Acronis

Acronis Инфраструктура 4.0

Backup Gateway Quick Start Guide

5 ноября 2020 г.

Заявление об авторских правах

Оглавление

ГЛАВА 1

Введение

1.1 Об этом руководстве

В этом руководстве описывается развертывание продукта Acronis Инфраструктура на одиночном сервере с целью создания оконечных точек Backup Gateway.

1.2 Аппаратные требования для вариантов установки с Backup Gateway

Как правило, Acronis Инфраструктура устанавливается как минимум на пяти серверах, чтобы полностью задействовать встроенные средства обеспечения высокой доступности и избыточности данных. Однако, если вы хотите использовать только Backup Gateway, можно развернуть базовую инфраструктуру на одном виртуальном или физическом сервере. Хотя в этом случае может потребоваться обеспечить избыточность данных другими способами, иначе существует риск потери пользовательских данных. Вы можете сделать следующее.

- Использовать виртуальную машину (ВМ) как минимум с двумя виртуальными жесткими дисками (рекомендуется три диска). В этом случае только один жесткий диск будет использоваться для хранения данных и необходимо будет убедиться, что избыточность ВМ обеспечивается решением виртуализации, на базе которого она работает.
- Использовать физический сервер как минимум с двумя дисками (рекомендуется три диска). Учтите, что вам потребуется больше дисков для хранения, чтобы обеспечить избыточность данных. Дополнительные сведения о планировании конфигурации сервера см. в разделе Planning node hardware configurations.

В следующей таблице перечислены *минимальные* аппаратные требования для сервера с Backup Gateway.

Таблица 1.2.1: Аппаратные требования сервера

Тип	**Сервер управления с хранилищем и Backup Gateway**
ЦП	64-разрядные процессоры x86 с включенными аппаратными расширениями виртуализации AMD-V или Intel VT. 4 ядра*
ОЗУ	8 ГБ
Хранилище	1 диск: система + метаданные, жесткий диск SATA 120 ГБ 1 диск: хранилище, жесткий диск SATA, размер по необходимости**
Сеть	10 GbE для трафика хранилища 1 GbE для прочего трафика

* Ядро ЦП может представлять собой физическое ядро многоядерного процессора при развертывании на физическом сервере или виртуальное ядро при развертывании в ВМ.

Если вы планируете использовать Backup Gateway для хранения резервных копий в облаке, убедитесь, что в локальном кластере хранилища 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.

ГЛАВА 2

Установка продукта Acronis Инфраструктура

Чтобы установить продукт Acronis Инфраструктура, сделайте следующее.

1. Подготовьте загрузочный носитель с помощью ISO-образа дистрибутива (подключите его к виртуальному диску IPMI, создайте загрузочный USB-накопитель или настройте PXE-сервер).
2. Загрузите сервер с выбранного носителя.
3. На экране приветствия выберите **Установить Acronis Инфраструктура**.
4. На шаге 1 внимательно прочитайте лицензионное соглашение с конечным пользователем. Примите условия, установив флажок **Я принимаю лицензионное соглашение с конечным пользователем**, и нажмите кнопку **Далее**.
5. На шаге 2 настройте статический IP-адрес для сетевого интерфейса и укажите имя хоста: либо полное доменное имя (< >.< >), либо краткое имя (< >).
6. На шаге 3 выберите часовой пояс. Дата и время будут заданы посредством NTP. Для выполнения синхронизации потребуется подключение к Интернету.
7. На шаге 4 укажите тип устанавливаемого сервера. Сначала разверните один первичный сервер. Затем разверните нужное количество вторичных серверов.
   - Если вы развертываете первичный сервер, выберите два сетевых интерфейса: один для настройки и управления системными сервисами и один для доступа к панели администрирования. Также создайте и подтвердите пароль для учетной записи суперадминистратора панели администрирования.

- Если вы развертываете вторичный сервер, укажите IP-адрес сервера управления и токен. И то и другое можно получить из панели администрирования. Войдите на панель администрирования через порт 8888. IP-адрес панели отображается в консоли после развертывания первичного сервера. Введите имя пользователя по умолчанию `admin` и пароль учетной записи суперадминистратора. На панели администрирования откройте раздел **Инфраструктура** > **Серверы** и нажмите **Подключить сервер**, чтобы вызвать экран с адресом сервера управления и токеном.

  Сервер может появиться на экране **Инфраструктура** > **Серверы** со статусом **Без назначения** сразу после проверки токена. Однако его можно будет присоединить к кластеру хранилища только после завершения установки.

8. На шаге 5 выберите диск для операционной системы. Диску будет назначена дополнительная роль **Система**, хотя вы все равно сможете настроить его для хранения данных на панели администрирования. Также можно создать программный массив RAID1 для системного диска, чтобы обеспечить его высокую производительность и доступность.
9. На шаге 6 введите и подтвердите пароль для учетной записи пользователя root и нажмите **Начать установку**.

После завершения установки сервер автоматически перезагрузится. IP-адрес панели администрирования будет отображен в строке приветствия.

ГЛАВА 3

Создание кластера хранилища данных

Для создания кластера 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**.

Отслеживать создание кластера можно на экране **Инфраструктура** > **Серверы**. Создание может занять некоторое время в зависимости от количества настраиваемых дисков. Кластер будет создан после завершения автоматической настройки.

ГЛАВА 4

Добавление хранилищ в Acronis Cyber Backup или Acronis Cyber Backup Cloud

Примечание: Если вы хотите перенести Acronis Storage Gateway, пропустите шаги, описанные в этой главе, и перейдите к разделу *Перенос резервных копий из старых решений* (страница 23).

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).

4.1 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.

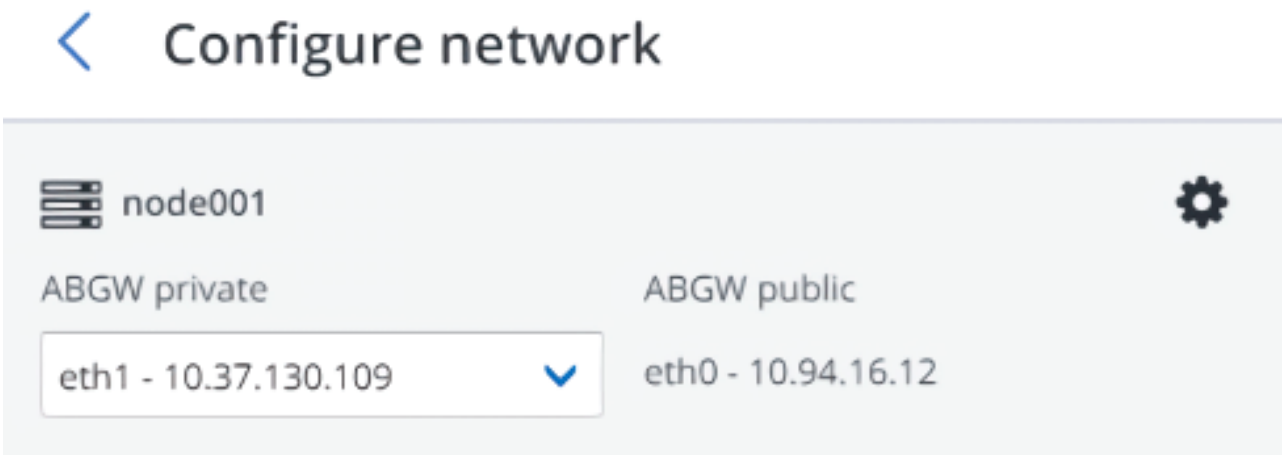
1. В окне **Инфраструктура** > **Сети** убедитесь, что в сети, которые вы собираетесь использовать, добавлены типы трафика **ABGW внутр.** и **ABGW внешн.**
2. В меню слева нажмите **Сервисы хранилища** > **Резервное копирование**.
3. Выберите серверы, на которых будут работать сервисы шлюза, и нажмите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

