КИБЕРПРОТЕКТ

КИБЕР Инфраструктура

Версия 6.5

Руководство по быстрому старту Backup Gateway

Редакция: 28.11.2024

Заявление об авторских правах

Содержание

1 О кратком руководстве Backup Gateway

Кибер Инфраструктура представляет собой новое поколение гиперконвергентных инфраструктур, предназначенных как для поставщиков услуг, так и для конечных пользователей. Это горизонтально масштабируемое, экономичное и многофункциональное решение, которое сочетает в себе универсальное хранилище данных с высокопроизводительной виртуализацией.

Кибер Инфраструктура работает как единое целое с Кибер Бэкап, набором продуктов Кибер Бэкап Облачный. Решение сводит к минимуму количество технологий, необходимых в центрах обработки данных, и обеспечивает дополнительные улучшения в плане производительности.

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

2 Аппаратные требования для вариантов установки с Backup Gateway

Как правило, Кибер 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.

  Примечание
  Поддерживаются только виртуальные машины с BIOS.

- 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 требованиях к оборудованию см. в разделе «Системные требования» в руководстве администратора.

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

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[1]
ОЗУ	8 ГБ
Хранилище	1 диск: система + метаданные, жесткий диск SATA 120 ГБ 1 диск: хранилище, жесткий диск SATA, размер по необходимости[2]
Сеть	10 GbE для трафика хранилища 1 GbE для прочего трафика

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

[2]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 «Создание хранилища резервных копий в общедоступном облаке» руководства администратора.

3 Установка Кибер Инфраструктура

Чтобы установить продукт Кибер Инфраструктура, выполните следующие действия.

1. Получите ISO-образ дистрибутива. Для этого зайдите на страницу продукта и отправьте запрос на пробную версию. ISO-образ также можно скачать из Кибер Бэкап Облачный.
   a. Перейдите на портал управления и выберите **НАСТРОЙКИ** > **Хранилища** в меню слева.
   b. Нажмите **Добавить хранилище резервных копий** и в открывшемся окне нажмите кнопку **Загрузить ISO-образ**.
2. Подготовьте загрузочный носитель с помощью ISO-образа дистрибутива (подключите его к виртуальному диску IPMI, создайте загрузочный USB-накопитель или настройте PXE-сервер).
3. Загрузите сервер с выбранного носителя.
4. На экране приветствия выберите **Установить Кибер Инфраструктура**.
5. 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**.
6. На шаге 2 настройте статический IP-адрес для сетевого интерфейса и укажите имя хоста: либо полное доменное имя (**<имя_хоста>.<имя_домена>**), либо краткое имя (**<имя_хоста>**). Не рекомендуется использовать динамический IP-адрес, поскольку это может вызвать проблемы с доступом к серверам. Проверьте правильность сетевых настроек.
7. На шаге 3 выберите часовой пояс. Дата и время будут заданы посредством NTP. Для выполнения синхронизации потребуется подключение к Интернету.
8. 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. Этот сервер будет сервером управления.
   - 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.
9. 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.

10. 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.

4 Создание кластера хранилища данных

Для создания кластера хранилища выполните следующие действия.

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

5 Добавление расположений в Кибер Бэкап или Кибер Бэкап Облачный

Хранилище резервных копий использует шлюз Backup Gateway в качестве точки доступа к хранилищу. Эта функциональность предназначена для поставщиков услуг, которые используют Кибер Бэкап и/или Кибер Бэкап Облачный и хотят хранить резервные копии клиентских данных в локальном кластере, в облаке (например, Yandex Object Storage, VK Cloud Storage и SberCloud OBS) или на устройстве NAS (по протоколу NFS).

Хранилище резервных копий позволяет поставщикам услуг легко настраивать хранение данных в собственном формате с поддержкой дедупликации, который используется продуктами Киберпротект. Кроме того, можно включить георепликацию данных хранилища.

Хранилище резервных копий поддерживает следующие места назначения:

- Кластеры хранилища Кибер Инфраструктура с помехоустойчивым кодированием, которое обеспечивает избыточность данных.
- Тома NFS.
- Публичные облачные сервисы, включая ряд решений S3, а также Yandex Object Storage, VK Cloud Storage и SberCloud OBS.

Хотя ваш выбор должен основываться на конкретных требованиях и сценарии использования, рекомендуется хранить данные резервных копий в локальном кластере хранилища Кибер Инфраструктура. 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. Кроме того, при использовании внешних мест назначения избыточность должна обеспечиваться внешним хранилищем. Само хранилище резервных копий не обеспечивает избыточности данных и не производит дедупликации.

Примечание
При настройке Backup Gateway необходимо будет указать учетные данные администратора вашего продукта Кибер Бэкап.

Ограничения

- Чтобы можно было зарегистрировать Backup Gateway в Кибер Бэкап Облачный, для вашего тенанта партнера должна быть отключена двухфакторная проверка подлинности (2FA). Вы также можете отключить ее для выбранного пользователя в тенанте с поддержкой 2FA, как описано в Руководстве администратора партнера в разделе "Управление двухфакторной проверкой подлинности для пользователей", и указать учетные данные этого пользователя.

