storage account** (Учетная запись хранилища) создайте новую учетную запись. На панели **Create storage account** (Создать учетную запись хранилища) укажите имя для учетной записи, выберите **StorageV2 (general purpose V2)** (Хранилище V2 общего назначения) в разделе **Account kind** (Вид учетной записи) и нажмите **OK**.
   c. В поле **Storage account container** (Контейнер учетной записи хранения) укажите имя.
   d. В разделе **Public IP address** (Публичный IP-адрес) создайте новый IP-адрес. На панели **Create public IP address** (Создать публичный IP-адрес) укажите имя для IP-адреса, выберите **Static** (Статический) в области **Assignment** (Назначение) и нажмите **OK**.



e. В поле **DNS prefix** (Префикс DNS) укажите префикс для Backup Gateway, например **backupgateway**.

f. Нажмите **Next: Cyber Backup Cloud settings** (Далее: параметры Cyber Backup Cloud).

Шлюз Backup Gateway будет зарегистрирован в Кибер Бэкап Облачный под статическим общедоступным IP-адресом и доменным именем.

Замечание
Общедоступный IP-адрес и доменное имя нельзя будет изменить позже.

6. На вкладке **Cyber Backup Cloud settings** (Параметры Cyber Backup Cloud) введите данные партнерской учетной записи в Кибер Бэкап Облачный. URL-адрес облачного портала управления должен быть указан по умолчанию. Нажмите **Next: Review + create** (Далее: просмотреть и создать).

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 Кибер Облачные Сервисы, и указать учетные данные этого пользователя. Двухфакторную проверку можно снова включить после развертывания Backup Gateway.

7. На вкладке **Review + create** (Просмотреть и создать) проверьте правильность всех параметров, дождитесь прохождения проверки и нажмите **Create** (Создать).
8. На панели **Create** (Создать) ознакомьтесь с условиями использования и политикой конфиденциальности и нажмите **Create** (Создать).

После запуска ВМ выполните вход на панель администрирования Кибер Облачные Сервисы и убедитесь, что новый продукт Кибер Инфраструктура отображается в разделе **Расположения**

(дополнительные сведения см. в документации по Кибер Облачные Сервисы). Затем выполните тестовое резервное копирование в облако Azure, чтобы убедиться, что все работает правильно.

4 Добавление дискового пространства в продукт Кибер 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 «Общие сведения о распределяемом дисковом пространстве» в руководстве администратора по командной строке.
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. Например, сравнение размеров твердотельных накопителей премиум-класса в Azure показывает, что общая пропускная способность двух терабайтных дисков больше, чем у одного 2-терабайтного диска. Поэтому следует внимательно рассмотреть свои потребности и рекомендации поставщика облачных сервисов.