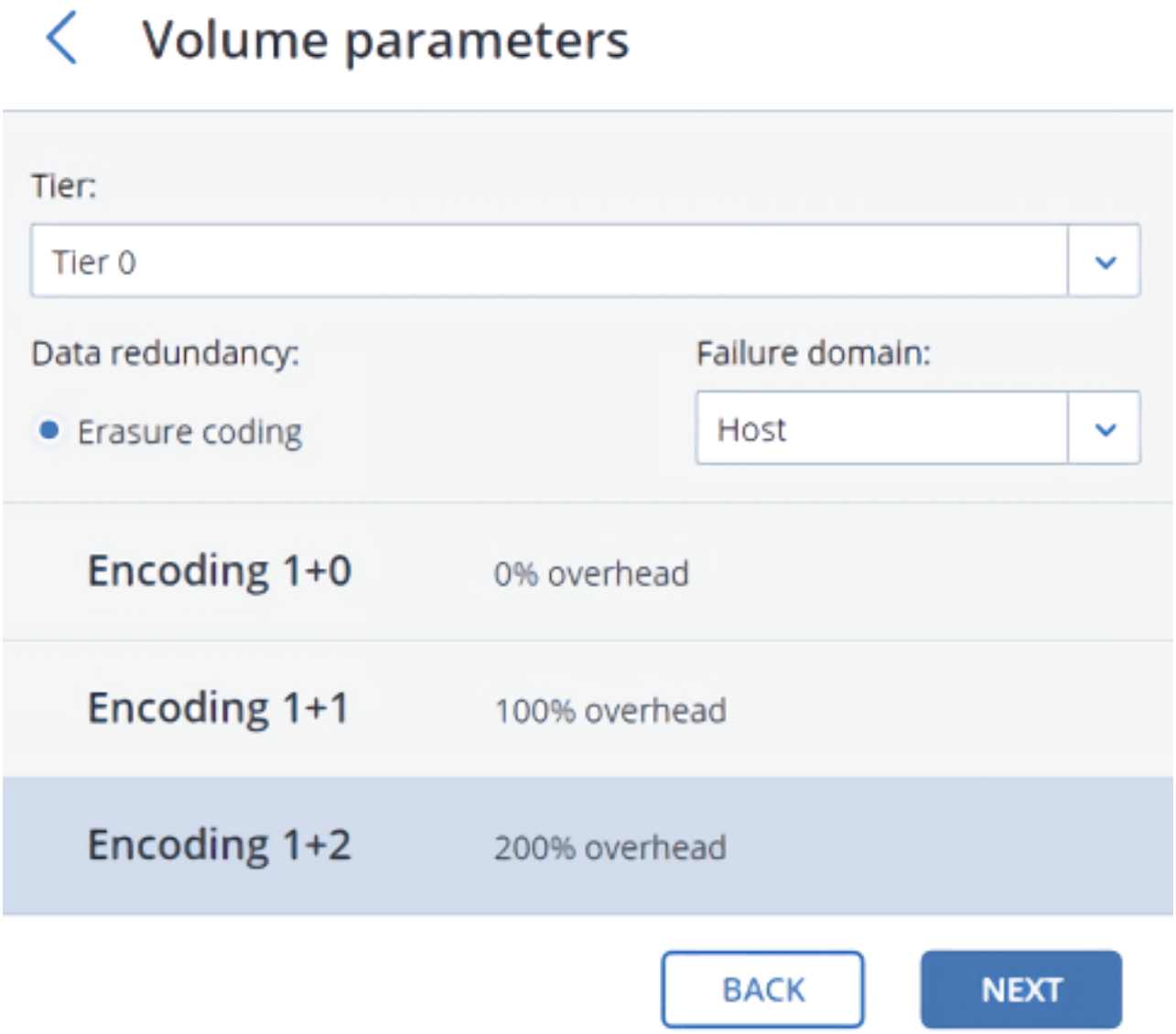
4. Выберите **Этот кластер Acronis Инфраструктура** в качестве типа хранилища.

5. Убедитесь, что в раскрывающемся списке выбран правильный сетевой интерфейс. Нажмите кнопку **Далее**.

   При необходимости нажмите значок шестерни и настройте сетевые интерфейсы сервера в окне **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**.

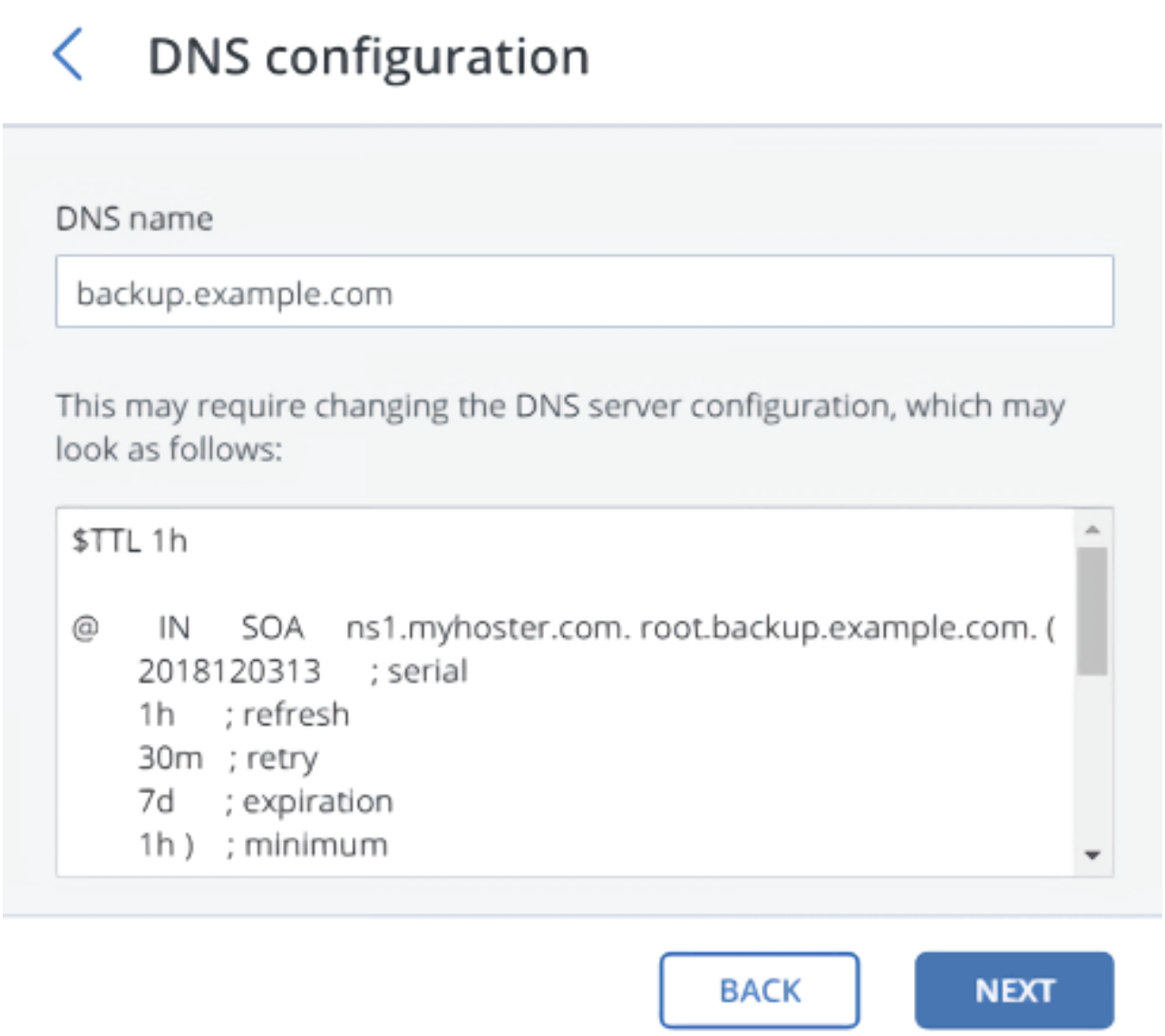


Избыточность за счет репликации не поддерживается для Backup Gateway. Для помехоустойчивого кодирования изменение схемы избыточности отключено, поскольку оно может снизить производительность кластера. Причина в том, что перекодирование потребляет значительный объем ресурсов кластера в течение длительного 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**.

4.2 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.

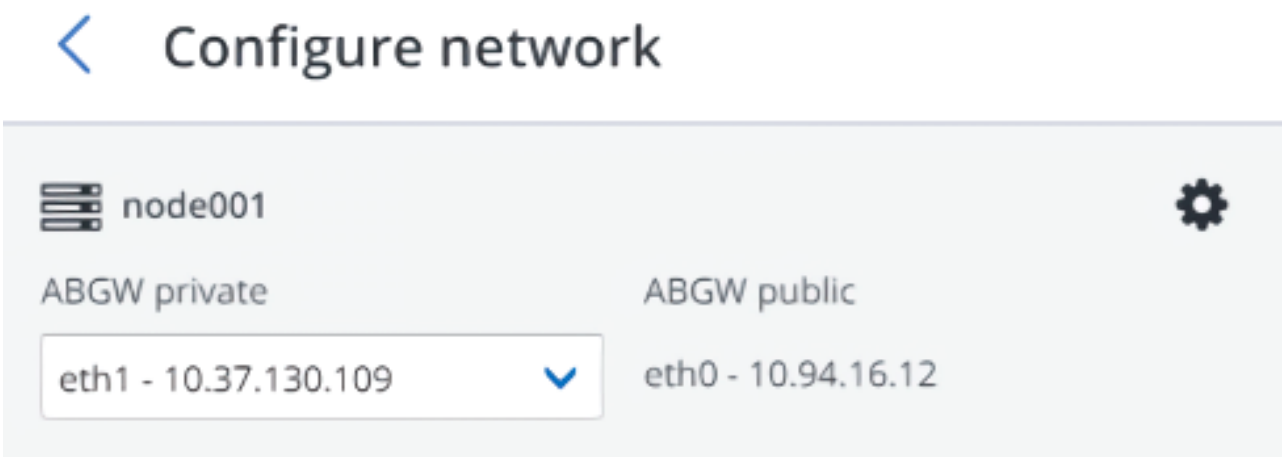
1. В окне **Инфраструктура** > **Сети** убедитесь, что в сети, которые вы собираетесь использовать, добавлены типы трафика **ABGW внутр.** и **ABGW внешн.**

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.

