

# КИБЕРПРОТЕКТ



# КИБЕР Инфраструктура

Версия 5.5

Руководство по быстрому старту Backup Gateway  
для VMware vSphere

Редакция: 22.04.2024

## 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.

# Содержание

<b>1</b>	<b>О кратком руководстве Backup Gateway для VMware vSphere</b>	<b>4</b>
<b>2</b>	<b>Требования</b>	<b>5</b>
<b>3</b>	<b>Настройка сетей</b>	<b>6</b>
<b>4</b>	<b>Создание виртуальных машин</b>	<b>9</b>
<b>5</b>	<b>Развертывание продукта Кибер Инфраструктура на виртуальных машинах</b>	<b>13</b>
5.1	Развертывание сервера управления	13
5.2	Развертывание подчиненных серверов	13
<b>6</b>	<b>Добавление дискового пространства в продукт Кибер Инфраструктура</b>	<b>15</b>
<b>7</b>	<b>Добавление расположений в Кибер Бэкап или Кибер Бэкап Облачный</b>	<b>17</b>
7.1	Подключение к локальному кластеру хранилища через Backup Gateway	18
7.2	Подключение к внешним томам NFS через Backup Gateway	19
7.3	Подключение к публичному облачному хранилищу через Backup Gateway	22

# 1 О кратком руководстве Backup Gateway 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.

## 2 Требования

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

- Версия VMware vSphere: 6.7 и выше
- Версия VM: 14 и выше
- Используется виртуальная машина с BIOS.
- Минимум 8 ГБ ОЗУ для каждой виртуальной машины с Backup Gateway.
- Минимум 464 ГБ дискового пространства для каждой виртуальной машины с Backup Gateway (два диска хранилища по 200 ГБ и системный диск на 64 ГБ). Шаблон продукта Кибер Инфраструктура также занимает около 3 ГБ. Рекомендуемый максимальный размер одного виртуального диска – 16 ТБ.

---

### Внимание

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.

---

### Примечание

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

---

## 3 Настройка сетей

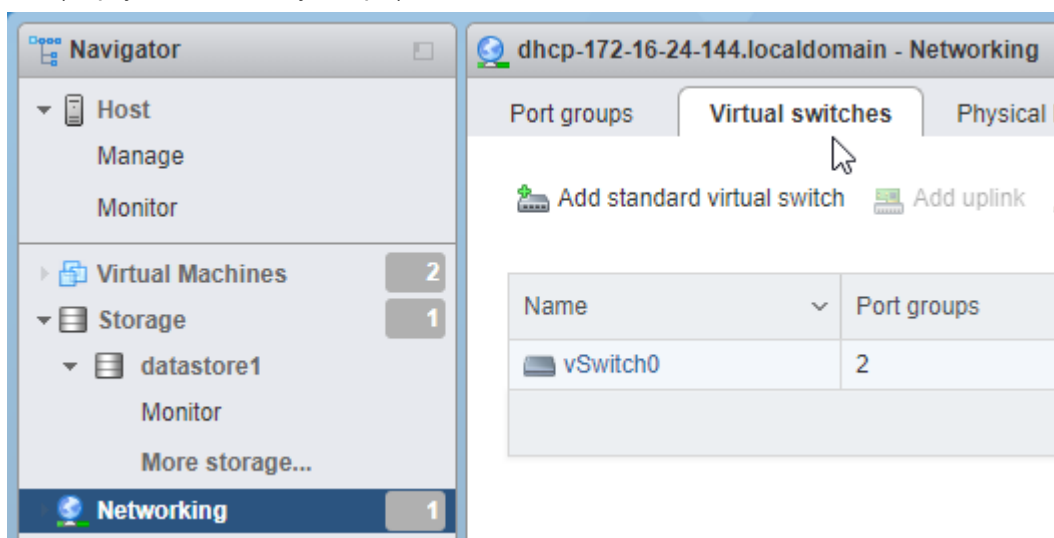
Для работы продукта Кибер Инфраструктура обычно требуются две сети: публичная для внешних подключений и частная для обмена данными между виртуальными машинами. Можно использовать уже настроенную внешнюю сеть, но рекомендуется создать выделенную частную сеть, даже если частная сеть уже существует. Для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

