

Акронис

Инфозащита

Acronis Инфраструктура 3.5

Backup Gateway Quick Start Guide

16 июля 2020 г.

Заявление об авторских правах

Авторские права ©ООО «Акронис-Инфозащита» 2020. Все права защищены.

Наименование Linux является зарегистрированным товарным знаком Линуса Торвальдса.

VMware и VMware Ready являются торговыми знаками и (или) зарегистрированными торговыми знаками компании VMware, Inc. в США и (или) других странах.

Windows и MS-DOS — зарегистрированные товарные знаки корпорации Майкрософт.

Все остальные упоминаемые товарные знаки могут быть зарегистрированными товарными знаками тех или иных фирм.

Распространение существенно измененных версий данного руководства запрещено без явного разрешения владельца авторских прав.

Распространение настоящих или переработанных материалов, входящих в данное руководство, в виде печатного издания (книги) запрещено без письменного разрешения их владельца.

ДОКУМЕНТАЦИЯ ПОСТАВЛЯЕТСЯ «КАК ЕСТЬ». НЕ СУЩЕСТВУЕТ НИКАКИХ ЯВНО ВЫРАЖЕННЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ ОБЯЗАТЕЛЬСТВ, ПОДТВЕРЖДЕНИЙ ИЛИ ГАРАНТИЙ, В ТОМ ЧИСЛЕ И СВЯЗАННЫХ С ТОВАРНОСТЬЮ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ИЛИ ПРИГОДНОСТЬЮ ЕГО ДЛЯ ИСПОЛЬЗОВАНИЯ В ОПРЕДЕЛЕННЫХ ЦЕЛЯХ, НАСКОЛЬКО ТАКАЯ ОГРАНИЧЕННОСТЬ ОТВЕТСТВЕННОСТИ ДОПУСКАЕТСЯ ЗАКОНОМ.

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. Обновляемый список кода сторонних производителей и условия лицензии, применимые к программному обеспечению и/или службе, см. по адресу <http://kb.acronis.com/content/7696>.

Оглавление

1. Введение	1
1.1 Об этом руководстве	1
1.2 Аппаратные требования для вариантов установки с Backup Gateway	1
2. Установка продукта Acronis Инфраструктура	3
3. Создание кластера хранилища данных	5
4. Подключение Acronis Backup к внутренним хранилищам через Backup Gateway	7
4.1 Подключение к локальному кластеру хранилища через Backup Gateway	8
4.2 Подключение к внешним томам NFS через Backup Gateway	11
4.3 Подключение к публичному облачному хранилищу через Backup Gateway	14
4.3.1 Важные требования и ограничения	15
4.3.2 Настройка Backup Gateway	16
5. Обновление сертификата для Backup Gateway	18
6. Перерегистрация Backup Gateway на новом экземпляре Acronis Backup Advanced	20
7. Перенос резервных копий из старых решений	21
7.1 Перенос резервных копий из Acronis Storage 1.5	22
7.2 Перенос резервных копий из Acronis Storage Gateway 1.6 и 1.7 (NFS)	27
8. Мониторинг шлюза Backup Gateway	31
9. Освобождение серверов от Backup Gateway	33

ГЛАВА 1

Введение

1.1 Об этом руководстве

В этом руководстве описывается развертывание продукта Acronis Инфраструктура на одиночном сервере с целью создания конечных 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 (VM) как минимум с двумя виртуальными жесткими дисками (рекомендуется три). В этом случае только один жесткий диск будет использоваться для хранения данных, и необходимо будет убедиться, что избыточность VM обеспечивается решением виртуализации, на базе которого она работает.
- Использовать физический сервер как минимум с двумя дисками (рекомендуется три). Учтите, что вам потребуется больше дисков для хранения, чтобы обеспечить избыточность данных. Дополнительные сведения о планировании конфигурации сервера см. в документе 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	2 сетевых интерфейса 1 GbE

* 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 документе [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 с дистрибутивом (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 NIC и укажите имя хоста: либо полное доменное имя (имя хоста, имя домена), либо краткое имя (имя хоста).
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. То и другое можно получить из панели администрирования. Войдите в 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. В панели администрирования откройте раздел **ИНФРАСТРУКТУРА > Серверы** и нажмите **ДОБАВИТЬ СЕРВЕР**, чтобы вызвать экран с адресом сервера управления и токеном.

