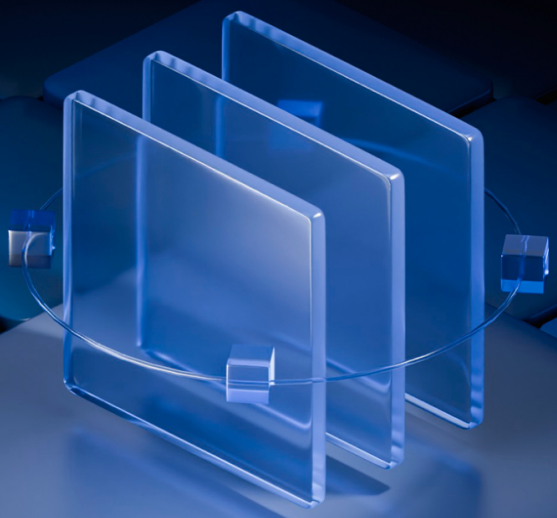
КИБЕРПРОТЕКТ

КИБЕР Хранилище

Версия 6.5



Руководство пользователя хранилища

Редакция: 11.09.2026

© ООО «Киберпротект», 2026

ООО «Киберпротект» является правообладателем данного документа.

Все права защищены.

Распространение измененных версий данного руководства, а также переработанных материалов, входящих в данное руководство, запрещено без явного разрешения владельца авторских прав.

ДОКУМЕНТ ПРЕДОСТАВЛЯЕТСЯ «КАК ЕСТЬ». ДОКУМЕНТ НЕ ПРЕДПОЛАГАЕТ ОБЯЗАТЕЛЬСТВ И/ИЛИ ГАРАНТИЙ ПРАВООБЛАДАТЕЛЯ ОТНОСИТЕЛЬНО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, НАСКОЛЬКО ТАКОЕ ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ ДОПУСКАЕТСЯ ЗАКОНОМ, ВКЛЮЧАЯ, СРЕДИ ПРОЧЕГО, ГАРАНТИИ КОММЕРЧЕСКОЙ ЦЕННОСТИ, УДОВЛЕТВОРИТЕЛЬНОГО КАЧЕСТВА, ПРИГОДНОСТИ ДЛЯ КОНКРЕТНОЙ ЦЕЛИ.

Оглавление

Поддерживаемые типы хранилищ **1**

Доступ к корзинам S3 . . . . . **2**

Доступ к хранилищу S3 с помощью CyberDuck 2

Управление версиями корзин S3 3

Подключение хранилища S3 с помощью Mountain Duck 4

Создание корзин S3 в подключенном хранилище S3 6

Политики именования корзин и ключей S3 6

Доступ к целевым устройствам iSCSI **7**

Доступ к целевым устройствам iSCSI из VMware ESXi 7

Доступ к целевым устройствам iSCSI из Linux 9

Доступ к целевым устройствам iSCSI из Microsoft Hyper-V 11

Доступ к томам NFS **19**

Подключение экспортов NFS в Linux 19

Подключение экспортов NFS в macOS 19

Поддерживаемые типы хранилищ

Поставщик услуг может настроить продукт Кибер Хранилище для хранения ваших данных в трех типах хранилищ:

- Хранилище объектов S3 для хранения неограниченного количества объектов (файлов).
- Блочное хранилище iSCSI для виртуализации, баз данных и других потребностей.
- Тома NFS для хранения неограниченного количества файлов посредством распределенной файловой системы.

В следующих разделах подробно описаны способы доступа к данным в продукте Кибер Хранилище.

Доступ к корзинам S3

Для доступа к корзинам S3 получите следующие сведения (учетные данные) от системного администратора:

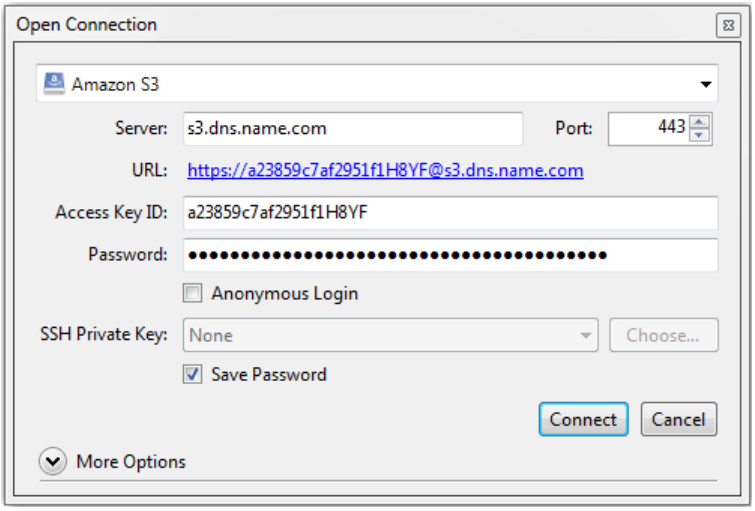
- DNS-имя оконечной точки S3,
- идентификатор ключа доступа,
- секретный ключ доступа.

Продукт Кибер Хранилище позволяет получать доступ к данным S3 через стороннее приложение S3, например Cyberduck, Mountain Duck и т. п.

Доступ к хранилищу S3 с помощью CyberDuck

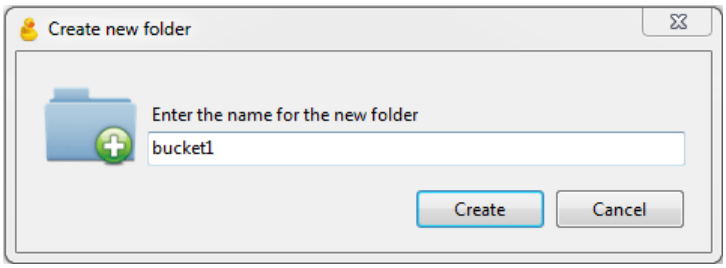
Чтобы получить доступ к продукту Кибер Хранилище с помощью CyberDuck, выполните следующие действия.

1. В CyberDuck нажмите **Открыть подключение**.
2. Укажите учетные данные.
   - Доменное имя оконечной точки S3.
   - **Идентификатор ключа доступа** и **Пароль**, секретный ключ доступа пользователя хранилища объектов.



   По умолчанию подключение устанавливается через протокол HTTPS. Чтобы использовать CyberDuck поверх HTTP, необходимо установить специальный профиль S3.

3. После того как подключение будет установлено, выберите **Файл** → **Создать папку**, чтобы создать корзину.