5.1 Подключение к локальному кластеру хранилища через Backup Gateway

Ограничения

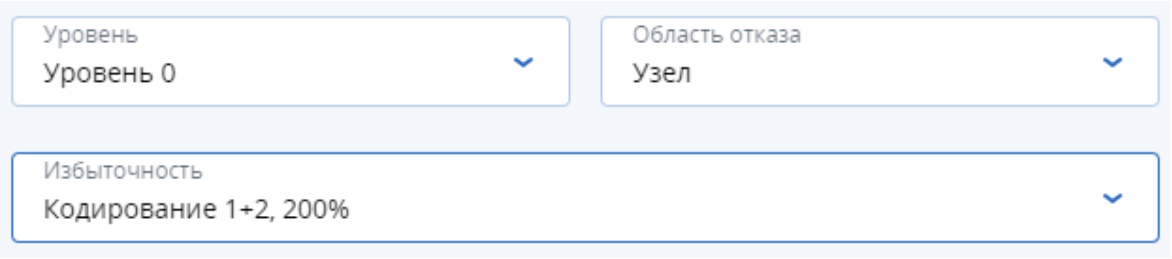
- Избыточность за счет репликации не поддерживается для хранилищ резервных копий.

Предварительные требования

- В целевом хранилище достаточно места как для существующих, так и для новых резервных копий.
- Убедитесь, что на каждом сервере, который будет присоединен к кластеру хранилища резервных копий, открыт TCP-порт 44445 для исходящих подключений к Интернету, а также для входящих подключений от продукта Кибер Бэкап.

Как выбрать локальный кластер в качестве места назначения резервных копий

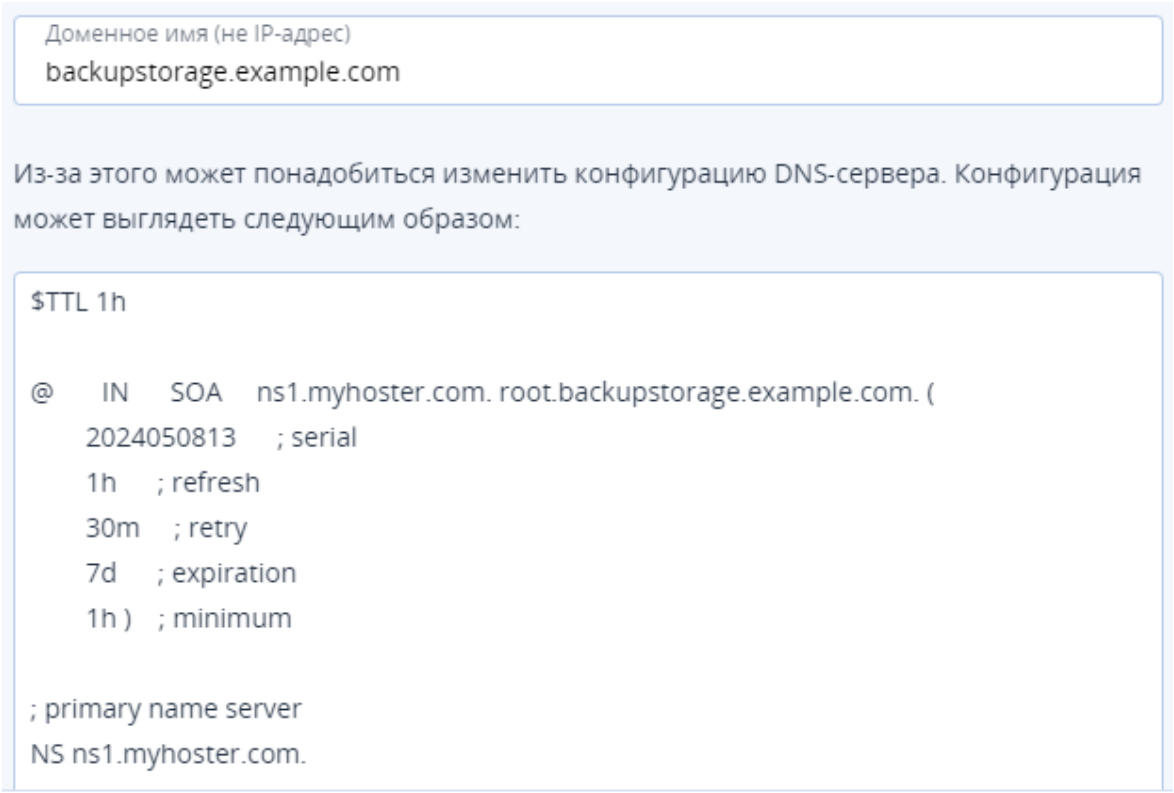
1. На экране **Инфраструктура** > **Сети** убедитесь, что в сети, которые вы собираетесь использовать, добавлены типы трафика **Резервное копирование (ABGW) внутр.** и **Резервное копирование (ABGW) внешн.**
2. Откройте экран **Сервисы хранилища** > **Резервные копии** и нажмите **Создать хранилище резервных копий**.
3. На шаге **Место назначения резервных копий** выберите **Кибер Инфраструктура кластер**.
4. На шаге **Серверы** выберите серверы, которые нужно добавить в кластер хранилища резервных копий, и нажмите **Далее**.
5. На шаге **Политика хранения** выберите нужный уровень, область отказов и режим избыточности данных. Дополнительные сведения см. в разделе «Политики хранилища» в руководстве администратора. Затем нажмите кнопку **Далее**.



