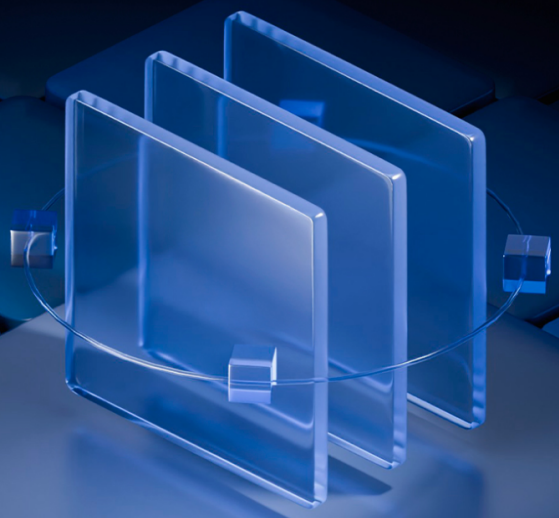
КИБЕРПРОТЕКТ

КИБЕР Хранилище

Версия 6.7



Руководство по быстрому старту
Backup Gateway для образов QCOW2

Редакция: 20.07.2026

Оглавление

О кратком руководстве Backup Gateway для образов QCOW2

В этом руководстве объясняется, как развернуть продукт Кибер Хранилище из образов QCOW2 и настроить Backup Gateway.

В общих чертах потребуется выполнить следующие действия.

1. Создать виртуальные машины для продукта Кибер Хранилище.
2. Развернуть продукт Кибер Хранилище на виртуальных машинах.
3. Настроить Backup Gateway.

Инструкции по настройке ПО Кибер Хранилище для определенного сценария использования см. в Руководстве администратора.

Требования

Необходимо использовать виртуальную машину с BIOS.

Для работы продукта Кибер Хранилище необходимы следующие ресурсы:

- Минимум 8 ГБ ОЗУ для каждой виртуальной машины с Backup Gateway.
- Минимум 425 ГБ дискового пространства для каждой виртуальной машины с Backup Gateway (два диска хранилища по 200 ГБ и системный диск на 25 ГБ). Шаблон продукта Кибер Хранилище также занимает около 35 ГБ. Рекомендуемый максимальный размер одного виртуального диска — 16 ТБ.

  Важно

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

- Два виртуальных сетевых адаптера: один должен быть подключен к публичной сети, другой — к частной.

  В публичной сети пользователям должны быть доступны панель администрирования и интерфейсы доступа к данным. В частной сети будут обмениваться данными серверы продукта Кибер Хранилище.

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

Примечание

Полные требования к оборудованию для сценария со шлюзом резервного копирования приведены в Руководстве администратора.

Развертывание продукта Кибер Хранилище на виртуальных машинах

Для создания кластера потребуется развернуть один сервер управления, а также при необходимости два или четыре подчиненных сервера.

Развертывание сервера управления

Вам понадобится облачный образ для развертывания первого узла кластера (с панелью администрирования) — виртуальный диск QCOW2.

Настройка сервера управления

1. Создайте виртуальную машину в соответствии с требованиями (см. раздел *Требования*). Используйте загруженный образ в качестве системного диска.
2. Запустите виртуальную машину. Вам понадобится указать SSH-ключ для установки в ВМ.

   Загруженный образ будет инициализирован сервисом cloud-init. Будет инициализирован кластер хранилища, создан пароль от панели администрирования (узнать его можно из файла `/.initial-admin-password`) и установлен предоставленный SSH-ключ.

Теперь можно приступить к развертыванию подчиненных серверов, если они требуются для вашего сценария. Если необходим только один сервер для шлюза Backup Gateway, переходите к разделу *Добавление расположений в Кибер Бэкап или Кибер Бэкап Облачный*.

Развертывание подчиненных серверов

Чтобы развернуть подчиненный сервер на виртуальной машине, необходимо создать его, а затем добавить в кластер хранилища.

Вам понадобится облачный образ для развертывания последующих узлов кластера — виртуальный диск QCOW2.

