

КИБЕРПРОТЕКТ



КИБЕР

Инфраструктура

Версия 5.5

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

1	Поддерживаемые типы хранилищ	4
2	Доступ к корзинам S3	5
2.1	Управление корзинами с помощью пользовательской панели Кибер Инфраструктура	5
2.1.1	Вход на пользовательскую панель	5
2.1.2	Добавление, удаление и перечисление корзин S3	6
2.1.3	Создание, удаление и перечисление папок	7
2.1.4	Загрузка и скачивание файлов	8
2.2	Доступ к хранилищу S3 с помощью CyberDuck	8
2.2.1	Управление версиями корзин S3	9
2.3	Подключение хранилища S3 с помощью Mountain Duck	10
2.3.1	Создание корзин S3 в подключенном хранилище S3	12
2.4	Политики именования корзин и ключей S3	12
3	Доступ к целевым устройствам iSCSI	13
3.1	Доступ к целевым устройствам iSCSI из VMware ESXi	13
3.2	Доступ к целевым устройствам iSCSI из Linux	14
3.3	Доступ к целевым устройствам iSCSI из Microsoft Hyper-V	17
4	Доступ к томам NFS	23
4.1	Подключение экспортов NFS в Linux	23
4.2	Подключение экспортов NFS в macOS	23

1 Поддерживаемые типы хранилищ

Поставщик услуг может настроить Кибер Инфраструктура 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 Кибер Инфраструктура.

2 Доступ к корзинам S3

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

- IP-адрес пользовательской панели
- DNS-имя конечной точки S3
- Идентификатор ключа доступа
- Секретный ключ доступа

Кибер Инфраструктура позволяет получать доступ к данным S3 несколькими способами:

- Через пользовательскую панель Кибер Инфраструктура
- Через стороннее приложение S3, например Cyberduck, Mountain Duck и т. п.

2.1 Управление корзинами с помощью пользовательской панели Кибер Инфраструктура

В этом разделе описано, как управлять корзинами и их содержимым с пользовательской панели Кибер Инфраструктура.

2.1.1 Вход на пользовательскую панель

Для входа на пользовательскую панель Кибер Инфраструктура выполните следующие действия.

1. На любом компьютере с доступом к веб-интерфейсу откройте в веб-браузере `http://<IP_адрес_панели_пользователя>:8888/s3/`.

Примечание

Если вы используете самоподписанный сертификат, добавьте его в исключения браузера.

Log in

ENDPOINT

s3.example.com

Use secure transfer (SSL)

ACCESS KEY ID

d9fde6a530879f59HB8U

SECRET ACCESS KEY

.....

LOG IN

2. На экране входа введите учетные данные и нажмите **Войти**.

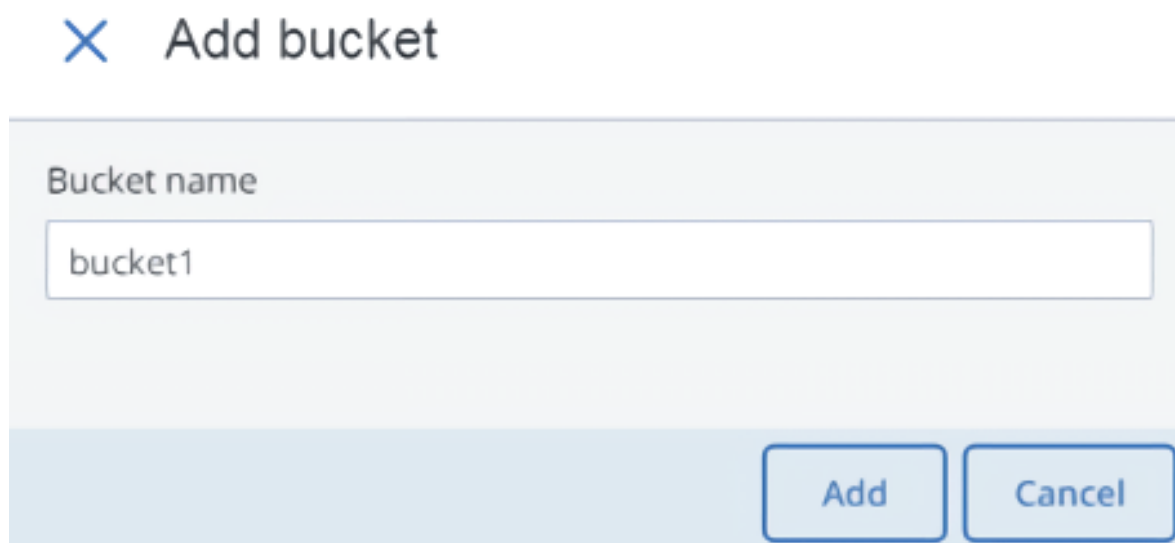
После входа в веб-интерфейс откроется экран **Корзины** со списком корзин. Здесь можно управлять корзинами, а также папками и файлами, хранящимися внутри корзин.

Для выхода щелкните по значку пользователя в правом верхнем углу любого экрана и нажмите **Выйти**.

2.1.2 Добавление, удаление и перечисление корзин S3

На экране **Корзины**:

- Чтобы добавить новую корзину, нажмите **Добавить корзину**, укажите имя и нажмите **Добавить**.



Используйте имена корзин, соответствующие соглашениям об именовании DNS.

Дополнительные сведения об именовании корзин см. в разделе "Политики именования корзин и ключей S3" (стр. 12).

- Чтобы удалить корзину, выделите ее и нажмите **Удалить**.
- Чтобы вывести список содержимого корзины, щелкните по ее имени в списке.