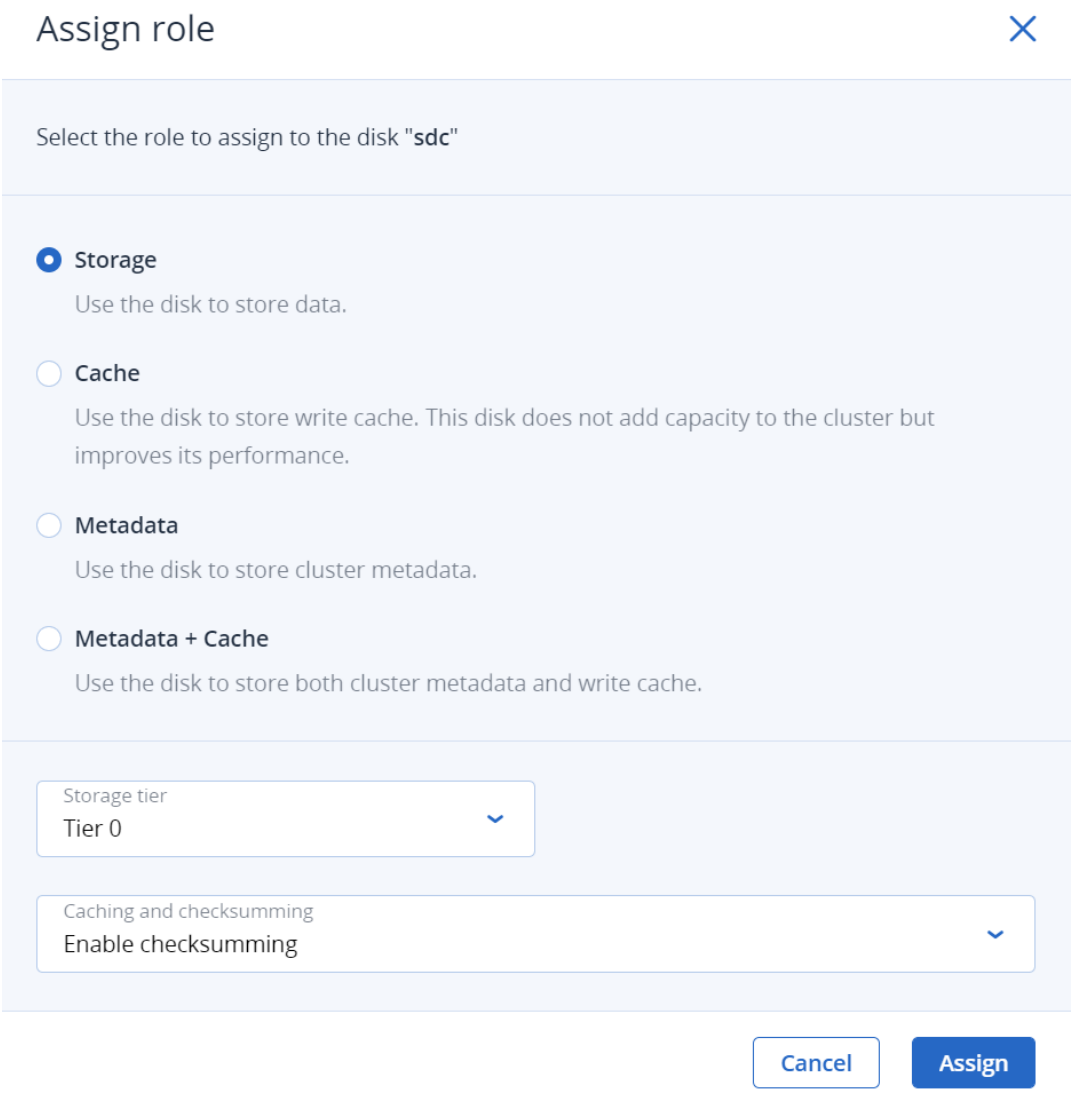
Если вы хотите увеличить физическое пространство в кластере хранилища, необходимо создать и присоединить новые диски данных. Не используйте функцию **изменения размера диска** Azure на вашей ВМ Кибер Инфраструктура, поскольку размер файловой системы не будет изменен соответствующим образом. Вместо этого создайте новый управляемый диск данных и присоедините его, как описано ниже.

Создайте и присоедините новый диск к ВМ Кибер Инфраструктура, как показано в разделе Добавление диска данных. После этого добавленный диск 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 Отключение диска данных с помощью портала.

5 Выполнение дополнительных задач

Как правило, требуется только создать и запустить ВМ с продуктом Кибер Инфраструктура в Azure, чтобы хранить резервные копии в облаке Azure. Вход в продукт Кибер Инфраструктура при этом не требуется.

Однако, если необходимо выполнить некоторые дополнительные задачи, которые требуют входа в продукт Кибер Инфраструктура, можно получить доступ к ВМ Azure, используя доменное имя и учетные данные пользователя, указанные во время развертывания ВМ. Также потребуется открыть порт для ВМ.

Замечание
Кибер Инфраструктура всегда отображает диски Microsoft Azure (в том числе твердотельные накопители премиум-класса) как жесткие диски, поскольку Hyper-V не предоставляет информации о типе диска.

Задачи, связанные с Backup Gateway, которые можно выполнить в продукте Кибер Инфраструктура, 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