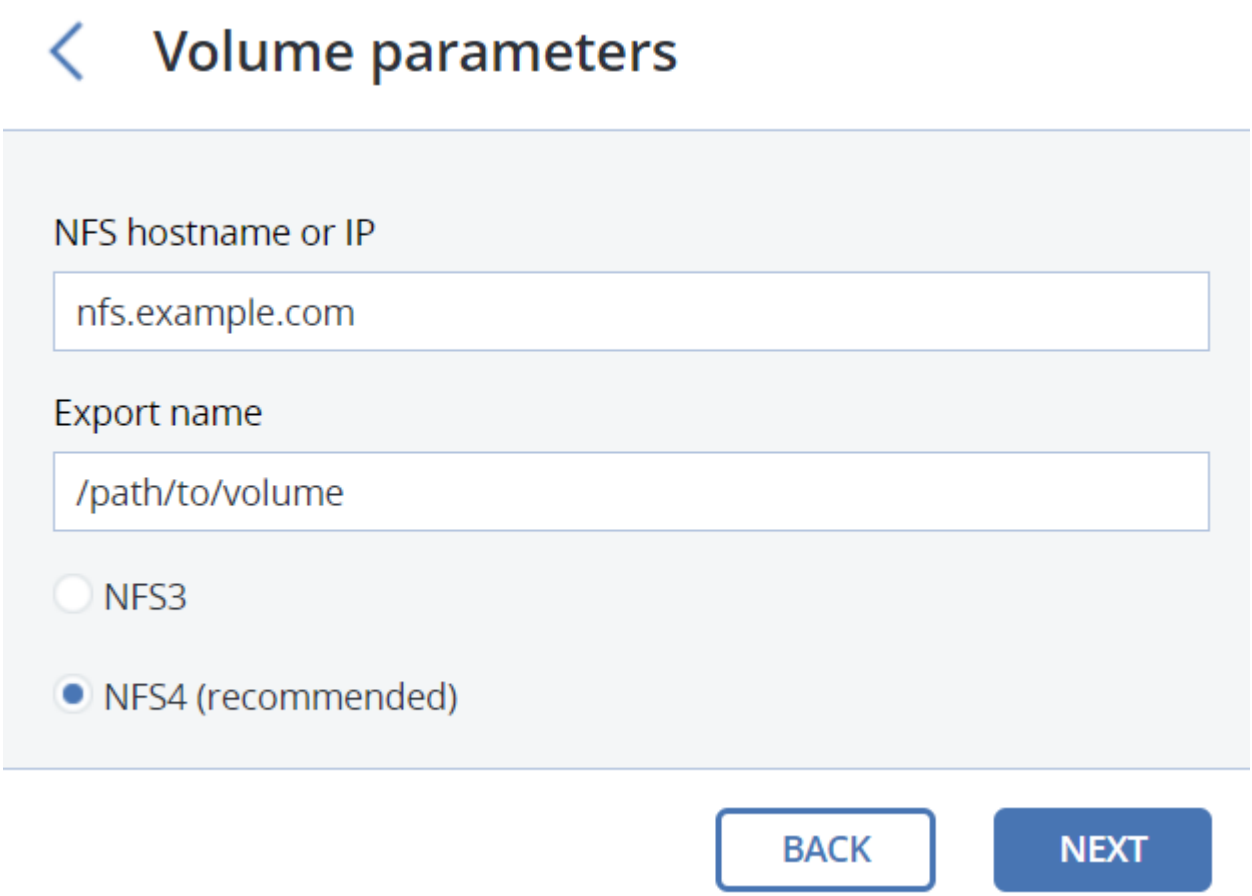
   Примечание: Серверы отображаются с небольшими значками, представляющими их роли внутри кластера. Дополнительные сведения о значках см. в статье https://kb.acronis.com/content/61024.

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 в окне **Конфигурация сети**.



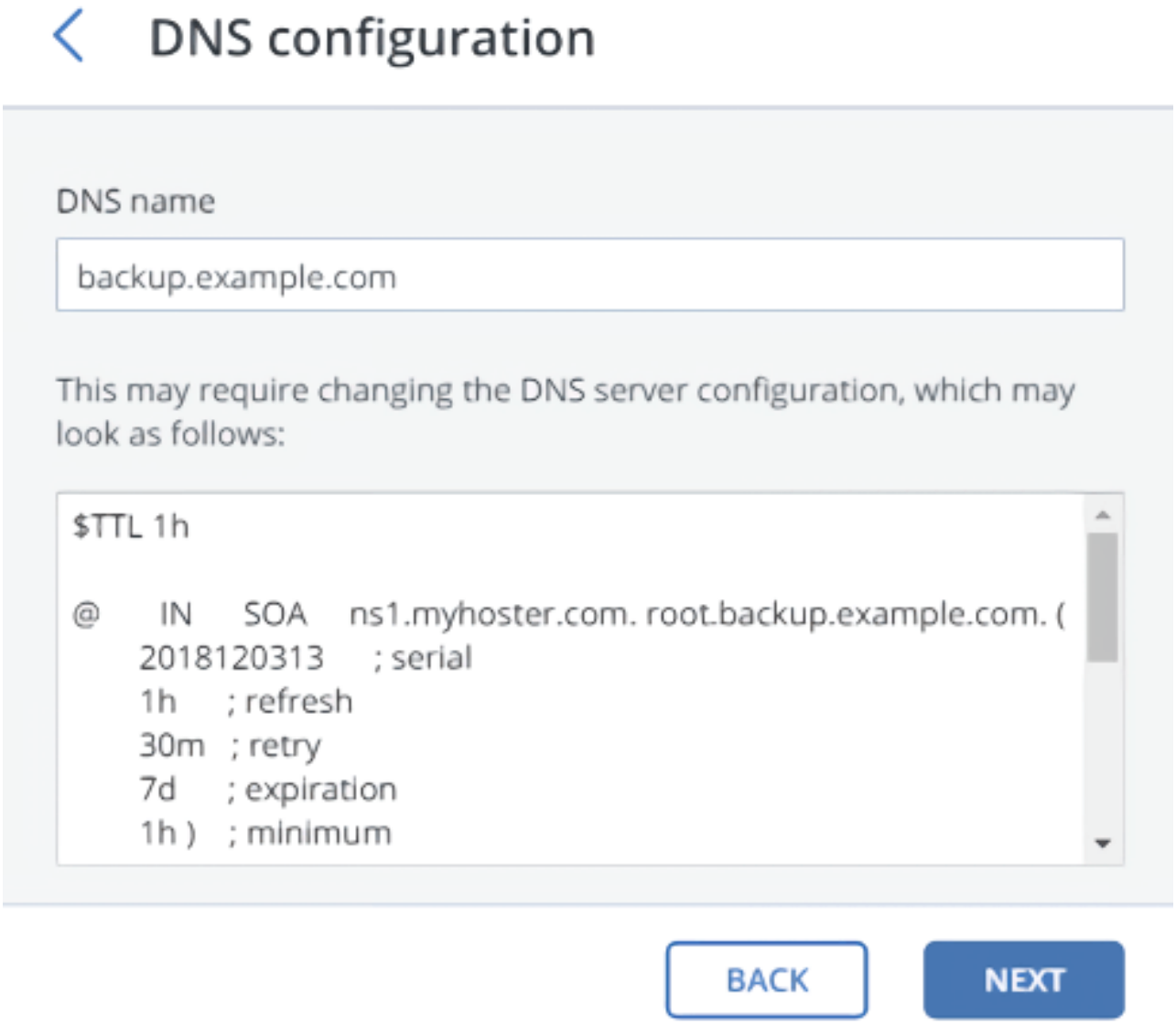
6. На панели **Параметры тома** укажите имя хоста или IP-адрес тома NFS, имя экспорта, а также выберите версию NFS. Рекомендуется версия NFS4, поскольку она обеспечивает лучшую масштабируемость и производительность по сравнению с версией NFS3, которая имеет ограничения в протоколе. Нажмите кнопку **Далее**.



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**.

4.3 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.

4.3.1 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 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.

- 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.
- 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.

4.3.2 Настройка Backup Gateway

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

Для настройки Backup Gateway выполните следующие действия.

