Acronis

Acronis Инфраструктура 4.0

Backup Gateway Quick Start Guide for VMware vSphere

5 ноября 2020 г.

Заявление об авторских правах

Оглавление

ГЛАВА 1

Об этом руководстве

В этом руководстве объясняется, как развернуть продукт Acronis Инфраструктура и настроить Backup Gateway на VMware vSphere.

В общих чертах потребуется выполнить следующие действия.

1. Настроить сети.
2. Создать виртуальные машины для продукта Acronis Инфраструктура.
3. Развернуть продукт Acronis Инфраструктура на виртуальных машинах.

Все эти шаги подробно описываются в следующих главах.

После развертывания продукт Acronis Инфраструктура необходимо настроить для вашего сценария. Шаги по настройке шлюза резервного копирования приведены в разделе *Добавление хранилищ в Acronis Cyber Backup или Acronis Cyber Backup Cloud* (страница 17). Остальные инструкции доступны в руководстве администратора.

1.1 Требования

Для работы продукта Acronis Инфраструктура на VMware vSphere убедитесь в соблюдении следующих требований.

- Версия VMware vSphere: 6.7 и выше
- Версия ВМ: 14 и выше
- На хосте должно быть достаточно памяти. Для сервера с одним диском хранилища, на котором работает Backup Gateway, требуется как минимум 8 ГБ ОЗУ.

- В хранилище данных vSphere должно быть достаточно свободного пространства. Каждая виртуальная машина занимает как минимум 425 ГБ (два диска хранилища по 200 ГБ и системный диск на 25 ГБ). Шаблон продукта Acronis Инфраструктура также занимает около 35 ГБ. Максимальный рекомендуемый размер одного виртуального диска — 16 ТБ.

  Важно: Планируйте размер виртуальных дисков заранее и резервируйте достаточно пространства для ожидаемого увеличения объема данных. Размер дисков нельзя изменить позже, но можно добавить новые диски.

- Для использования шлюза резервного копирования продукт Acronis Инфраструктура можно развернуть на одной виртуальной машине. Однако для сценариев общего назначения рекомендуется создать три или пять виртуальных машин, чтобы обеспечить балансировку нагрузки и высокую доступность.

Примечание: Полные требования к оборудованию для сценария со шлюзом резервного копирования приведены в разделе Hardware requirements.

ГЛАВА 2

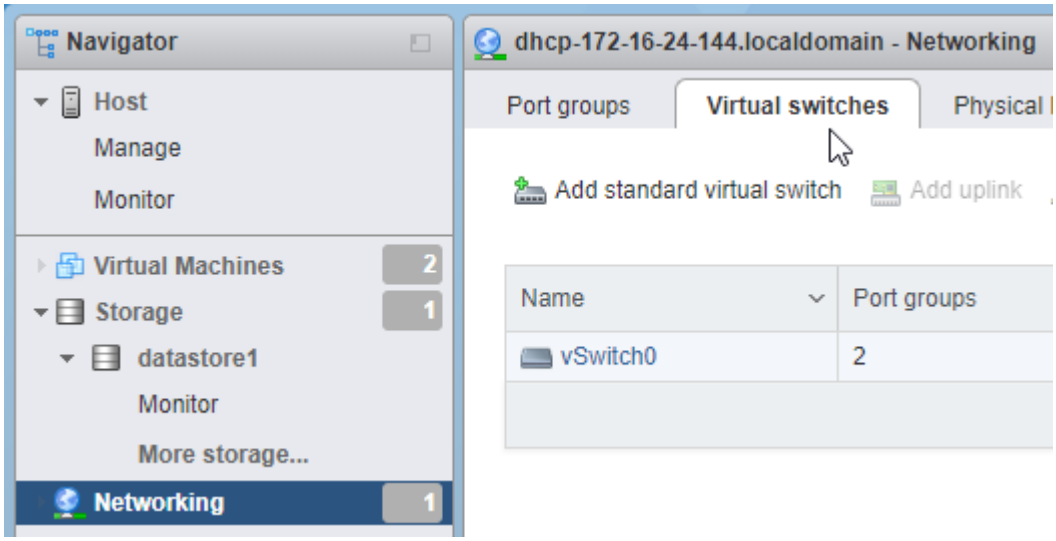
Настройка сетей

Для работы продукта Acronis Инфраструктура обычно требуются две сети: публичная для внешних подключений и частная для обмена данными между виртуальными машинами. Можно использовать уже настроенную внешнюю сеть, но рекомендуется создать выделенную частную сеть, даже если частная сеть уже существует. Для создания частной сети потребуется виртуальный коммутатор с настроенными параметрами безопасности и группа портов.

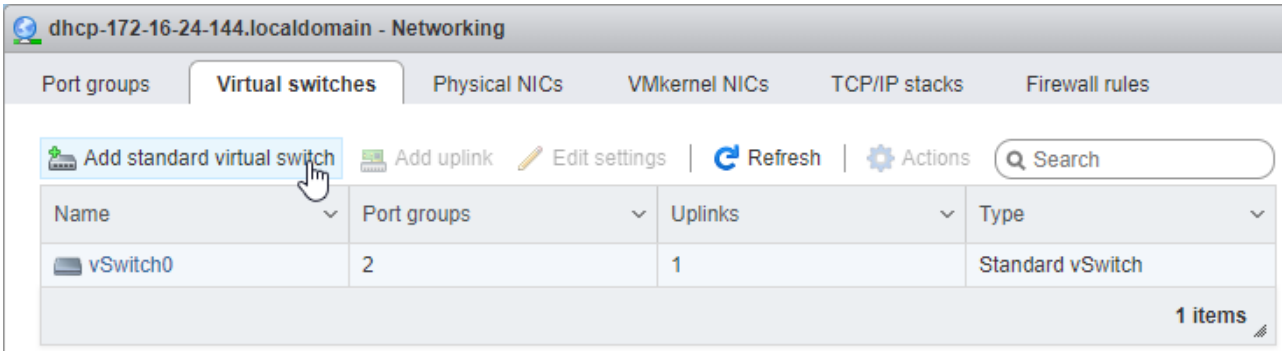
Примечание: Полные требования к сети приведены в разделе Planning the network.

Чтобы создать виртуальный коммутатор, выполните следующие действия.

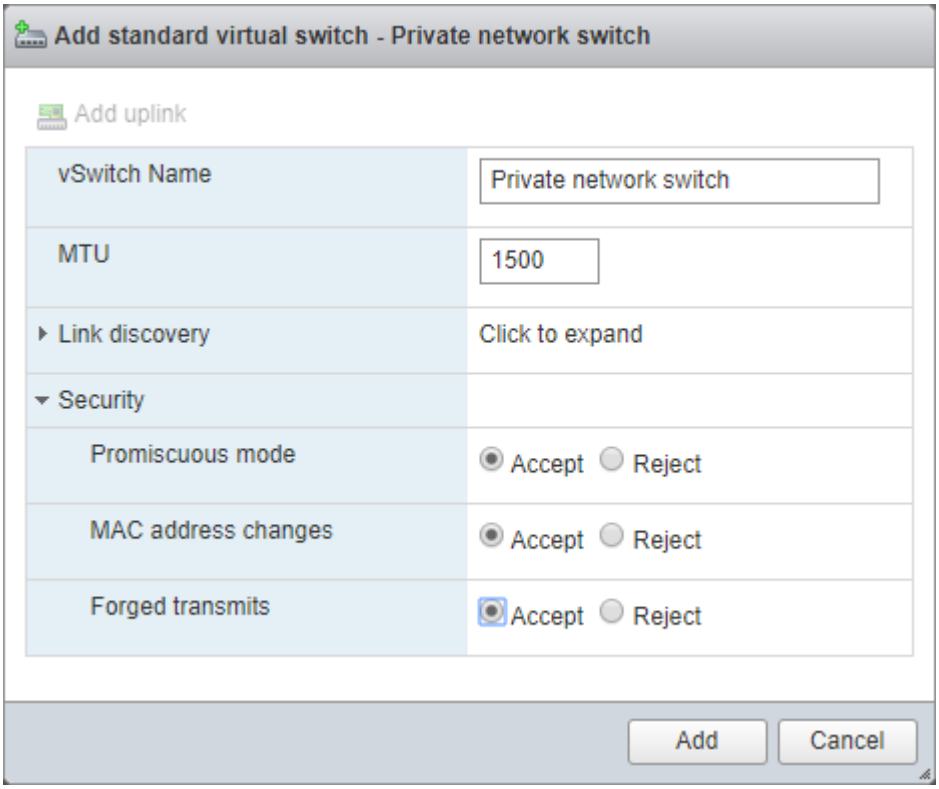
1. В клиенте Host Client нажмите **Networking** (Сети) в меню слева. Откройте вкладку **Virtual switches** (Виртуальные коммутаторы).