2.1.2.1 Перечисление содержимого корзины S3 в браузере

Можно перечислить содержимое корзины с помощью веб-браузера. Для этого откройте URL-адрес, состоящий из внешнего DNS-имени конечной точки S3, указанной при создании кластера S3, и имени корзины, например **s3.example.com/mybucket**.

Примечание

Также можно скопировать ссылку на содержимое корзины, щелкнув по ней правой кнопкой мыши в CyberDuck и затем выбрав **Копировать URL-адрес**.

2.1.3 Создание, удаление и перечисление папок

На экране содержимого корзины:

- Чтобы создать папку, нажмите **Новая папка**, укажите имя папки в окне **Новая папка** и нажмите **Добавить**.

✕ New folder

Folder name

Add

Cancel

- Чтобы удалить папку, выделите ее и нажмите **Удалить**.
- Чтобы вывести список содержимого папки, щелкните по ее имени.

2.1.4 Загрузка и скачивание файлов

На экране содержимого корзины или папки:

- Чтобы загрузить файлы в S3, нажмите **Загрузить** и выберите файлы для отправки.

Buckets > bucket1 👤

Type	Name	Size	Last modified	
📁	file1.test	5.3 MB	Dec 07 18:34	📁 New folder
📁	folder1/			📄 Download file
				📄 Upload file
				⚙️ Get certificate
				✅ Verify

Uploading file 1 of 1

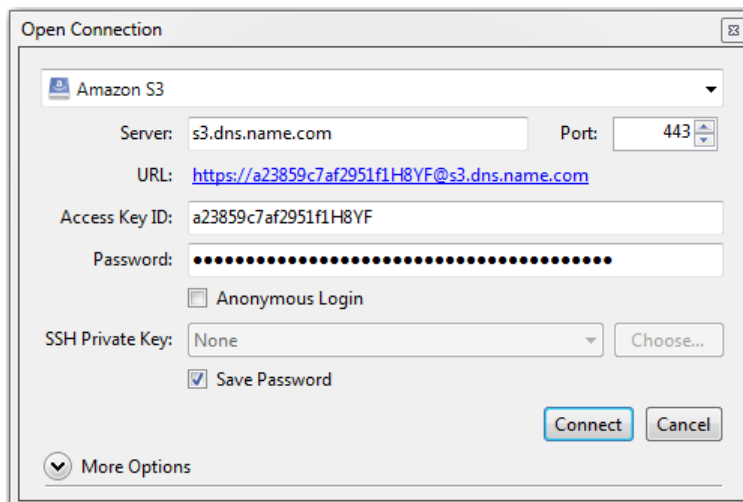
file2.test 103.8 MB

- Чтобы скачать файлы, выберите их и нажмите **Скачать**.

2.2 Доступ к хранилищу S3 с помощью CyberDuck

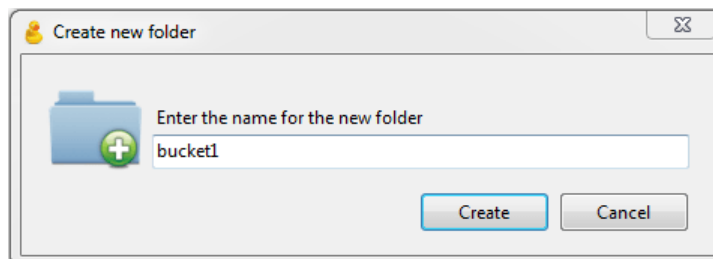
Чтобы получить доступ к Кибер Инфраструктура с помощью CyberDuck, выполните следующие действия.

1. В CyberDuck нажмите **Открыть подключение**.
2. Укажите учетные данные.
 - Доменное имя окончной 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.



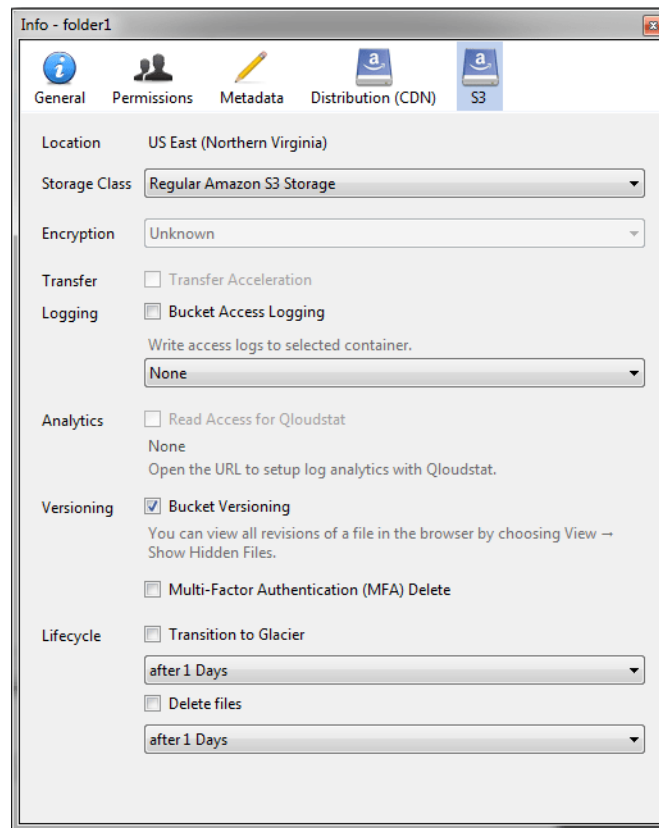
4. Укажите имя для новой корзины, а затем нажмите **Создать**. Используйте имена корзин, соответствующие соглашениям об именовании DNS. Дополнительные сведения об именовании корзин см. в разделе "Политики именованя корзин и ключей S3" (стр. 12).