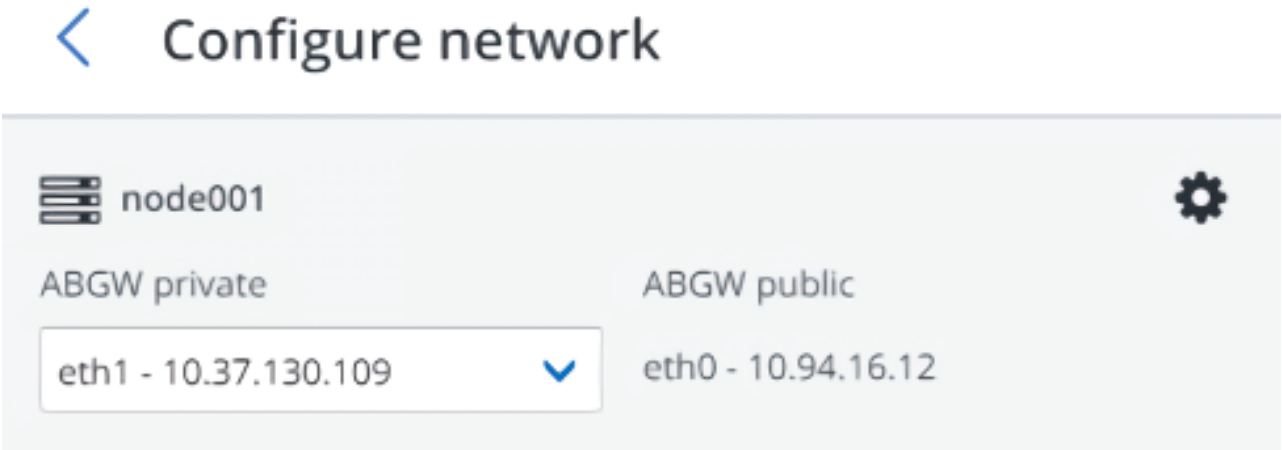
1. В окне **Инфраструктура** > **Сети** убедитесь, что в сети, которые вы собираетесь использовать, добавлены типы трафика **ABGW внутр.** и **ABGW внешн.**
2. В меню слева нажмите **Сервисы хранилища** > **Резервное копирование**.
3. Выберите серверы, на которых будут работать сервисы шлюза, и нажмите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

ГЛАВА 5

Updating the certificate for Backup Gateway

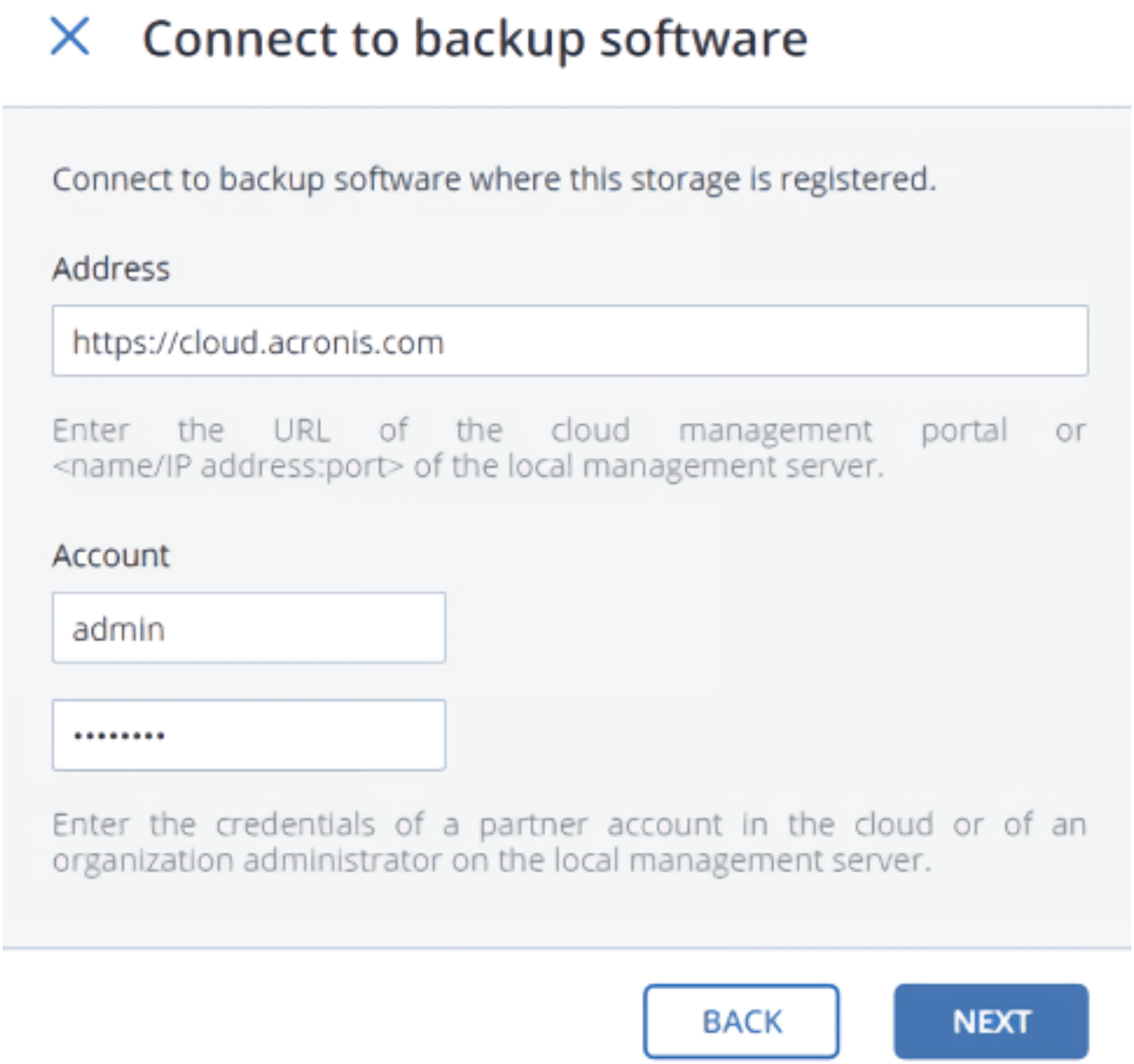
When you register a Backup Gateway in Acronis Cyber Backup Cloud or Acronis Cyber Backup, they exchange certificates that are valid for one year. One and a half months before expiration, you will be alerted about the expiring certificate in the admin panel. To update the certificate, you need to connect to your backup software and renew the certificate. Do the following:

1. On the **Storage services** > **Backup storage** screen, click **Update certificate**.
2. На панели **Подключение** укажите следующую информацию для вашего продукта Acronis.

   Важно: Make sure that two-factor authentication (2FA) is disabled for your partner account. You can also disable it for a specific user within a 2FA-enabled tenant, as described in Acronis Cyber Cloud documentation, and specify the user credentials.

   2.1. In **Address**, specify the address of the Acronis Cyber Backup Cloud management portal (for example, https://cloud.acronis.com/) or the hostname/IP address and port of the Acronis Cyber Backup management server (for example, http://192.168.1.2:9877).

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



3. Нажмите кнопку **Далее**.
4. На всех серверах, входящих в кластер Backup Gateway, перезапустите сервис:

```
# systemctl restart vstorage-abgw
```

ГЛАВА 6

Перерегистрация Backup Gateway на новом экземпляре Acronis Cyber Backup

Чтобы переключить настроенный шлюз Backup Gateway на другой экземпляр Acronis Cyber Backup, перерегистрируйте шлюз на этом экземпляре. Для этого выполните следующие действия.

1. В окне **Сервисы хранилища** > **Резервное копирование** нажмите **Перерегистрация**.
2. На вкладке **Перерегистрация в Acronis Backup** укажите следующие сведения.
   2.1. В поле **Адрес** укажите имя хоста/IP-адрес целевого сервера управления и порт 9877 (например, http://192.168.1.2:9877). Обратите внимание, что адрес следует задавать с использованием протокола HTTP, а не HTTPS.
   2.2. В поле **Аккаунт** укажите данные учетной записи администратора сервера управления.
3. Нажмите кнопку **Готово**.

ГЛАВА 7

Перенос резервных копий из старых решений

С помощью Backup Gateway можно перенести резервные копии из Acronis Storage 1.5 и Acronis Storage Gateway 1.6 и 1.7 в выбранное внутреннее хранилище: локальный кластер хранилища, внешний том NFS или публичное облако.

Однако миграция во внутренние хранилища NFS недоступна, если в качестве Backup Gateway выбрано несколько серверов.

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

Процедуру миграции можно описать следующим образом.

1. Учетные данные суперпользователя (root) для доступа по протоколу SSH к выбранному исходному хранилищу передаются сервису Backup Gateway.
2. Backup Gateway устанавливает прокси-сервер для исходного хранилища, который перенаправляет входящие запросы от агентов Acronis Backup к исходному хранилищу на шлюз Backup Gateway.
3. Backup Gateway начинает перемещение резервных копий в выбранное внутреннее хранилище. Данные, которые еще не были перенесены, отображаются в разделе **Остаток миграции** в окне **Сводка** Backup Gateway. Когда раздел опустеет, это будет означать, что все данные перенесены.

После запуска миграции данные новых и инкрементных резервных копий сохраняются в целевом хранилище. Резервные копии из исходного хранилища передаются в фоновом режиме. Весь процесс прозрачен для агентов резервного копирования, которые продолжают работу без прерываний.

4. Чтобы можно было освободить исходное хранилище после завершения миграции, запросы от агентов Acronis Backup направляются непосредственно на шлюз Backup Gateway, в обход прокси исходного хранилища. Действия, которые следует выполнить, зависят от способа регистрации исходного хранилища в Acronis Cyber Backup Cloud:

   - Если исходное хранилище уже зарегистрировано под доменным именем, необходимо изменить IP-адрес, сопоставляемый с этим именем, на адреса серверов Backup Gateway.
   - Если исходное хранилище зарегистрировано под IP-адресом, настоятельно рекомендуется перерегистрировать Backup Gateway в Acronis Cyber Backup Cloud под доменным именем, которое преобразуется в IP-адреса серверов Backup Gateway. Использование доменного имени упростит переход, и вам не нужно будет перенастраивать Acronis Cyber Backup Cloud даже при изменении серверов Backup Gateway (хотя все равно потребуется откорректировать IP-адреса, соответствующие доменному имени).

