КИБЕРПРОТЕКТ

cyberprotect.ru

Кибер Инфраструктура

4.7

Руководство по быстрому старту Backup Gateway для VMware vSphere

РЕДАКЦИЯ: 11.04.2022

Заявление об авторских правах

Все права защищены.

Все остальные упоминаемые товарные знаки могут быть зарегистрированными товарными знаками соответствующих владельцев.

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.

© ООО Киберпротект, 2022

Оглавление

© ООО Киберпротект, 2022

1 О кратком руководстве BackupGateway для VMware vSphere

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

В общих чертах потребуется выполнить следующие действия.

1. Настроить сети.
2. Создать виртуальные машины для продукта Кибер Инфраструктура.
3. Развернуть продукт Кибер Инфраструктура на виртуальных машинах.
4. Настройка Backup Gateway.

Инструкции по настройке Кибер Инфраструктура для определенного сценария использования см. в руководстве администратора.

© ООО Киберпротект, 2022

2 Требования

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

- Версия VMware vSphere: 6.7 и выше
- Версия ВМ: 14 и выше
- На хосте должно быть достаточно памяти. Для сервера с одним диском хранилища, на котором работает Backup Gateway, требуется как минимум 8 ГБ ОЗУ.
- В хранилище данных vSphere должно быть достаточно свободного пространства. Каждая виртуальная машина занимает как минимум 425 ГБ (два диска хранилища по 200 ГБ и системный диск на 25 ГБ). Шаблон продукта Кибер Инфраструктура 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.

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

Замечание
Полные требования к оборудованию для сценария со шлюзом резервного копирования приведены в разделе «Системные требования» руководства администратора.

© ООО Киберпротект, 2022

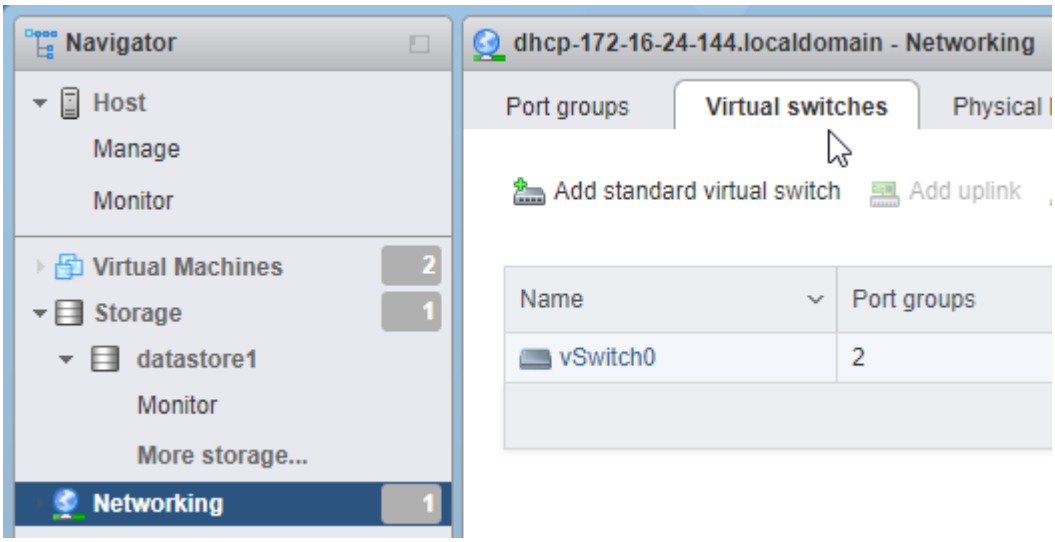
3 Настройка сетей

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

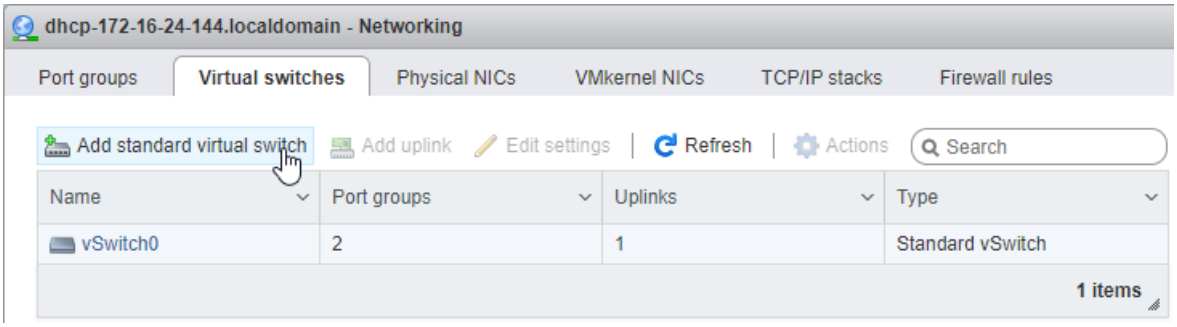
Замечание
Полные требования к сети см. в разделе «Требования к сети и рекомендации» руководства администратора.

Чтобы создать виртуальный коммутатор

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



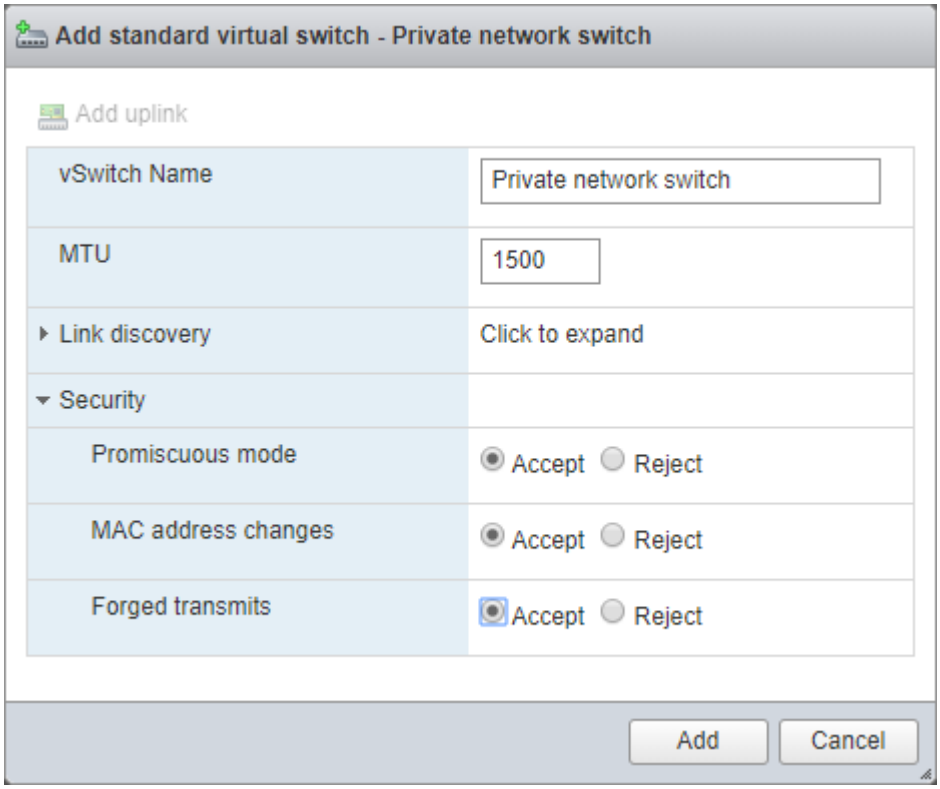
2. Нажмите **Add standard virtual switch** (Добавить стандартный виртуальный коммутатор) на панели инструментов.