2. Нажмите **Add standard virtual switch** (Добавить стандартный виртуальный коммутатор) на панели инструментов.

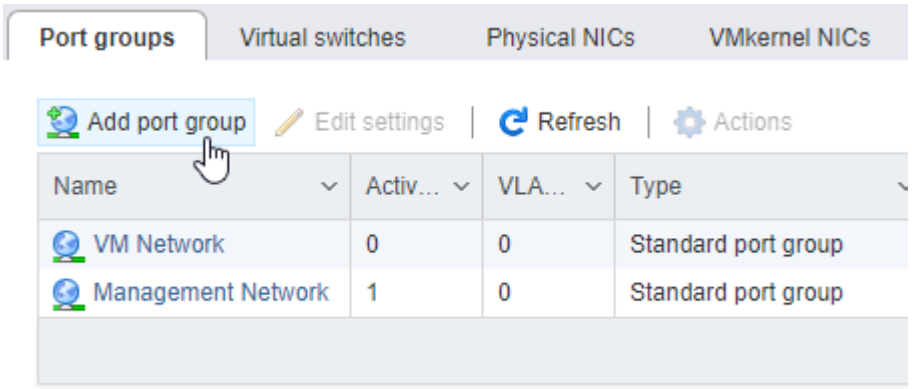


3. Введите имя коммутатора и разверните пункт **Security** (Безопасность). Выберите **Accept** (Принять) для параметров **Promiscuous mode** (Неразборчивый режим), **MAC address changes** (Изменения MAC-адреса) и **Forged transmits** (Подделка передаваемого трафика).

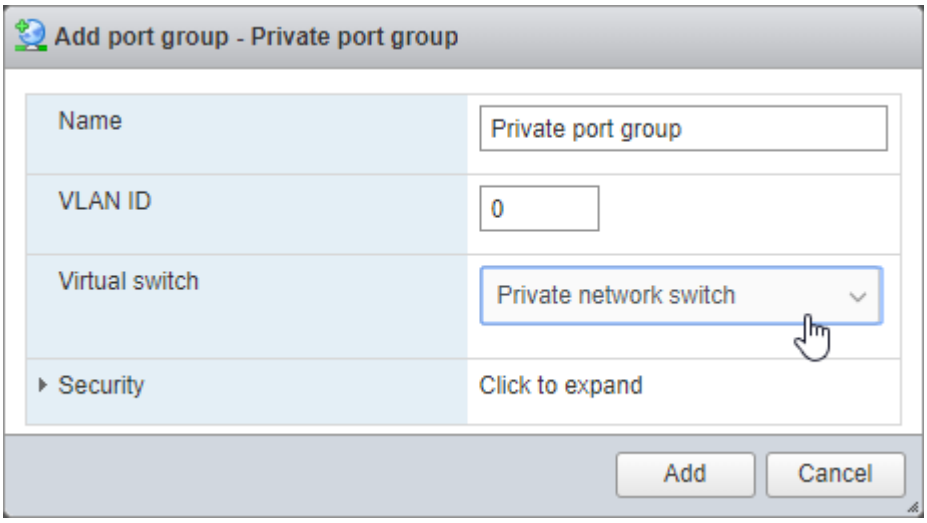


Чтобы создать группу портов, выполните следующие действия.

1. Откройте вкладку **Port groups** (Группы портов) и нажмите **Add port group** (Добавить группу портов) на панели инструментов.



2. Введите имя группы портов. Выберите виртуальный коммутатор, созданный ранее.

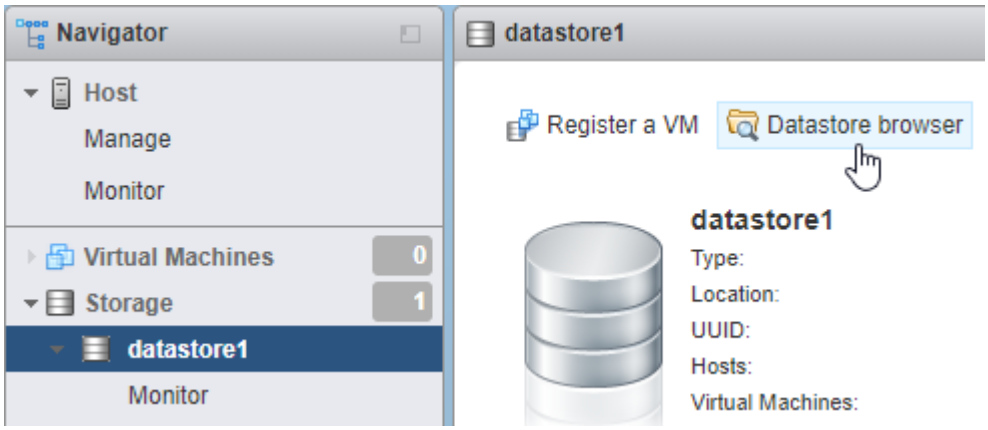


ГЛАВА 3

Создание виртуальных машин

Сначала скачайте образ продукта Acronis Инфраструктура здесь и распакуйте его. Затем загрузите два файла VMDK в хранилище данных VMware vSphere.

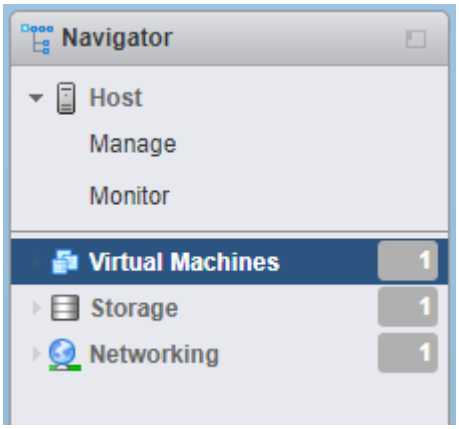
1. На панели **Navigator** (Навигация) щелкните нужное хранилище данных. На панели инструментов хранилища нажмите **Datastore browser** (Обозреватель хранилища данных).
2. В окне **Datastore browser** (Обозреватель хранилища данных) создайте каталог с таким же именем, как у виртуальной машины.



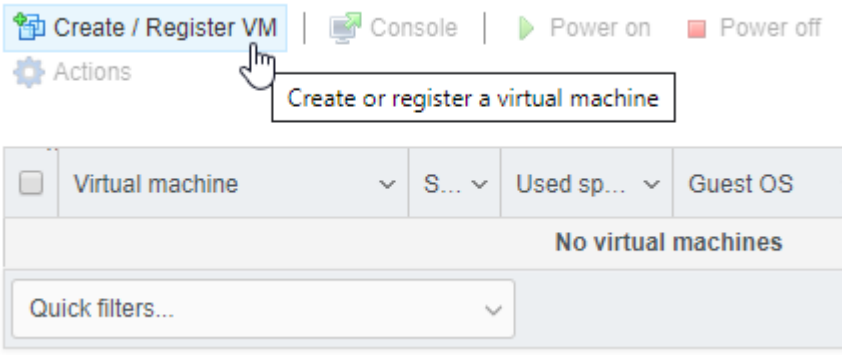
3. Загрузите образ продукта Acronis Инфраструктура (два файла VMDK) в этот каталог.