     Либо, если вы не хотите использовать доменное имя, необходимо дождаться завершения миграции, выключить исходную и целевую машины и перенастроить сеть таким образом, чтобы открытый интерфейс целевой машины получил IP-адрес исходной машины.

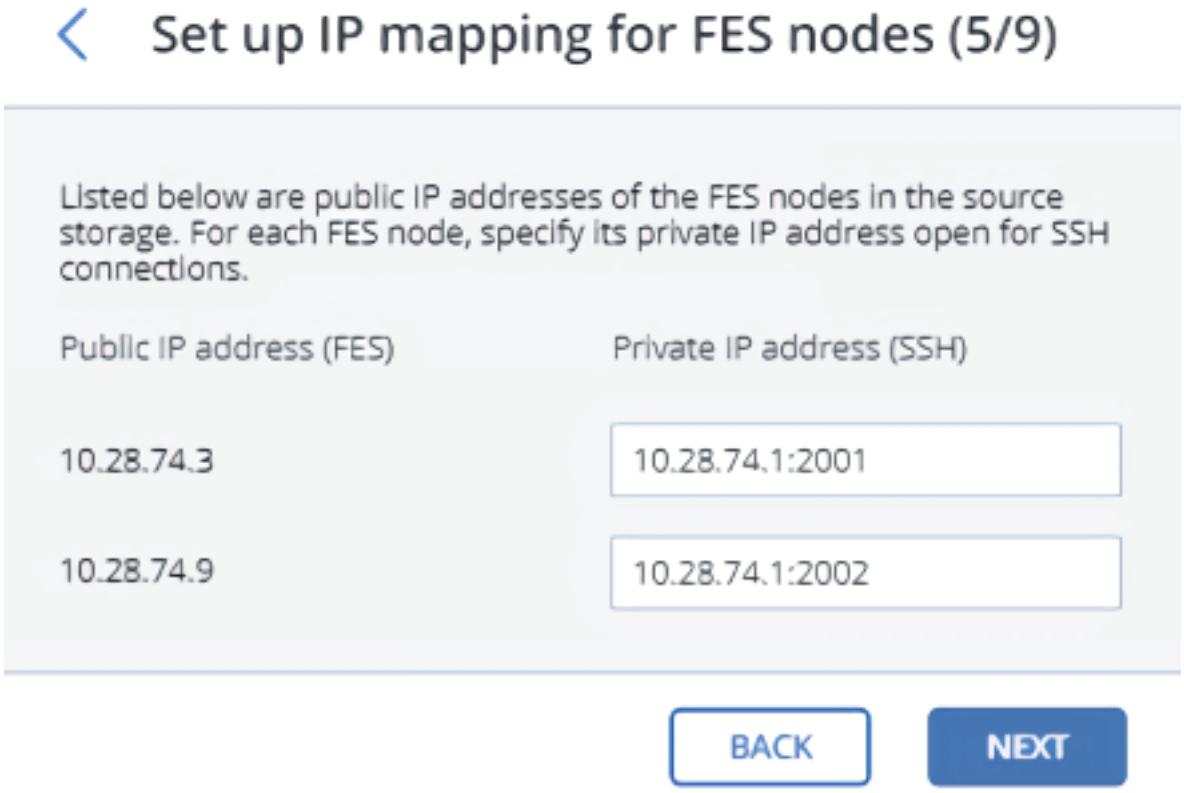
Конкретные шаги, которые следует выполнить в панели администратора для запуска миграции резервных копий, описаны в следующих подразделах.

7.1 Перенос резервных копий из Acronis Storage 1.5

1. Обновите все серверы Acronis Storage 1.5 до версии 1.5.65665 или выше, поскольку миграция из более старых версий не поддерживается. Для этого выполните вход в веб-консоль Acronis Storage, перейдите на страницу **Настройки** > **Обновление ПО**, загрузите последний ISO-образ и нажмите **Обновить**.
2. Выполните вход в новый кластер хранилища. В окне **Сервисы хранилища** > **Резервное копирование** > **Серверы** выберите один или несколько серверов и нажмите **Мигрировать**.

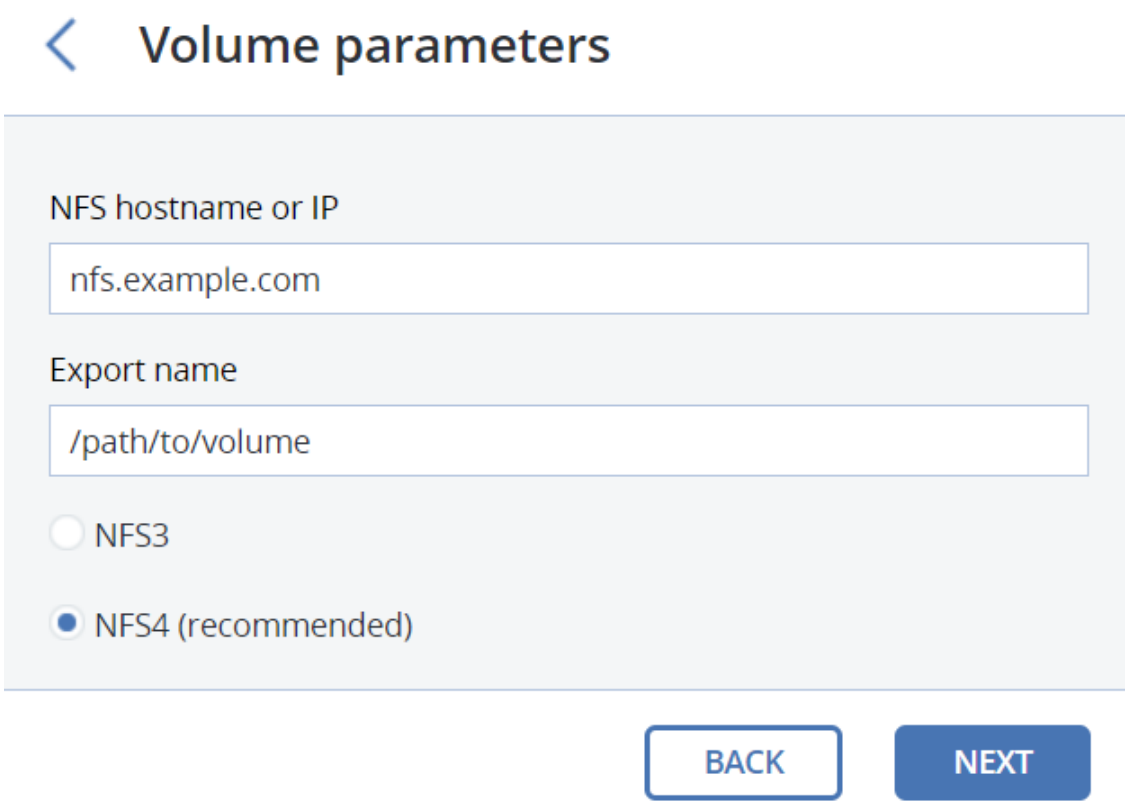
3. Выберите **Acronis Storage 1.5** и нажмите кнопку **Далее**.
4. Укажите доменное имя исходного хранилища, зарегистрированное в Acronis Cyber Backup Cloud, и нажмите кнопку **Далее**.

5. Введите учетные данные портала управления облаком для продукта Acronis Cyber Backup Cloud, в котором зарегистрировано исходное хранилище, и нажмите кнопку **Далее**.
6. Включите SSH-доступ на всех серверах FES хранилища Acronis Storage 1.5, в соответствии с инструкцией, и нажмите кнопку **Далее**.
7. Сопоставьте внешние IP-адреса серверов FES, доступных через SSH, с их внутренними IP-адресами и нажмите кнопку **Далее**. Этот шаг требуется для доступа к серверам FES через SSH-туннели.



8. Выберите тип хранилища, чтобы создать шлюз для одного из следующих мест назначения:
   - Локальный кластер хранилища
   - Внешний том NFS
   - Публичное облако
9. Убедитесь, что в раскрывающемся списке выбран правильный сетевой интерфейс. Нажмите кнопку **Далее**.