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

2.2.1 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](#).

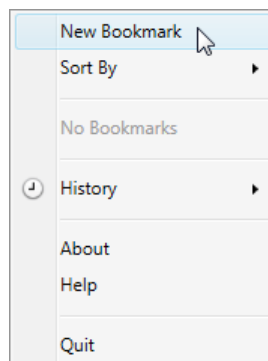
Управление версиями корзины по умолчанию отключено. В CyberDuck его можно включить в свойствах корзины, например:



2.3 Подключение хранилища S3 с помощью Mountain Duck

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

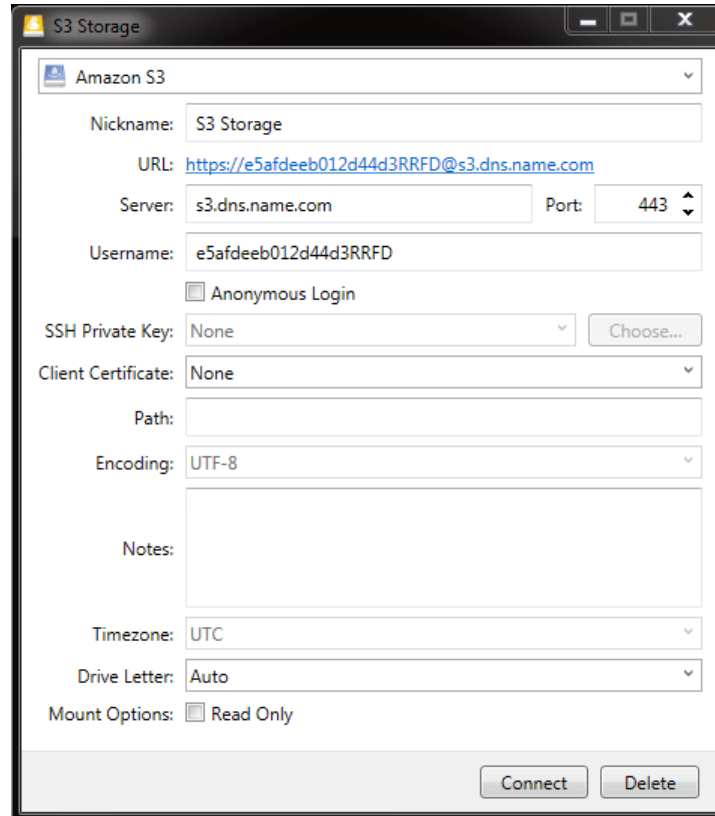
1. Если поставщик услуг предоставил вам SSL-сертификат, установите его.
2. В приложении Mountain Duck нажмите **Создать закладку**.



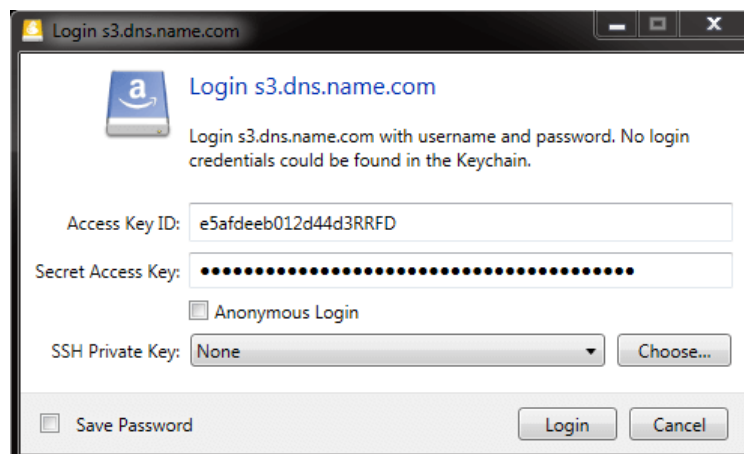
3. В окне свойств выберите профиль **Amazon S3** из первого раскрывающегося списка и укажите следующие параметры:

- 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.

2.3.1 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. "Политики именования корзин и ключей S3" (стр. 12)), 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.

2.4 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.

3 Доступ к целевым устройствам iSCSI

В этом разделе описаны способы прикрепления целевых устройств iSCSI к операционным системам и сторонних решений для виртуализации, которые поддерживают явный режим ALUA.

3.1 Доступ к целевым устройствам iSCSI из VMware ESXi

Перед использованием томов Кибер Инфраструктура 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:

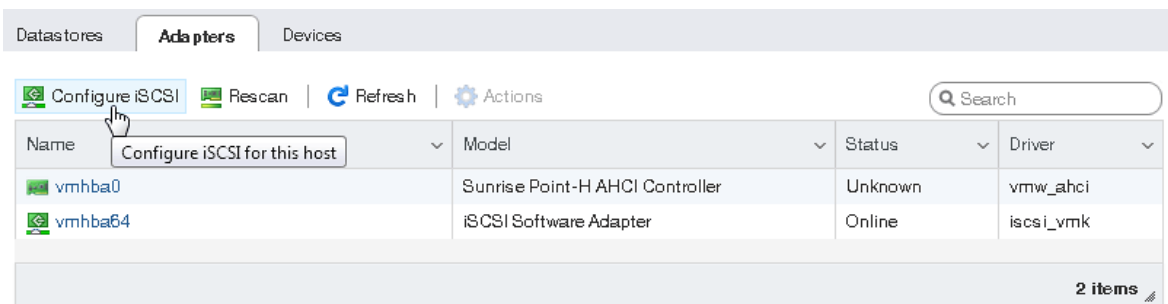
```
# esxcli storage nmp satp rule add --satp VMW_SATP_ALUA --vendor VSTORAGE \
--model VSTOR-DISK --psp VMW_PSP_RR -c tpgs_on
```