3. Введите имя коммутатора и разверните пункт **Security** (Безопасность). Выберите **Accept** (Принять) для параметров **Promiscuous mode** (Неразборчивый режим), **MAC address changes**

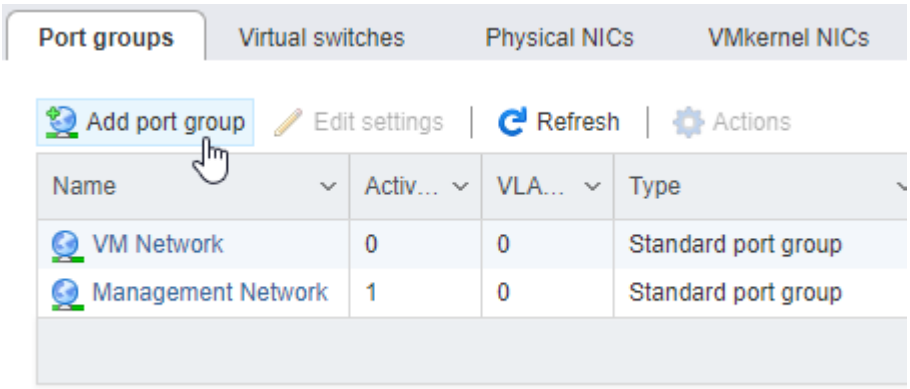
© ООО Киберпротект, 2022

(Изменения MAC-адреса) и **Forged transmits** (Подделка передаваемого трафика).



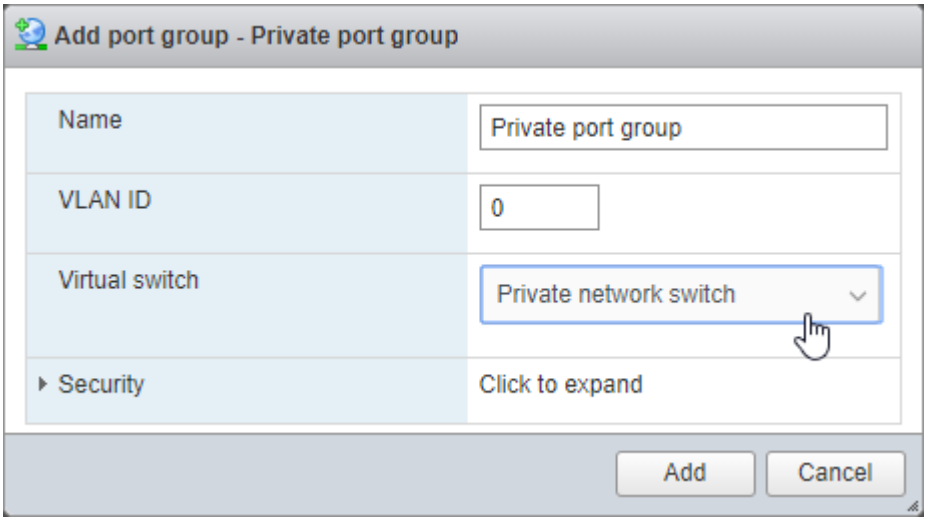
Чтобы создать группу портов

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



© ООО Киберпротект, 2022

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



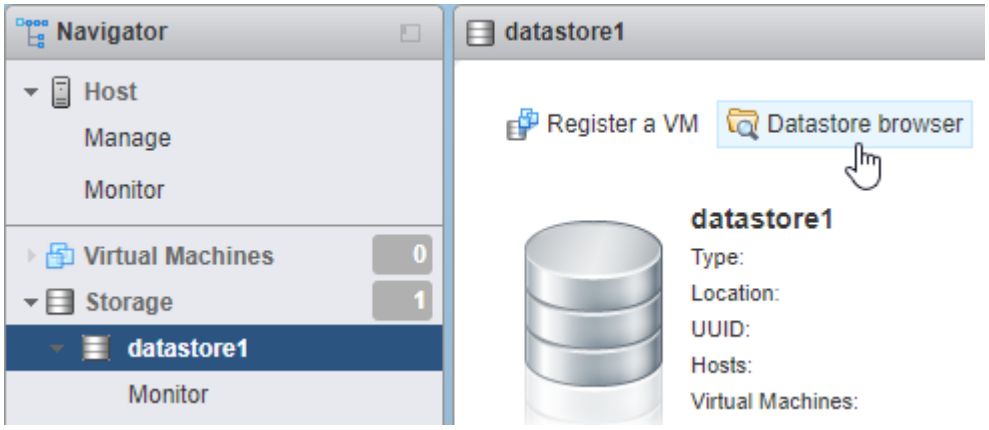
© ООО Киберпротект, 2022

4 Создание виртуальных машин

Прежде всего следует загрузить образ Кибер Инфраструктура в хранилище данных VMware vSphere. После этого можно приступать к созданию виртуальных машин.

Чтобы отправить образ Кибер Инфраструктура

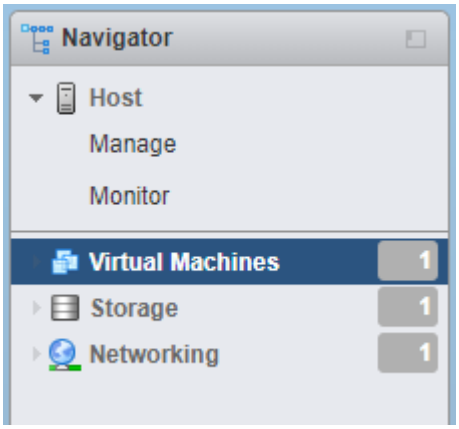
1. Загрузите образ Кибер Инфраструктура отсюда и распакуйте 2 файла VMDK.
2. На панели **Navigator** (Навигация) щелкните по нужному хранилищу данных. На панели инструментов хранилища нажмите **Datastore browser** (Обозреватель хранилища данных).
3. В окне **Datastore browser** (Обозреватель хранилища данных) создайте каталог с таким же именем, как у виртуальной машины.



4. Загрузите образ продукта Кибер Инфраструктура (два файла VMDK) в этот каталог.