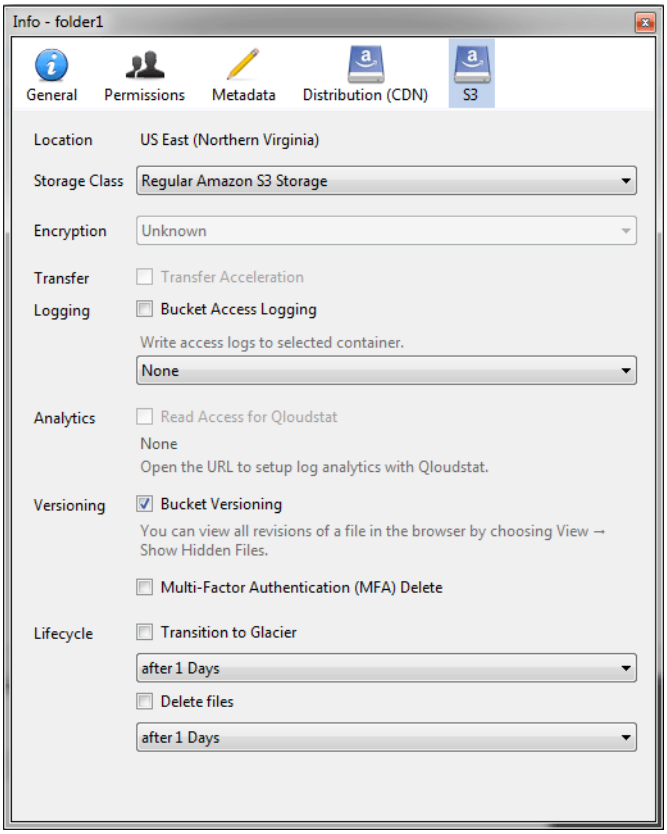
4. Укажите имя для новой корзины, а затем нажмите **Создать**. Используйте имена корзин, соответствующие соглашениям об именовании DNS. Дополнительные сведения об именовании корзин см. в разделе *Политики именования корзин и ключей S3*.

Новая корзина появится в CyberDuck. Вы можете управлять ею и ее содержимым.

Управление версиями корзин S3

Управление версиями позволяет поддерживать несколько вариантов одного объекта в одной и той же корзине. С его помощью можно хранить, извлекать и восстанавливать любую версию любого объекта, хранящегося в вашей корзине S3. С управлением версиями можно легко восстанавливать систему после как непреднамеренных действий пользователей, так и сбоев приложений. Дополнительные сведения об управлении версиями корзин см. в документации Amazon.

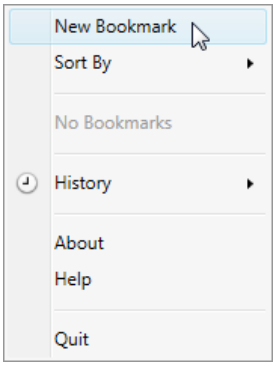
Управление версиями корзин по умолчанию отключено. В CyberDuck его можно включить в свойствах корзины, например:



Подключение хранилища S3 с помощью Mountain Duck

Mountain Duck позволяет подключить хранилище S3 продукта Кибер Хранилище и обращаться к нему как к обычному диску. Выполните следующие действия.

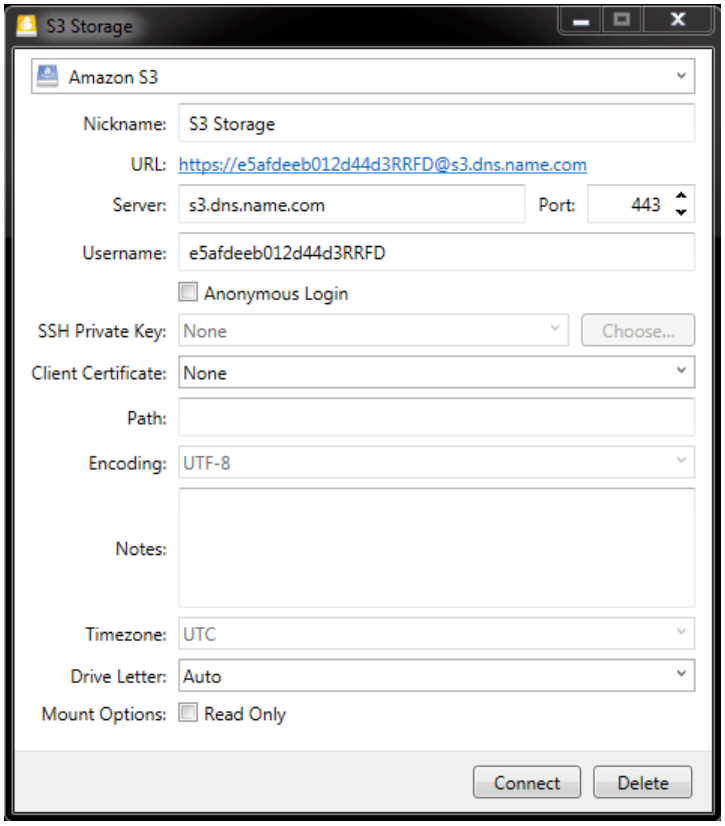
1. Если поставщик услуг предоставил вам SSL-сертификат, установите его.
2. В приложении Mountain Duck нажмите **Создать закладку**.



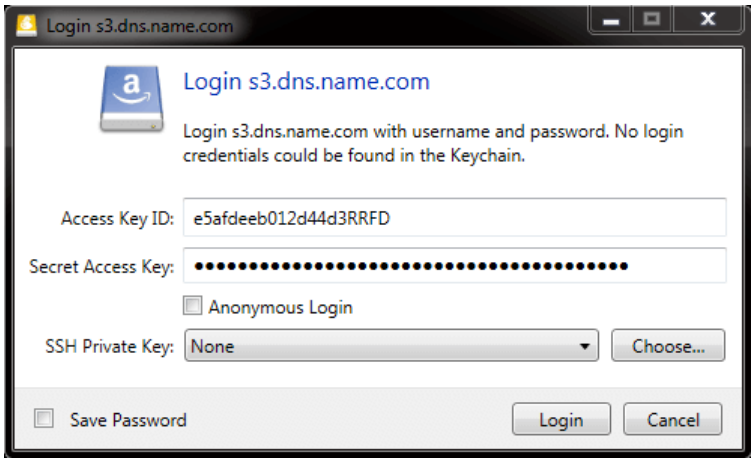
3. В окне свойств выберите профиль **Amazon S3** из первого раскрывающегося списка и укажите следующие параметры:
   - имя диска в поле **Псевдоним**,

- DNS-имя оконечной точки в поле **Сервер**,
- идентификатор ключа доступа в поле **Имя пользователя**.

Нажмите **Подключить**.



4. В окне входа укажите **Секретный ключ доступа** и нажмите **Войти**.



Mountain Duck подключит хранилище S3 в виде диска. На диске вы сможете управлять корзинами и сохранять в них файлы.

Создание корзин S3 в подключенном хранилище S3

Операционные системы Windows и macOS, поддерживаемые приложением Mountain Duck, интерпретируют корзины как папки в случае подключения хранилища S3 как диска. В обеих операционных системах имя новой папки по умолчанию содержит пробелы. Это нарушает соглашения об именовании корзин (см. раздел *Политики именования корзин и ключей S3*), поэтому нельзя создать новую корзину непосредственно в подключенном хранилище S3. Чтобы создать корзину в подключенном хранилище S3, создайте папку с именем, соответствующим соглашениям об именовании DNS, в любом другом месте и скопируйте ее в корневой каталог подключенного хранилища S3.