Выполните следующие действия, чтобы создать виртуальную машину для продукта Acronis Инфраструктура:

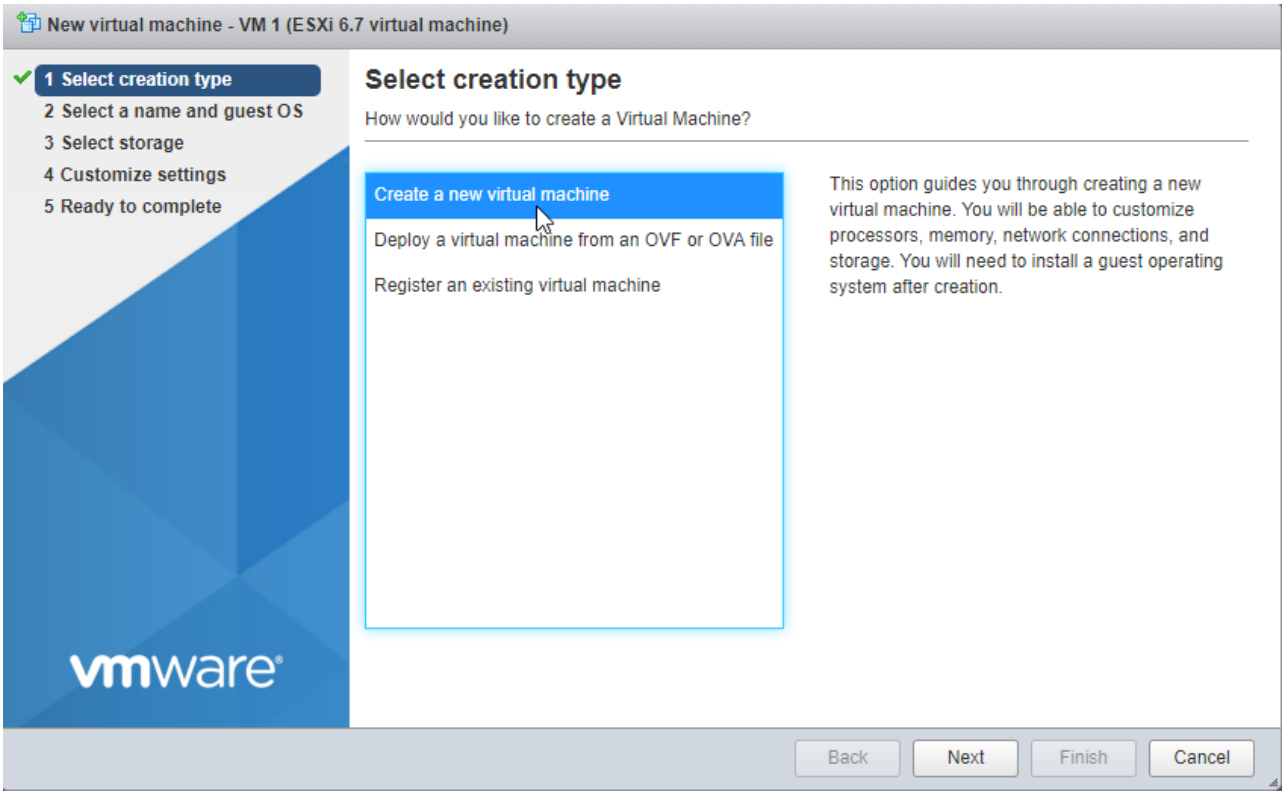
1. В клиенте Host Client нажмите **Virtual Machines** (Виртуальные машины) в меню слева.



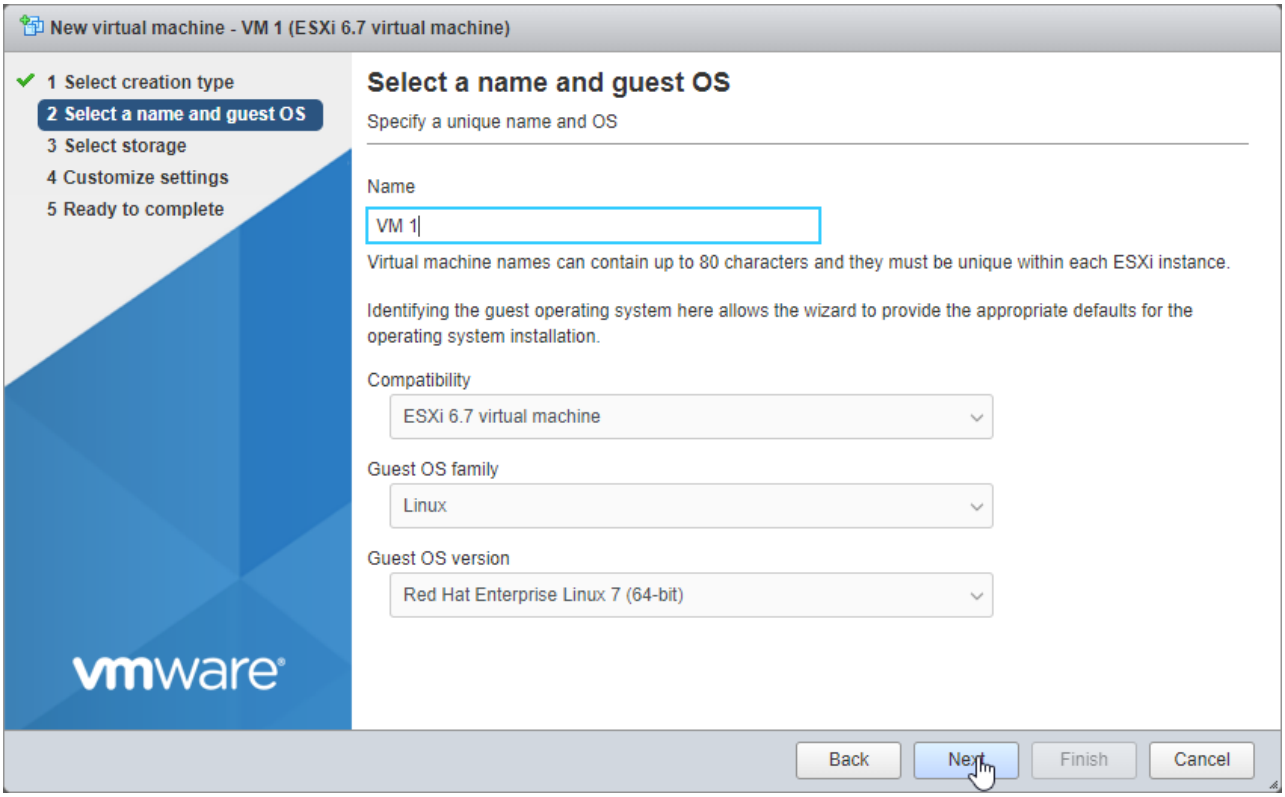
2. Нажмите **Create / Register VM** (Создать/зарегистрировать ВМ) на панели инструментов.



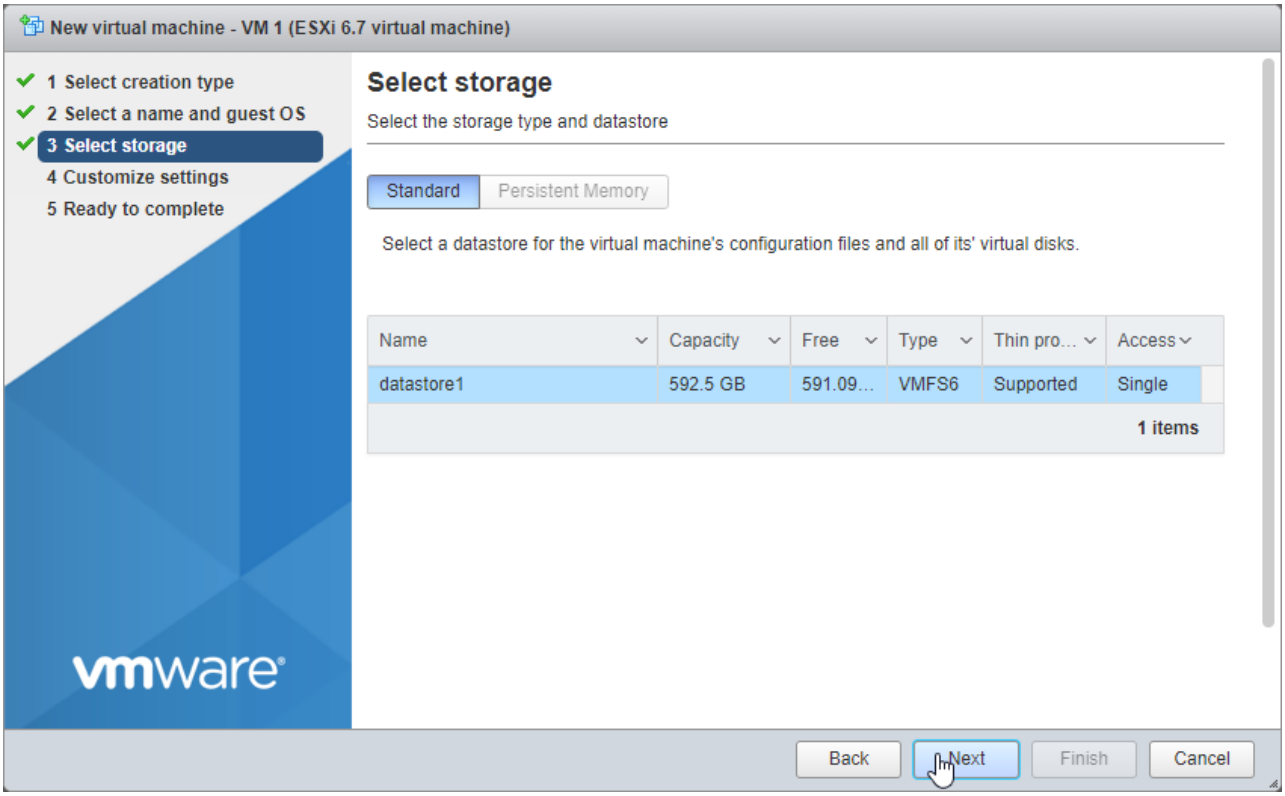
3. В мастере **New virtual machine** (Новая виртуальная машина) на шаге 1 выберите **Create a new virtual machine** (Создать новую виртуальную машину). Нажмите **Next** (Далее).