### Примечание

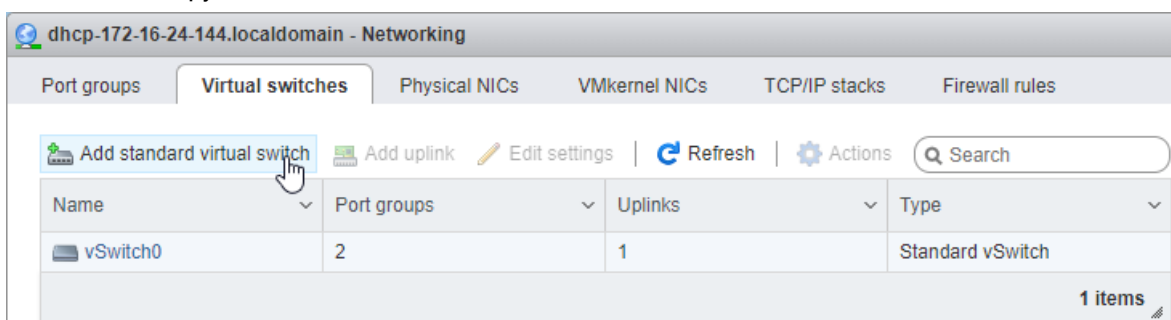
Полные требования к сети см. в разделе «Требования к сети и рекомендации» руководства администратора.

### 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**

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

**Add standard virtual switch - Private network switch**

Add uplink

vSwitch Name	Private network switch
MTU	1500
▶ Link discovery	Click to expand
▼ Security	
Promiscuous mode	<input checked="" type="radio"/> Accept <input type="radio"/> Reject
MAC address changes	<input checked="" type="radio"/> Accept <input type="radio"/> Reject
Forged transmits	<input checked="" type="radio"/> Accept <input type="radio"/> Reject

Add Cancel

### Чтобы создать группу портов

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

Port groups Virtual switches Physical NICs VMkernel NICs

**Add port group** Edit settings Refresh Actions

Name	Activ...	VLA...	Type
VM Network	0	0	Standard port group
Management Network	1	0	Standard port group

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

Add port group - Private port group	
Name	Private port group
VLAN ID	0
Virtual switch	Private network switch
▶ Security	Click to expand

Add Cancel



## 4 Создание виртуальных машин

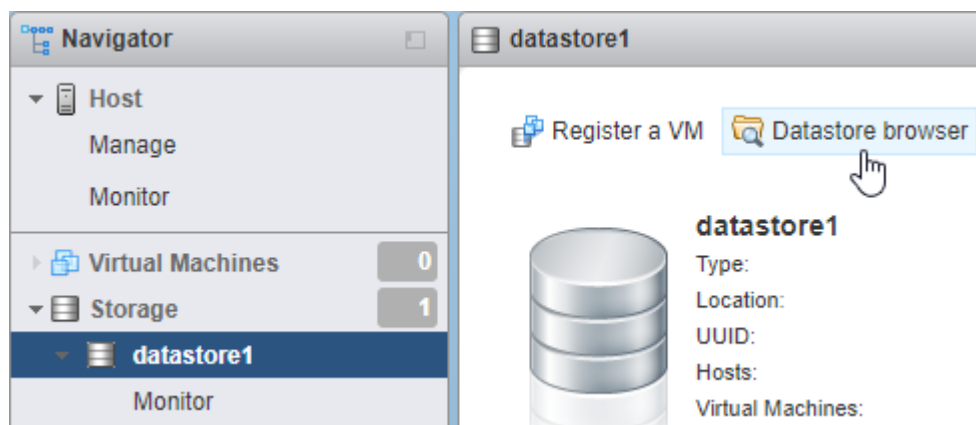
Прежде всего следует поместить образы продукта Кибер Инфраструктура в хранилище данных VMware vSphere. После этого можно приступить к созданию виртуальных машин.

### Примечание

Для создания виртуальных машин вы также можете использовать [шаблон виртуальной машины OVA](#).

### Чтобы поместить образы продукта Кибер Инфраструктура в хранилище данных VMware vSphere

1. Загрузите облачный образ для развертывания узлов кластера – [виртуальный диск для VMware \(VMDK\)](#). Один и тот же образ используется для развертывания первого (с панелью администрирования) и последующих узлов кластера.
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 именем создаваемой виртуальной машины.