Создание подчиненного сервера

1. Создайте виртуальную машину в соответствии с требованиями (см. раздел *Требования*). Используйте загруженный образ в качестве системного диска.
2. Запустите виртуальную машину. Вам понадобится указать SSH-ключ для установки в ВМ.

   Загруженный образ будет инициализирован сервисом cloud-init. Будет установлен предоставленный SSH-ключ.
3. Получите токен и адрес сервера управления в панели администрирования.
   1. Войдите в панель администрирования по ее IP-адресу и порту 8888.

      При необходимости добавьте сертификат безопасности в исключения браузера.
   2. В панели администрирования откройте раздел **Инфраструктура** → **Серверы** и нажмите **Подключить сервер**, чтобы вызвать экран с адресом сервера управления и токеном.
4. Зарегистрируйте сервер в панели администрирования:

   ```
   $ sudo bash /usr/libexec/vstorage-ui-agent/bin/register-storage-node.sh -m <MN_IP_address> -
   ↪t <token>
   ```

   В этой команде `<MN_IP_address>` — IP-адрес частного сетевого интерфейса на сервере с панелью администрирования, а `<token>` — токен, полученный в панели администрирования.

Дополнительные сведения см. в разделе ”Повторное добавление неназначенных серверов” в Руководстве администратора.

Добавление подчиненного сервера в кластер хранилища

1. На экране **Инфраструктура** → **Серверы** щелкните по неназначенному серверу.
2. На правой панели сервера нажмите **Присоединить к кластеру**.
3. Нажмите **Присоединить**, чтобы автоматически назначить роли дискам и добавить сервер в текущее расположение. Вместо этого можно нажать значок шестерни, чтобы вручную настроить роли дисков или расположение сервера.

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

Теперь можно приступать к настройке продукта Кибер Хранилище для нужного сценария. Инструкции по выполнению различных задач настройки приведены в Руководстве администратора.

Добавление дискового пространства в продукт Кибер Хранилище

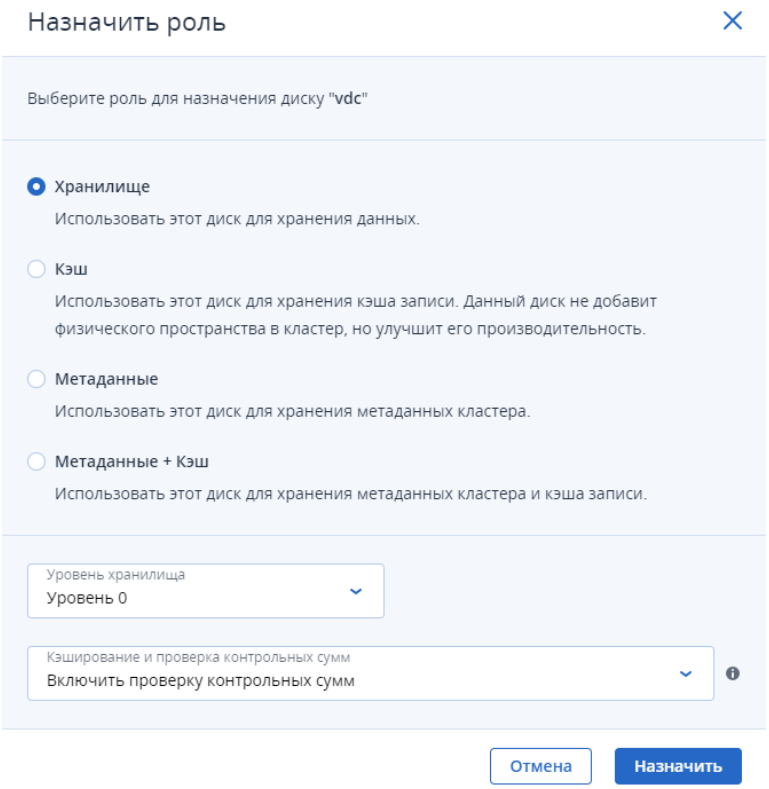
Перед созданием новых дисков обратите внимание на следующие рекомендации по выбору размера.