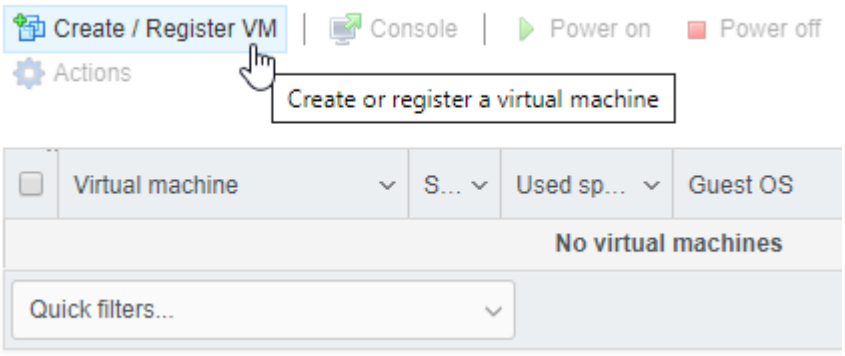
Чтобы создать виртуальную машину для продукта Кибер Инфраструктура

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

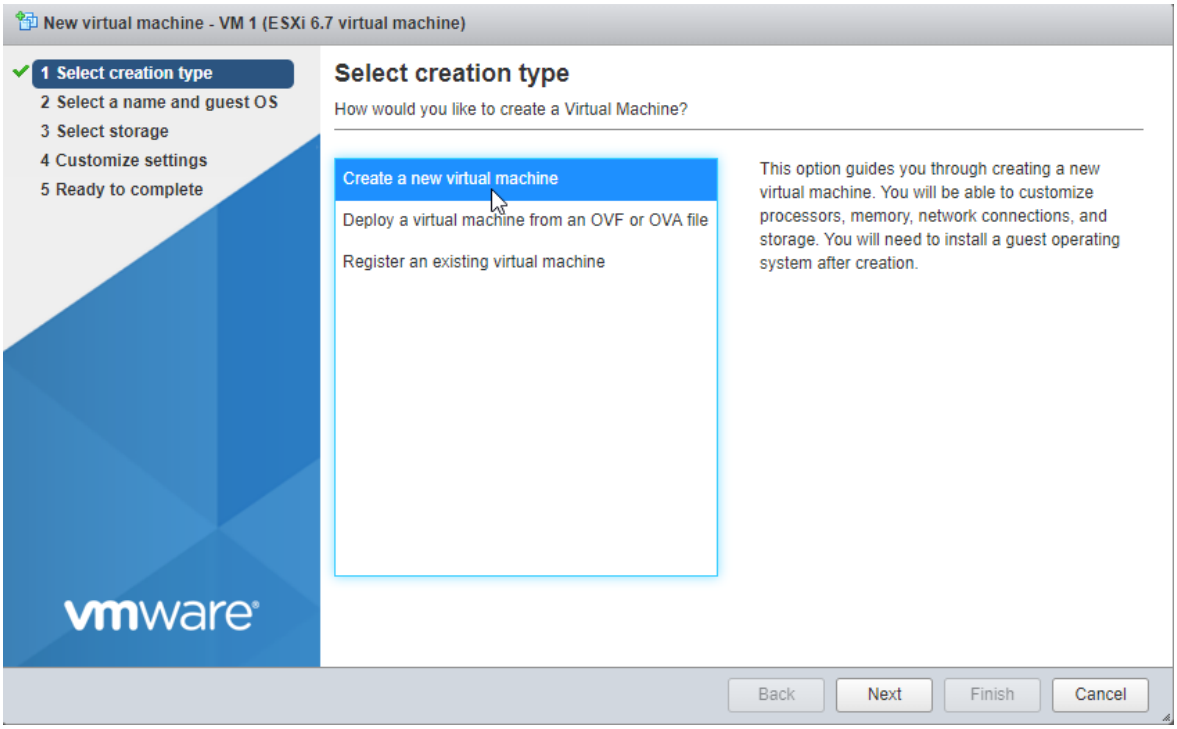


2. Нажмите **Create/Register VM** (Создать/зарегистрировать ВМ) на панели инструментов.

© ООО Киберпротект, 2022

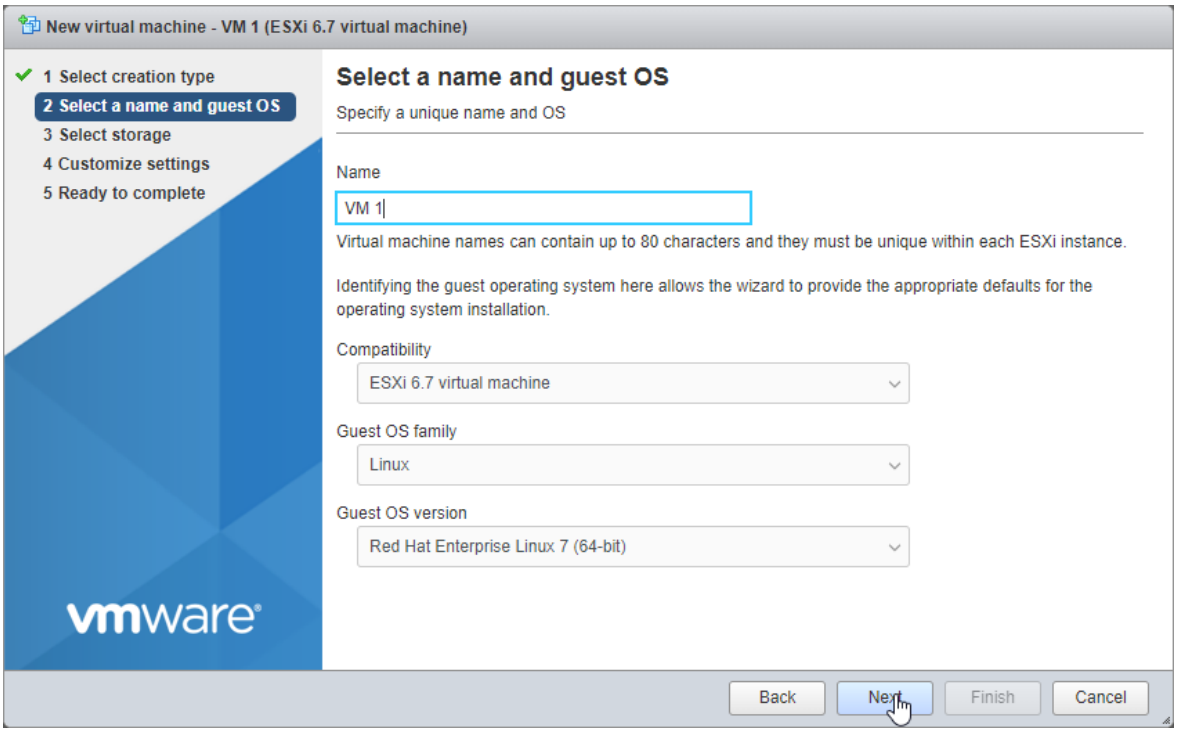


3. В мастере **New virtual machine** (Новая виртуальная машина) на шаге 1 выберите **Create a new virtual machine** (Создать новую виртуальную машину). Нажмите **Next** (Далее).