4. На шаге 2 введите имя для виртуальной машины и выберите гостевую ОС. Нажмите **Next** (Далее).

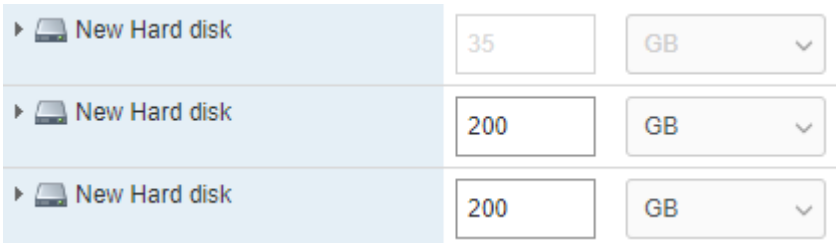


5. На шаге 3 выберите тип хранилища и хранилище данных. Убедитесь, что в хранилище данных достаточно свободного пространства.

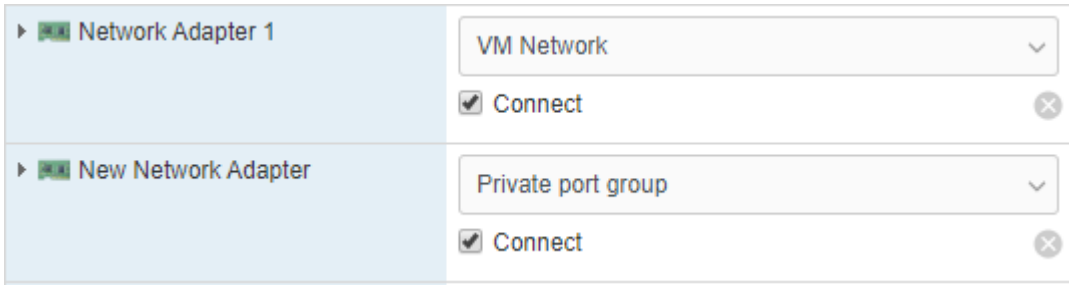


6. На шаге 4 удалите существующий жесткий диск и нажмите **Add hard disk** (Добавить жесткий диск) на панели инструментов. Выберите **Existing hard disk** (Существующий жесткий диск) и перейдите к образу, ранее загруженному в хранилище данных. Нажмите **Select** (Выбрать).

7. Снова нажмите **Add hard disk** (Добавить жесткий диск) на панели инструментов. Выберите **New standard hard disk** (Новый стандартный жесткий диск). Установите для него размер 200 ГБ. Повторите этот шаг, чтобы добавить еще один жесткий диск размером 200 ГБ. В итоге у вас должно быть три жестких диска: 35, 200 и 200 ГБ.



8. В окне **Customize settings** (Настроить параметры) нажмите **Add network adapter** (Добавить сетевой адаптер) на панели инструментов. Убедитесь, что один адаптер подключен к внешней сети, а другой — к частной группе портов, созданной ранее.



9. На шаге 5 проверьте конфигурацию и нажмите **Finish** (Готово).
10. Выберите виртуальную машину в меню **Navigator** (Навигация) и запустите ее.

Повторите эти шаги, чтобы создать нужное количество виртуальных машин для вашего сценария (см. раздел *Требования* (страница 1)).

ГЛАВА 4

Развертывание продукта Acronis Инфраструктура на виртуальных машинах

После запуска виртуальной машины выполните следующие действия.

1. Выполните вход как пользователь `storage-user` с использованием пароля по умолчанию (то есть `password`). Вам сразу же будет предложено сменить пароль. Например:

   ```
   You are required to change your password immediately (root enforced)
   WARNING: Your password has expired.
   You must change your password now and login again!
   Changing password for user storage-user.
   Changing password for storage-user.
   (current) UNIX password:
   New password:
   Retype new password:
   passwd: all authentication tokens updated successfully.
   ```

   В строке `(current) UNIX password` введите `password`; в строке `New password` и `Retype new password` введите новый пароль. Пароль будет изменен как для пользователя `storage-user`, так и для привилегированного пользователя.

2. Снова выполните вход как пользователь `storage-user` с новым паролем, а затем переключитесь на привилегированного пользователя.

   ```
   $ sudo su
   ```

3. Настройте и включите сетевой интерфейс `eth1`.

```
# cat > /etc/sysconfig/network-scripts/ifcfg-eth1 << EOF
ARPCHECK=”no”
BOOTPROTO=”static”
IPADDR=192.168.1.<node>
NETMASK=255.255.255.0
DEVICE=”eth1”
IPV6INIT=”yes”
IPV6_AUTOCONF=”yes”
NAME=”eth1”
ONBOOT=”yes”
EOF
# ifup eth1
```

где <node> — номер сервера: 2 для сервера управления, 3 для первого подчиненного сервера и так далее.

4. Проверьте, что IP-адрес назначен и интерфейс работает, например, с помощью команды `ip -4 a show eth1`.

Дальнейшая настройка зависит от роли сервера. Потребуется развернуть один сервер управления, а также при необходимости два или четыре подчиненных сервера.

4.1 Развертывание сервера управления

1. Чтобы зарегистрировать сервер управления и инициализировать его панель администрирования, выполните следующую команду от имени привилегированного пользователя:

```
# echo ’<passwd>’ | /usr/libexec/vstorage-ui-backend/bin/configure-backend.sh \
-i <int_net> -x <ext_net>
# systemctl start vstorage-ui-backend
# systemctl start vstorage-ui-agent
# /usr/libexec/vstorage-ui-agent/bin/register-storage-node.sh -m <mn_IP>
```

где <passwd> — желаемый пароль администратора; <int_net> — внутренний (частный) сетевой интерфейс; <ext_net> — внешний (публичный) сетевой интерфейс; <mn_IP> — IP-адрес сервера управления.

2. Перезагрузите виртуальную машину. IP-адрес панели администрирования будет отображен в строке приветствия терминала. Теперь можно выполнить вход на панель администрирования через порт 8888. Используйте имя пользователя `admin` и пароль привилегированного пользователя для сервера управления, указанный на предыдущем шаге.

На панели администрирования развернутый сервер будет отображаться на экране **Инфраструктура** > **Серверы** со статусом **Не назначен**.

3. На экране **Инфраструктура** > **Сети** нажмите **Изменить**. Сделайте тип трафика **API вычислений** доступным для внешней сети и нажмите **Сохранить**.

Теперь необходимо создать кластер хранилища. Выполните следующие действия.

1. Откройте экран **Инфраструктура** > **Серверы** и нажмите **Создать кластер хранилища**.
2. (Необязательно) Чтобы настроить роли дисков или расположение сервера, щелкните значок шестерни.
3. Введите имя для кластера. Имя может содержать только буквы латинского алфавита (a-z, A-Z), цифры (0–9) и дефисы (-).
4. При необходимости включите шифрование.
5. Нажмите **Создать**.

Кластер хранилища готов. Теперь можно приступить к развертыванию подчиненных серверов, если они требуются для вашего сценария. Если необходим только один сервер для шлюза резервного копирования, переходите к разделу *Добавление хранилищ в Acronis Cyber Backup или Acronis Cyber Backup Cloud* (страница 17).

4.2 Развертывание подчиненных серверов

Чтобы развернуть подчиненный сервер на виртуальной машине, выполните следующие действия.

1. Получите IP-адрес сервера управления и токен из панели администрирования. Для этого откройте раздел **Инфраструктура** > **Серверы** и нажмите **Подключить сервер**, чтобы вызвать экран с адресом сервера управления и токеном.
2. Откройте терминал виртуальной машины и зарегистрируйте подчиненный сервер на панели администрирования, выполнив следующую команду:

   ```
   # /usr/libexec/vstorage-ui-agent/bin/register-storage-node.sh -m <mn_addr> -t <token>
   ```

   где `<mn_addr>` — IP-адрес сервера управления; `<token>` — токен, полученный на панели администрирования.