6. На шаге **DNS** укажите внешнее доменное имя для хранилища резервных копий, например **backupstorage.example.com**. Агенты резервного копирования будут использовать это доменное имя и TCP-порт 44445 для передачи данных в хранилище. Затем нажмите кнопку **Далее**.

Внимание

- Настройте свой DNS-сервер в соответствии с примером, приведенным на панели администратора.
- При каждом изменении сетевой конфигурации серверов в кластере хранилища резервных копий корректируйте записи DNS соответствующим образом.



Примечание

В сложных средах можно использовать HAProxy для создания масштабируемой избыточной платформы балансировки нагрузки, которую можно легко перемещать или переносить, независимо от продукта Кибер Инфраструктура. Дополнительные сведения см. в статье Как запустить хранилище за HAProxy.

7. На шаге **Учетная запись Киберпротект** укажите следующую информацию для вашего продукта Киберпротект:
   - URL-адрес портала управления облаком или имя хоста/IP-адрес и порт локального сервера управления (например, http://192.168.1.2:9877)
   - Данные партнерской учетной записи в облаке или учетные данные администратора организации на локальном сервере управления.
8. На шаге **Сводка** просмотрите конфигурацию и нажмите **Создать**.

5.2 Подключение к внешним томам NFS через Backup Gateway

Ограничения

- Кибер Инфраструктура не обеспечивает избыточность данных поверх томов NFS. В зависимости от реализации тома NFS могут обеспечивать собственную аппаратную или программную избыточность.
- Только один сервер кластера может хранить резервные копии на томе NFS.
- Каждый экспорт NFS используется только одним шлюзом. В частности, не следует подключать два экземпляра продукта Кибер Инфраструктура к одному экспорту NFS для хранения резервных копий.
- Несколько полных резервных копий, хранящихся на томе NFS, могут потреблять дополнительное дисковое пространство из-за задержки автоматического уплотнения, которое выполняется для каждой резервной копии по очереди.

Предварительные требования

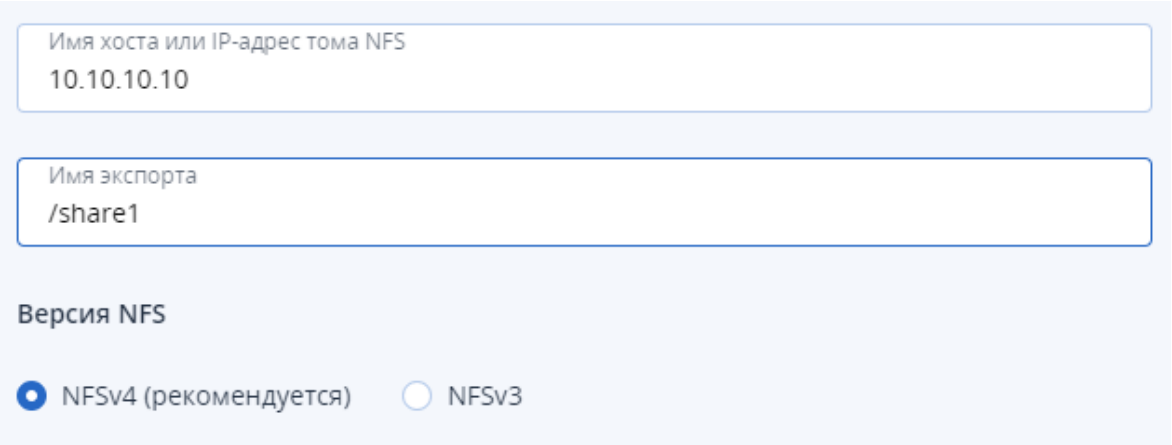
- В целевом хранилище достаточно места как для существующих, так и для новых резервных копий.
- Убедитесь, что на каждом сервере, который будет присоединен к кластеру хранилища резервных копий, открыт TCP-порт 44445 для исходящих подключений к Интернету, а также для входящих подключений от продукта Кибер Бэкап.
- Убедитесь, что у сервера, который будет присоединен к хранилищу резервных копий, есть доступ к внешнему NFS-хранилищу.

Как выбрать внешний том NFS в качестве места назначения резервных копий

1. На экране **Инфраструктура** > **Сети** убедитесь, что в сети, которые вы собираетесь использовать, добавлены типы трафика **Резервное копирование (ABGW) внутр.** и **Резервное копирование (ABGW) внешн.**
2. Откройте экран **Сервисы хранилища** > **Резервные копии** и нажмите **Создать хранилище резервных копий**.
3. На шаге **Место назначения резервной копии** выберите **Том Network File System (NFS)**.
4. На шаге **Серверы** выберите один сервер для добавления в кластер хранилища резервных копий и нажмите кнопку **Далее**.
5. На шаге **Том NFS** укажите имя хоста или IP-адрес тома NFS, имя экспорта и версию NFS. Затем нажмите кнопку **Далее**.