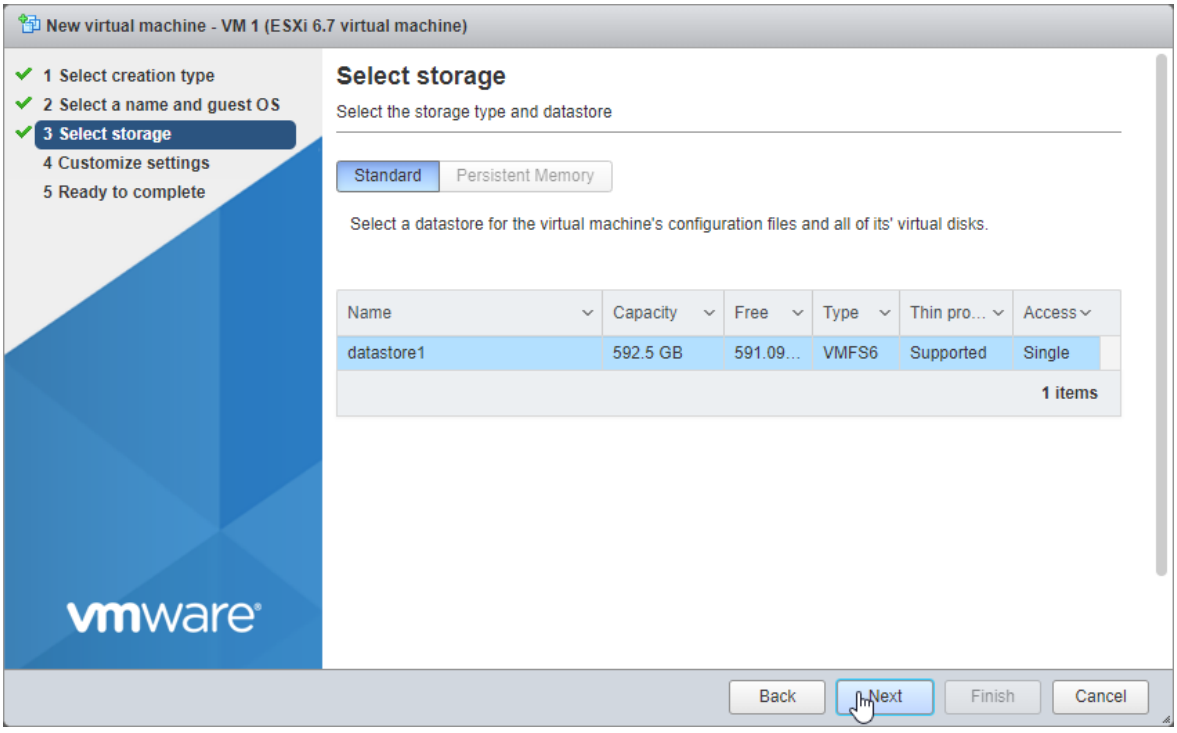


4. На шаге 2 введите имя для виртуальной машины и выберите гостевую ОС. Нажмите **Next** (Далее).

© ООО Киберпротект, 2022



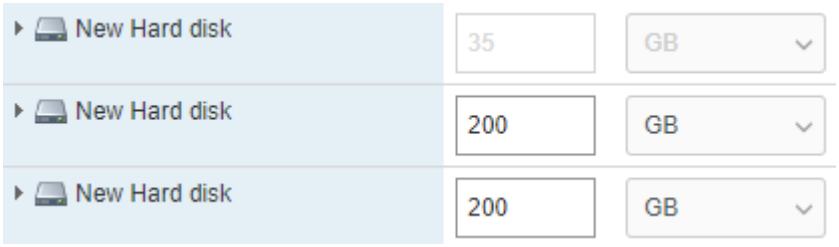
5. На шаге 3 выберите тип хранилища и хранилище данных. Убедитесь, что в хранилище данных достаточно свободного пространства.



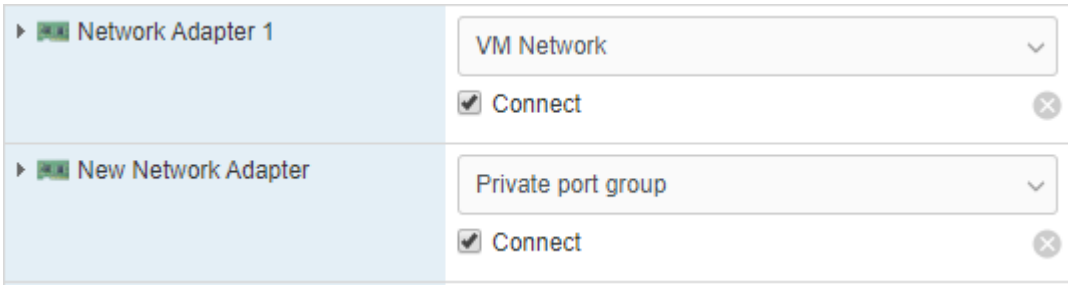
6. На шаге 4 удалите существующий жесткий диск и нажмите **Add hard disk** (Добавить жесткий диск) на панели инструментов. Выберите **Existing hard disk** (Существующий жесткий диск) и перейдите к образу, ранее загруженному в хранилище данных. Нажмите **Select** (Выбрать).
7. Снова нажмите **Add hard disk** (Добавить жесткий диск) на панели инструментов. Выберите **New standard hard disk** (Новый стандартный жесткий диск). Установите для него размер 200 ГБ.

© ООО Киберпротект, 2022

Повторите этот шаг, чтобы добавить еще один жесткий диск размером 200 ГБ. В итоге у вас должно быть три жестких диска: 35, 200 и 200 ГБ.



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



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

Повторите эти шаги, чтобы создать нужное количество виртуальных машин для вашего сценария (см. раздел "Требования" (р. 5)).

© ООО Киберпротект, 2022

5 Развертывание продукта Кибер Инфраструктура на виртуальных машинах

После запуска виртуальной машины выполните следующие действия.

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

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

   В строке (current) UNIX password введите password; в строке New password и Retype new password введите новый пароль. Пароль будет изменен как для пользователя **storage-user**, так и для привилегированного пользователя.
2. Снова выполните вход как пользователь **storage-user** с новым паролем, а затем переключитесь на привилегированного пользователя.

   ```
   $ sudo su
   ```

3. Настройте и включите сетевой интерфейс **eth1**.

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

   где <node> – номер сервера: 2 для сервера управления, 3 для первого подчиненного сервера и так далее.
4. Проверьте, что IP-адрес назначен и интерфейс работает, например с помощью команды ip -4 a show eth1.

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

© ООО Киберпротект, 2022

5.1 Развертывание сервера управления

Чтобы развернуть сервер управления на виртуальной машине, необходимо настроить его, а затем создать на нем кластер хранилища.

Чтобы настроить сервер управления

1. Зарегистрируйте сервер управления и запустите на нем панель администрирования.
   a. На сервере выполните следующую команду от имени привилегированного пользователя, чтобы настроить компонент панели администрирования:

      ```
      echo <password> | /usr/libexec/vstorage-ui-backend/bin/configure-backend.sh -i <private_
      iface> -x <public_iface>
      ```

      где:
      - <password> – желаемый пароль администратора;
      - <private_iface> – имя частного сетевого интерфейса;
      - <private_iface> – имя внешнего сетевого интерфейса.

   b. Запустите сервис панели администрирования на сервере.

      ```
      # systemctl start vstorage-ui-backend
      ```

   c. Зарегистрируйте сервер на панели администрирования.

      ```
      # /usr/libexec/vstorage-ui-agent/bin/register-storage-node.sh -m <MN_IP_address> -x
      <public_iface>
      ```

      где:
      - <MN_IP_address> – IP-адрес частного сетевого интерфейса сервера;
      - <private_iface> – имя внешнего сетевого интерфейса.