- Если в кластере несколько серверов, они должны быть одинакового размера для эффективного обеспечения избыточности. В этом случае данные будут распределены по серверам более равномерно. Дополнительные сведения см. в разделе ”Общие сведения о распределяемом дисковом пространстве” в Руководстве администратора.
- Одинаковый размер дисков помогает более равномерно распределять нагрузку. Внутри кластера диски используются пропорционально их размеру. Например, если у вас есть диск размером 10 ТБ и диск размером 2 ТБ, при загрузке кластера на 50 % на дисках будет использовано 5 и 1 ТБ соответственно.

Если вы хотите увеличить физическое пространство в кластере хранилища, добавьте виртуальный диск к виртуальной машине. Он появится в списке дисков сервера на панели администрирования продукта Кибер Хранилище. Затем настройте диск, как описано далее.

Настройка нового диска в панели администрирования

1. На экране **Инфраструктура** → **Серверы** щелкните по имени сервера с созданным диском. Перейдите на вкладку **Диски** для просмотра всех дисков сервера.
2. Найдите созданный ранее диск в списке дисков и щелкните по нему.
3. На правой панели диска нажмите **Назначить роль**.
4. В окне **Назначить роль** выберите роль `Хранилище`, укажите уровень хранилища и при необходимости включите проверку контрольных сумм. Дополнительные сведения см. в Руководстве администратора.


Назначить роль
Выберите роль для назначения диску "vdc"
Хранилище
Использовать этот диск для хранения данных.
Кэш
Использовать этот диск для хранения кэша записи. Данный диск не добавит физического пространства в кластер, но улучшит его производительность.
Метаданные
Использовать этот диск для хранения метаданных кластера.
Метаданные + Кэш
Использовать этот диск для хранения метаданных кластера и кэша записи.
Уровень хранилища
Уровень 0
Кэширование и проверка контрольных сумм
Включить проверку контрольных сумм
Отмена
Назначить

Добавление расположений в Кибер Бэкап или Кибер Бэкап Облачный

Хранилище резервных копий использует шлюз резервного копирования (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 продукта Кибер Хранилище 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 сценариях использования, рекомендуется хранить данные резервных копий в локальном кластере хранилища продукта Кибер Хранилище. 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, и указать учетные данные этого пользователя.

Подключение к локальному кластеру хранилища через Backup Gateway

Ограничения

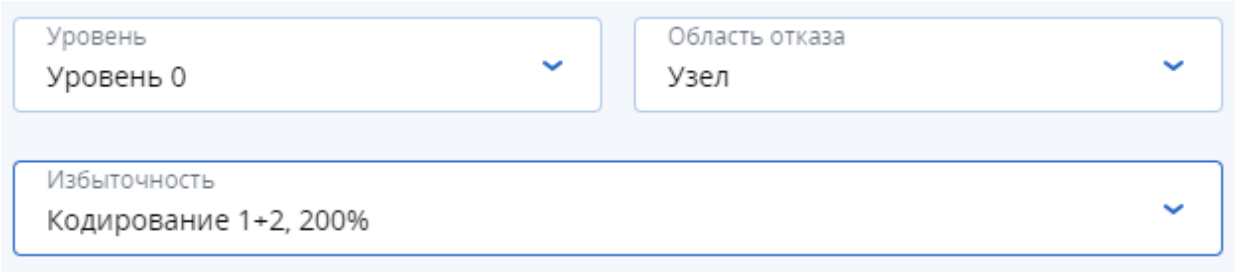
- Избыточность за счет репликации не поддерживается для хранилищ резервных копий.

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.