На панели администрирования только что зарегистрированный подчиненный сервер будет отображаться на экране **Инфраструктура** > **Серверы** со статусом **Не назначен**.

3. Добавьте подчиненный сервер в кластер хранилища.

   3.1. На экране **Инфраструктура** > **Серверы** щелкните неназначенный сервер.

   3.2. На правой панели сервера нажмите **Присоединить к кластеру**.

   3.3. Нажмите **Присоединить**, чтобы Acronis Инфраструктура автоматически назначила роли дискам и добавила сервер к текущему кластеру. Вместо этого можно нажать значок шестерни, чтобы вручную настроить роли дисков или расположение сервера.

Повторите эти шаги для каждого подчиненного сервера. Когда все серверы будут добавлены в кластер хранилища, можно включить высокую доступность для сервера управления на экране **Настройки** > **Сервер управления** > **Высокая доступность**.

Теперь можно приступать к настройке продукта Acronis Инфраструктура для нужного сценария. Инструкции по выполнению различных задач настройки приведены в руководстве администратора.

ГЛАВА 5

Добавление дискового пространства в продукт Acronis Инфраструктура

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

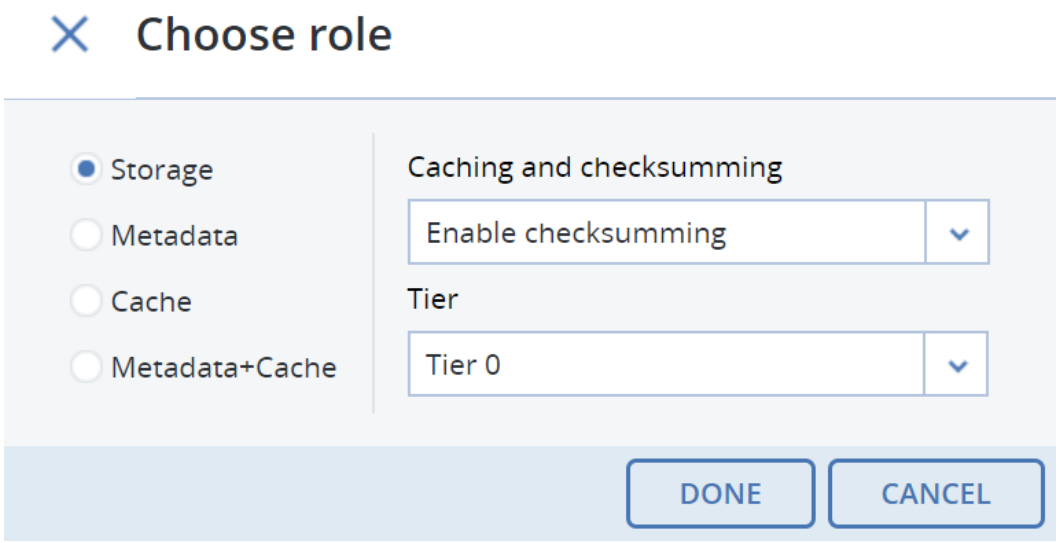
1. Если в кластере несколько серверов, они должны быть одинакового размера для эффективного обеспечения избыточности. В этом случае данные будут распределены по серверам более равномерно. Дополнительные сведения см. в разделе Understanding allocatable disk space.
2. Одинаковый размер дисков помогает 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.

Если вы хотите увеличить физическое пространство в кластере хранилища, можно добавить на серверы новые виртуальные диски. Не используйте функцию **расширения дисков** VMware vSphere на виртуальной машине Acronis Инфраструктура, поскольку размер файловой системы не будет изменен соответствующим образом. Вместо этого необходимо будет создать новый виртуальный диск и добавить его в виртуальную машину, как описано ниже.

Добавьте новый виртуальный диск в виртуальную машину, как показано в разделе Добавление нового жесткого диска в виртуальную машину. После этого диск 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.



ГЛАВА 6

Добавление хранилищ в Acronis Cyber Backup или Acronis Cyber Backup Cloud

Точка доступа к хранилищу Backup Gateway (также называемая шлюзом) предназначена для поставщиков услуг, которые используют Acronis Cyber Backup и/или Acronis Cyber Backup Cloud и хотят организовать локальное хранилище для резервных копий клиентских данных.

Backup Gateway позволяет поставщикам услуг легко настраивать хранилища для данных в собственном формате с поддержкой дедупликации, который используется продуктами Acronis.

Backup Gateway поддерживает следующие внутренние хранилища:

- Кластеры хранилища с программной избыточностью за счет помехоустойчивого кодирования
- тома NFS
- Публичные облачные сервисы, включая ряд решений S3, а также Microsoft Azure, OpenStack Swift и Google Cloud Platform

Хотя ваш выбор должен основываться на конкретных требованиях и сценарии использования, рекомендуется хранить данные резервных копий Acronis в локальном кластере хранилища. В этом случае достигается наилучшая производительность благодаря оптимизации каналов WAN и локальности данных. Хранение резервных копий на томе NFS или в публичном облаке предполагает постоянную передачу данных и другие дополнительные нагрузки, что снижает общую производительность.

Обратите внимание на следующие моменты.

- При настройке Backup Gateway необходимо будет указать учетные данные администратора вашего продукта Acronis Backup.
- Если с Backup Gateway используется не локальное, а внешнее хранилище (например, NFS), то избыточность должна обеспечиваться этим внешним хранилищем. Сам шлюз Backup Gateway не обеспечивает избыточности данных и не производит дедупликации.
- Чтобы можно было зарегистрировать Backup Gateway в Acronis Cyber Backup Cloud, для вашей партнерской учетной записи должна быть отключена двухфакторная проверка подлинности (2FA).

6.1 Подключение к локальному кластеру хранилища через Backup Gateway

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

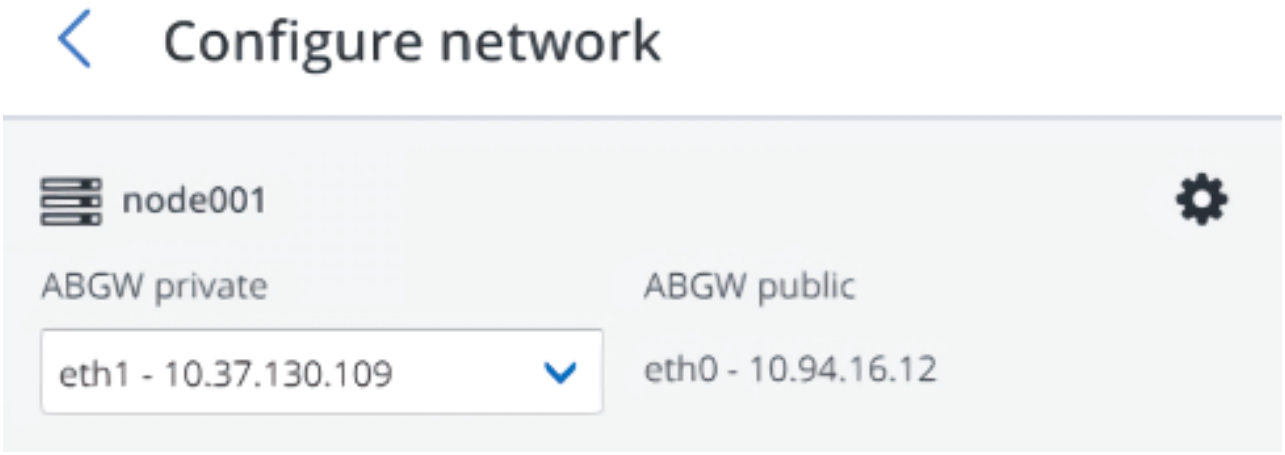
Для настройки Backup Gateway выполните следующие действия.

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.