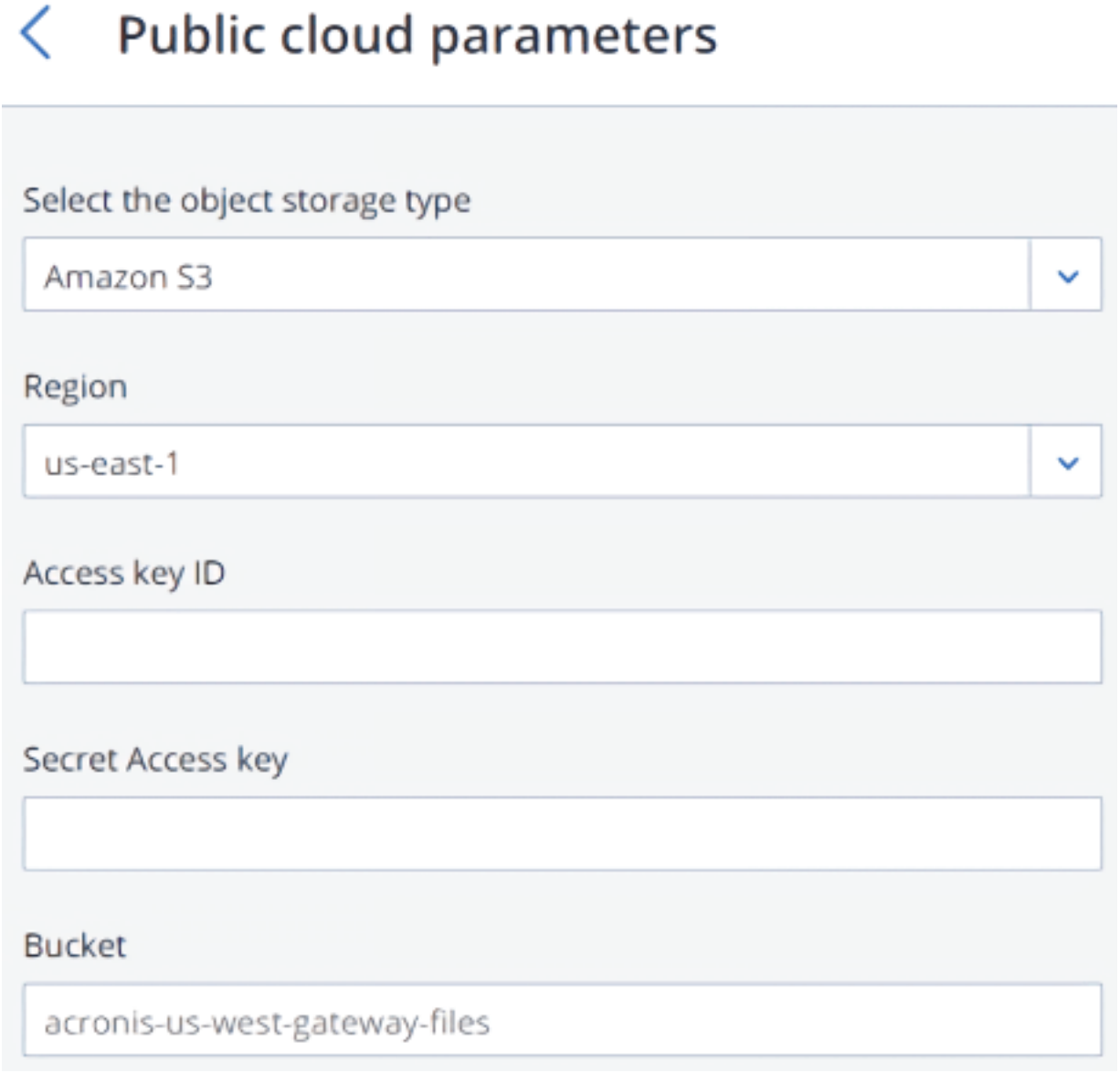
   При необходимости нажмите значок шестерни и настройте сетевые интерфейсы сервера в окне **Конфигурация сети**.
10. Настройте целевое внутреннее хранилище следующим образом.
    - Для кластера хранилища выберите нужный уровень, область отказа и режим избыточности.
    - Для тома NFS укажите имя хоста или IP-адрес, имя и путь экспорта, а также выберите версию NFS.



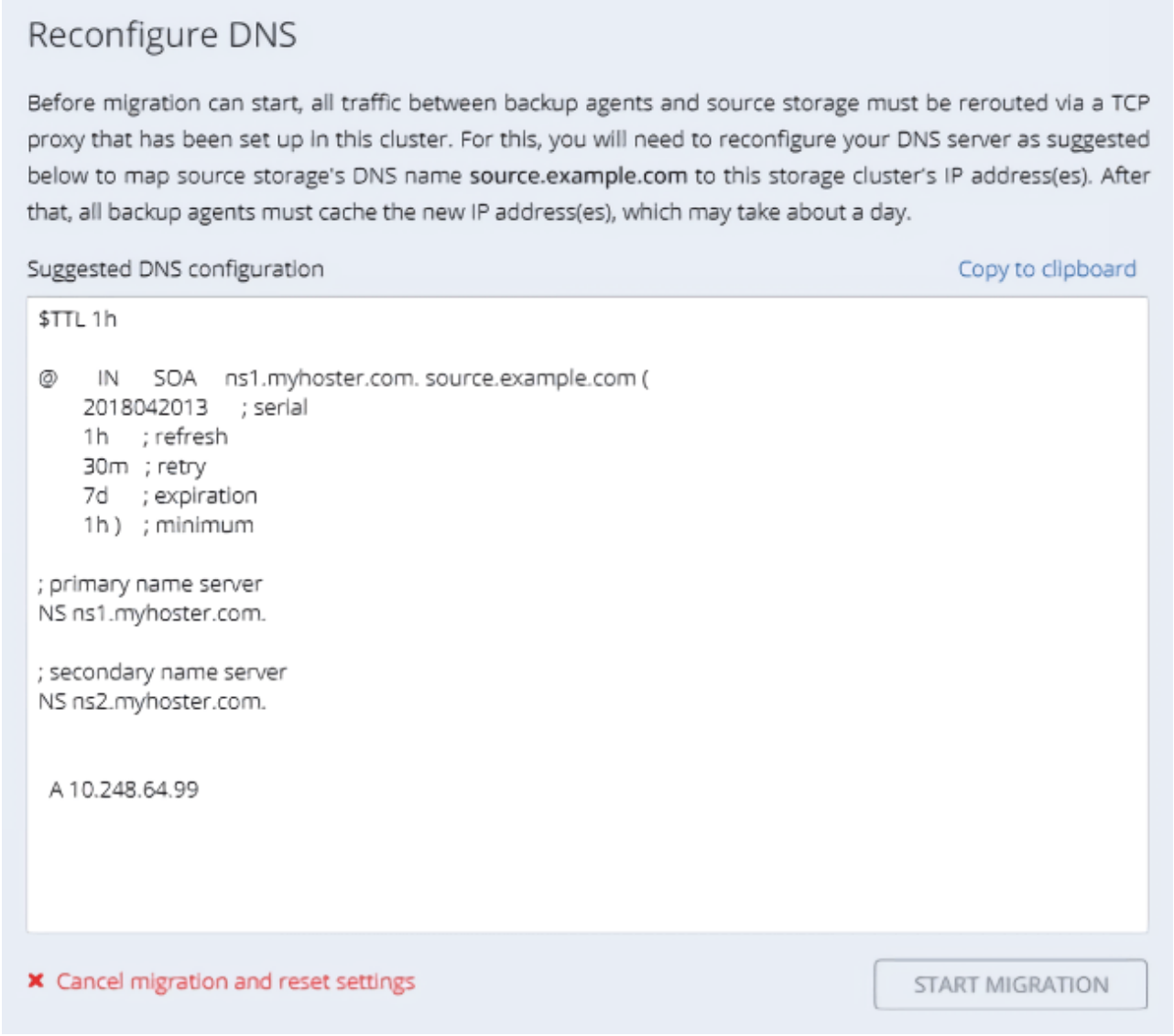
- Для публичного облака выберите поставщика облачного сервиса, укажите учетные данные и имя папки (корзины, контейнера).

  Для каждого кластера Backup Gateway следует использовать отдельный контейнер объектов.

  Нажмите кнопку **Далее**.



11. Проверьте параметры исходного и целевого хранилища и нажмите **Proceed**.
12. На следующей панели выполните инструкции по сопоставлению доменного имени исходного хранилища с IP-адресами нового кластера хранилища. После обновления конфигурации DNS подождите 24 часа, пока все агенты резервного копирования не выполнят кэширование новых IP-адресов. До этого времени кнопка **Начать миграцию** будет неактивна. После перенаправления всех агентов резервного копирования на новый кластер кнопка станет активной и вы сможете начать миграцию.



В зависимости от объема данных миграция может занять до нескольких дней.

7.2 Перенос резервных копий из Acronis Storage Gateway 1.6 и 1.7 (NFS)

1. Отключите брандмауэр или напрямую откройте TCP-порт 44446 на исходном шлюзе Acronis Storage Gateway.

    - Чтобы отключить брандмауэр, выполните команду

```
# systemctl stop firewalld
```

- Чтобы открыть TCP-порт 44446 в брандмауэре, выполните следующие действия.