Примечание

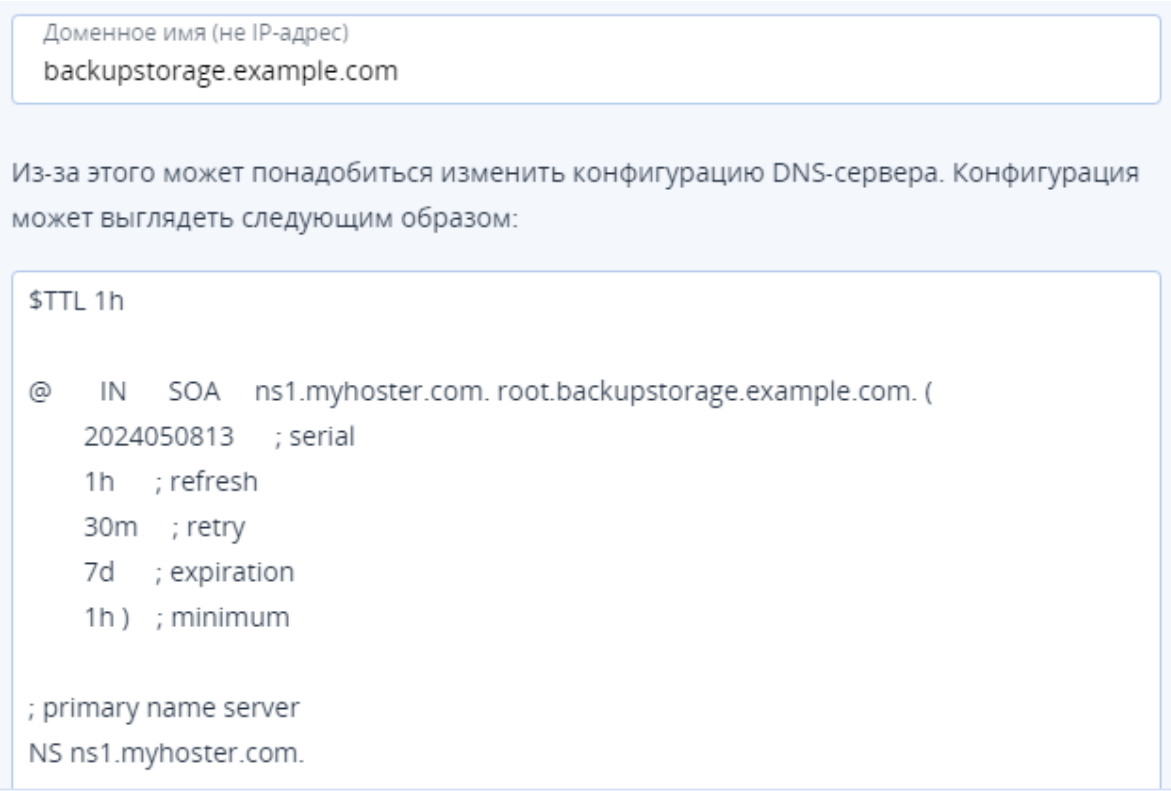
Рекомендуется использовать NFS версии 4, поскольку она обеспечивает лучшую масштабируемость и производительность по сравнению с версией 3, которая имеет ограничения в протоколе.



6. На шаге **DNS** укажите внешнее доменное имя для хранилища резервных копий, например **backupstorage.example.com**. Агенты резервного копирования будут использовать это доменное имя и TCP-порт 44445 для передачи данных в хранилище. Затем нажмите кнопку **Далее**.

Внимание

- Настройте свой DNS-сервер в соответствии с примером, приведенным на панели администратора.
- При каждом изменении сетевой конфигурации серверов в кластере хранилища резервных копий корректируйте записи DNS соответствующим образом.



7. На шаге **Учетная запись Киберпротект** укажите следующую информацию для вашего продукта Киберпротект:
   - URL-адрес портала управления облаком или имя хоста/IP-адрес и порт локального сервера управления (например, http://192.168.1.2:9877)
   - Данные партнерской учетной записи в облаке или учетные данные администратора организации на локальном сервере управления.
8. На шаге **Сводка** просмотрите конфигурацию и нажмите **Создать**.

5.3 Подключение к публичному облачному хранилищу через Backup Gateway

Backup Gateway позволяет Кибер Бэкап Облачный или Кибер Бэкап использовать для хранения резервных копий публичные облачные сервисы и локальные хранилища объектов:

- Yandex Object Storage
- VK Cloud Storage
- SberCloud OBS
- CloudMTS S3 Object Storage
- 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.

Резервные копии представляют собой холодные данные со специфической схемой доступа: к этим данным обращаются редко, но они должны быть немедленно доступны при обращении. Для этого сценария экономичным вариантом будут классы хранилищ, предназначенные для долгосрочного хранения редко используемых данных. Рекомендуются следующие классы хранилищ:

- **Ice** в Yandex Object Storage
- **Cold** в SberCloud OBS
- **Infrequent Access** в Amazon S3
- **Cool Blob Storage** в Microsoft Azure
- **Nearline** и **Coldline Storage** в 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 Кибер Бэкап Облачный для хранения данных резервного копирования.

Ограничения

- При работе с публичным облаком Backup Gateway использует локальное хранилище для промежуточного копирования, а также для хранения служебной информации. Это означает, что данные, предназначенные для загрузки в публичное облако, сначала сохраняются локально и только после этого отправляются в место назначения. По этой причине для сохранности данных крайне важно, чтобы локальное хранилище было постоянным и избыточным. Использование временных дисков может привести к потере данных.
- 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.
- 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.
- Для каждого кластера хранилища резервных копий требуется отдельный контейнер объектов.
- Избыточность за счет репликации не поддерживается для хранилищ резервных копий.