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

   На панели администрирования развернутый сервер будет отображаться на экране **Инфраструктура** > **Серверы** со статусом **Не назначен**.
3. На экране **Инфраструктура** > **Сети** щелкните по значку карандаша рядом с типом трафика **API вычислений**, доступным для внешней сети, и нажмите **Сохранить**.
4. Добавьте тип трафика **API вычислений** для внешней сети.
   a. На экране **Инфраструктура** > **Сети** щелкните по значку карандаша рядом с типом трафика **API вычислений**.
   b. Добавьте этот тип трафика во внешнюю сеть с помощью переключателя.
   c. Щелкните галочку, чтобы применить изменения.

© ООО Киберпротект, 2022

Чтобы создать кластер хранилища данных

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

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" (p. 19).

5.2 Развертывание подчиненных серверов

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

Чтобы настроить подчиненный сервер

1. Получите токен и адрес сервера управления на панели администрирования.
   a. Выполните вход на панель администрирования через порт 8888. IP-адрес панели отображается в консоли после развертывания главного сервера. Используйте имя пользователя по умолчанию, указанное на экране входа в систему, и пароль привилегированного пользователя главного сервера.
      При появлении запроса добавьте сертификат безопасности в исключения браузера.
   b. На панели администрирования откройте раздел **Инфраструктура** > **Серверы** и нажмите **Подключить сервер**, чтобы вызвать экран с адресом сервера управления и токеном.
2. Откройте терминал виртуальной машины и зарегистрируйте подчиненный сервер на панели администрирования, выполнив следующую команду:

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

   где:
   - <MN_IP_address> — IP-адрес частного сетевого интерфейса на сервере с панелью администрирования;
   - <token> — токен, полученный на панели администрирования.

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

Чтобы добавить подчиненный сервер в кластер хранилища

© ООО Киберпротект, 2022

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 Инфраструктура для нужного сценария. Инструкции по выполнению различных задач настройки приведены в руководстве администратора.

© ООО Киберпротект, 2022

6 Добавление дискового пространства в продукт Кибер Инфраструктура

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 по командной строке.
- Одинаковый размер дисков помогает более равномерно распределять нагрузку. Внутри кластера диски используются пропорционально их размеру. Например, если у вас есть диск размером 10 ТБ и диск размером 2 ТБ, при загрузке кластера на 50 % на дисках будет использовано 5 и 1 ТБ соответственно.

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

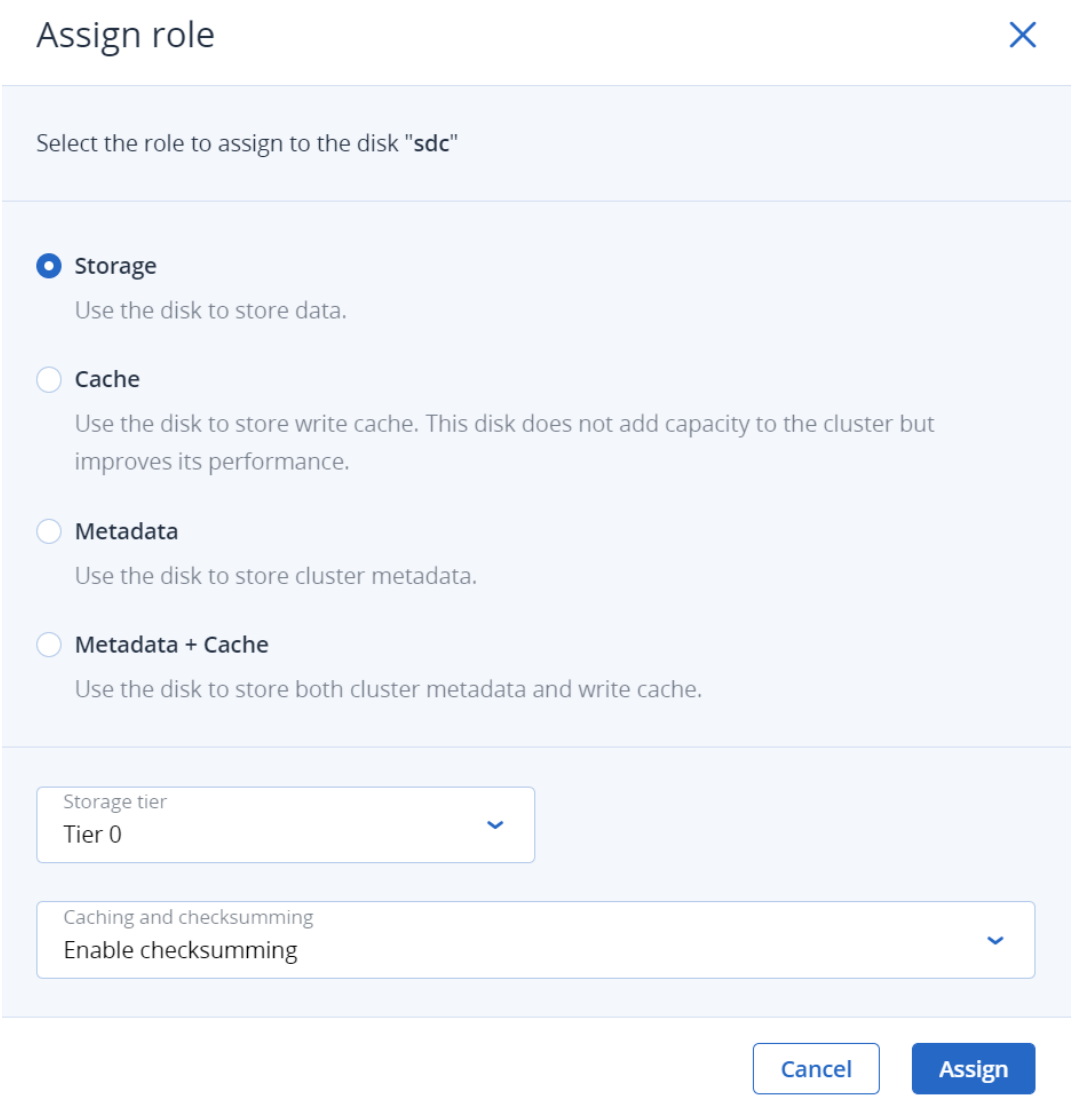
Добавьте новый виртуальный диск в виртуальную машину, как показано в разделе Добавление нового жесткого диска в виртуальную машину. После этого диск будет отображаться в списке дисков сервера на панели администрирования продукта Кибер Инфраструктура.

Как настроить новый диск на панели администрирования

1. На экране **Инфраструктура** > **Серверы** щелкните по имени сервера с созданным диском. Перейдите на вкладку **Диски** для просмотра всех дисков сервера.
2. Щелкните по диску без роли, созданный ранее.
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

© ООО Киберпротект, 2022

разделе «Настройка новых дисков вручную» в руководстве администратора.



© ООО Киберпротект, 2022

7 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, Google Cloud, Microsoft Azure и AWS S3) 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 Microsoft Azure, OpenStack Swift и Google Cloud Platform

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.

Замечание
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 вашей партнерской учетной записи должна быть отключена двухфакторная проверка подлинности (2FA).