- Чтобы задать PSP для определенного устройства, выполните:

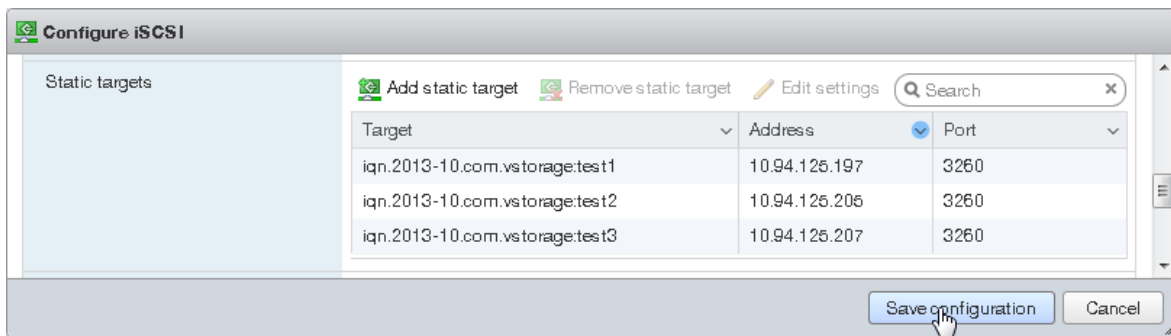
```
# esxcli storage core claimrule load
```

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

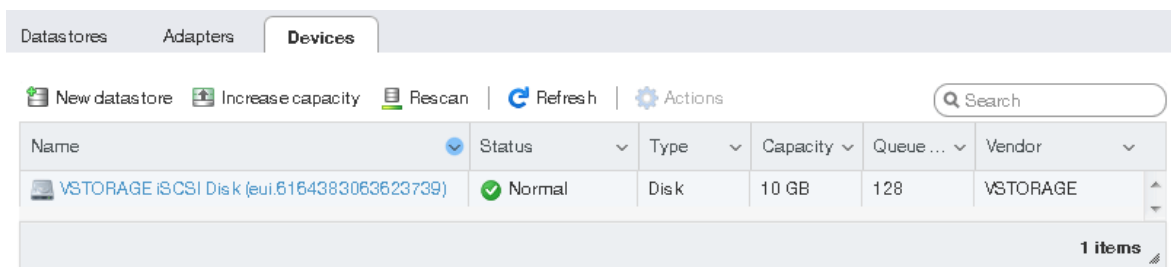
1. В Navigator перейдите на вкладку **Хранилище > Адаптеры** и нажмите **Настроить iSCSI**.



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.

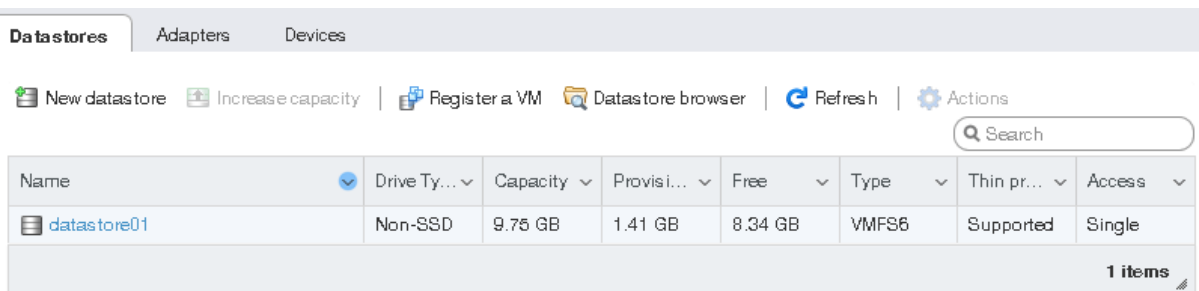


4. Выберите диск и нажмите **Создать хранилище данных**. В открывшемся мастере введите имя для хранилища данных и выберите параметры создания разделов. Нажмите **Завершить**, чтобы фактически разбить диск на разделы.

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](#).

3.2 Доступ к целевым устройствам iSCSI из Linux

Чтобы подключить iSCSI-инициатор на основе Linux к целевым устройствам iSCSI продукта Кибер Инфраструктура, 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
36000000000000000000000000b50326ea44e3 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 36000000000000000000000000b50326ea44e3
Disk /dev/mapper/360000000000000000000000b50326ea44e3: 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 36000000000000000000b50326ea44e3 – идентификатор устройства Multipath, сопоставленный из идентификатора тома 61c9d567-4666-4c16-8030-b50326ea44e3.

Теперь можно создать разделы на устройстве iSCSI (/dev/mapper/36000000000000000000000000b50326ea44e3 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/36000000000000000000000000b50326ea44e3
```

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
```

3.3 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.

- a. Включите поддержку дисков iSCSI.