Сервер может появиться на экране **ИНФРАСТРУКТУРА > Серверы** в списке **НЕНАЗНАЧЕН** 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. Дisku будет назначена дополнительная роль **Система**, хотя вы все равно сможете настроить его для хранения данных в 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 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 щелкните сервер в списке **НЕНАЗНАЧЕН**.
2. На экране обзора сервера щелкните **Создать кластер**.
3. В поле **Кластер** введите имя для кластера. Имя может содержать только буквы латинского алфавита (a-z, A-Z), цифры (0-9), символы подчеркивания («_») и дефисы («-»).

✕ New cluster

Create cluster on node **node001**

Cluster

Storage interface

  
  Encryption 

NEW CLUSTER **ADVANCED CONFIGURATION**

4. Нажмите **Создать кластер**.

Отслеживать создание кластера можно в списке **ИСПРАВЕН** экрана **ИНФРАСТРУКТУРА > Серверы**.
Создание может занять некоторое время в зависимости от количества настраиваемых дисков. Кластер будет создан после завершения автоматической настройки.

ГЛАВА 4

Подключение Acronis Backup к внутренним хранилищам через Backup Gateway

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 21).

Точка доступа к хранилищу Backup Gateway (также называемая «шлюзом») предназначена для поставщиков услуг, которые используют Acronis Backup Cloud и/или Acronis Backup Advanced 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 хранения 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 избыточность данных и не производит дедупликацию.
- Чтобы можно было зарегистрировать Backup Gateway в Acronis 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** в меню справа.
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.**

< Configure network

node001 ⚙️

ABGW private ABGW public

eth1 - 10.37.130.109 eth0 - 10.94.16.12

6. На вкладке **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.

< Volume parameters

Tier:

Tier 0 ▼

Data redundancy: Failure domain:

Erasure coding Host ▼

Encoding 1+0	0% overhead
Encoding 1+1	100% overhead
Encoding 1+2	200% overhead

BACK
NEXT

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.

Нажмите кнопку **ДАЛЕЕ**.

7. На вкладке **Настройка DNS** укажите внешнее DNS-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.

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

Важно: При каждом изменении серверов в кластере Backup Gateway корректируйте настройки DNS соответствующим образом.

< DNS configuration

DNS name

This may require changing the DNS server configuration, which may look as follows:

```
$TTL 1h
@ IN SOA ns1.myhoster.com. root.backup.example.com. (
2018120313 ;serial
1h ;refresh
30m ;retry
7d ;expiration
1h ) ;minimum
```

BACK NEXT

Нажмите кнопку **Далее**.

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.

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

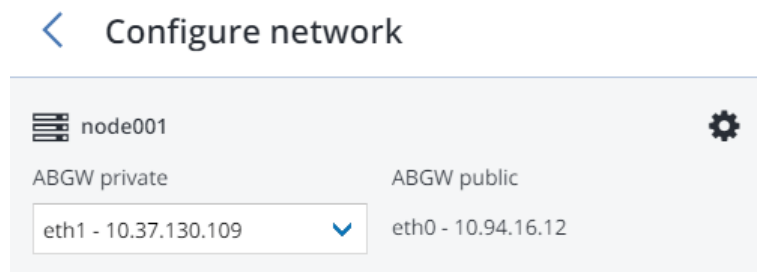
1. На томе NFS достаточно места для резервных копий.
2. Каждый экспорт NFS используется только одним шлюзом. В частности, не следует настраивать два экземпляра продукта Acronis Инфраструктура на использование одного и того же экспорта NFS для хранения резервных копий.

Для настройки Backup Gateway выполните следующие действия.