7.1 Подключение к локальному кластеру хранилища через Backup Gateway

Ограничения

© ООО Киберпротект, 2022

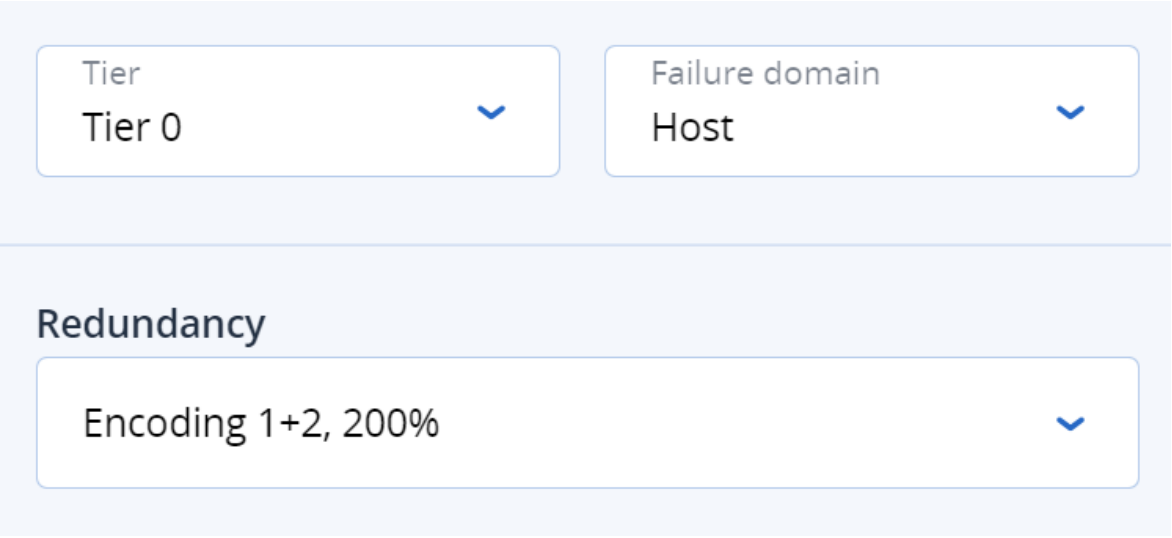
- Избыточность за счет репликации не поддерживается для хранилищ резервных копий.

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 хранения** > **Хранилище резервных копий** 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**.

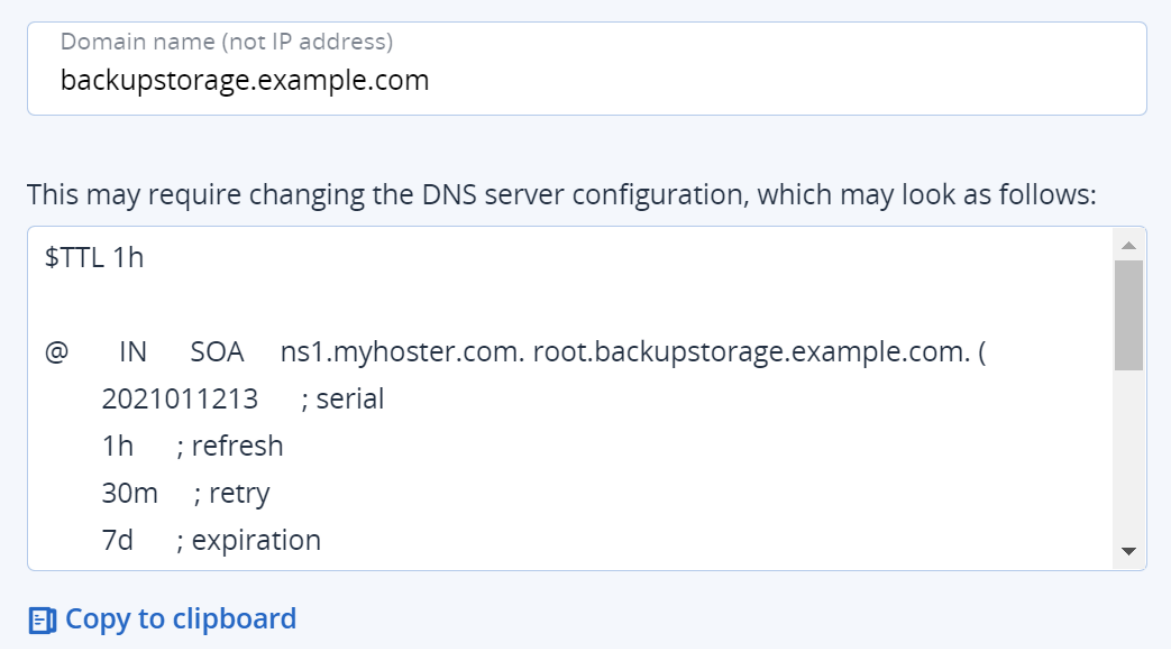


6. На шаге **DNS** укажите внешнее доменное имя для хранилища резервных копий, например **backupstorage.example.com**. Агенты резервного копирования будут использовать это доменное имя и TCP-порт 44445 для передачи данных в хранилище. Затем нажмите кнопку **Далее**.

© ООО Киберпротект, 2022

Важно

- 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.



Замечание

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 https://kb.cyberprotect.ru/content/64787.

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**.

7.2 Подключение к внешним томам NFS через Backup Gateway

Ограничения

© ООО Киберпротект, 2022

- 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

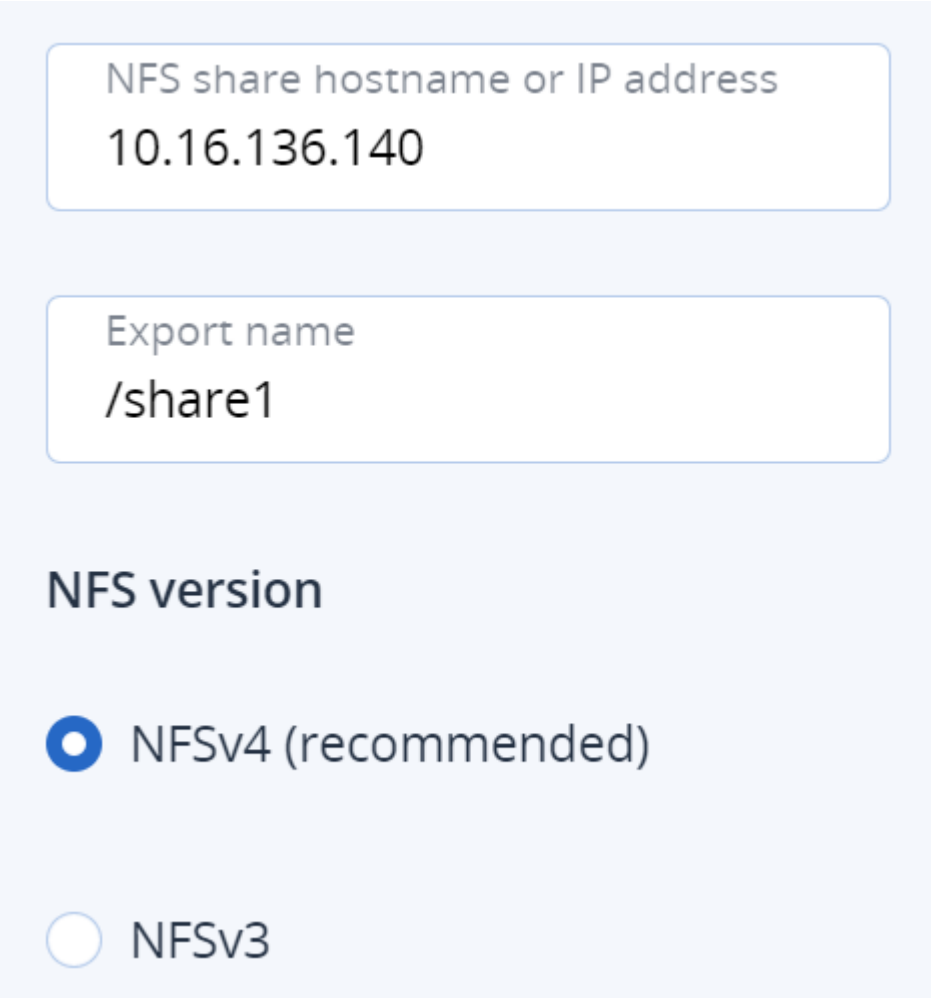
- В целевом хранилище достаточно места как для существующих, так и для новых резервных копий.
- Убедитесь, что на каждом сервере, который будет присоединен к кластеру хранилища резервных копий, открыт TCP-порт 44445 для исходящих подключений к Интернету, а также для входящих подключений от продукта Кибер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