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

- b. 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
```

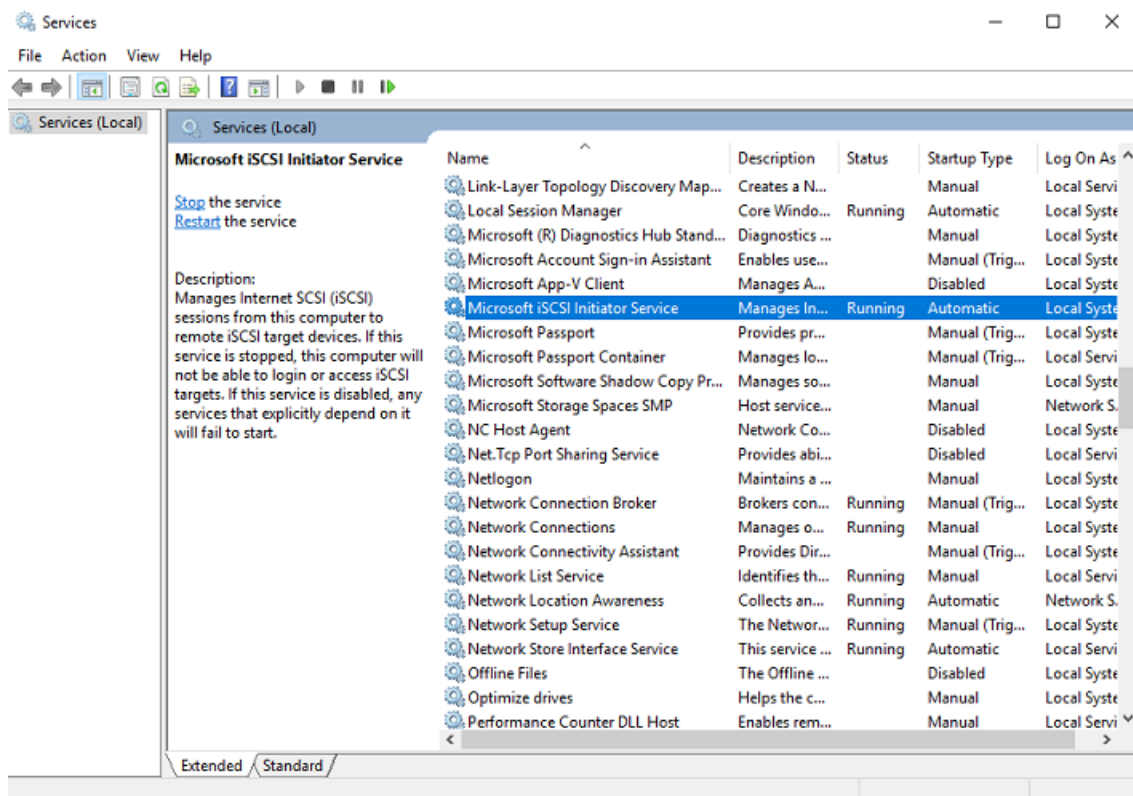
- c. Включите верификацию пути. По умолчанию инициатор будет верифицировать каждый путь каждые 30 секунд.

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

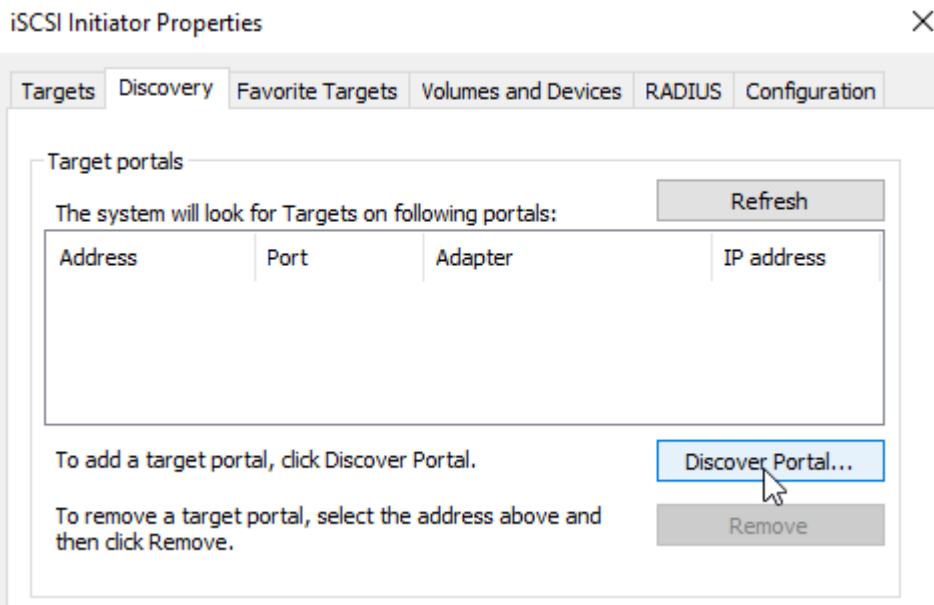
- d. Перезагрузите сервер.

3. Подключите целевые устройства к инициатору iSCSI следующим образом.

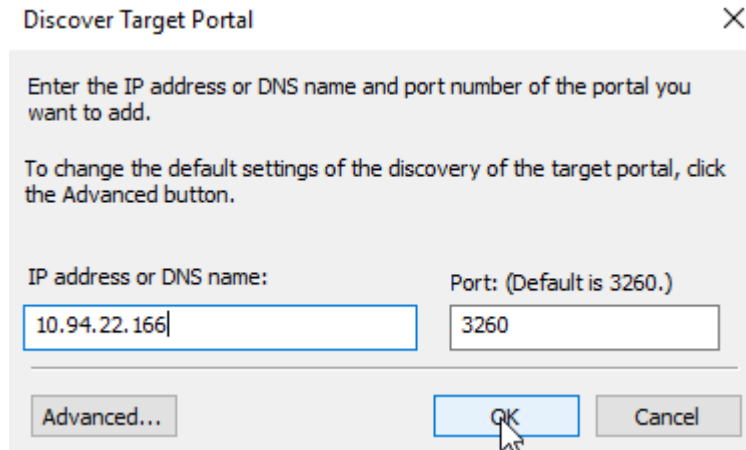
- a. В окне **Панель управления > Система и безопасность > Администрирование > Сервисы** убедитесь, что **Сервис инициатора Майкрософт iSCSI** работает и для него установлен тип запуска **Автоматически**.