Политики именования корзин и ключей S3

Рекомендуется использовать имена корзин, соответствующие соглашениям об именовании DNS:

- длиной от 3 до 63 символов;
- должны начинаться и заканчиваться буквой нижнего регистра или цифрой;
- могут содержать буквы нижнего регистра, цифры, точки (.), дефисы (-) и символы подчеркивания (_);
- могут представлять собой ряд допустимых частей имен (описанных ранее), разделенных точками.

Ключ объекта может быть строкой из любых символов в кодировке UTF-8 длиной до 1024 байт.

Доступ к целевым устройствам iSCSI

В этом разделе описаны способы подключения целевых устройств iSCSI к операционным системам и сторонним решениям управления виртуализацией, которые поддерживают явный режим ALUA.

Доступ к целевым устройствам iSCSI из VMware ESXi

Перед использованием томов продукта Кибер Хранилище с VMware ESXi необходимо настроить продукт для надлежащей работы с активными/пассивными массивами хранения данных ALUA. Рекомендуется переключиться на политику выбора пути `VMW_PSP_RR` для избежания проблем. Например, в VMware ESXi 6.5:

- Чтобы задать PSP по умолчанию для всех устройств, выполните:

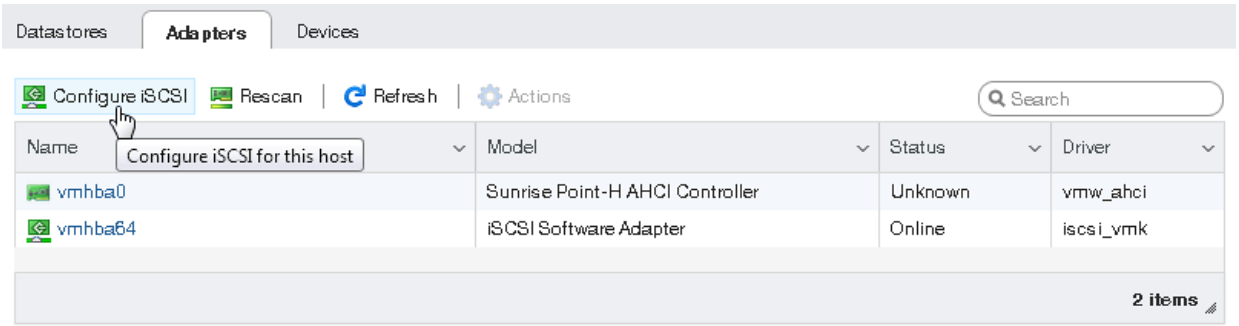
```
# esxcli storage nmp satp rule add --satp VMW_SATP_ALUA --vendor VSTORAGE \
--model VSTOR-DISK --psp VMW_PSP_RR -c tpgs_on
```

- Чтобы задать PSP для определенного устройства, выполните:

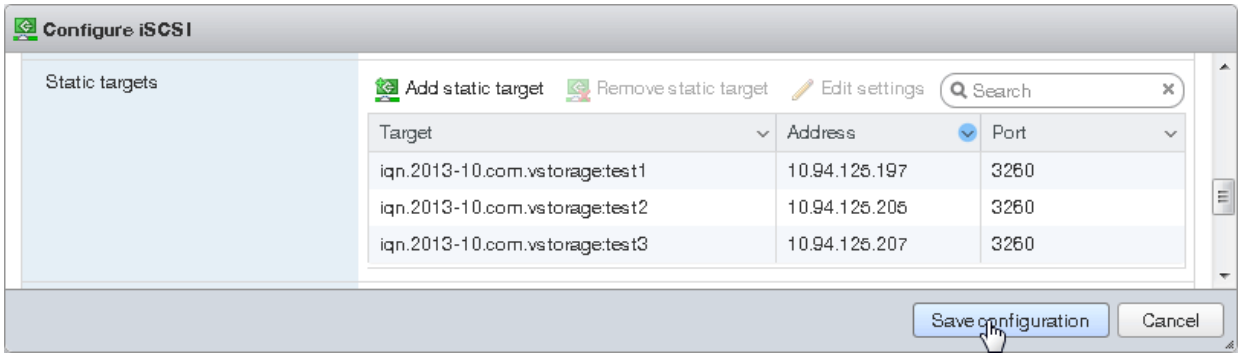
```
# esxcli storage core claimrule load
```

Теперь можно перейти к созданию хранилищ данных из томов продукта Кибер Хранилище, экспортированных через iSCSI. Выполните вход на веб-панель VMware ESXi, а затем выполните следующие действия.

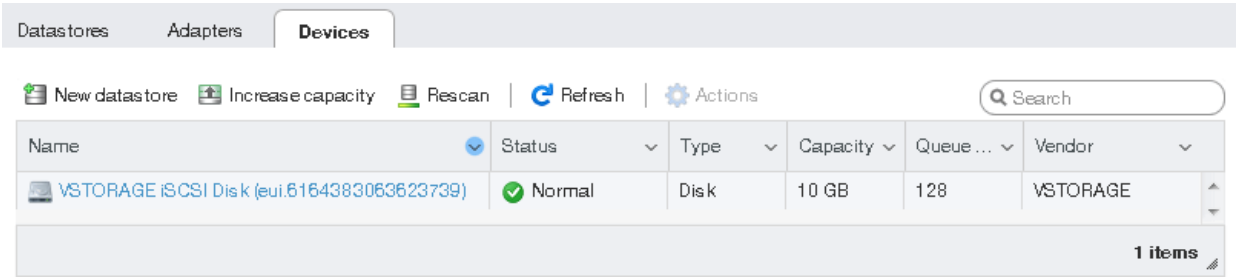
1. В Navigator перейдите на вкладку **Хранилище** → **Адаптеры** и нажмите **Настроить iSCSI**.



2. В окне **Настройка iSCSI** щелкните **Добавить статическое целевое устройство** В разделе **Статические целевые устройства**, укажите IQN для целевых устройств, IP-адреса и порты. Нажмите **Сохранить конфигурацию**.