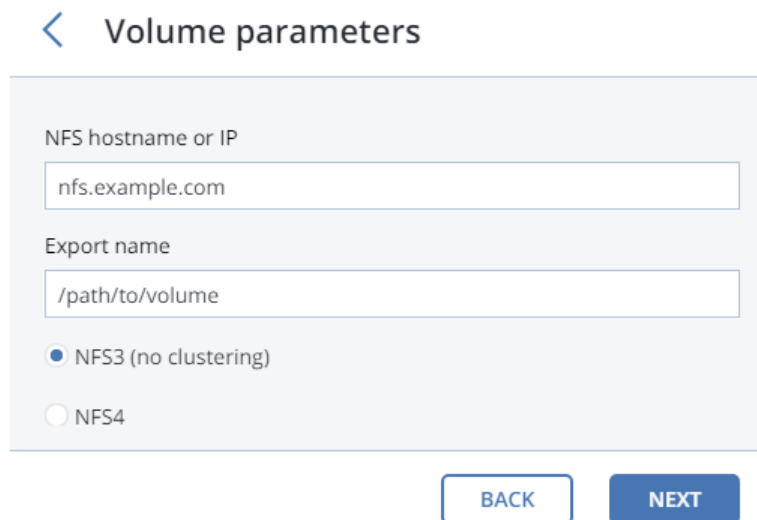
1. В окне **ИНФРАСТРУКТУРА > Сети** убедитесь, что в сети, которые вы собираетесь использовать, добавлены типы трафика **ABGW внутр.** и **ABGW внешн.**

2. В меню слева нажмите **СЕРВИСЫ ХРАНИЛИЩА > Резервное копирование**.
3. Выберите серверы, на которых будут работать сервисы шлюза, и нажмите **Создать шлюз** в меню справа.
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 вкладке **Параметры тома** укажите имя хоста или IP-адрес тома NFS, а также имя экспорта. Нажмите кнопку **ДАЛЕЕ**.



7. На вкладке **Настройка DNS** укажите внешнее DNS-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.

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

Важно: При каждом изменении серверов в кластере Backup Gateway корректируйте настройки DNS соответствующим образом.

< DNS configuration

DNS name

backup.example.com

This may require changing the DNS server configuration, which may look as follows:

```
$TTL 1h
@ IN SOA ns1.myhoster.com. root.backup.example.com. (
  2018120313 ;serial
  1h ;refresh
  30m ;retry
  7d ;expiration
  1h ) ;minimum
```

BACK NEXT

Нажмите кнопку **Далее**.

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.

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

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.
- Используйте отдельный контейнер объектов для каждого кластера Backup Gateway.

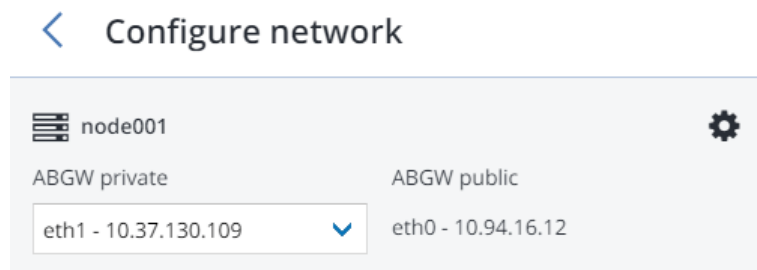
4.3.2 Настройка Backup Gateway

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** в меню справа.
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.

Используйте отдельный контейнер объектов для каждого кластера Backup Gateway.

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.

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

Обновление сертификата для Backup Gateway

При регистрации шлюза Backup Gateway в Acronis Backup Cloud или Acronis Backup Advanced эти решения обмениваются между собой сертификатами со сроком действия в один год. За полтора месяца до окончания срока вы получите уведомление в панели администратора. Для обновления сертификата необходимо подключиться к продукту для резервного копирования и продлить сертификат. Выполните следующие действия.

1. В окне **СЕРВИСЫ ХРАНИЛИЩА** > **Резервное копирование** нажмите **Обновить сертификат**.
2. На панели **Подключение** 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.

- В поле **Адрес** укажите адрес портала управления Acronis Backup Cloud (например, <https://cloud.acronis.com/>) или имя хоста/IP-адрес и порт сервера управления Acronis Backup Advanced (например, <http://192.168.1.2:9877>).
- В поле **Аккаунт** укажите данные партнерской учетной записи в облаке или учетной записи администратора организации на локальном сервере управления.