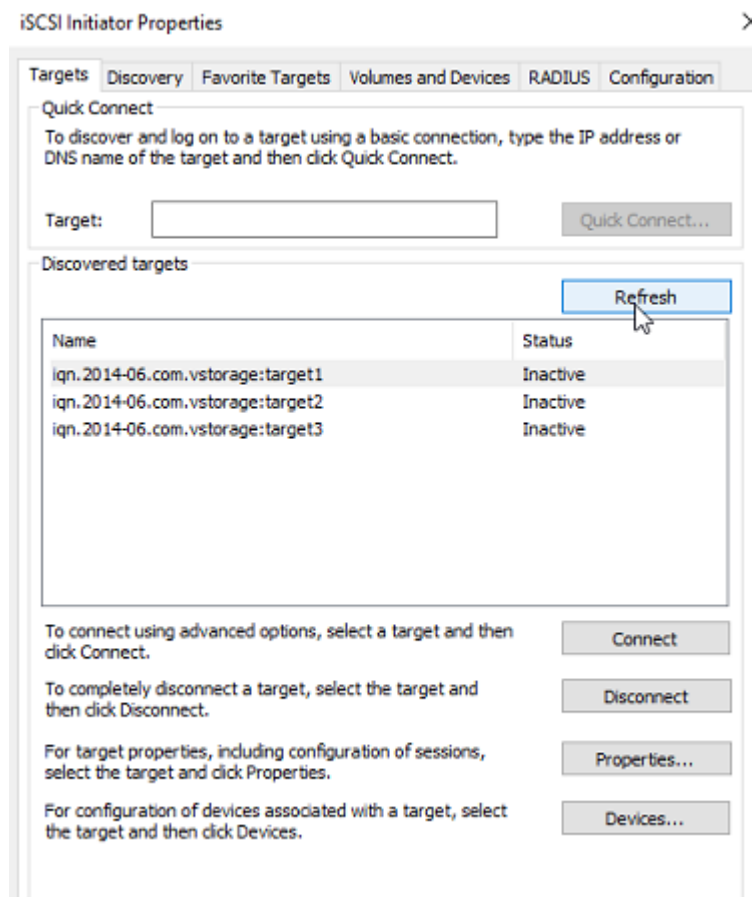
- b. Запустите **Инициатор iSCSI**.
- c. В окне **Свойства инициатора iSCSI** откройте вкладку **Обнаружение** и нажмите **Обнаружить портал**.



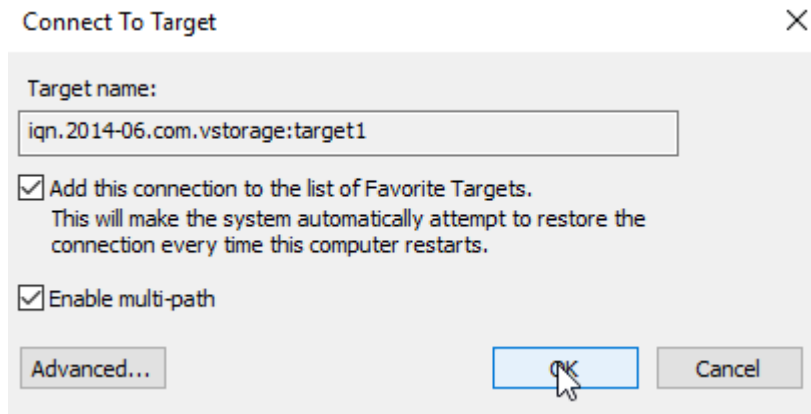
- d. В окне **Обнаружение целевого портала** введите целевой IP-адрес и нажмите кнопку **ОК**. Повторите этот шаг для каждого целевого устройства из целевой группы.



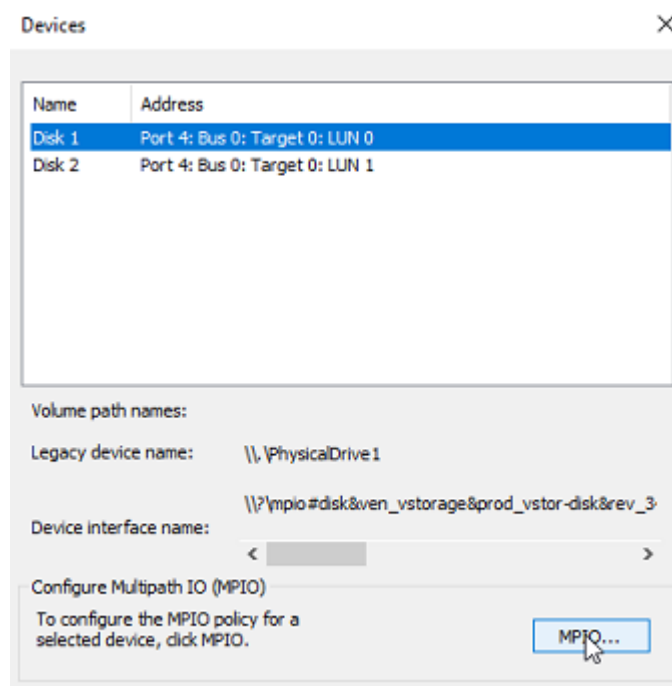
- e. На вкладке **Целевые устройства** нажмите **Обновить**, чтобы обнаружить добавленные целевые устройства.



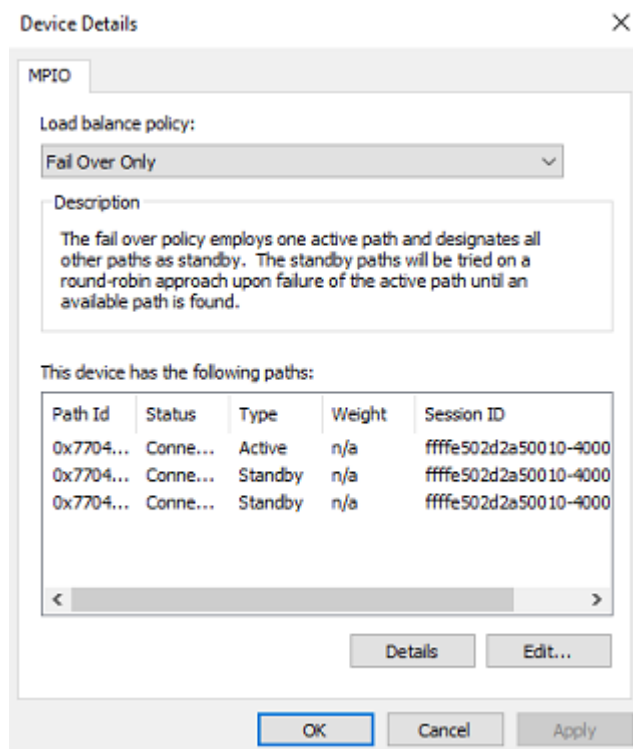
- f. Нажмите **Подключить** для каждого целевого устройства, чтобы подключить его к инициатору. В окне **Подключение к целевому устройству** установите флажок **Включить множественный путь** и нажмите кнопку **ОК**.