Выбор локального кластера в качестве места назначения резервных копий

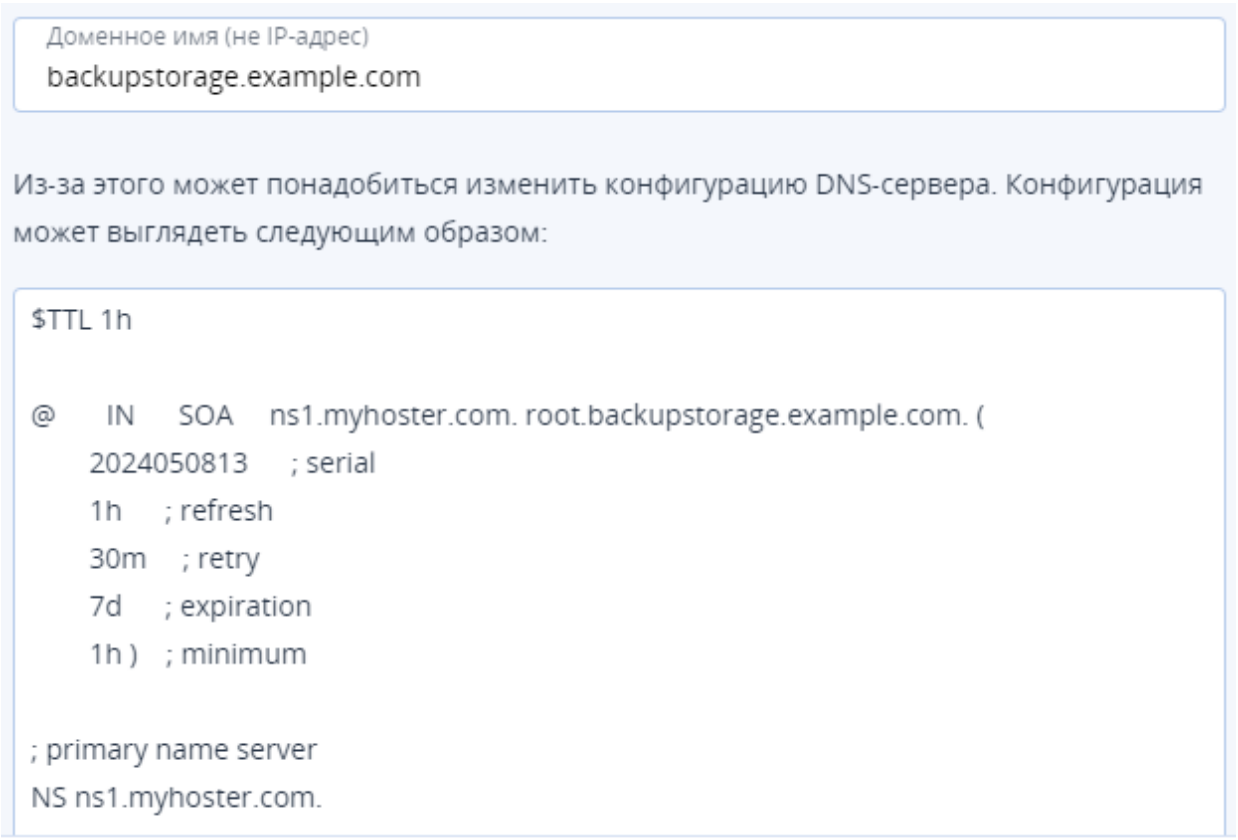
1. На экране **Инфраструктура** → **Сети** убедитесь, что в сети, которые вы собираетесь использовать, добавлены типы трафика **Резервное копирование (ABGW) внутр.** и **Резервное копирование (ABGW) внешн.**
2. Откройте экран **Сервисы хранилища** → **Резервные копии** и нажмите **Создать хранилище резервных 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 отказа 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**.

Важно

- Настройте свой DNS-сервер в соответствии с примером, приведенным в 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 Хранилище. Дополнительные сведения см. в статье Как запустить хранилище за HAProxy.

7. На шаге **Учетная запись Киберпротект** укажите следующую информацию для вашего продукта:
   - 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**.