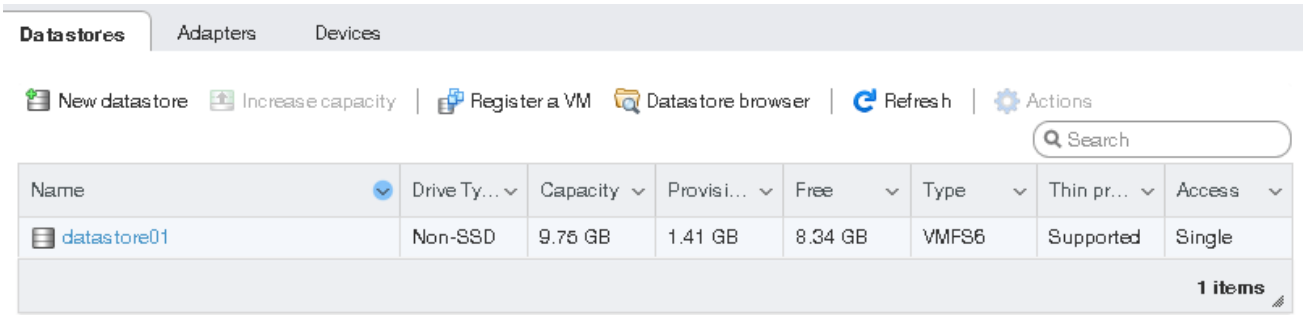
3. Перейдите на вкладку **Устройства** и нажмите **Обновить**. В списке устройств появится только что добавленный диск.



4. Выберите диск и нажмите **Создать хранилище данных**. В открывшемся мастере введите имя для хранилища данных и выберите параметры создания разделов. Нажмите **Завершить**, чтобы фактически разбить диск на разделы.

> **Предупреждение**
>
> При разбивке диска на разделы все данные с него будут удалены.

В списке хранилищ данных появится готовый к использованию диск. Теперь можно просматривать его содержимое с помощью обозревателя хранилища данных и выделить его ресурсы для виртуальных машин.



> **Примечание**

Если узел ESXi потеряет связь с хранилищами данных VMFS3 или VMFS5, следуйте инструкциям в статье базы знаний #2113956.

Доступ к целевым устройствам iSCSI из Linux

Чтобы подключить iSCSI-инициатор на основе Linux к целевым устройствам iSCSI продукта Кибер Хранилище, работающим в режиме ALUA, выполните следующие действия.

1. Убедитесь, что установлены необходимые пакеты.

   - В системах на базе RPM (CentOS и др.) выполните:

```
# yum install iscsi-initiator-utils device-mapper-multipath
```

   - В системах на базе DEB (Debian и Ubuntu) выполните:

```
# apt-get install open-iscsi multipath-tools
```

2. Создайте и измените файл конфигурации `/etc/multipath.conf` следующим образом.

```
<...>
devices {
  device {
    vendor ”VSTORAGE”
    product ”VSTOR-DISK”
    features ”2 pg_init_retries 50”
    hardware_handler ”1 alua”
    path_grouping_policy group_by_node_name
    path_selector ”round-robin 0”
    no_path_retry queue
    user_friendly_names no
    flush_on_last_del yes
    failback followover
    path_checker tur
    detect_prio no
    prio alua
  }
}
<...>
```

3. Загрузите модуль ядра и запустите сервис множественных путей.

```
# modprobe dm-multipath
# systemctl start multipathd; systemctl enable multipathd
```

4. При необходимости включите параметры CHAP `node.session.auth.*` и `discovery.sendtargets.auth.*` в `/etc/iscsi/iscsid.conf`.

5. Запустите сервисы iSCSI.

```
# systemctl start iscsi iscsid
# systemctl enable iscsi iscsid
```

6. Выполните обнаружение всех целевых устройств по их IP-адресам, например:

```
# iscsiadm -m discovery -t st -p 10.94.91.49 10.94.91.49 3260,1 \
iqn.2014-06.com.vstorage:target1
# iscsiadm -m discovery -t st -p 10.94.91.54 10.94.91.54:3260,1 \
iqn.2014-06.com.vstorage:target2
# iscsiadm -m discovery -t st -p 10.94.91.55 10.94.91.55:3260,1 \
iqn.2014-06.com.vstorage:target3
```

7. Выполните вход на обнаруженные целевые устройства, например:

```
# iscsiadm -m node -T iqn.2014-06.com.vstorage:target1 -l
# iscsiadm -m node -T iqn.2014-06.com.vstorage:target2 -l
# iscsiadm -m node -T iqn.2014-06.com.vstorage:target3 -l
```

8. Определите идентификатор устройства Multipath, например:

```
# multipath -ll
360000000000000000000b50326ea44e3 dm-10 VSTORAGE,VSTOR-DISK
size=200G features='2 pg_init_retries 50' hwhandler='1 alua' wp=rw
|-+- policy='round-robin 0' prio=50 status=active
| `- 6:0:0:1 sdf 8:80  active ready running
|-+- policy='round-robin 0' prio=1 status=enabled
| `- 8:0:0:1 sdj 8:144 active ghost running
`-+- policy='round-robin 0' prio=1 status=enabled
  `- 7:0:0:1 sdh 8:112 active ghost running
# fdisk -l | grep 360000000000000000000b50326ea44e3
Disk /dev/mapper/360000000000000000000b50326ea44e3: 10.7 GB, \
10737418240 bytes, 20971520 sectors
```

Также идентификатор устройства Multipath можно получить путем добавления

`36000000000000000000` к последним шести байтам идентификатора тома. В приведенном выше примере `360000000000000000000b50326ea44e3` — идентификатор устройства Multipath, сопоставленный из идентификатора тома `61c9d567-4666-4c16-8030-b50326ea44e3`.

Теперь можно создать разделы на устройстве iSCSI (`/dev/mapper/360000000000000000000b50326ea44e3` в данном примере), а также отформатировать и подключить его к серверу инициатора с помощью стандартных средств Linux.

Когда вам больше не требуется внешнее устройство iSCSI, его можно удалить из сервера инициатора следующим образом.

1. Убедитесь, что устройство iSCSI не используется.
2. Отключите множественные пути к устройству, например:

```
# multipath -f /dev/mapper/360000000000000000000b50326ea44e3
```

3. Выполните выход с целевых устройств iSCSI, например:

```
# iscsiadm -m node -T iqn.2014-06.com.vstorage:target1 -p 10.94.91.49:3260 -u
# iscsiadm -m node -T iqn.2014-06.com.vstorage:target2 -p 10.94.91.54:3260 -u
# iscsiadm -m node -T iqn.2014-06.com.vstorage:target3 -p 10.94.91.55:3260 -u
```

4. Удалите целевые устройства iSCSI, например:

```
# iscsiadm -m node -o delete -T iqn.2014-06.com.vstorage:target1 \
-p 10.94.91.49:3260
# iscsiadm -m node -o delete -T iqn.2014-06.com.vstorage:target2 \
-p 10.94.91.54:3260
# iscsiadm -m node -o delete -T iqn.2014-06.com.vstorage:target3 \
-p 10.94.91.55:3260
```

Доступ к целевым устройствам iSCSI из Microsoft Hyper-V

Перед подключением iSCSI-инициатора Microsoft Hyper-V к целевым устройствам iSCSI, работающим в режиме ALUA, необходимо установить и настроить компонент Multipath I/O (MPIO). Этот компонент можно использовать, начиная с Windows Server 2008 R2. Чтобы подключить инициатор, например, на сервере Microsoft Hyper-V Server 2016, выполните следующие действия.