- g. На вкладке **Целевые устройства** нажмите **Устройства...**, выберите подключенный LUN и нажмите **МPIO...**

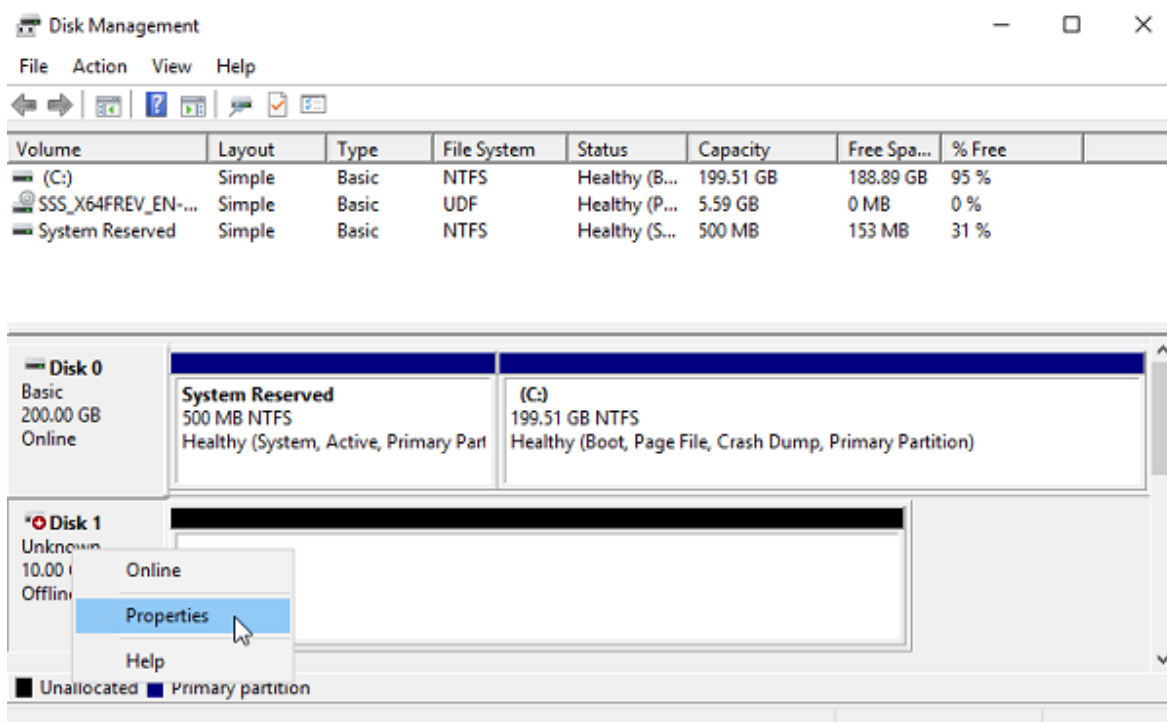


- h. Убедитесь, что подключенный LUN имеет несколько путей.

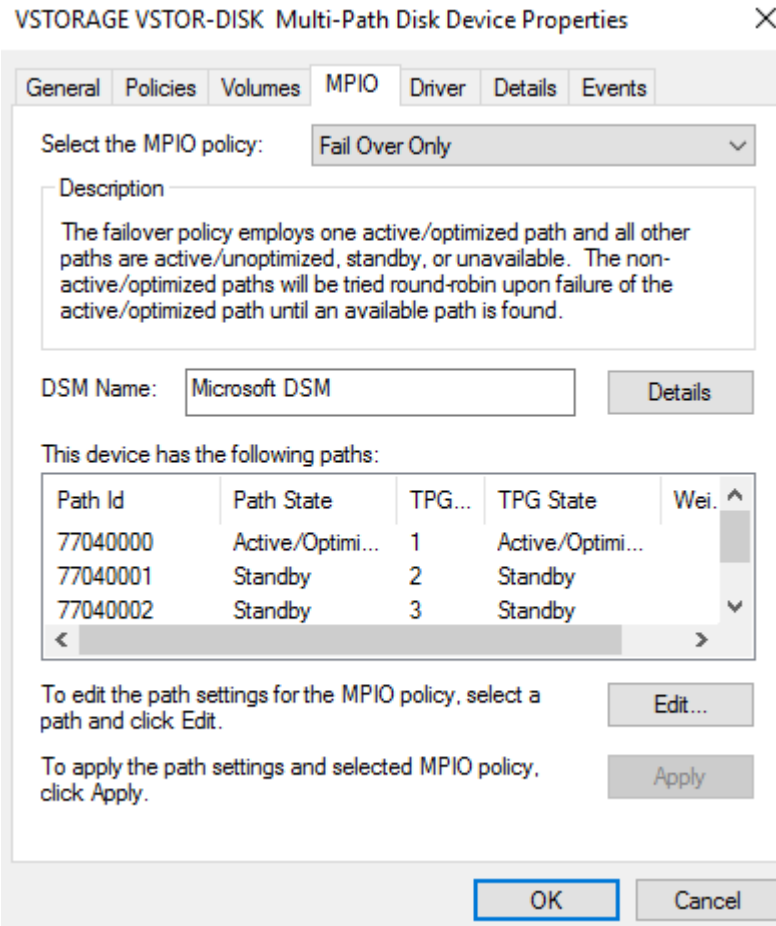


Теперь можно инициализировать только что добавленный диск для использования в Microsoft Hyper-V. Выполните следующие действия.

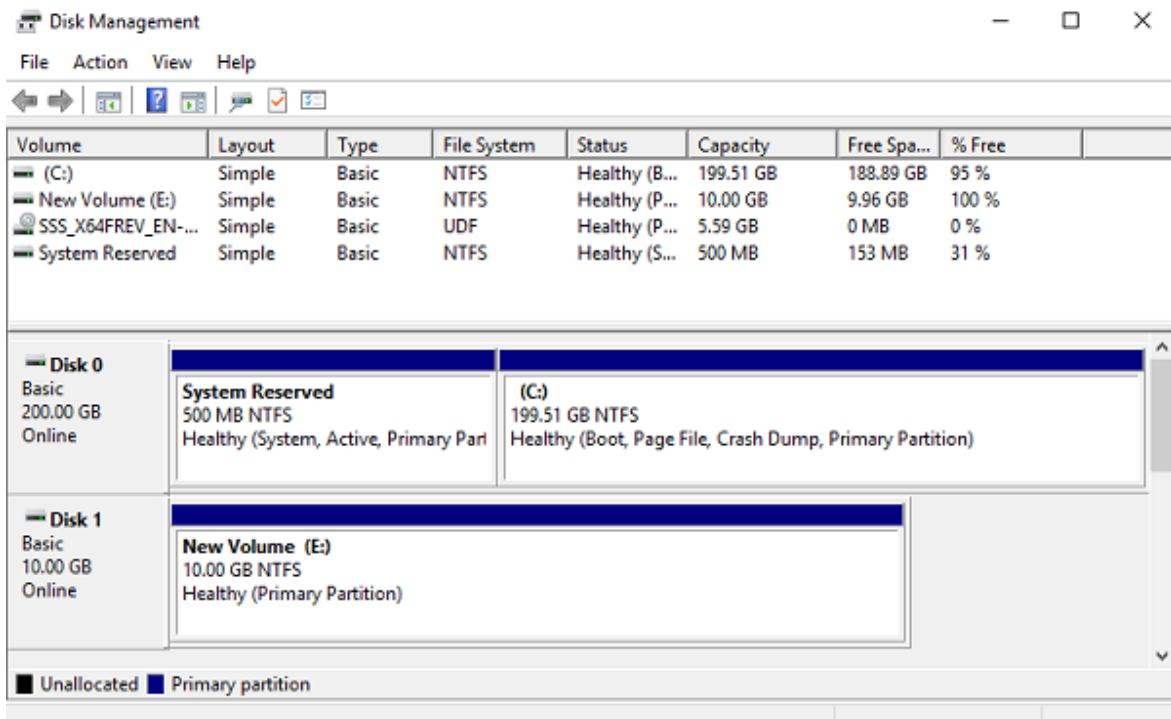
1. Откройте **Управление дисками**, щелкните правой кнопкой мыши по добавленному диску и выберите **Свойства** из раскрывающегося меню.



2. Проверьте настройки на вкладке **МPIO**. Первое подключенное целевое устройство становится **активным/оптимизированным** и предпочтительным путем.



3. Разделите и отформатируйте диск обычным образом.



4 Доступ к томам NFS

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

Примечание

В настоящее время Кибер Инфраструктура не поддерживает встроенный NFS-клиент Windows.

4.1 Подключение экспортов NFS в Linux

Экспорт NFS, созданный в Кибер Инфраструктура, 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 Инфраструктура 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.

4.2 Подключение экспортов NFS в macOS

Экспорт NFS, созданный в Кибер Инфраструктура, 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 Инфраструктура 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>/`.