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

© ООО Киберпротект, 2022

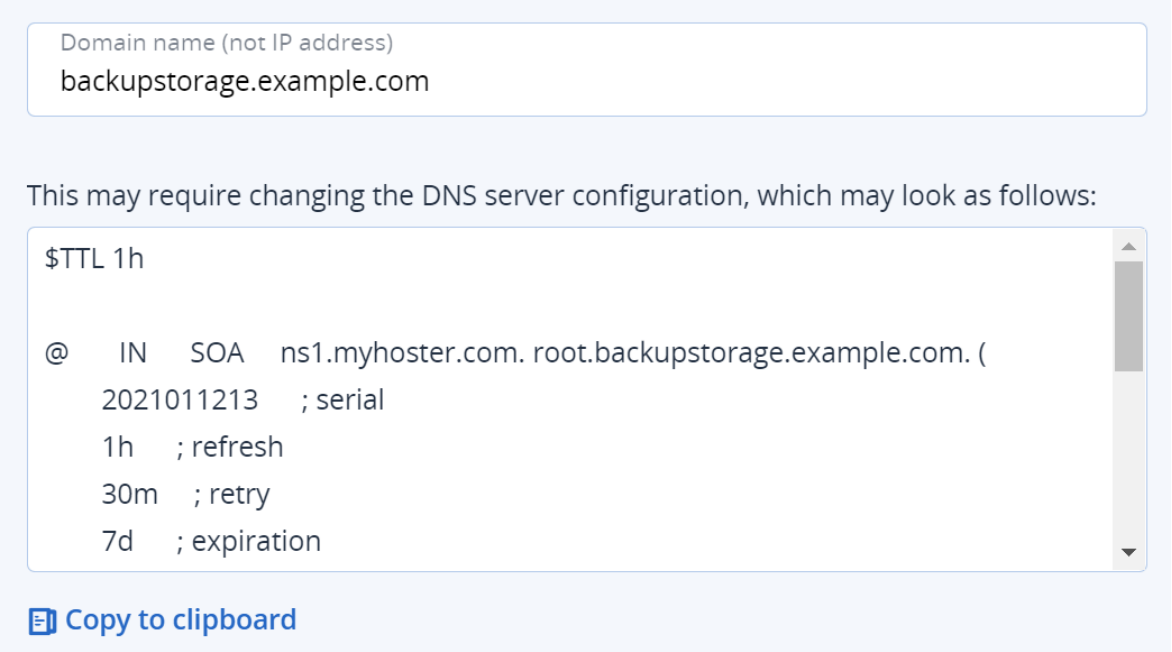


6. На шаге **DNS** укажите внешнее доменное имя для хранилища резервных копий, например **backupstorage.example.com**. Агенты резервного копирования будут использовать это доменное имя и TCP-порт 44445 для передачи данных в хранилище. Затем нажмите кнопку **Далее**.

Важно

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

© ООО Киберпротект, 2022



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**.

7.3 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:

- Amazon S3
- IBM Cloud
- Alibaba Cloud
- IIJ
- Cleversafe
- Cloudian
- Microsoft Azure
- Объектное хранилище Swift
- Softlayer (Swift)

© ООО Киберпротект, 2022

- 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:

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

Классы архивных хранилищ, такие как Amazon S3 Glacier, Azure Archive Blob или Google Archive, не могут использоваться для резервного копирования, поскольку не предоставляют мгновенного доступа к данным. Большая задержка при доступе (несколько часов) делает технически невозможным просмотр архивов, быстрое восстановление данных и создание инкрементных резервных копий. Хотя архивные хранилища, как правило, очень экономичны, следует учитывать, что существуют различные факторы, определяющие стоимость. В действительности общая стоимость публичного облачного хранилища складывается из платы за хранение данных, операции, трафик, извлечение данных, досрочное удаление и т. д. Например, сервис архивного хранилища может брать полугодовую стоимость хранения всего за одну операцию восстановления данных. Если предполагается более частый доступ к данным, то добавочные расходы значительно повышают общую стоимость хранилища. Чтобы избежать низкой скорости извлечения данных и сократить расходы, рекомендуем использовать Кибер Облачные Сервисы 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

© ООО Киберпротект, 2022

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.