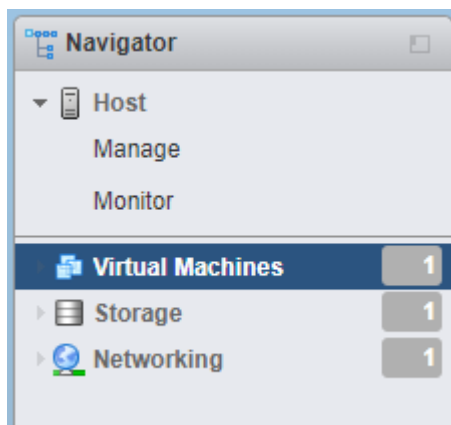


4. Поместите в этот каталог виртуальный диск для узла кластера.

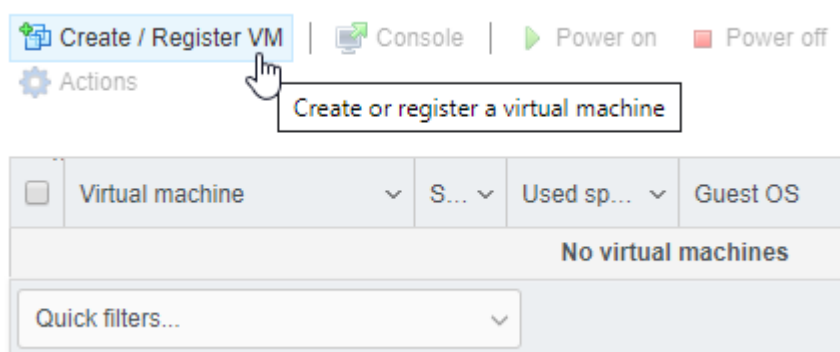
Повторите эти шаги, чтобы поместить по одному виртуальному диску для каждой создаваемой виртуальной машины.

### Чтобы создать виртуальную машину для продукта Кибер Инфраструктура

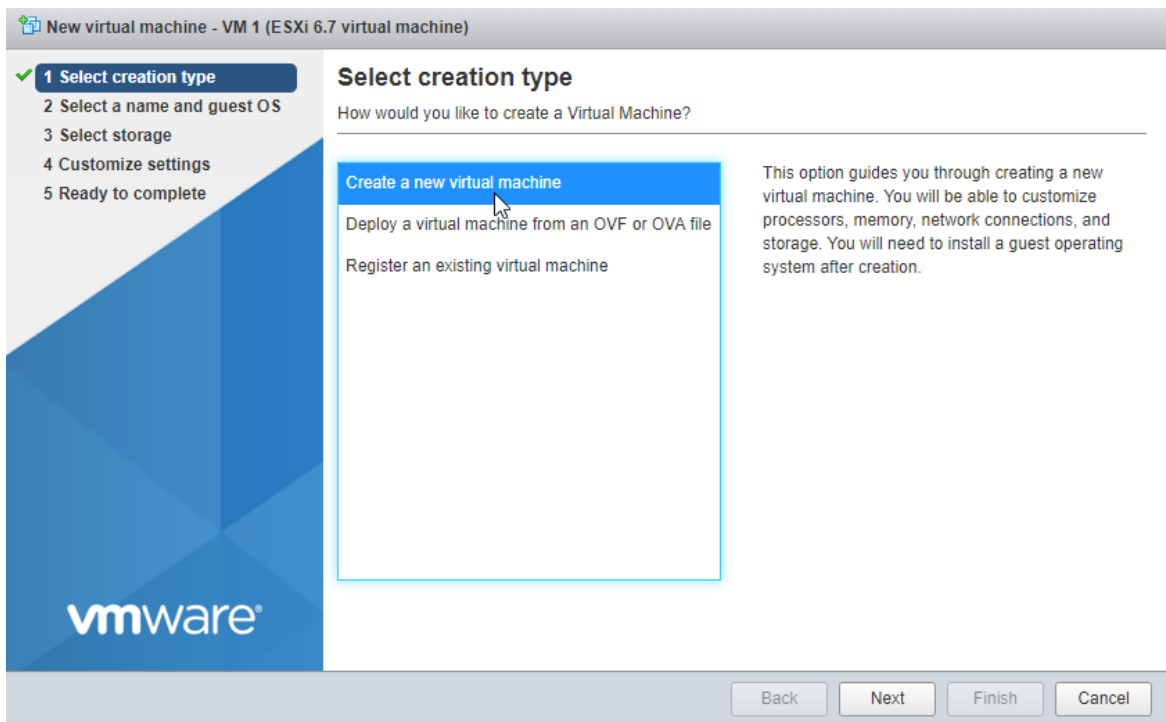
1. В клиенте Host Client нажмите **Virtual Machines** (Виртуальные машины) в меню слева.