1. Запустите Windows PowerShell с правами администратора и установите MPIO.

```
> Enable-WindowsOptionalFeature -Online -FeatureName MultiPathIO
```

Сервер автоматически перезагрузится, чтобы завершить установку.

2. В консоли Windows PowerShell настройте MPIO следующим образом.

    1. Включите поддержку дисков iSCSI.

    ```
    > Enable-MSDSMAutomaticClaim -BusType iSCSI
    ```

    2. Установите политику переключения при сбое ”Только переключение при сбое”. В этой политике используется единый активный путь для передачи всего ввода-вывода, а все остальные пути являются резервными. Если по активному пути произойдет сбой, будет использоваться один из резервных путей. После восстановления пути он снова станет активным.

    ```
    > Set-MSDSMGlobalDefaultLoadBalancePolicy -Policy FOO
    ```

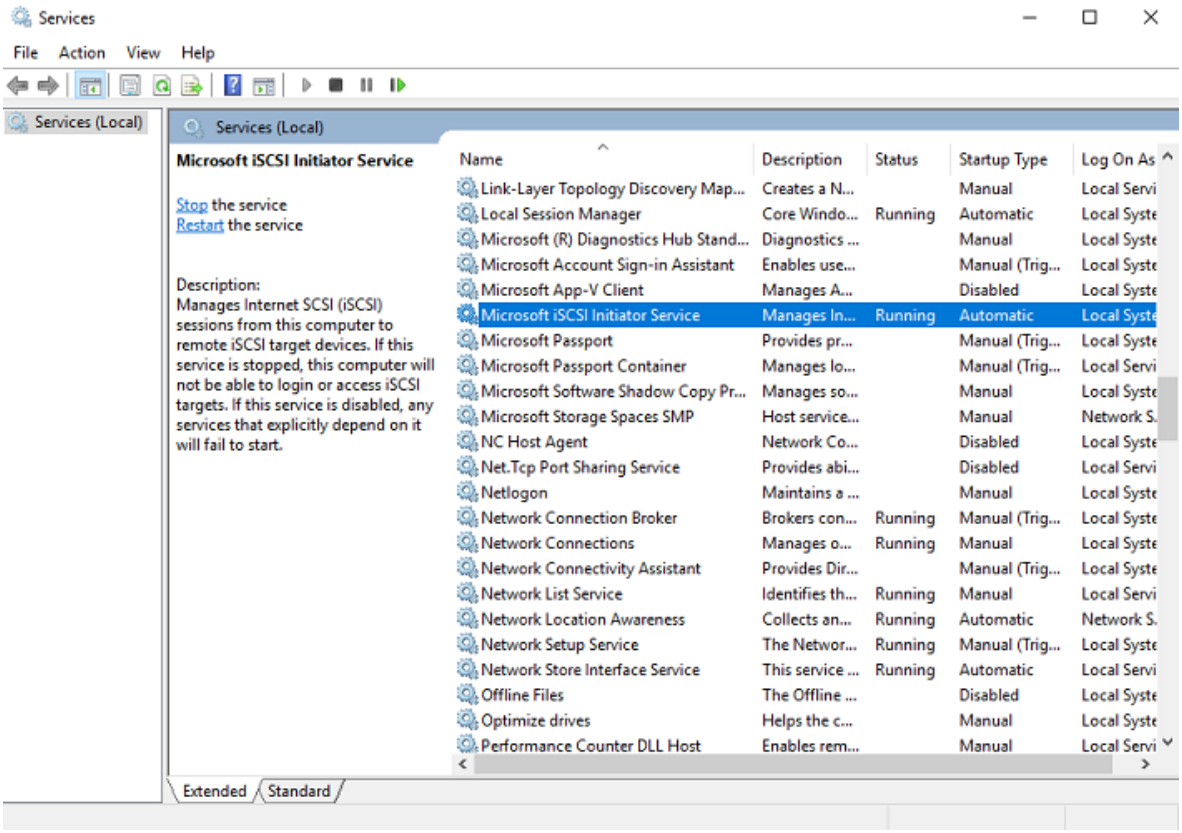
    3. Включите верификацию пути. По умолчанию инициатор будет верифицировать каждый путь каждые 30 секунд.

    ```
    > Set-MPIOSetting -NewPathVerificationState Enabled
    ```

    4. Перезагрузите сервер.

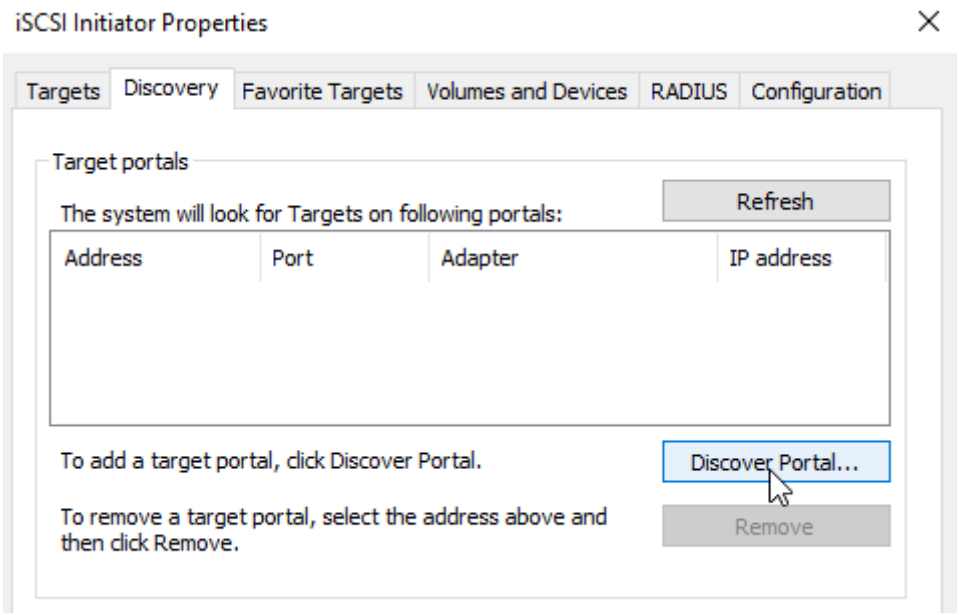
3. Подключите целевые устройства к инициатору iSCSI следующим образом.

    1. В окне **Панель управления → Система и безопасность → Администрирование → Сервисы** убедитесь, что **Сервис инициатора Майкрософт iSCSI** работает и для него установлен тип запуска **Автоматически**.