Подключение к внешним томам NFS через Backup Gateway

Ограничения

- Кибер Хранилище 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 Хранилище 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

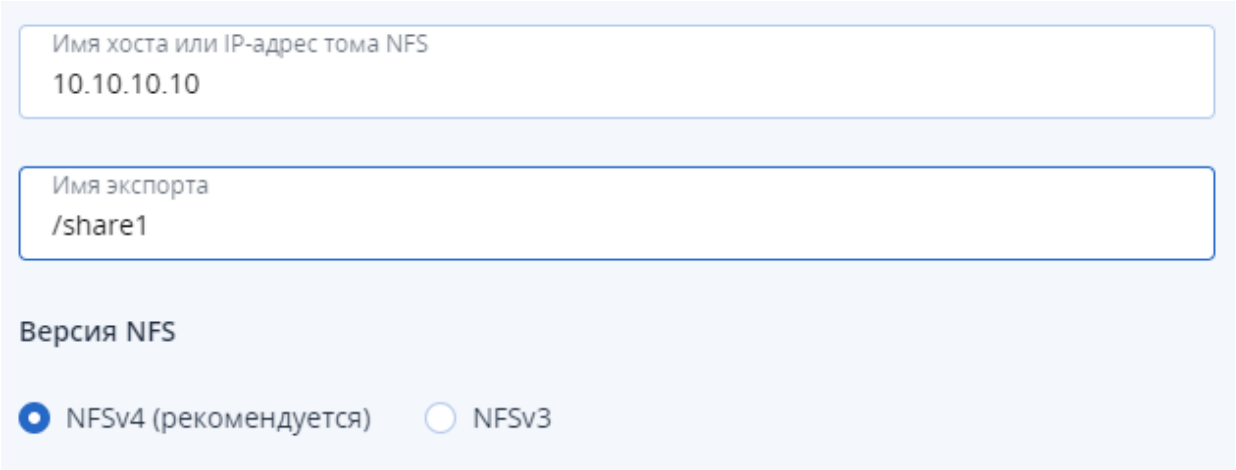
- В целевом хранилище достаточно места как для существующих, так и для новых резервных копий.
- Убедитесь, что на каждом сервере, который будет присоединен к кластеру хранилища резервных копий, открыт TCP-порт 44445 для исходящих подключений к Интернету, а также для входящих подключений от продукта Кибер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

- Убедитесь, что у сервера, который будет присоединен к хранилищу резервных копий, есть доступ к внешнему NFS-хранилищу.

Выбор внешнего тома 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**.

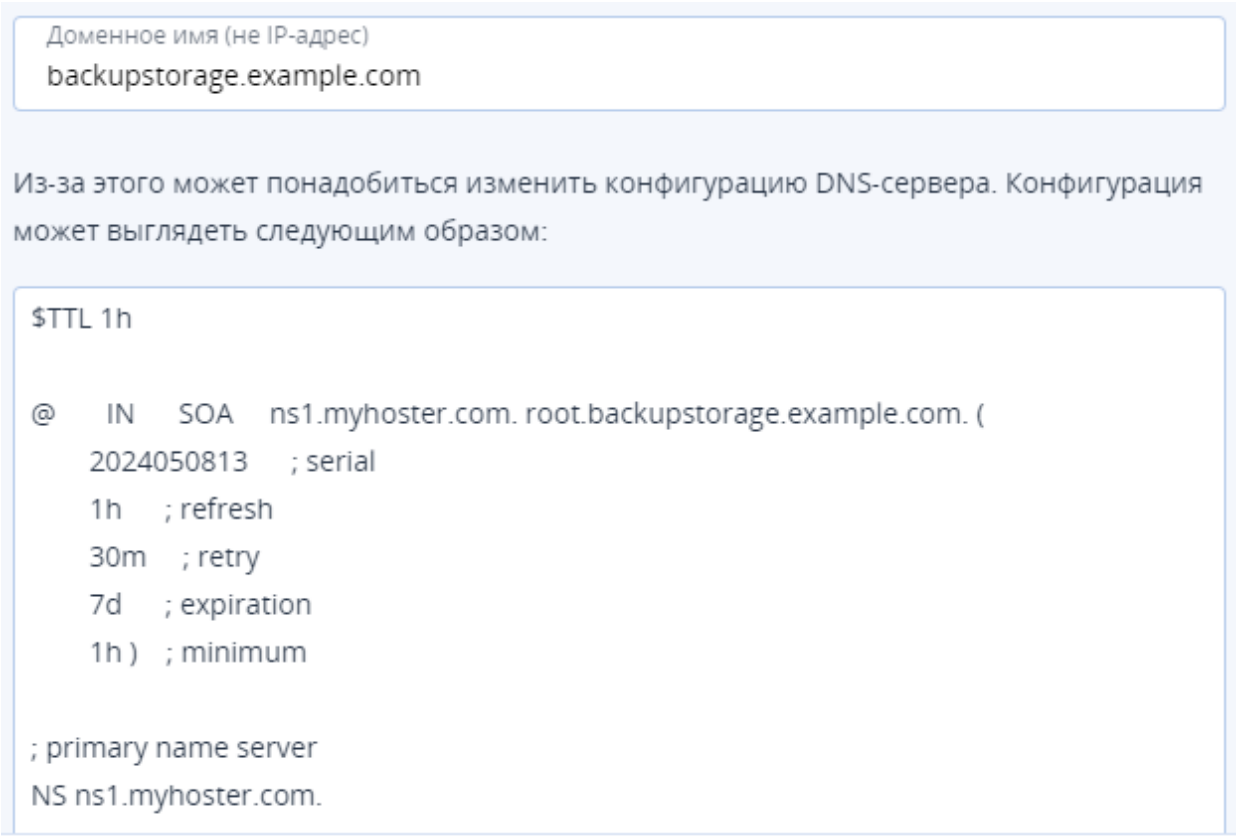
> **Примечание**
>
> Рекомендуется использовать NFS версии 4, поскольку она обеспечивает лучшую масштабируемость и производительность по сравнению с версией 3, которая имеет ограничения в протоколе.