✕ Connect to backup software

Connect to backup software where this storage is registered.

Address

Enter the URL of the cloud management portal or <name/IP address;port> of the local management server.

Account

Enter the credentials of a partner account in the cloud or of an organization administrator on the local management server.

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 Backup Advanced

Чтобы переключить настроенный шлюз Backup Gateway на другой экземпляр Acronis Backup Advanced, 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.
 - 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.
 - 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 Backup Cloud: по IP-адресу или доменному имени.
 - 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 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 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 Backup Cloud, и нажмите кнопку **ДАЛЕЕ**.

← Enter source storage DNS (2/9)

Specify the DNS name of the source storage registered in Acronis Backup Cloud.

DNS name

BACK NEXT

5. Введите учетные данные портала управления облаком для продукта Acronis 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.

← Set up IP mapping for FES nodes (5/9)

Listed below are public IP addresses of the FES nodes in the source storage. For each FES node, specify its private IP address open for SSH connections.

Public IP address (FES)	Private IP address (SSH)
10.28.74.3	<input type="text" value="10.28.74.1:2001"/>
10.28.74.9	<input type="text" value="10.28.74.1:2002"/>

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.

< Volume parameters

NFS hostname or IP

Export name

NFS3 (no clustering)
 NFS4

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

Используйте отдельный контейнер объектов для каждого кластера Backup Gateway.

< Public cloud parameters

Select the object storage type
 ▾

Region
 ▾

Access key ID

Secret Access key

Bucket

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.

Reconfigure DNS

Before migration can start, all traffic between backup agents and source storage must be rerouted via a TCP proxy that has been set up in this cluster. For this, you will need to reconfigure your DNS server as suggested below to map source storage's DNS name `source.example.com` to this storage cluster's IP address(es). After that, all backup agents must cache the new IP address(es), which may take about a day.

Suggested DNS configuration [Copy to clipboard](#)

```
$TTL 1h

@   IN   SOA  ns1.myhoster.com. source.example.com (
      2018042013   ; serial
      1h   ; refresh
      30m  ; retry
      7d   ; expiration
      1h ) ; minimum

; primary name server
NS ns1.myhoster.com.

; secondary name server
NS ns2.myhoster.com.

A 10.248.64.99
```

✖ Cancel migration and reset settings START MIGRATION

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. В 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**.

< Connect to source (2/7)

Specify the address of the source storage (as registered in Backup Cloud) and the root password to that machine.

Hostname or IP address

Password

Make sure the SSH service is running and port 22 is open for incoming connections.

5. Введите учетные данные портала управления облаком для продукта Acronis Backup Cloud, в котором зарегистрировано исходное хранилище, и нажмите кнопку **ДАЛЕЕ**.
6. Если исходное хранилище зарегистрировано в Acronis Backup Cloud под IP-адресом, откроется окно настройки DNS. В этом окне нажмите **ПЕРЕРЕГИСТРИРОВАТЬ, ИСПОЛЬЗУЯ DNS** и укажите доменное имя исходного хранилища (рекомендуется, см. выше). Либо, если вы хотите продолжить использовать IP-адрес, нажмите **ПРОДОЛЖИТЬ С IP-АДРЕСОМ**.

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

Важно: При каждом изменении серверов в кластере Backup Gateway корректируйте настройки 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.

< Volume parameters

NFS hostname or IP
nfs.example.com

Export name
/path/to/volume

NFS3 (no clustering)
 NFS4

BACK NEXT

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

Используйте отдельный контейнер объектов для каждого кластера Backup Gateway.