Предварительные требования

- В целевом хранилище достаточно места как для существующих, так и для новых резервных копий.
- Убедитесь, что на каждом сервере, который будет присоединен к кластеру хранилища резервных копий, открыт TCP-порт 44445 для исходящих подключений к Интернету, а также для входящих подключений от продукта Кибер Бэкап.

Как выбрать публичное облако в качестве места назначения резервных копий

1. На экране **Инфраструктура** > **Сети** убедитесь, что в сети, которые вы собираетесь использовать, добавлены типы трафика **Резервное копирование (ABGW) внутр.** и **Резервное копирование (ABGW) внешн.**
2. Откройте экран **Сервисы хранилища** > **Резервные копии** и нажмите **Создать хранилище резервных копий**.
3. На шаге **Место назначения резервной копии** выберите **Облачный сервис**.
4. На шаге **Серверы** выберите серверы, которые нужно добавить в кластер хранилища резервных копий, и нажмите **Далее**.
5. На шаге **Облачный сервис** укажите информацию, связанную с поставщиком облачного сервиса.
   a. Выберите поставщика облачного сервиса. Если ваш сервис совместим с S3, но отсутствует в списке, попробуйте **AuthV2-совместимый (S3)** или **AuthV4-совместимый (S3)** сервис.

b. В зависимости от поставщика укажите **Регион**, **URL аутентификации (Keystone)** или **URL точки доступа**.

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

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

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

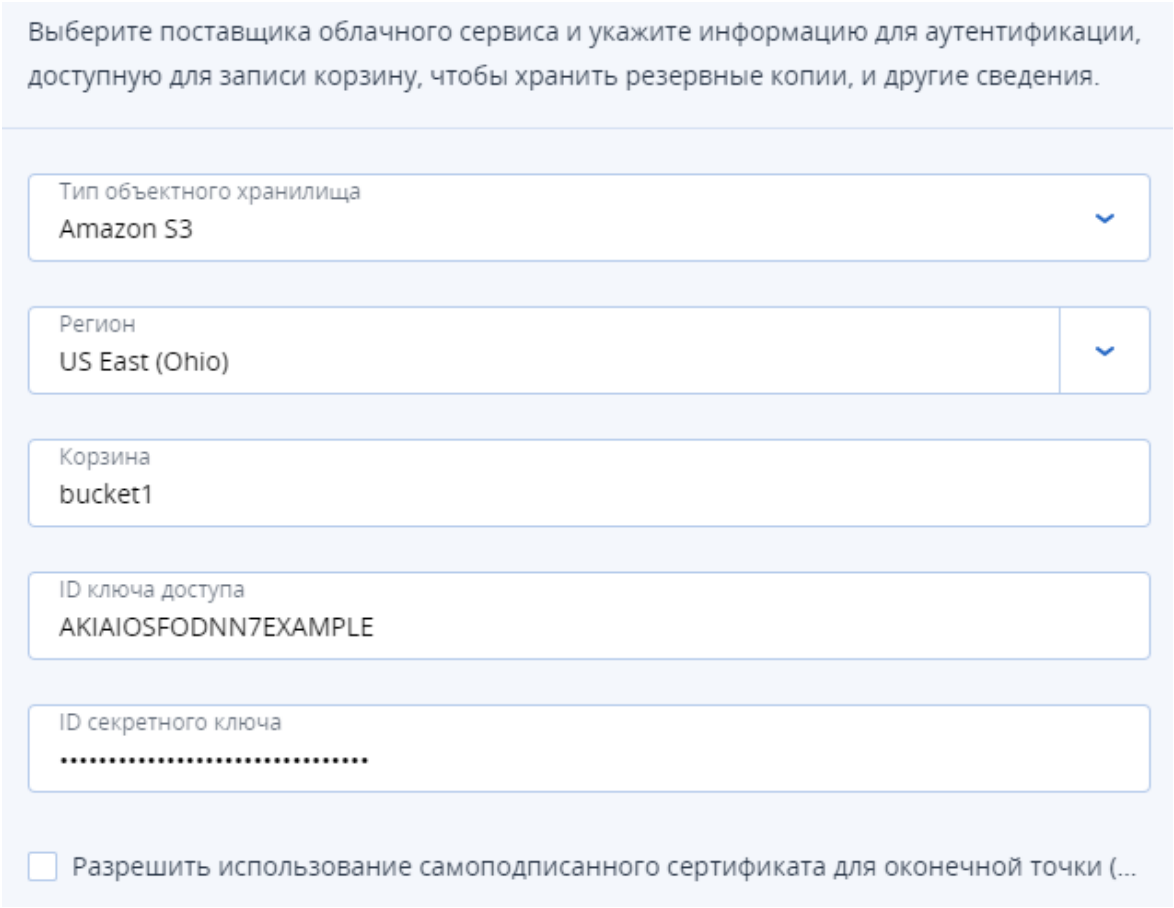
   Для каждого кластера хранилища резервных копий следует использовать отдельный контейнер объектов.

f. Для объектного хранилища типа **AuthV4-совместимый (S3)** укажите, какую модель адресации необходимо использовать для доступа.