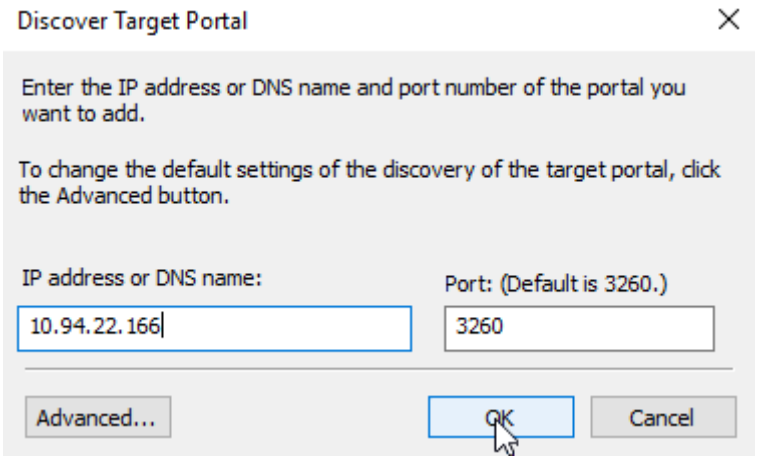


2. Запустите **Инициатор iSCSI**.

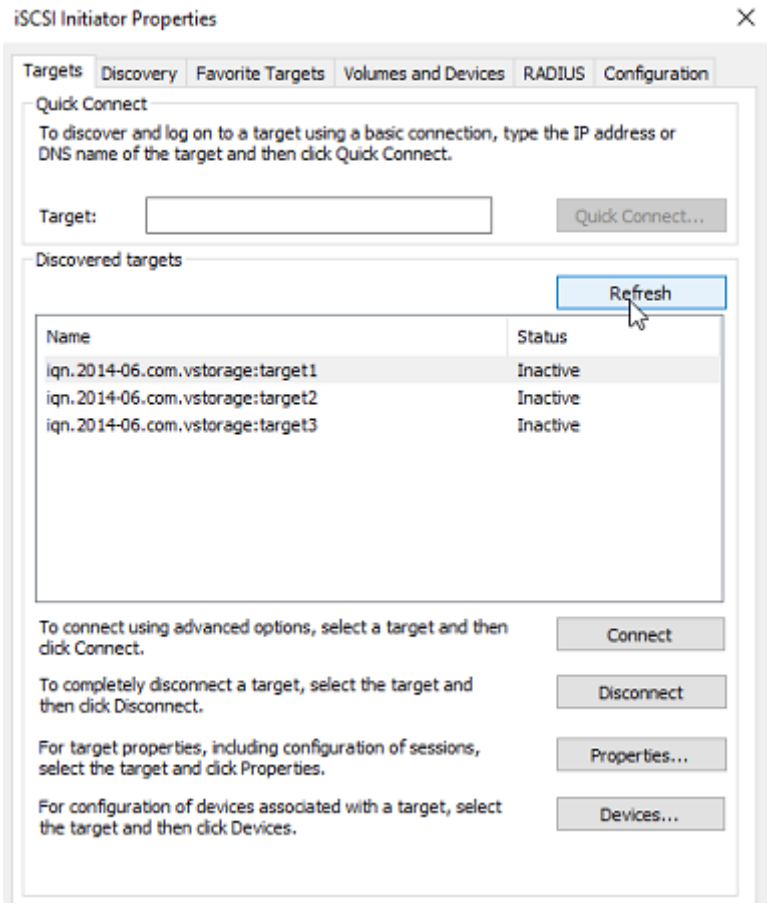
3. В окне **Свойства инициатора iSCSI** откройте вкладку **Обнаружение** и нажмите **Обнаружить портал**.



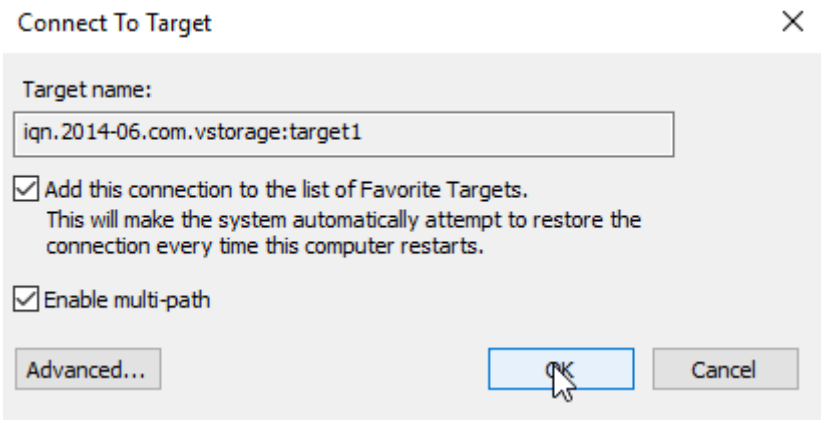
4. В окне **Обнаружение целевого портала** введите целевой IP-адрес и нажмите кнопку **ОК**. Повторите этот шаг для каждого целевого устройства из целевой группы.



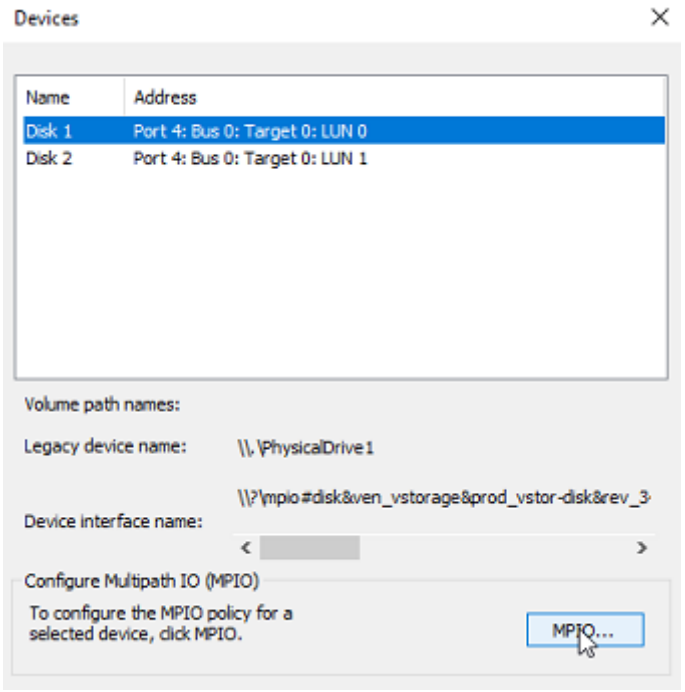
5. На вкладке **Целевые устройства** нажмите **Обновить**, чтобы обнаружить добавленные целевые устройства.