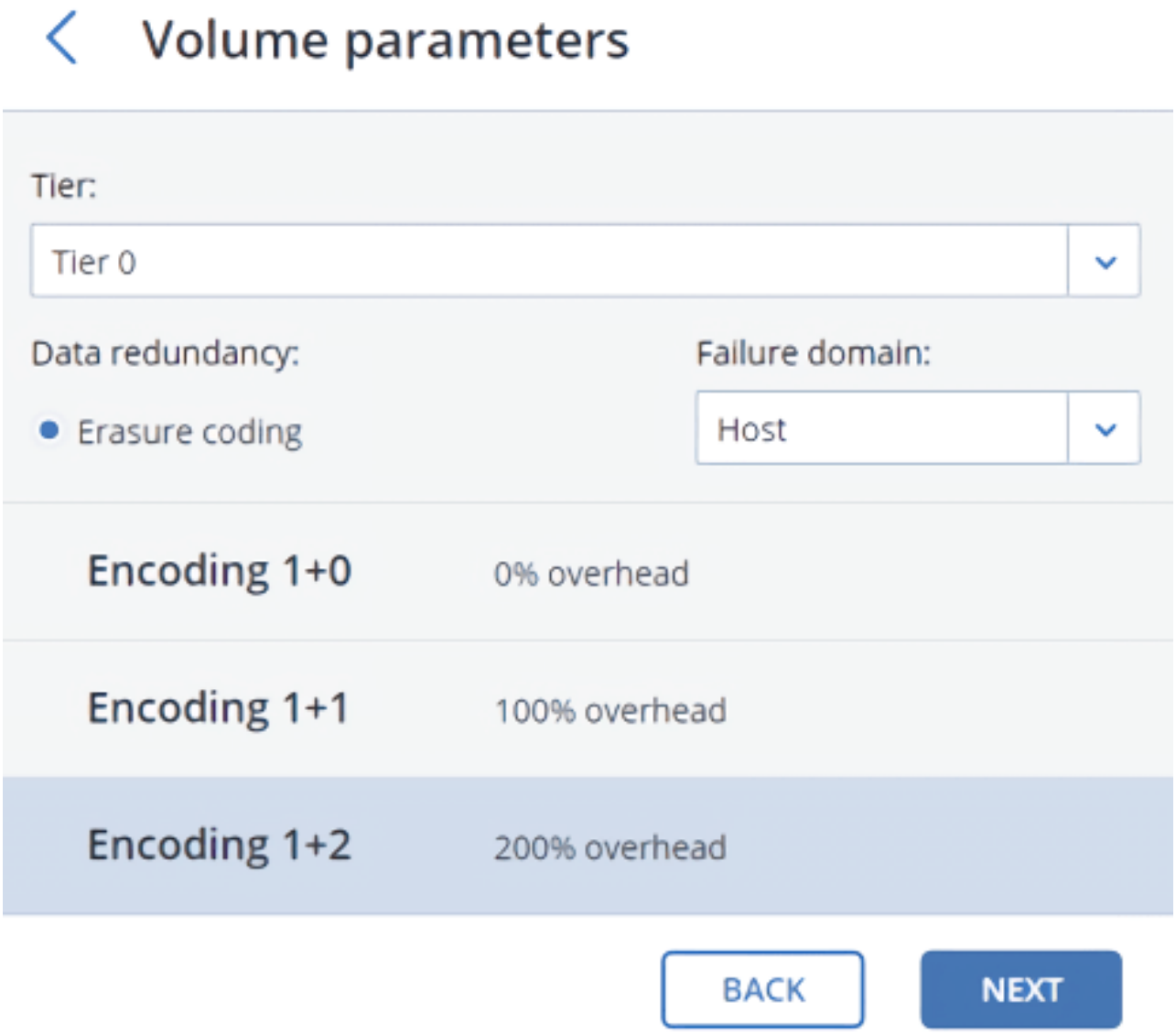
   Примечание: Серверы отображаются с небольшими значками, представляющими их роли внутри кластера. Дополнительные сведения о значках см. в статье https://kb.acronis.com/content/61024.

4. Выберите **Этот кластер Acronis Инфраструктура** 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 тома** выберите нужный уровень, область отказов и режим избыточности данных. Дополнительные сведения см. в разделах Understanding storage tiers, Understanding failure domains и Understanding data redundancy. Нажмите кнопку **Далее**.

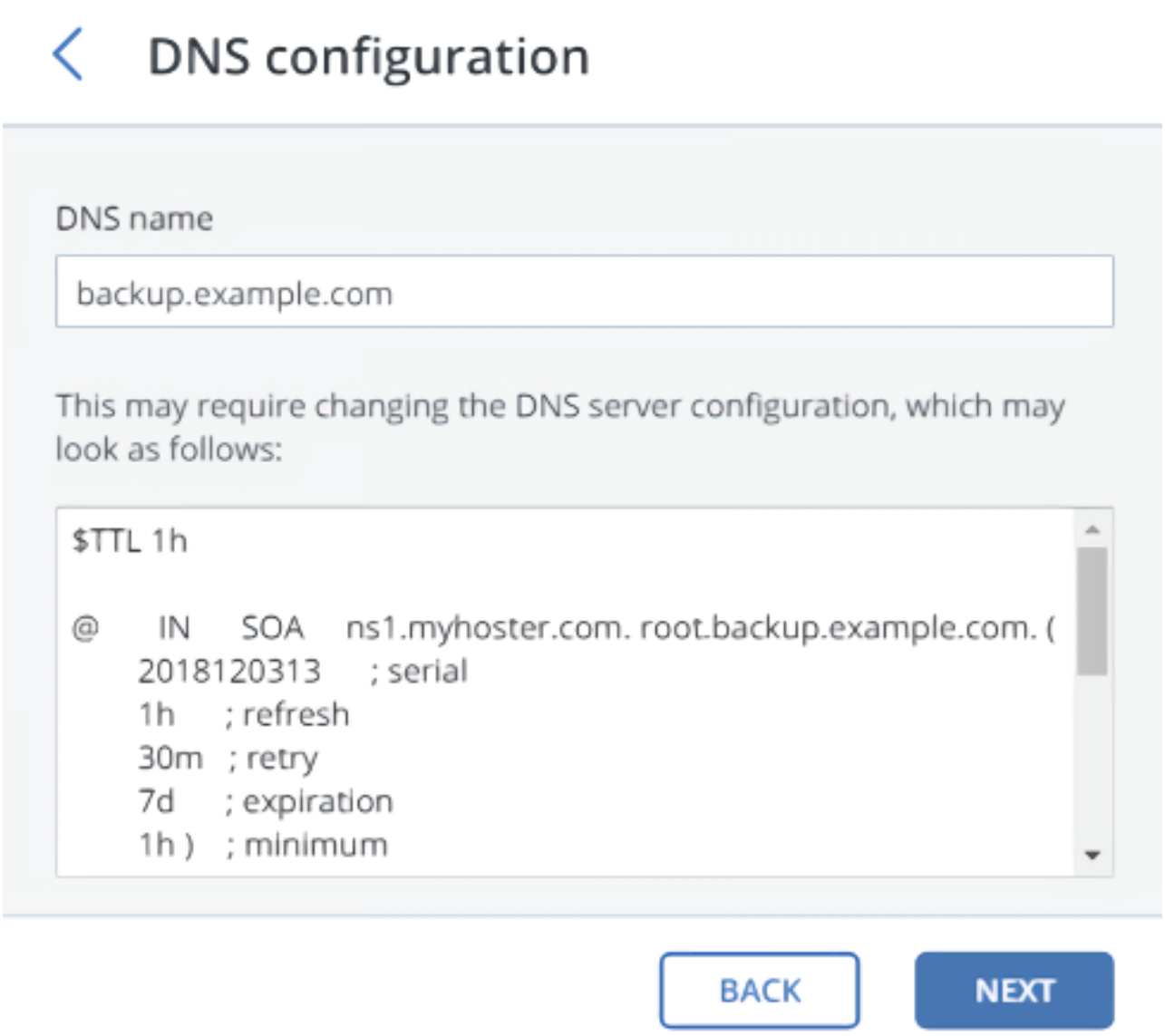


Избыточность за счет репликации не поддерживается для Backup Gateway. Для помехоустойчивого кодирования изменение схемы избыточности отключено, поскольку оно может снизить производительность кластера. Причина в том, что перекодирование потребляет значительный объем ресурсов кластера в течение длительного времени. Если вы все равно хотите изменить схему избыточности, обратитесь в техническую поддержку.

7. На панели **Настройка DNS** укажите внешнее доменное имя для этого шлюза, например `backupgateway.example.com`. Убедитесь, что на каждом сервере, где работает сервис шлюза, открыт порт для исходящих подключений к Интернету и входящих подключений от вашего продукта Acronis Backup. Агенты резервного копирования будут использовать этот адрес и порт для передачи данных в хранилище. Нажмите кнопку **Далее**.

Важно: Настройте свой DNS-сервер в соответствии с примером, приведенным в панели администратора.

Важно: При каждом изменении сетевой конфигурации серверов в кластере Backup Gateway корректируйте записи DNS соответствующим образом.