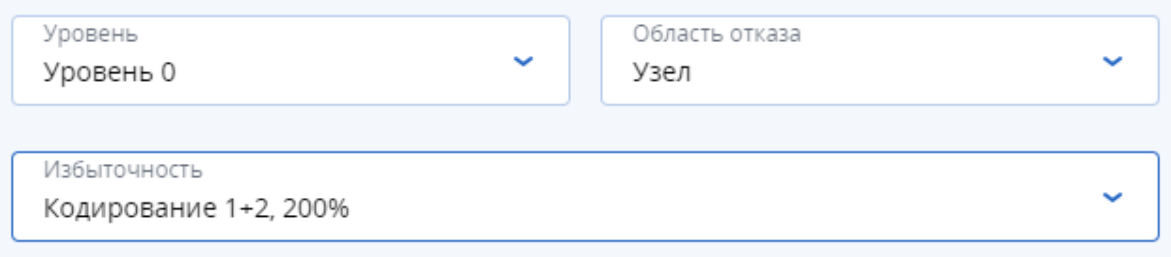
   - Virtual-hosted style URLs. Адреса вида https://mybucket.s3.example.com/myobject.txt. Предназначена для облачных S3-хранилищ.
   - Path-style URLs. Адреса вида https://s3.example.com/mybucket/myobject.txt. Предназначена для локальных S3-хранилищ.

   Модель Virtual-hosted style URLs используется по умолчанию. Для использования модели Path-style URLs установите флажок **Использовать адресацию path-style**.

g. Нажмите кнопку **Далее**.



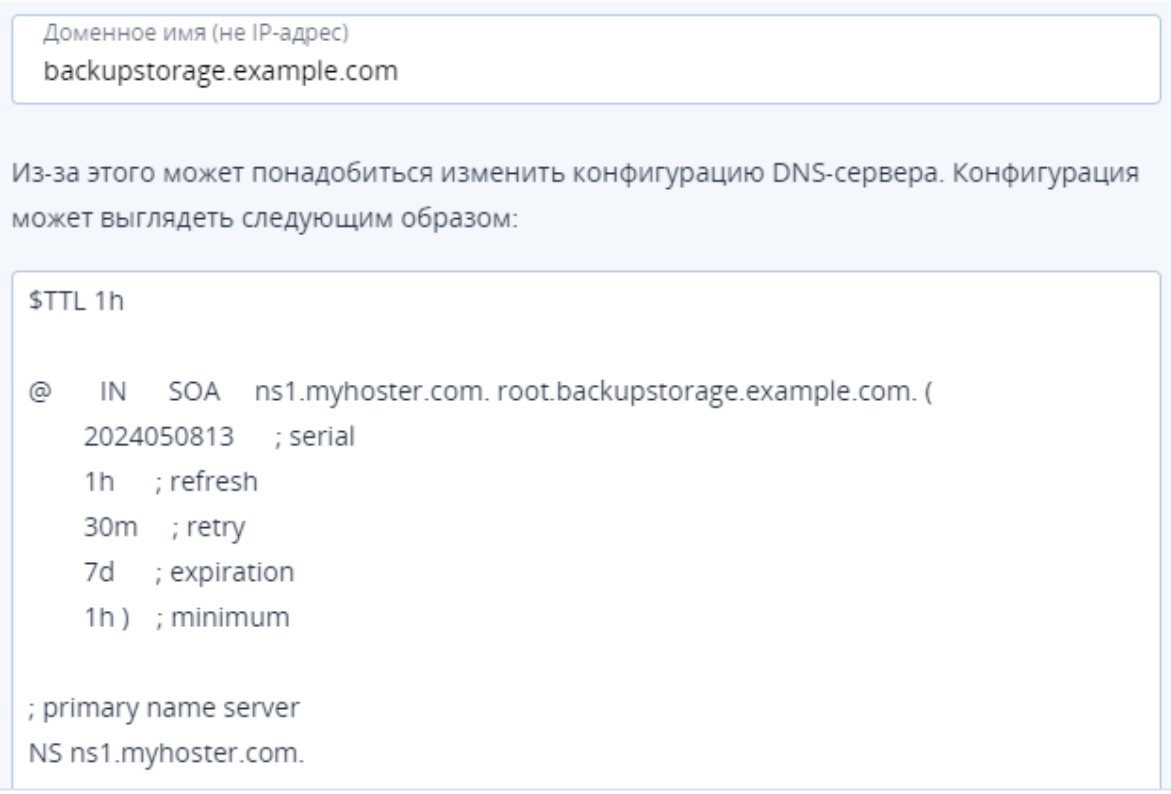
6. На шаге **Политика хранения** выберите нужный уровень, область отказов и режим избыточности данных. Избыточность за счет репликации не поддерживается для Backup Gateway. Дополнительные сведения см. в разделе «Политики хранилища» в руководстве администратора. Затем нажмите кнопку **Далее**.



7. На шаге **DNS** укажите внешнее доменное имя для хранилища резервных копий, например **backupstorage.example.com**. Агенты резервного копирования будут использовать это доменное имя и TCP-порт 44445 для передачи данных в хранилище. Затем нажмите кнопку **Далее**.

Внимание

- Настройте свой DNS-сервер в соответствии с примером, приведенным на панели администратора.
- При каждом изменении сетевой конфигурации серверов в кластере хранилища резервных копий корректируйте записи DNS соответствующим образом.



Примечание

В сложных средах можно использовать HAProxy для создания масштабируемой избыточной платформы балансировки нагрузки, которую можно легко перемещать или переносить, независимо от продукта Кибер Инфраструктура. Дополнительные сведения см. в статье Как запустить хранилище за HAProxy.