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



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).

The screenshot shows the 'New virtual machine - VM 1 (ESXi 6.7 virtual machine)' wizard. The left sidebar shows the progress: 1. Select creation type (checked), 2. Select a name and guest OS (highlighted), 3. Select storage, 4. Customize settings, 5. Ready to complete. The main area is titled 'Select a name and guest OS' and includes a text input for 'Name' containing 'VM 1'. Below this is a note: 'Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance. Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.' There are three dropdown menus: 'Compatibility' (ESXi 6.7 virtual machine), 'Guest OS family' (Linux), and 'Guest OS version' (Red Hat Enterprise Linux 7 (64-bit)). At the bottom right, there are buttons for 'Back', 'Next' (with a mouse cursor), 'Finish', and 'Cancel'.

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

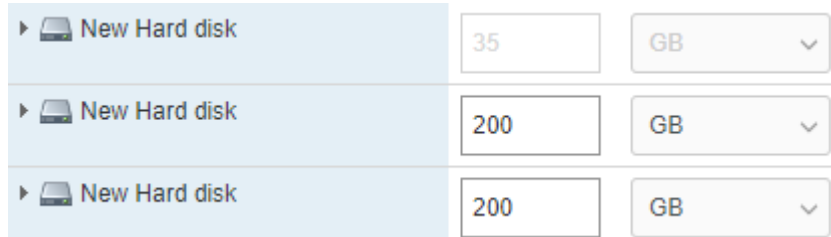
The screenshot shows the 'New virtual machine - VM 1 (ESXi 6.7 virtual machine)' wizard at Step 3: 'Select storage'. The left sidebar shows progress: 1. Select creation type (checked), 2. Select a name and guest OS (checked), 3. Select storage (highlighted), 4. Customize settings, 5. Ready to complete. The main area is titled 'Select storage' and includes a sub-header 'Select the storage type and datastore'. There are two radio buttons: 'Standard' (selected) and 'Persistent Memory'. Below is a note: 'Select a datastore for the virtual machine's configuration files and all of its' virtual disks.' A table lists available datastores:

Name	Capacity	Free	Type	Thin pro...	Access
datastore1	592.5 GB	591.09...	VMFS6	Supported	Single

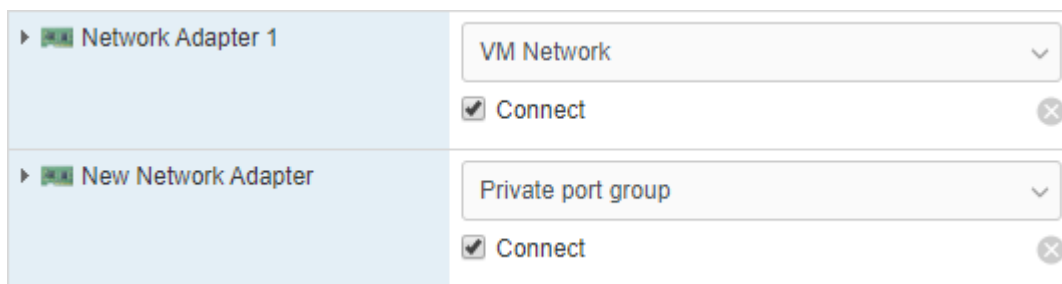
At the bottom right, there are buttons for 'Back', 'Next' (with a mouse cursor), 'Finish', and 'Cancel'.

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. 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" (стр. 5)).