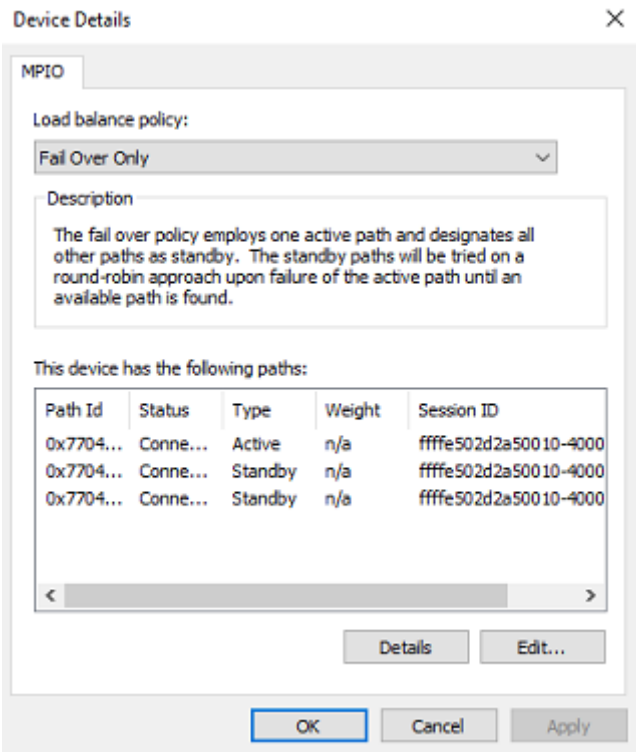
6. Нажмите **Подключить** для каждого целевого устройства, чтобы подключить его к инициатору. В окне **Подключение к целевому устройству** установите флажок **Включить множественный путь** и нажмите кнопку **ОК**.



7. На вкладке **Целевые устройства** нажмите **Устройства...**, выберите подключенный LUN и нажмите **MPIO...**

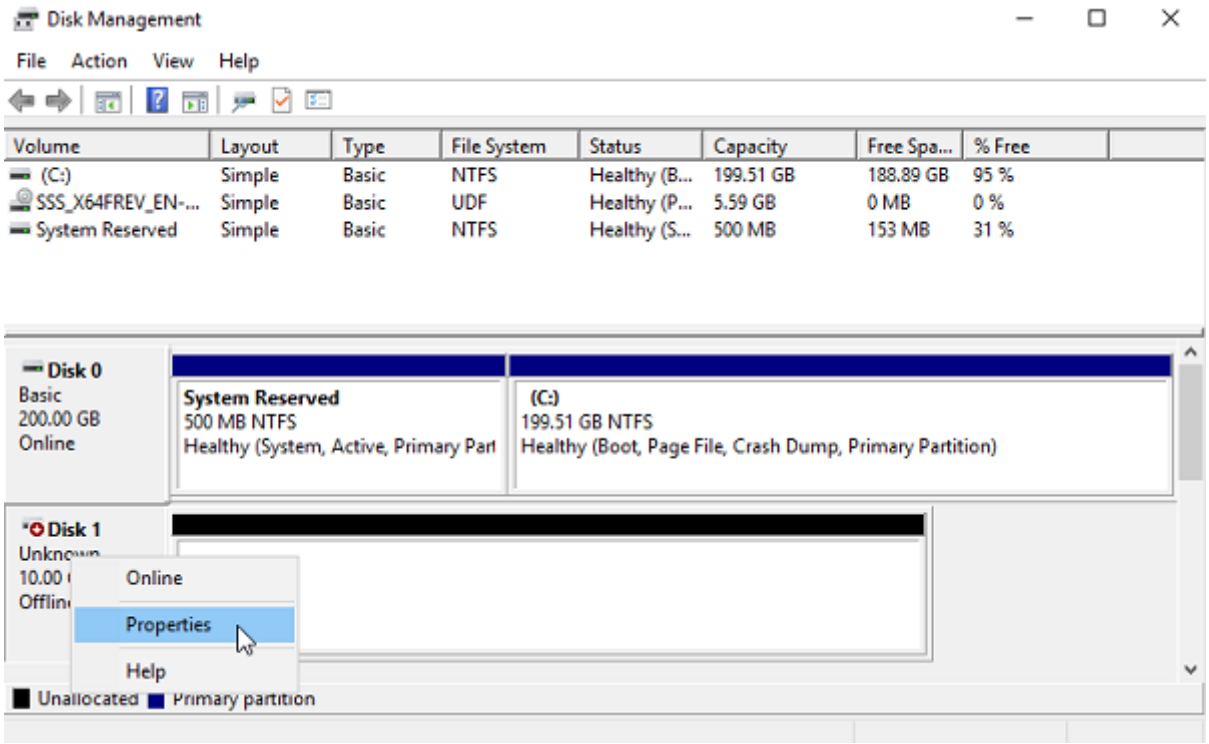


8. Убедитесь, что подключенный LUN имеет несколько путей.



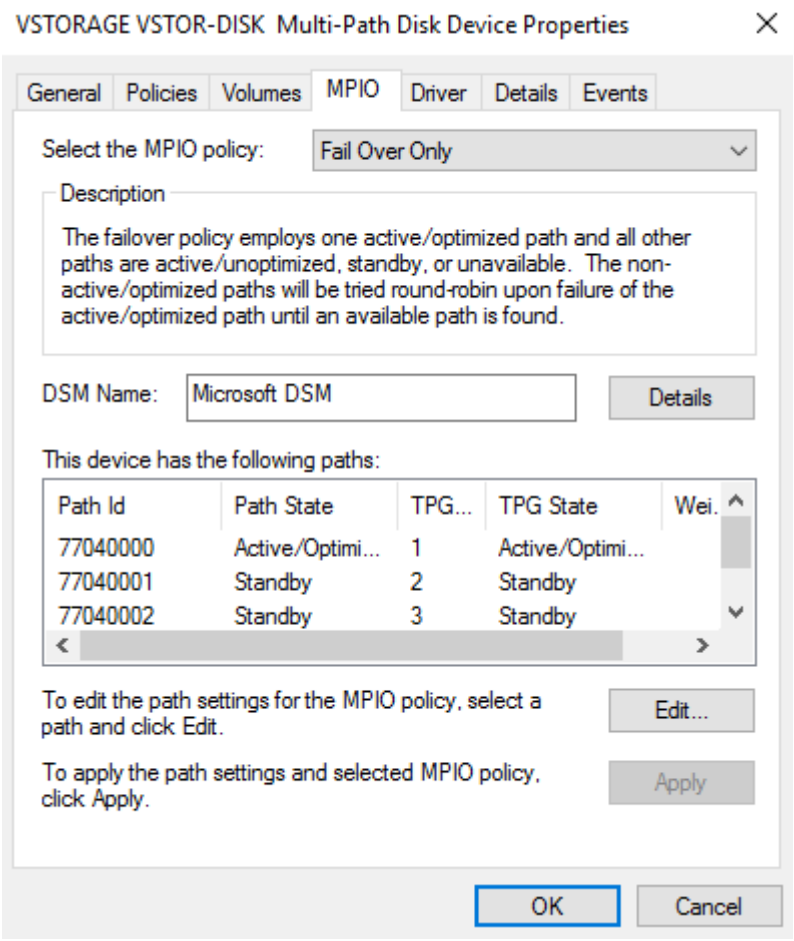
Теперь можно инициализировать только что добавленный диск для использования в Microsoft Hyper-V. Выполните следующие действия.

1. Откройте **Управление дисками**, щелкните правой кнопкой мыши по добавленному диску и выберите **Свойства** из раскрывающегося меню.