8. 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.

8.1. 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).

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

9. Затем нажмите кнопку **Готово**.

6.2 Подключение к внешним томам NFS через Backup Gateway

Обратите внимание на следующие ограничения.

- Acronis Инфраструктура не обеспечивает избыточность данных поверх томов NFS. В зависимости от реализации, тома NFS могут обеспечивать собственную аппаратную или программную избыточность.
- В текущей версии продукта Acronis Инфраструктура только один сервер кластера может хранить резервные копии на томе NFS.

Прежде чем приступить, убедитесь в следующем.

1. На томе NFS достаточно места для резервных копий.
2. Каждый экспорт NFS используется только одним шлюзом. В частности, не следует настраивать два экземпляра продукта Acronis Инфраструктура на использование одного и того же экспорта NFS для хранения резервных копий.

Для настройки Backup Gateway выполните следующие действия.

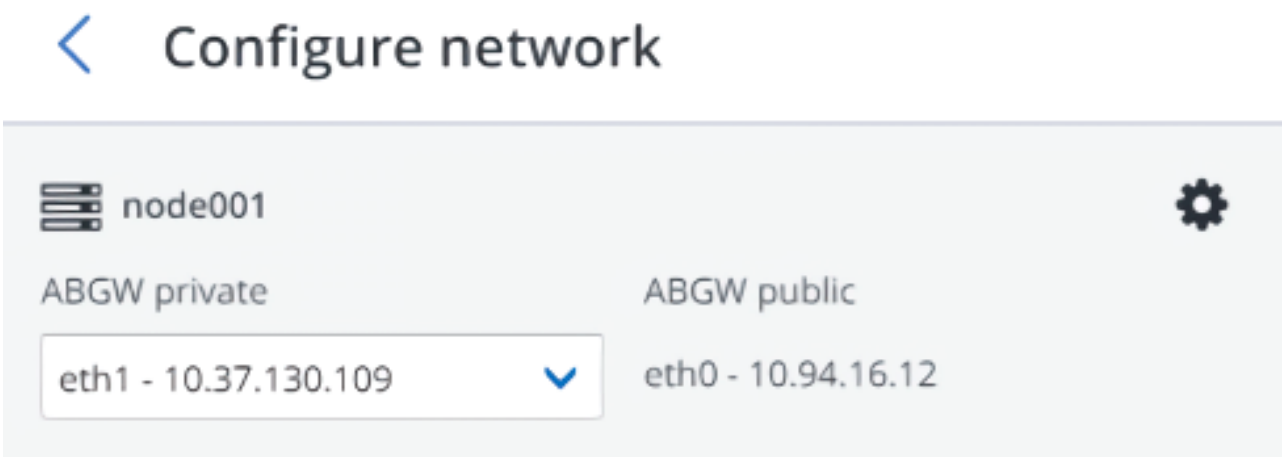
1. На экране **Инфраструктура** > **Сети** убедитесь, что в сети, которые вы собираетесь использовать, добавлены типы трафика **ABGW внутр.** и **ABGW внешн.**

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.

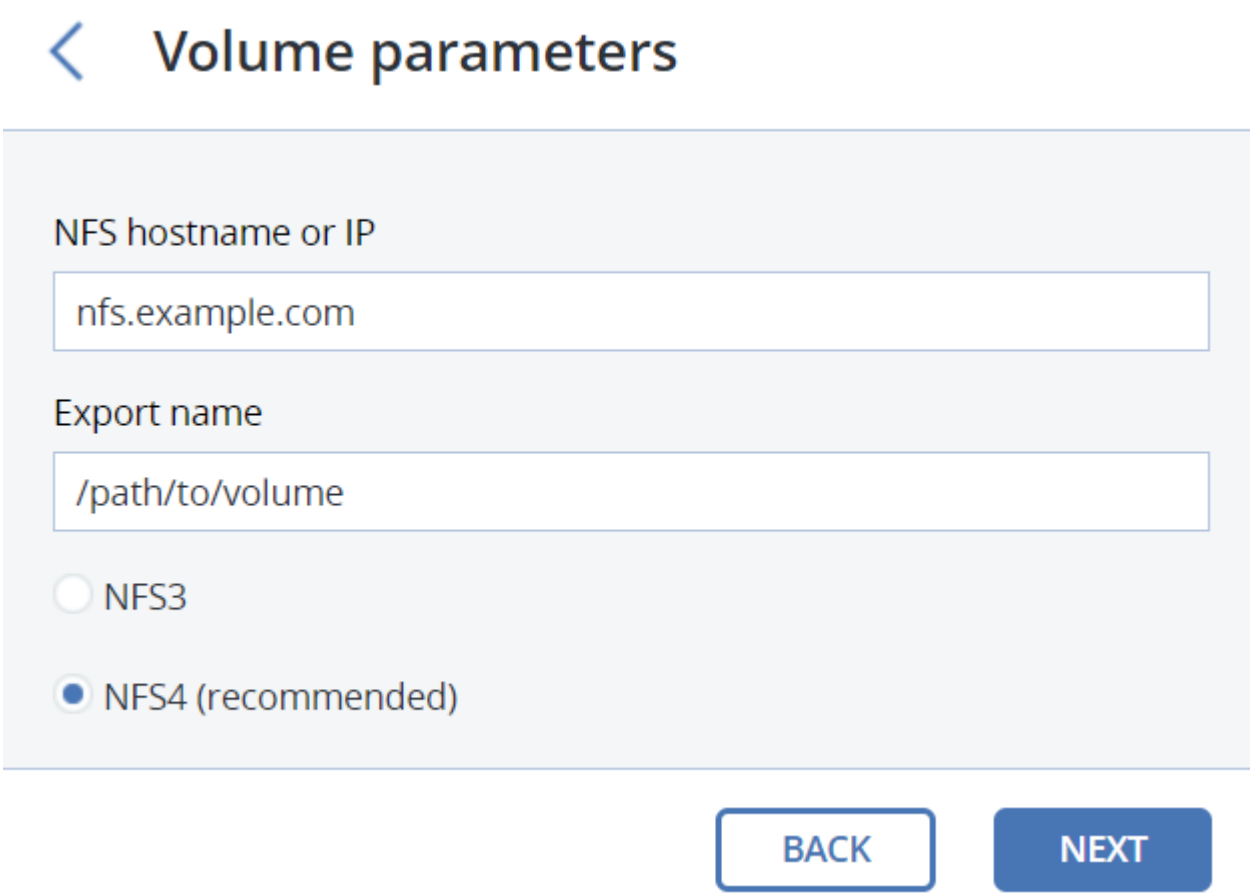
   Примечание: Серверы отображаются с небольшими значками, представляющими их роли внутри кластера. Дополнительные сведения о значках см. в статье https://kb.acronis.com/content/61024.

4. Выберите **Network File System** 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**.