8. На шаге **Учетная запись Киберпротект** укажите следующую информацию для вашего продукта Киберпротект:
   - URL-адрес портала управления облаком или имя хоста/IP-адрес и порт локального сервера управления (например, http://192.168.1.2:9877)
   - Данные партнерской учетной записи в облаке или учетные данные администратора организации на локальном сервере управления.
9. На шаге **Сводка** просмотрите конфигурацию и нажмите **Создать**.

6 Добавление серверов от Backup Gateway

Можно добавить дополнительные серверы, которые будут служить местами размещения резервных копий из Кибер Бэкап и/или Кибер Бэкап Облачный, для высокой доступности и масштабируемости хранилища резервных копий.

Как добавить серверы к хранилищу резервных копий

1. Перейдите на экран **Сервисы хранилища** > **Резервные копии** > **Серверы**.
2. Нажмите **Добавить сервер**.
3. Выберите серверы для присоединения к кластеру хранилища резервных копий и нажмите **Добавить**.

Серверы будут добавлены к хранилищу резервных копий, и на них будет работать сервис Backup Gateway.

7 Обновление сертификата для Backup Gateway

При регистрации Backup Gateway в Кибер Бэкап Облачный или Кибер Бэкап они обмениваются сертификатами, которые действуют в течение трех лет. За полтора месяца до окончания этого периода вы получите уведомление о скором истечении срока действия сертификата на панели администрирования.

Предварительные требования

- Убедитесь, что для вашего тенанта партнера отключена двухфакторная проверка подлинности (2FA). Вы также можете отключить ее для конкретного пользователя при включенной двухфакторной проверке для тенанта, как описано в Руководстве администратора партнера в разделе "Управление двухфакторной проверкой подлинности для пользователей", и указать учетные данные этого пользователя.
- Если включен контроль входа для веб-интерфейса Кибер Бэкап Облачный, убедитесь, что внешний IP-адрес кластера хранилища резервных копий добавлен в список разрешенных IP-адресов, как описано в Руководстве администратора партнера в разделе "Ограничение доступа к веб-интерфейсу".

Чтобы обновить сертификат

1. На экране **Сервисы хранилища** > **Резервное копирование** перейдите на вкладку **Настройки** и нажмите **Сертификат**.
2. Укажите данные партнерской учетной записи в облаке или учетные данные администратора организации на локальном сервере управления.
3. Нажмите **Обновить**.
4. На всех серверах, входящих в кластер хранилища резервных копий, перезапустите сервис:

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

8 Перерегистрация Backup Gateway на новом экземпляре Кибер Бэкап

Чтобы переключить настроенное хранилище резервных копий на другой экземпляр Кибер Бэкап, необходимо перерегистрировать шлюз на этом экземпляре.

Как перерегистрировать хранилище резервных копий

1. На экране **Сервисы хранилища** > **Резервные копии** перейдите на вкладку **Настройки** и нажмите **Перерегистрация**.
2. Укажите имя хоста или IP-адрес целевого сервера управления и порт 9877 (например, http://192.168.1.2:9877), а затем введите учетные данные для сервера управления.

   Примечание
   Адрес следует задавать с использованием протокола HTTP, а не HTTPS.

3. Нажмите **Сохранить**.

9 Изменение схемы избыточности для Backup Gateway

Можно обновить схему избыточности, которая используется для хранилища резервных копий, изменив политику хранилища. Такая настраиваемая схема избыточности обеспечивает высокую масштабируемость и максимальную эффективность хранилища резервных копий.

В процессе перекодирования данные частично хранятся с новой схемой избыточности и частично – со старой. При этом система использует политику хранилища с наименьшей избыточностью. Например, если вы меняете режим кодирования с 1+0 на 1+2, система будет использовать режим 1+0. В этом случае важно не отключать никакие серверы и диски хранилища до завершения процесса.

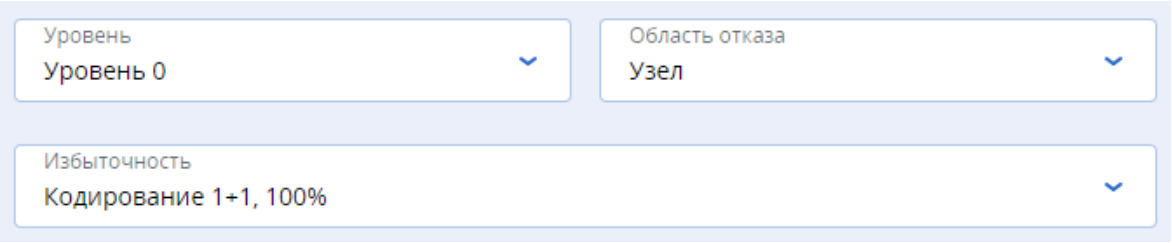
Внимание
Если вы изменили схему кодирования для кластера хранилища резервных копий с помощью специалистов технической поддержки, заново примените настройки избыточности на панели администрирования, чтобы гарантировать перекодирование всех данных.

Ограничения

- Избыточность за счет репликации не поддерживается для хранилищ резервных копий.

Как изменить политику хранилища

1. На экране **Сервисы хранилища** > **Резервные копии** перейдите на вкладку **Настройки** и нажмите **Политика хранения**.
2. Выберите нужный уровень хранилища, область отказов или режим избыточности данных. Дополнительные сведения см. в разделе «Политики хранилища» в руководстве администратора.