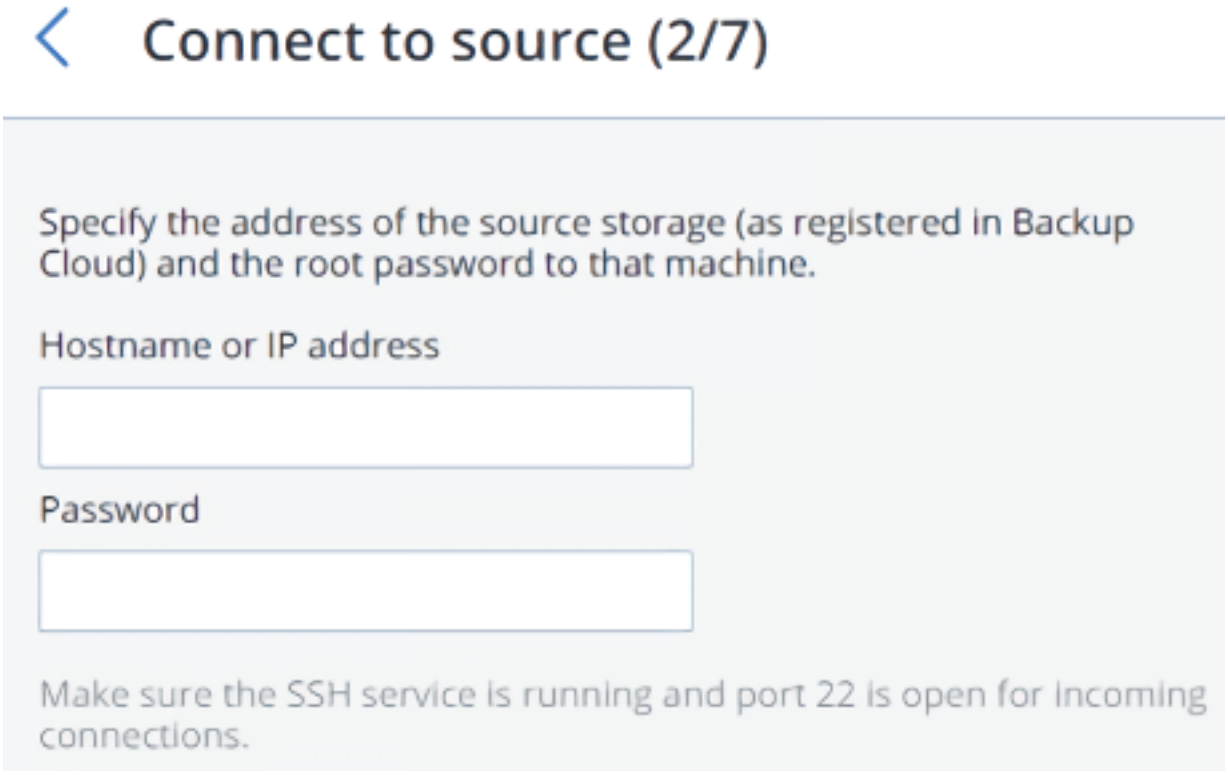
1.1. Определите зону, в которой открыт порт 44445:

```
# firewall-cmd --list-all-zones | grep active
mix_eth0 (active)
```

1.2. Добавьте нужный порт в эту же зону:

```
# firewall-cmd --zone=mix_eth0 --permanent --add-port=44446/tcp
# firewall-cmd --reload
```

2. На панели администратора сервера Backup Gateway перейдите в раздел **Сервисы хранилища** > **Резервное копирование** > **Серверы**, выберите серверы, на которых будут работать сервисы шлюза, и нажмите **Мигрировать**.
3. Выберите версию исходного хранилища и нажмите кнопку **Далее**.
4. Укажите сведения о подключении к исходному хранилищу и нажмите кнопку **Далее**.



5. Введите учетные данные портала управления облаком для продукта Acronis Cyber Backup Cloud, в котором зарегистрировано исходное хранилище, и нажмите кнопку **Далее**.

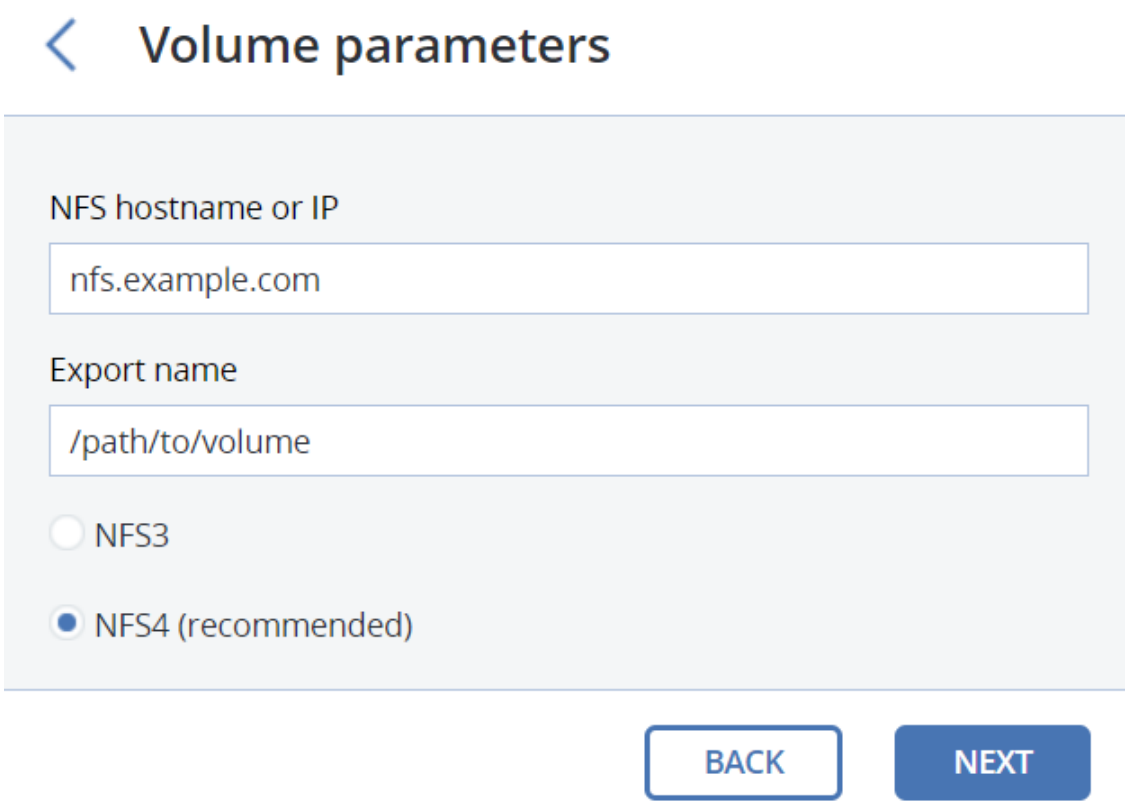
6. Если исходное хранилище зарегистрировано в Acronis Cyber Backup Cloud под IP-адресом, откроется окно настройки DNS. В этом окне нажмите **Продолжить с DNS** и укажите доменное имя исходного хранилища (рекомендуется, см. выше). Либо, если вы хотите продолжить использовать IP-адрес, нажмите **Продолжить с IP**.

   Если вы указали доменное имя, настройте DNS-сервер в соответствии с предложенным примером.

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

7. Выберите тип хранилища, чтобы создать шлюз для одного из следующих мест назначения:
   - Локальный кластер хранилища
   - Внешний том NFS
   - Публичное облако
8. Убедитесь, что в раскрывающемся списке выбран правильный сетевой интерфейс. Нажмите кнопку **Далее**.

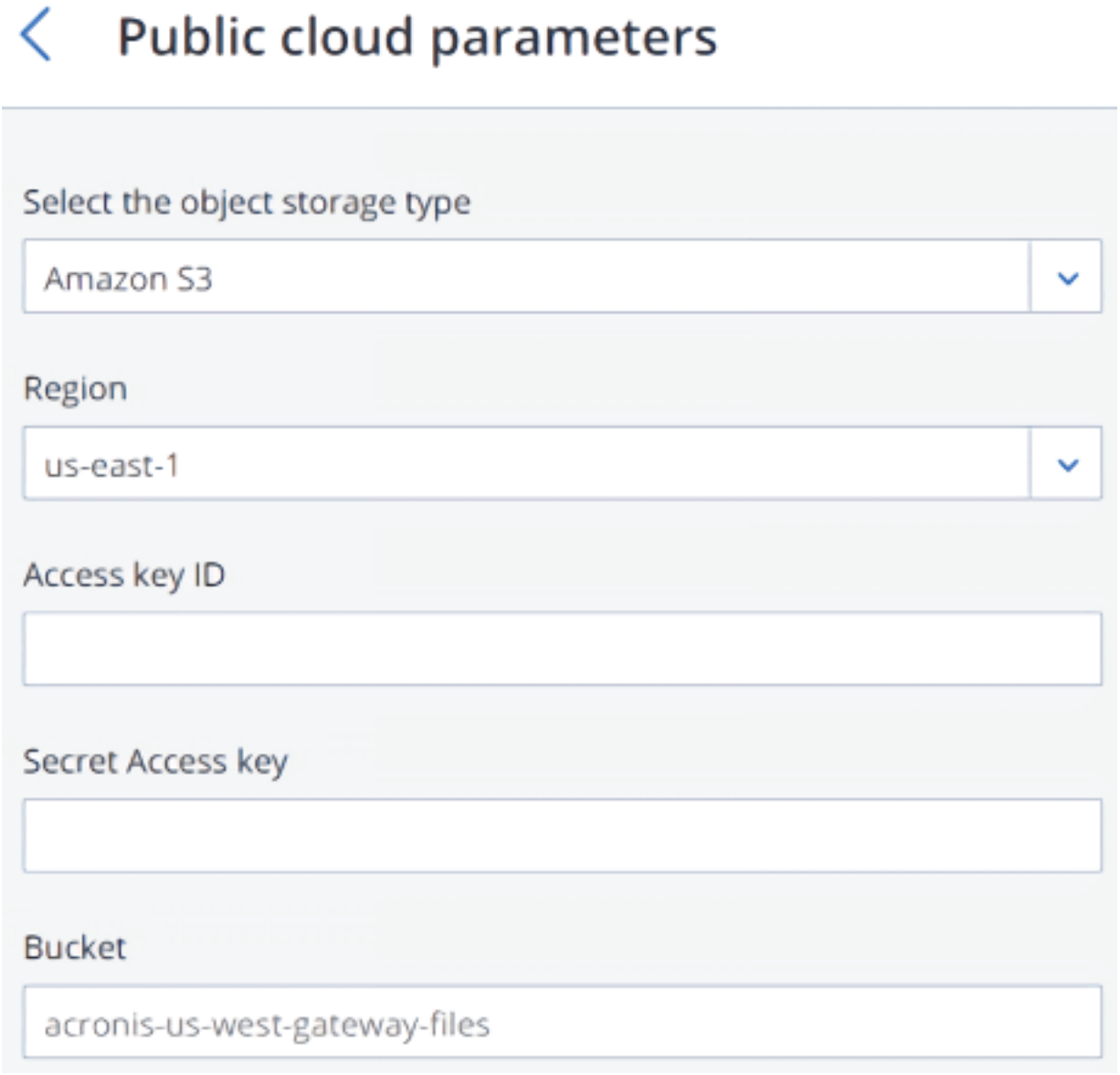
   При необходимости нажмите значок шестерни и настройте сетевые интерфейсы сервера в окне **Конфигурация сети**.
9. Настройте целевое внутреннее хранилище следующим образом.
   - Для кластера хранилища выберите нужный уровень, область отказа и режим избыточности.
   - Для тома NFS укажите имя хоста или IP-адрес, имя и путь экспорта, а также выберите версию NFS.