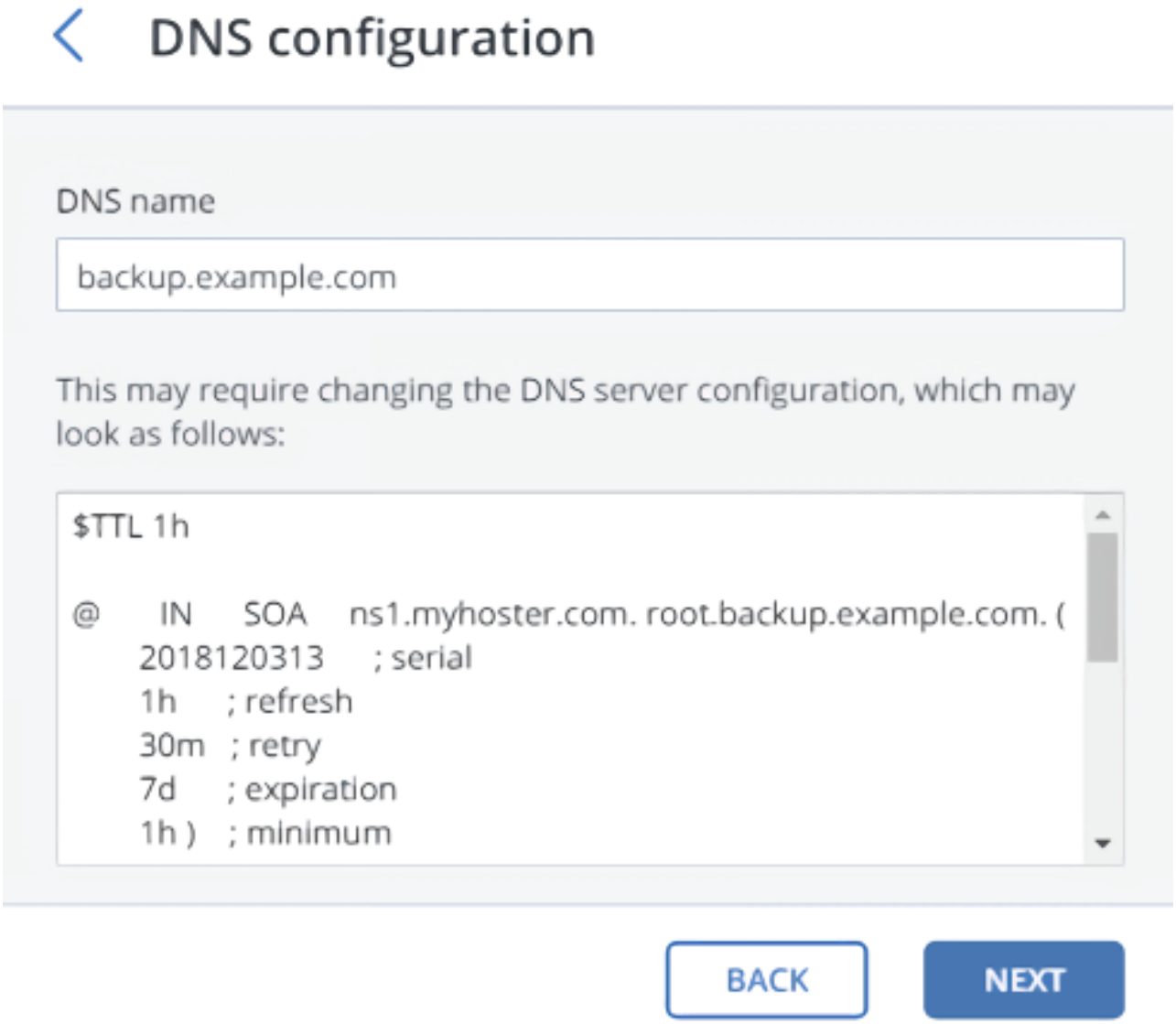
6. На панели **Параметры тома** укажите имя хоста или IP-адрес тома NFS, имя экспорта, а также выберите версию NFS. Рекомендуется версия NFS4, поскольку она обеспечивает лучшую масштабируемость и производительность по сравнению с версией NFS3, которая имеет ограничения в протоколе. Нажмите кнопку **Далее**.



7. На панели **Настройка DNS** укажите внешнее доменное имя для этого шлюза, например `backupgateway.example.com`. Убедитесь, что на каждом сервере, где работает сервис шлюза, открыт порт для исходящих подключений к Интернету и входящих подключений от вашего продукта Acronis Backup. Агенты резервного копирования будут использовать этот адрес и порт для передачи данных в хранилище. Нажмите кнопку **Далее**.

Важно: Настройте свой DNS-сервер в соответствии с примером, приведенным в панели администратора.

Важно: При каждом изменении сетевой конфигурации серверов в кластере Backup Gateway корректируйте записи DNS соответствующим образом.



8. 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.

8.1. 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).

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

9. Затем нажмите кнопку **Готово**.

6.3 Подключение к публичному облачному хранилищу через Backup Gateway

Backup Gateway позволяет Acronis Cyber Backup Cloud или Acronis Cyber Backup использовать для хранения резервных копий публичные облачные сервисы и локальные хранилища объектов.

- Amazon S3
- IBM Cloud
- Alibaba Cloud
- IIJ
- Cleversafe
- Cloudian
- Microsoft Azure
- Объектное хранилище Swift
- Softlayer (Swift)
- Google Cloud Platform
- Wasabi
- Другие решения, использующие S3

Однако по сравнению с локальными кластерами хранение данных резервных копий в публичном облаке увеличивает время задержки всех запросов ввода-вывода к резервным копиям и снижает производительность. По этой причине рекомендуется использовать в качестве внутреннего хранилища локальный кластер.

Поскольку резервные копии представляют собой «холодные» данные с особыми правами доступа, экономичным вариантом будут классы хранилищ, предназначенные для долгосрочного хранения редко используемых данных. Рекомендуемые классы хранилищ включают следующие:

- **Infrequent Access** для Amazon S3
- **Cool Blob Storage** для Microsoft Azure
- **Nearline** и **Coldline** Storage для Google Cloud Platform

Классы архивных хранилищ, такие как Amazon S3 Glacier, Azure Archive Blob или Google Archive, 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.

6.3.1 Важные требования и ограничения

1. 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 устойчивым и избыточным, во избежание потери данных. Существует несколько способов обеспечить устойчивость и избыточность хранилища. Можно развернуть Backup Gateway на нескольких серверах кластера и выбрать нужный режим избыточности. Если Acronis Инфраструктура с шлюзом развертывается на одном физическом сервере, локальное хранилище можно сделать избыточным посредством его репликации по локальным дискам. Если Acronis Инфраструктура с шлюзом развертывается на виртуальной машине, убедитесь, что избыточность обеспечивается решением виртуализации, на базе которого работает продукт.

2. 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.
3. 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.
4. Для каждого кластера Backup Gateway следует использовать отдельный контейнер объектов.

6.3.2 Настройка Backup Gateway

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

Для настройки Backup Gateway выполните следующие действия.

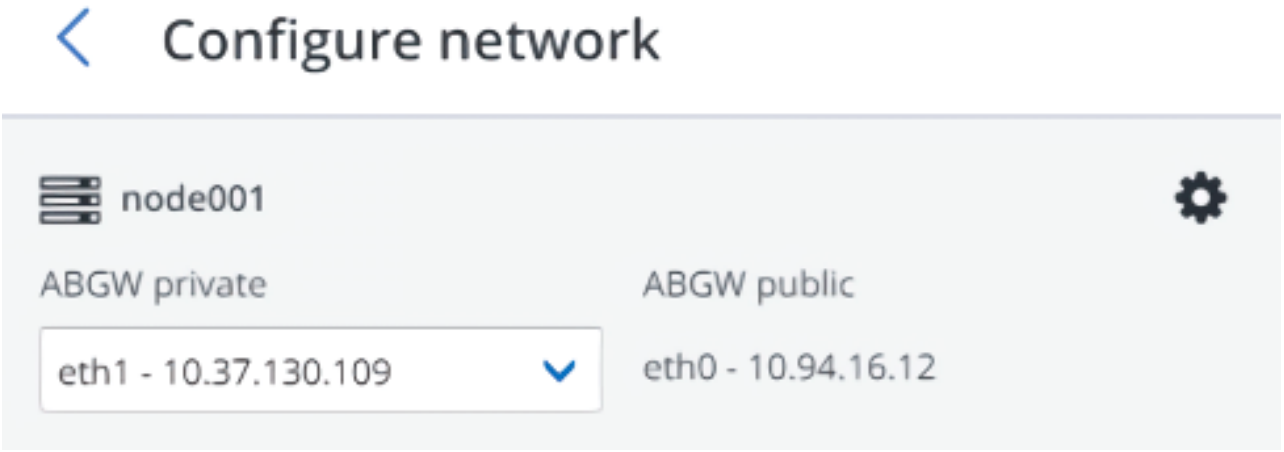
1. На экране **Инфраструктура** > **Сети** убедитесь, что в сети, которые вы собираетесь использовать, добавлены типы трафика **ABGW внутр.** и **ABGW внешн.**
2. В меню слева нажмите **Сервисы хранилища** > **Резервное копирование**.
3. Выберите серверы, на которых будут работать сервисы шлюза, и нажмите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

   6.1. Выберите поставщика облачного сервиса. Если ваш сервис совместим с S3, но отсутствует в списке, попробуйте **AuthV2-совместимый (S3)** или **AuthV4-совместимый (S3)** сервис.

   6.2. В зависимости от поставщика укажите **Регион**, **URL проверка подлинности (Keystone)** или **URL точки доступа**.

   6.3. При использовании объектного хранилища Swift укажите версию протокола аутентификации и необходимые для него атрибуты.

   6.4. Укажите учетные данные пользователя. При использовании Google Cloud выберите файл JSON с ключами для загрузки.

   6.5. Укажите папку (корзину, контейнер) для хранения резервных копий. Папка должна быть доступна для записи.

   Для каждого кластера Backup Gateway следует использовать отдельный контейнер объектов.

   Нажмите кнопку **Далее**.

7. 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.

7.1. 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).

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

8. Затем нажмите кнопку **Готово**.