3. Нажмите **Сохранить**.

После запуска процесса перекодирования на экране будет показан ход выполнения и приблизительное время завершения. Во время процесса можно выбрать другую схему избыточности. В этом случае текущий процесс перекодирования будет остановлен, а затем применена новая схема избыточности.

10 Мониторинг шлюза Backup Gateway

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

- **Серверы**. Диаграмма показывает количество и доступность серверов в кластере хранилища резервных копий.
- **Производительность**. Диаграмма показывает активность чтения и записи для сервисов хранилища резервных копий по времени.
- **Георепликация**. Диаграмма показывает скорость и остаток георепликации, то есть объем данных, которые еще не реплицированы. Если остаток не снижается со временем, это означает, что данные не удается реплицировать достаточно быстро. Причиной может быть недостаточная скорость передачи данных по сети, и может потребоваться проверить или обновить сетевое оборудование.
- **Задержка присоединения**. Диаграмма показывает время, потраченное на обработку запросов от агентов резервного копирования к хранилищу.
- **Регулировка присоединения**. Если диаграмма не пуста, значит, в базовом хранилище не хватает свободного пространства и хранилище резервных копий ограничивает пользовательские запросы для замедления потока данных.

  Два порога, мягкий и жесткий, устанавливаются для занятого пространства хранилища в процентах. При достижении мягкого порога хранилище резервных копий начинает ограничивать операции записи. Интенсивность ограничения зависит от использованного пространства и повышается до достижения жесткого порога. Когда занятое пространство достигает жесткого порога, ограничение начинает работать с максимальной интенсивностью. Значения порогов зависят от места назначения резервных копий и количества серверов в кластере хранилища.

Место назначения резервных копий	Количество серверов резервного копирования	Мягкий порог	Жесткий порог
Локальный кластер	1	93 %	95 %
	2+	90 %	92 %
NFS	1	93 %	95 %
Публичное облако	1	88 %	90 %
	2+	85 %	87 %

- **Объектное хранилище**. Диаграмма показывает скорость и остаток хранилища объектов, то есть объем данных, которые еще не загружены в публичное облако. Если остаток не снижается со временем, это означает, что данные не удается передать достаточно быстро. Причиной может быть недостаточная скорость передачи данных по сети, и может потребоваться проверить или обновить сетевое оборудование.

Также можно отслеживать состояние серверов хранилища резервных копий. Для этого перейдите в раздел **Сервисы хранилища** > **Резервное копирование** > **Серверы** и щелкните по нужному серверу. На вкладке **Сводка** на правой панели отображается статистика производительности.

- **ЦП/ОЗУ**: загрузка ЦП в процентах по времени и использование ОЗУ в ГиБ по времени
- **Частота успешных/неудачных запросов**: количество успешных и неудачных запросов на присоединение в секунду
- **Частота выходных/входных запросов**: количество запросов на чтение и запись в секунду
- **Пропускная способность**: объем данных, считываемых или записываемых в хранилище резервных копий в секунду
- **Задержка запросов**: время, потраченное на обработку запросов

11 Освобождение серверов от Backup Gateway

Хранилище резервных копий подключено к определенному месту назначения резервных копий. Если необходимо поменять место назначения, например с публичного облака на локальный кластер хранилища или с одной корзины облачного сервиса на другую, необходимо удалить хранилище резервных копий путем освобождения всех его серверов из кластера хранилища и создать новое.

При удалении хранилища резервных копий также отменяется его регистрация в продукте Кибер Бэкап, который теряет доступ к месту назначения резервных копий.

Ограничения

- Если выбрать принудительное освобождение и сохранить регистрацию Backup Gateway в продукте Кибер Бэкап, то в следующий раз необходимо будет зарегистрировать в продукте другой шлюз. Для этого придется удалить и создать заново не только хранилище резервных копий, но и весь кластер хранилища.

Как освободить сервер из хранилища резервных копий

1. Перейдите на экран **Сервисы хранилища** > **Резервные копии** > **Серверы**.
2. Щелкните по нужному серверу, а затем на правой панели сервера нажмите **Освободить**.
3. Нажмите **Освободить** в окне подтверждения.

Хранилище резервных копий остается в рабочем состоянии, пока в нем есть хотя бы один сервер.

Как освободить все серверы из хранилища резервных копий

1. Перейдите на экран **Сервисы хранилища** > **Резервные копии** > **Серверы**.
2. Выберите все серверы резервного копирования или щелкните по единственному серверу в кластере хранилища резервных копий и нажмите **Освободить**.
3. В окне **Освободить серверы**:
   - Выберите **(Рекомендуется) Корректно**, чтобы удалить шлюз Backup Gateway с сервера и отменить его регистрацию в продукте Кибер Бэкап.
   - Выберите **Принудительно**, чтобы удалить шлюз Backup Gateway с сервера, но не отменять его регистрацию в продукте Кибер Бэкап.

     Внимание
     Выбирайте этот вариант, только если уверены, что регистрация шлюза в продукте Кибер Бэкап уже отменена.
4. Если вы выбрали штатное освобождение, укажите данные учетной записи администратора для продукта Кибер Бэкап.
5. Нажмите кнопку **Освободить**.