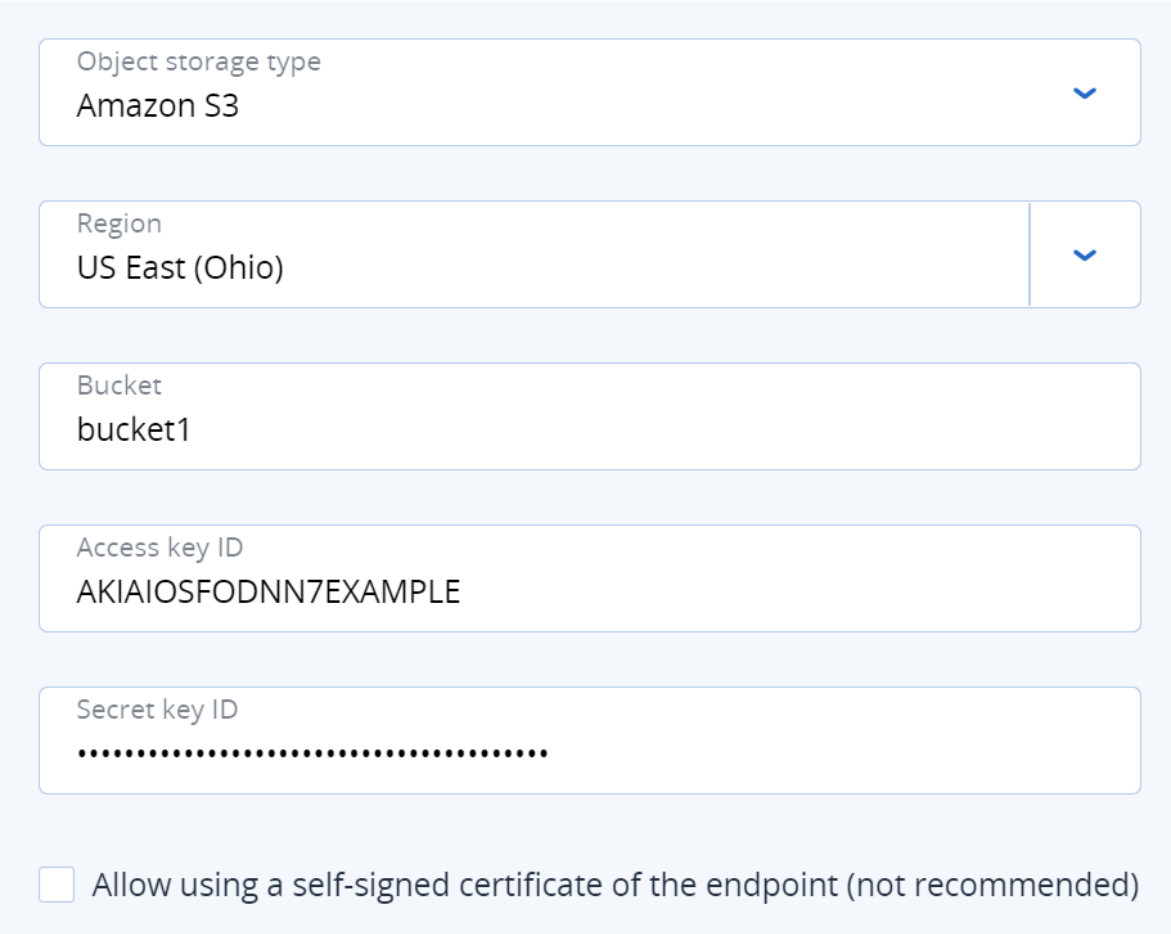
Как выбрать публичное облако в качестве места назначения резервных копий

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 хранения** > **Хранилище резервных копий** 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

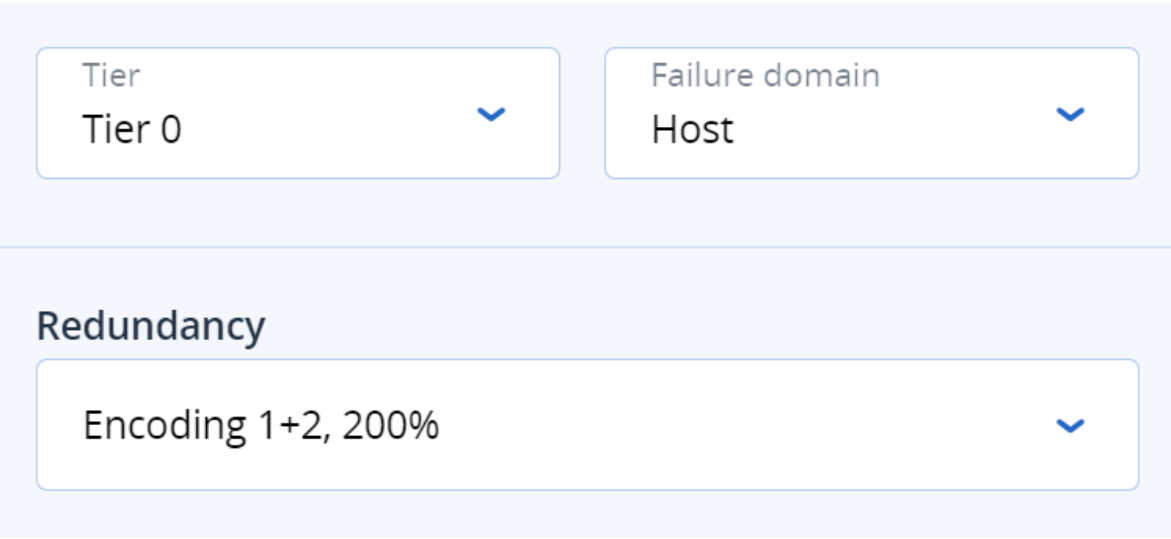
© ООО Киберпротект, 2022

контейнер объектов.

f. 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**.

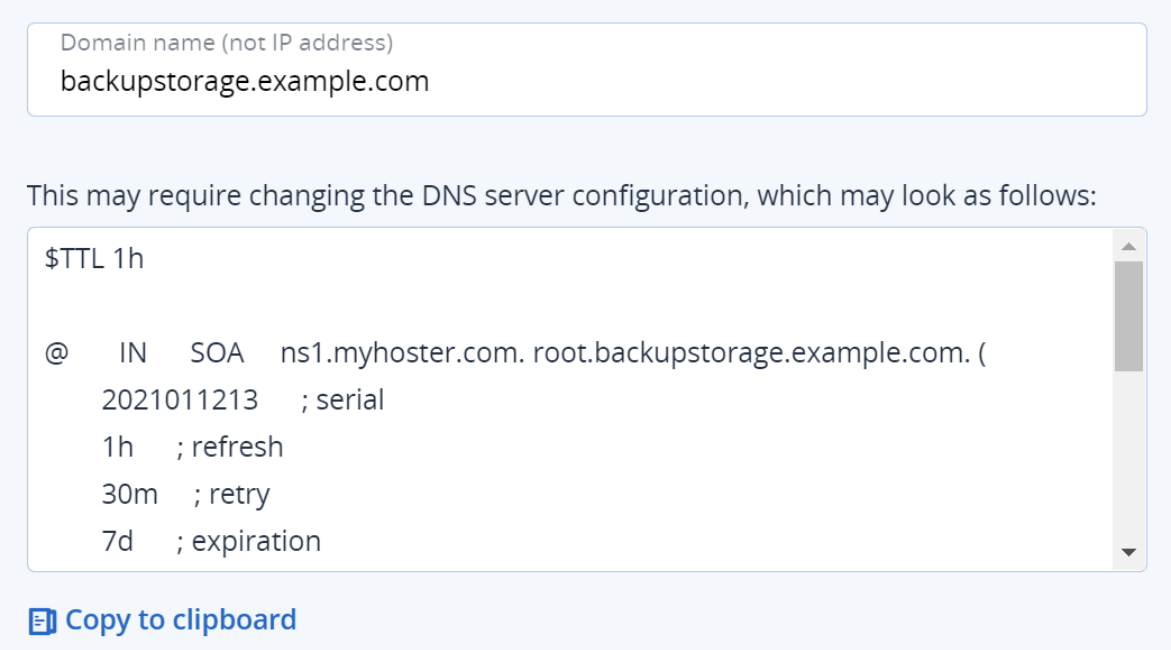


© ООО Киберпротект, 2022

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 на панели администратора.
- При каждом изменении сетевой конфигурации серверов в кластере хранилища резервных копий корректируйте записи DNS соответствующим образом.



Замечание

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 https://kb.cyberprotect.ru/content/64787.

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**.

© ООО Киберпротект, 2022