# 5 Развертывание продукта Кибер Инфраструктура на виртуальных машинах

После запуска виртуальной машины зайдите на нее через серийную консоль в панели управления. Укажите имя пользователя console-user и пароль cyberprotect. Для доступа по SSH узнайте пароль пользователя cloud-user из файла /.cloud-user-password.

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

## 5.1 Развертывание сервера управления

### *Чтобы настроить сервер управления*

Запустите автоматическое создание кластера:

```
$ sudo bash /usr/libexec/init-cluster
```

Пароль от панели администратора будет доступен в файле /.initial-admin-password.

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" (стр. 17).

## 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. Инициализируйте сетевые интерфейсы:

```
$ sudo bash /usr/libexec/init-ifaces
```

2. Получите токен и адрес сервера управления на панели администрирования.

- a. Войдите на панель администрирования по ее IP-адресу и порту 8888.  
При необходимости 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.

3. Зарегистрируйте сервер в панели администрирования:

```
$ sudo bash /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, а <token> – токен, полученный на панели администрирования.

Дополнительные сведения см. в разделе "Повторное добавление неназначенных серверов" в руководстве администратора.

***Чтобы добавить подчиненный сервер 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 приступить к настройке продукта Кибер Инфраструктура для нужного сценария. Инструкции по выполнению различных задач настройки приведены в руководстве администратора.

## 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.
- 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

разделе «Настройка новых дисков вручную» в руководстве администратора.

## Assign role ✕

Select the role to assign to the disk "sdc"

- Storage**  
Use the disk to store data.
- Cache**  
Use the disk to store write cache. This disk does not add capacity to the cluster but improves its performance.
- Metadata**  
Use the disk to store cluster metadata.
- Metadata + Cache**  
Use the disk to store both cluster metadata and write cache.

Storage tier  
Tier 0 ▼

Caching and checksumming  
Enable checksumming ▼

Cancel Assign



## 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, 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.

## 7.1 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**.

The screenshot shows a configuration interface for backup storage. It features three dropdown menus in a light blue background. The first dropdown is labeled 'Tier' and is set to 'Tier 0'. The second dropdown is labeled 'Failure domain' and is set to 'Host'. Below these is a section titled 'Redundancy' with a dropdown menu set to 'Encoding 1+2, 200%'. Each dropdown has a blue downward-pointing arrow on the right side.

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.

Domain name (not IP address)  
backupstorage.example.com

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

```
$TTL 1h

@   IN   SOA  ns1.myhoster.com. root.backupstorage.example.com. (
      2021011213   ; serial
      1h           ; refresh
      30m          ; retry
      7d           ; expiration
```

 **Copy to clipboard**

#### 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**.

## 7.2 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.

---

NFS share hostname or IP address  
10.16.136.140

Export name  
/share1

NFS version

NFSv4 (recommended)

NFSv3

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.
-

Domain name (not IP address)  
backupstorage.example.com

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

```
$TTL 1h

@ IN SOA ns1.myhoster.com. root.backupstorage.example.com. (
    2021011213 ; serial
    1h ; refresh
    30m ; retry
    7d ; expiration
```

 [Copy to clipboard](#)

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:

- Yandex Object Storage
- VK Cloud Storage
- SberCloud OBS
- CloudMTS S3 Object Storage
- Amazon S3
- IBM Cloud
- Alibaba Cloud
- I1J
- 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**.



- с. При использовании **объектного хранилища Swift** укажите версию протокола аутентификации и необходимые для него атрибуты.
- д. Укажите учетные данные пользователя. При использовании **Google Cloud** выберите файл JSON с ключами для загрузки.
- е. 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.
- ф. 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**.
- г. Нажмите кнопку **Далее**.

Object storage type  
Amazon S3

Region  
US East (Ohio)

Bucket  
bucket1

Access key ID  
AKIAIOSFODNN7EXAMPLE

Secret key ID  
.....

Allow using a self-signed certificate of the endpoint (not recommended)

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**.

Tier  
Tier 0

Failure domain  
Host

### Redundancy

Encoding 1+2, 200%

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.

Domain name (not IP address)  
backupstorage.example.com

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

```
$TTL 1h
@ IN SOA ns1.myhoster.com. root.backupstorage.example.com. (
  2021011213 ; serial
  1h ; refresh
  30m ; retry
  7d ; expiration
```

 Copy to clipboard

---

### 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**.