- Для публичного облака выберите поставщика облачного сервиса, укажите учетные данные и имя папки (корзины, контейнера).

  Для каждого кластера Backup Gateway следует использовать отдельный контейнер объектов.

  Нажмите кнопку **Далее**.



10. Проверьте параметры исходного и целевого хранилища и нажмите **Start migration**.

В зависимости от объема данных миграция может занять до нескольких дней.

ГЛАВА 8

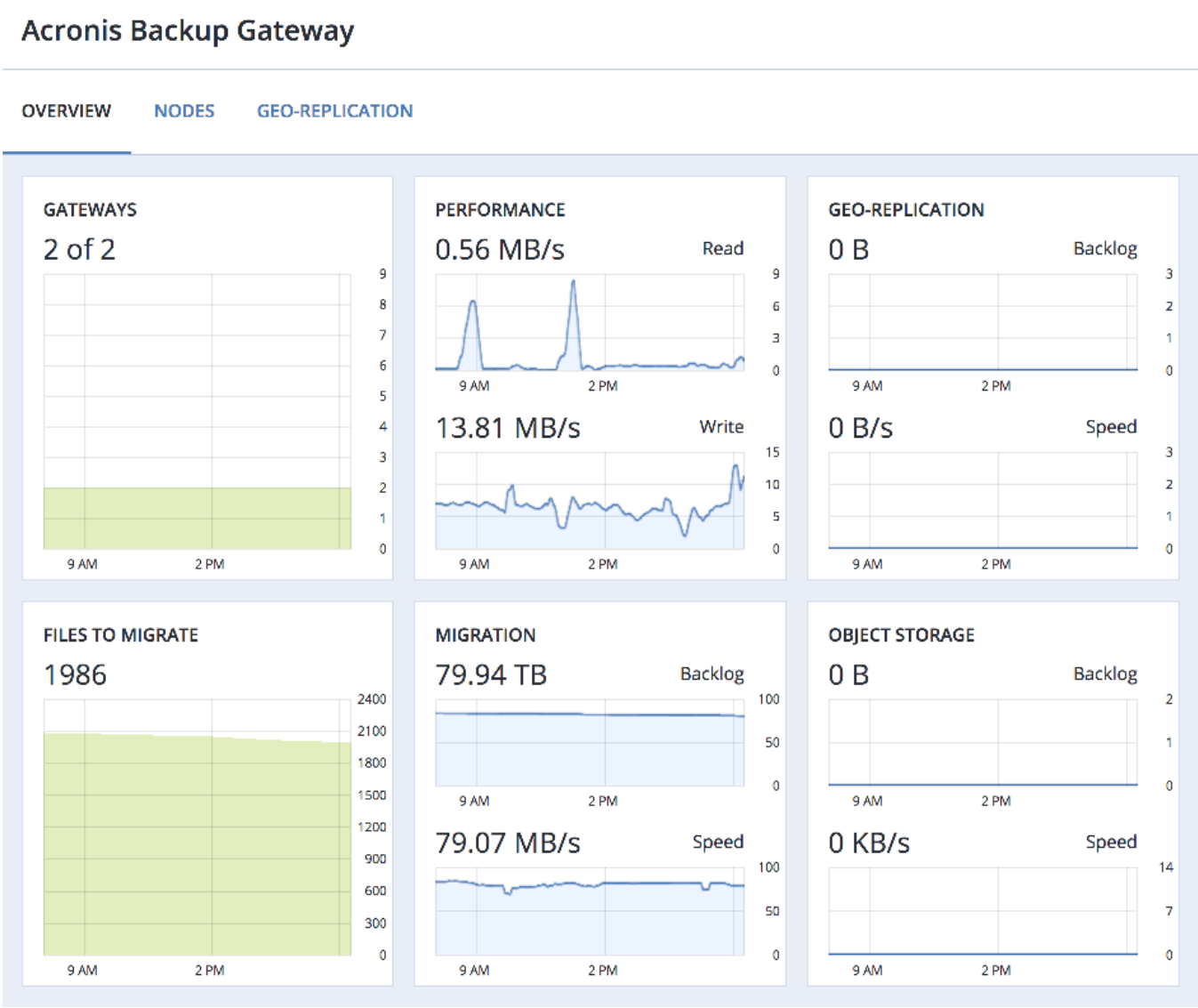
Мониторинг шлюза Backup Gateway

После создания шлюза Backup Gateway его состояние можно отслеживать в окне **Сервисы хранилища** > **Резервное копирование** > **Сводка**. На диаграммах отображается следующая информация:

- Производительность сервисов Backup Gateway
- Скорость и остаток георепликации (объем данных, которые еще не реплицированы)
- Скорость и остаток хранилища объектов (объем данных, которые еще не загружены в публичное облако)
- Скорость и остаток миграции (объем данных, которые еще не перенесены)
- Количество файлов, оставшихся в очереди миграции

При переносе резервных копий из Acronis Storage 1.5 или 1.7 остаток миграции будет больше объема данных в исходном хранилище. Причина в том, что Acronis Storage до версии 2.x использует старый протокол резервного копирования (FES), который пересылает больше данных по сети. Разница между размером данных в исходном хранилище и остатком также сильно зависит от политики хранения, используемой решением для резервного копирования. Несмотря на это, место, занимаемое перенесенными данными в целевом хранилище, не будет сильно отличаться от исходного.

Если остаток не снижается со временем, это означает, что данные не удается реплицировать, перенести или загрузить достаточно быстро. Причиной может быть недостаточная скорость передачи данных по сети, и может потребоваться проверить или обновить сетевое оборудование.


Acronis Backup Gateway
OVERVIEW
NODES
GEO-REPLICATION
GATEWAYS
2 of 2
9 AM
2 PM
PERFORMANCE
0.56 MB/s
Read
13.81 MB/s
Write
GEO-REPLICATION
0 B
Backlog
0 B/s
Speed
FILES TO MIGRATE
1986
MIGRATION
79.94 TB
Backlog
79.07 MB/s
Speed
OBJECT STORAGE
0 B
Backlog
0 KB/s
Speed

ГЛАВА 9

Освобождение серверов от Backup Gateway

Шлюз Backup Gateway предназначен для доступа к определенному внутреннему хранилищу. Если необходимо поменять внутреннее хранилище, например, с публичного облака на локальный кластер хранилища или с одной корзины облачного сервиса на другую, необходимо удалить шлюз Backup Gateway путем освобождения всех его серверов и создать новый.

При удалении шлюза Backup Gateway также отменяется его регистрация в продукте Acronis Backup, который теряет доступ к внутреннему хранилищу.

Для освобождения последнего сервера шлюза выполните следующие действия.

1. В окне **Сервисы хранилища** > **Резервное копирование** > **Серверы** выберите нужный сервер и нажмите **Освободить**.
2. На панели **Отменить регистрацию** выберите один из следующих вариантов.
   - **Штатное освобождение** (рекомендуется). Освобождает сервер, удаляет шлюз Backup Gateway и отменяет его регистрацию в продукте Acronis Backup.
   - **Принудительно**. Освобождает сервер, удаляет шлюз Backup Gateway, но не отменяет его регистрацию в продукте Acronis Backup.

     Важно: Выбирайте этот вариант, только если уверены, что регистрация шлюза в Acronis Backup уже отменена. В противном случае потребуется зарегистрировать новый шлюз в

Acronis Backup, а для этого необходимо будет удалить и создать заново не только шлюз Backup Gateway, но и весь кластер хранилища.

3. Укажите данные учетной записи администратора вашего продукта Acronis Backup и нажмите кнопку **Далее**. В случае принудительного освобождения просто нажмите **Далее**.