< Public cloud parameters

Select the object storage type

Amazon S3

Region

us-east-1

Access key ID

Secret Access key

Bucket

acronis-us-west-gateway-files

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:

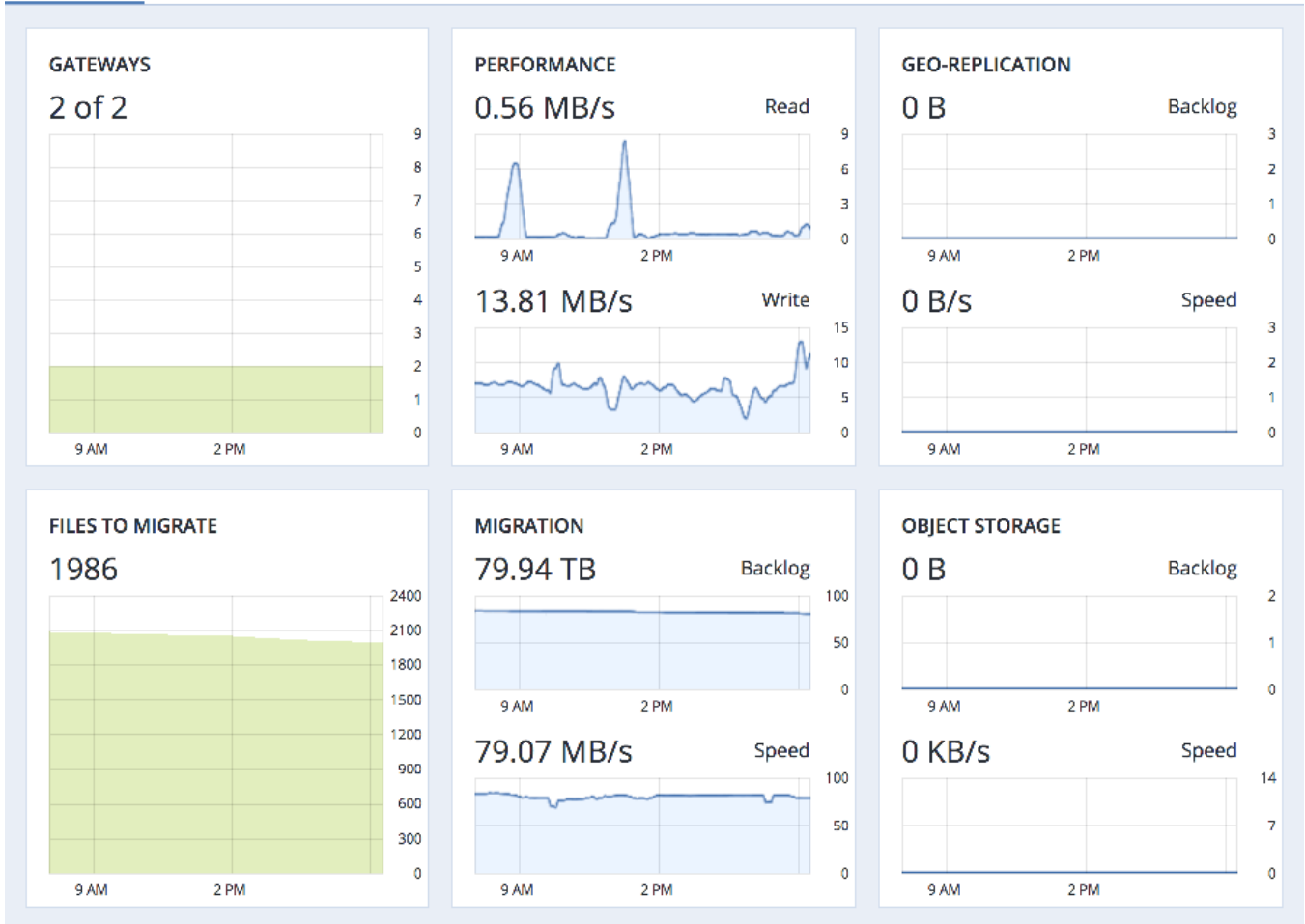
- производительность сервисов Backup Gateway
- скорость и остаток георепликации (объем данных, которые еще не реплицированы)
- скорость и остаток хранилища объектов (объем данных, которые еще не загружены в публичное облако)
- скорость и остаток миграции (объем данных, которые еще не перенесены)
- количество 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 удастся 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



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, см. примечание ниже). 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.

✕ Unregister from backup software

Graceful release ⓘ
 Forced release ⓘ

Unregister this storage from backup software.

Administrator account

Enter the credentials of a partner account in the cloud or of an organization administrator on the local management server.

NEXT

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