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**.

Важно

- Настройте свой DNS-сервер в соответствии с примером, приведенным в 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:
   - 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**.

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.

Выбор публичного облака 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.
   1. Выберите поставщика облачного сервиса. Если ваш сервис совместим с S3, но отсутствует в списке, попробуйте **AuthV2-совместимый (S3)** или **AuthV4-совместимый (S3)** сервис.
   2. В зависимости от поставщика укажите **Регион**, **URL аутентификации (Keystone)** или **URL точки доступа**.
   3. При использовании **объектного хранилища Swift** укажите версию протокола аутентификации и необходимые для него атрибуты.
   4. Укажите учетные данные пользователя. При использовании **Google Cloud** выберите файл JSON с ключами для загрузки.
   5. Укажите папку (корзину, контейнер) для хранения резервных копий. Папка должна быть доступна для записи.

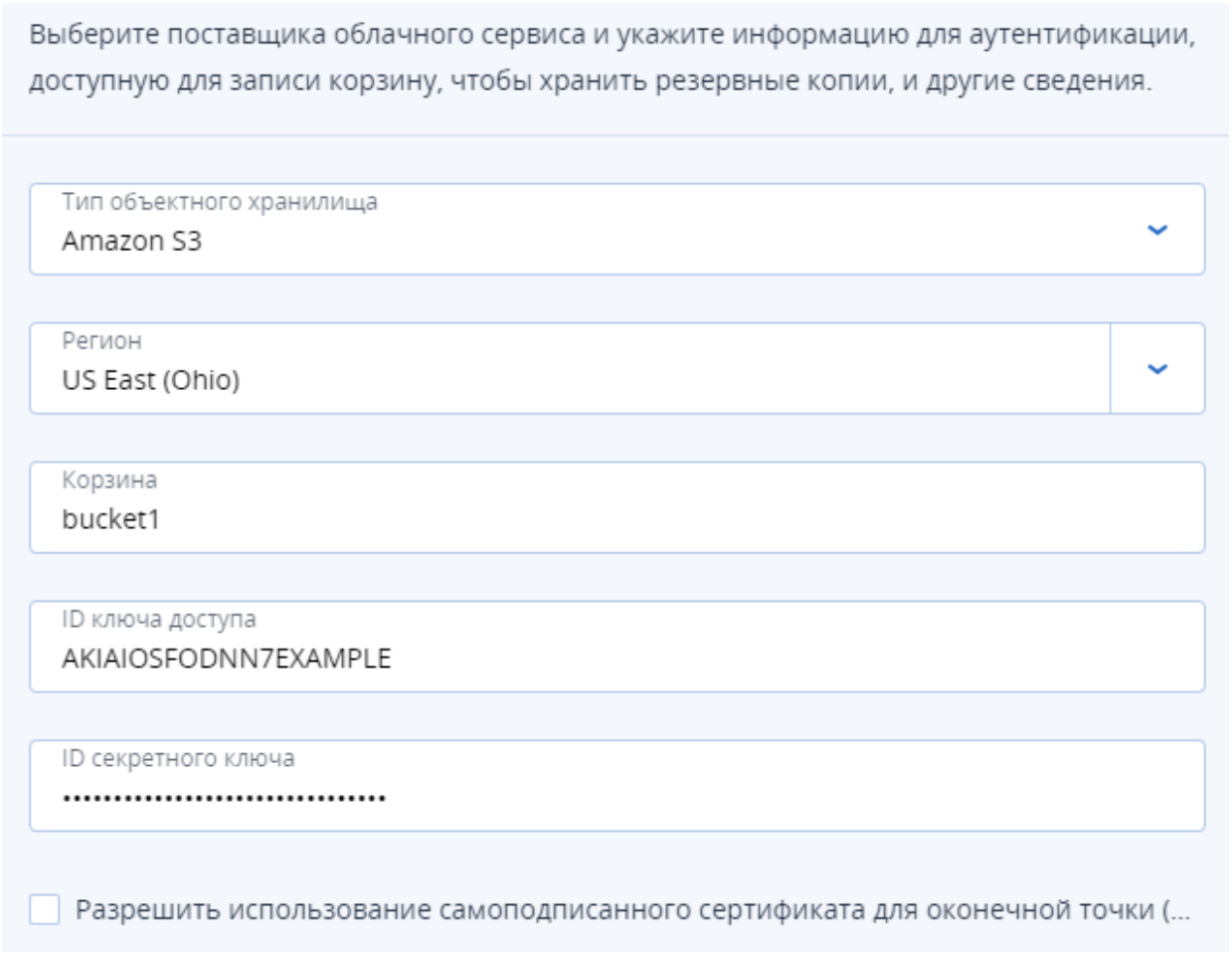
Для каждого кластера хранилища резервных копий следует использовать отдельный контейнер объектов.

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

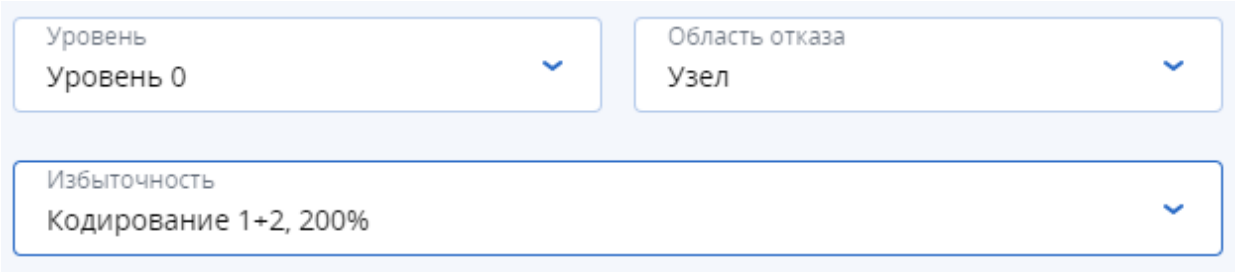
   - `Virtual-hosted style URLs`. Адреса вида `https://mybucket.s3.example.com/myobject.txt`. Предназначена для облачных S3-хранилищ.
   - `Path-style URLs`. Адреса вида `https://s3.example.com/mybucket/myobject.txt`. Предназначена для локальных S3-хранилищ.