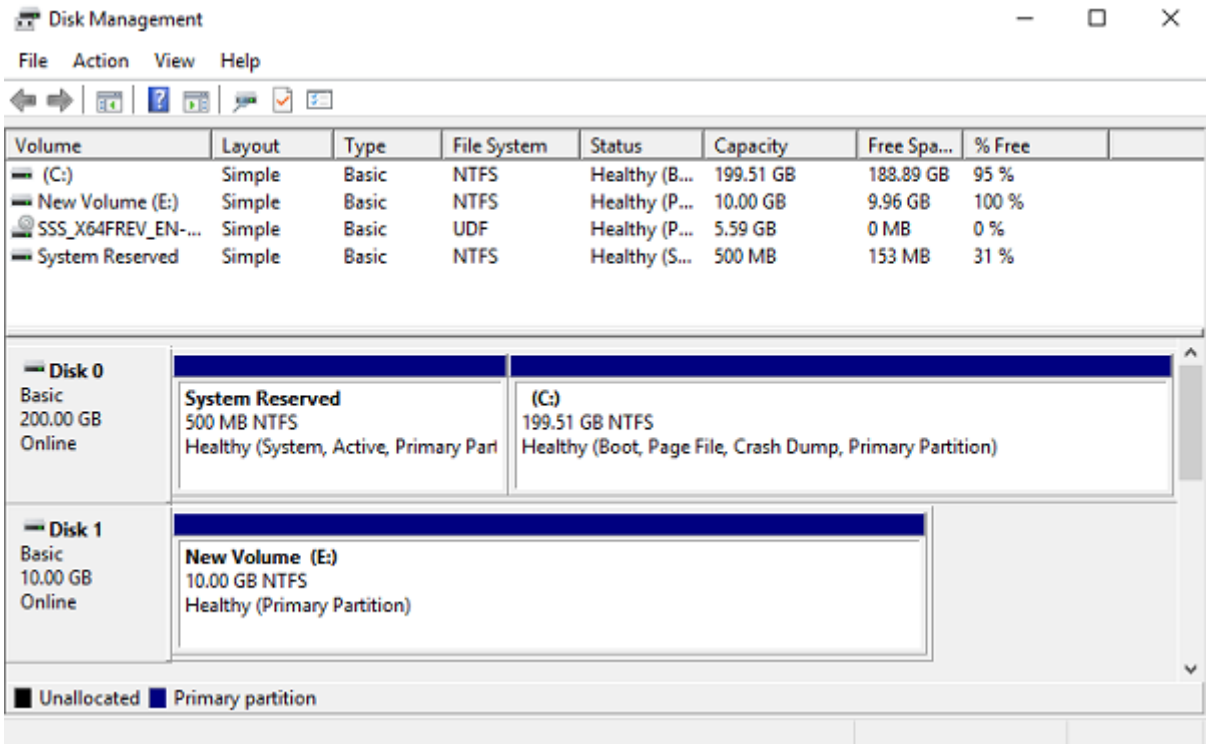


2. Проверьте настройки на вкладке **MPIO**. Первое подключенное целевое устройство становится

активным/оптимизированным и предпочтительным путем.



3. Разделите и отформатируйте диск обычным образом.


Disk Management
File Action View Help
Volume Layout Type File System Status Capacity Free Spa... % Free
(C:) Simple Basic NTFS Healthy (B... 199.51 GB 188.89 GB 95 %
New Volume (E:) Simple Basic NTFS Healthy (P... 10.00 GB 9.96 GB 100 %
SSS_X64FREV_EN-... Simple Basic UDF Healthy (P... 5.59 GB 0 MB 0 %
System Reserved Simple Basic NTFS Healthy (S... 500 MB 153 MB 31 %
Disk 0
Basic
200.00 GB
Online
System Reserved
500 MB NTFS
Healthy (System, Active, Primary Part
(C:)
199.51 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)
Disk 1
Basic
10.00 GB
Online
New Volume (E:)
10.00 GB NTFS
Healthy (Primary Partition)
Unallocated
Primary partition

Доступ к томам NFS

В этом разделе описаны способы подключения томов NFS продукта Кибер Хранилище в Linux и macOS.

> **Примечание**
>
> В настоящее время Кибер Хранилище не поддерживает встроенный NFS-клиент Windows.

Подключение экспортов NFS в Linux

Экспорт NFS, созданный в продукте Кибер Хранилище, можно подключить подобно любому другому каталогу, экспортированному через NFS. Вам понадобится IP-адрес (или имя хоста) тома NFS и идентификатор тома.

В консоли выполните следующие команды:

```
# mkdir /mnt/nfs
# mount -t nfs -o vers=4.0 <share_IP>:/<share_name>/ /mnt/nfs
```

где:

- `-o vers=4.0` — версия NFS, которая будет использоваться.

  Кибер Хранилище поддерживает версии NFS 4.0 и 4.1.

- `<share_IP>` — IP-адрес тома NFS. Также можно использовать имя хоста тома NFS.
- `/<share_name>/` — путь корневого экспорта, например `share1`. Для пользовательских экспортов укажите их полный путь, например `/<share_name>/export1`.
- `/mnt/nfs` — существующий локальный каталог, к которому будет подключен экспорт.

Подключение экспортов NFS в macOS

Экспорт NFS, созданный в продукте Кибер Хранилище, можно подключить подобно любому другому каталогу, экспортированному через NFS. Вам понадобится IP-адрес (или имя хоста) тома NFS и идентификатор тома.

Можно использовать командную строку или Finder.

- В консоли выполните следующие команды:

```
# mkdir /mnt/nfs
# mount -t nfs -o vers=4.0 <share_IP>:/<share_name>/ /mnt/nfs
```

где:

- `-o vers=4.0` — версия NFS, которая будет использоваться.

  Кибер Хранилище поддерживает версии NFS 4.0 и 4.1.

- `<share_IP>` — IP-адрес тома NFS. Также можно использовать имя хоста тома NFS.
- `/<share_name>/` — путь корневого экспорта, например `share1`. Для пользовательских экспортов укажите их полный путь, например `/<share_name>/export1`.
- `/mnt/nfs` — существующий локальный каталог, к которому будет подключен экспорт.

- В Finder выполните следующие действия.

  1. Задайте версию NFS 4.0. Для этого добавьте строку `nfs.client.mount.options = vers=4.0` в файл `/etc/nfs.conf`.
  2. В окне **Finder** → **Перейти** → **Подключение к серверу** укажите `nfs://192.168.0.51:/<share_name>/`

     где:

     - `192.168.0.51` — IP-адрес тома NFS, также можно использовать имя хоста тома NFS;
     - `/<share_name>/` — корневой путь экспорта. Для пользовательских экспортов укажите их полный путь, например `/<share_name>/export1`.

  3. Нажмите **Подключить**.

  Приложение Finder подключит экспорт к папке `/Volumes/<share_name>/`.