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

7. Нажмите кнопку **Далее**.



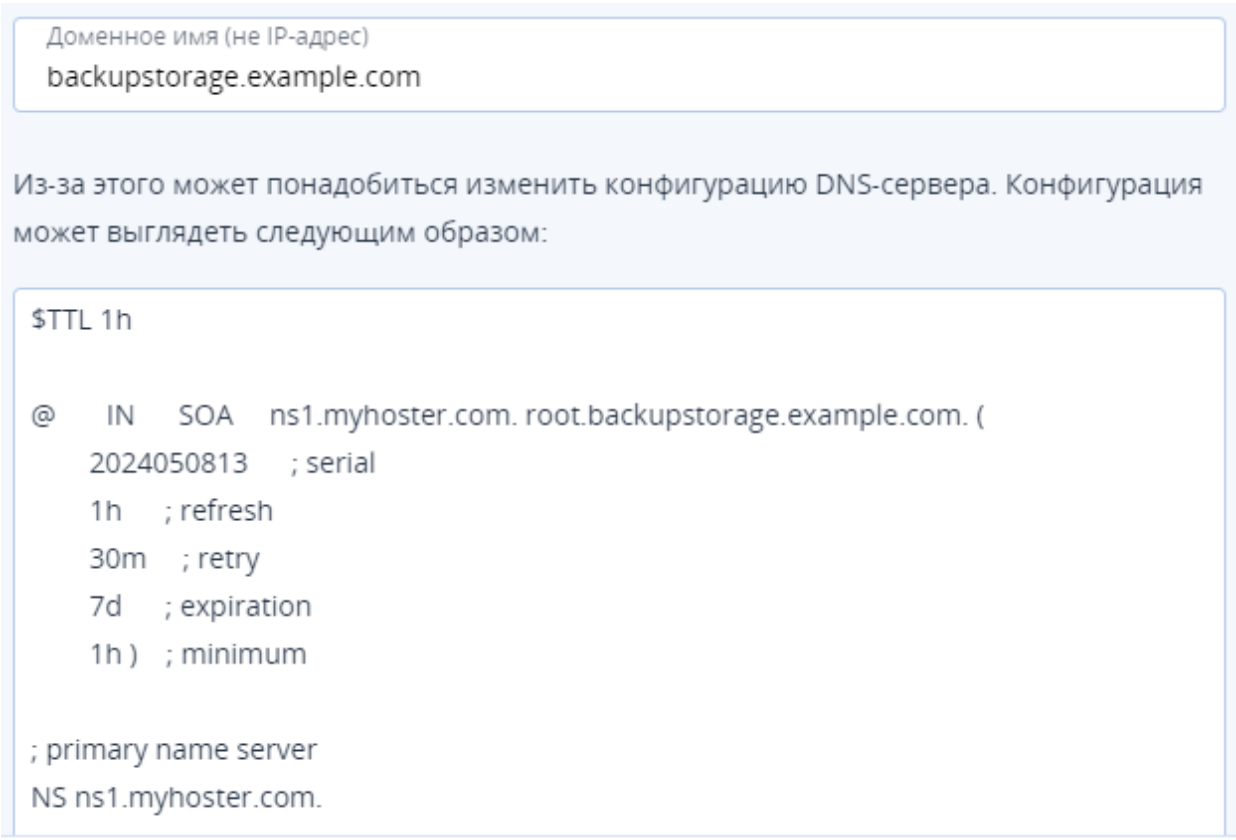
6. На шаге **Политика хранения** выберите нужный уровень, область отказа и режим избыточности данных. Избыточность за счет репликации не поддерживается для Backup Gateway. Дополнительные сведения см. в Руководстве администратора. Затем нажмите кнопку **Далее**.



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**.

Важно

- Настройте свой DNS-сервер в соответствии с примером, приведенным в 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 Хранилище. Дополнительные сведения см. в статье Как запустить хранилище за HAProxy.

8. На шаге **Учетная запись Киберпротект** укажите следующую информацию для вашего продукта:
   - 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**.