request-ru@raidix.com
raidix.ru

RAIDIX 5.3.1

Руководство по настройке ОС и платформ виртуализации

Редакция 2

2026

Содержание

Глава 1. Об этом руководстве....3
Что нового....3
Глава 2. Блочный доступ....4
Linux....6
Настройка multipath на Linux....6
Настройка соединения по iSCSI или iSER для Linux....7
Настройка соединения по Fibre Channel на Linux....9
Настройка соединения по SRP (InfiniBand) для Linux....9
ESXi....10
Специфика работы ESXi....10
Настройка multipath на ESXi....10
Подключение по iSCSI....12
Подключение по FC....14
Рекомендации для ESXi....14
Windows....21
Специфика работы Windows....21
Установка MPIO....21
Настройка FC на Windows Server....25
Настройка iSCSI на Windows Server....29
Отключение от iSCSI-таргета на Windows Server....37
zVirt....37
Специфика работы zVirt....37
Настройка multipath на zVirt....38
ROSA Virtualization....38
Специфика работы ROSA Virtualization....39
Настройка multipath на ROSA Virtualization....39
Глава 3. Файловый доступ....41
Монтирование общей папки на Linux....41
Монтирование общей папки на Windows....45
Монтирование общей папки на zVirt....45
Монтирование общей папки на ROSA Virtualization....46
Глава 4. Механизм Serial-over-LAN....47

raidix: 2026-03-31

Версия: 5.3.1:2:2

ГЛАВА 1. ОБ ЭТОМ РУКОВОДСТВЕ

В документе представлена информация о настройке файлового и блочного доступа хостов к ресурсам СХД, в том числе настройка многопутевого ввода-вывода (далее – multipath), способы монтирования общих папок, особенности работы различных хостов.

Информацию по протестированным и поддерживаемым сетевым адаптерам см. в документе «Характеристики продукта RAIDIX 5.3.1».

Что нового

Редакция	Изменения	Дата внесения изменения
1	Документ создан.	17.12.2025
2	В главе *Файловый доступ (стр. 41)* убраны нерабочие ссылки.	20.02.2026

ГЛАВА 2. БЛОЧНЫЙ ДОСТУП

Блочное хранилище используется чаще всего для виртуализации и работы с базами данных.

Настройка блочного хранилища состоит из настройки сети, хостов и СХД. Общий план настройки представлен ниже.

Схема настройки блочного доступа

Настройка блочного доступа состоит из следующих этапов:

1. Проверка первичной настройки СХД:
   - ПО RAIDIX установлено;
   - лицензия добавлена;
   - менеджмент-интерфейс настроен;
   - в случае двухконтроллерной системы, включён DC-режим;
   - в случае использования дисковой корзины, она подсоединена к СХД.
2. Предварительная подготовка:
   a. *Опционально:* настройка multipath на хосте (инициаторе) в зависимости от используемой ОС.

   Подробнее в этом документе в разделе с используемой ОС.

   b. Монтаж и настройка сети и сетевого оборудования между хостом (инициатором) и СХД (таргетом).

   c. Ознакомление с особенностями работы ОС хоста (инициатора) и создание RAID и LUN на СХД.

   Особенности ОС хостов см. в этом документе в разделах конкретных ОС.

   Убедитесь, что LUN, который планируется использовать для блочного доступа

   - имеет тип SCSI;
   - не используется в качестве SSD-кэша;
   - не используется для хранения метаданных репликации;
   - не является реплицированным LUN.

   d. *Опционально:* настройка резервных путей.

   Подробнее в документе «Руководство администратора RAIDIX 5.3.1».
3. Специфическая настройка *сети*, *инициатора* и *СХД* в зависимости от используемого транспортного протокола и ОС хоста:
   - Для iSCSI или iSER:
     a. Включение iSCSI (для iSER – и iSER) на СХД.

     Подробнее в документе «Руководство администратора RAIDIX 5.3.1».

     b. Создание таргета на СХД.

     Подробнее в документе «Руководство администратора RAIDIX 5.3.1».

     c. Настройка LUN на СХД:
     - Настройка доступа хоста (инициатора) к LUN (ресурсу) – «маскирование таргетов».

       Подробнее в документе «Руководство администратора RAIDIX 5.3.1».
     - Настройка типа доступа хоста (инициатора) к LUN (ресурсу) – «маскирование инициаторов».

       Подробнее в документе «Руководство администратора RAIDIX 5.3.1».

d. Настройка хоста (инициатора).

Подробнее в этом документе в разделах конкретных ОС.

- Для FC:

a. При подключении хоста к СХД через коммутатор:

i. Настройка зонирования на SAN-коммутаторах.

b. При прямом подключении хоста к СХД:

i. Коммутация по принципу «порт-к-порту», где нулевой порт инициатора соединяется с нулевым портом таргета, первый с первым и так далее.

- Все SFP-модули должны быть от одного производителя или совместимых моделей.
- Все FC-адаптеры должны быть от одного производителя или совместимых моделей.
- Все FC-адаптеры должны иметь идентичные настройки BIOS/UEFI.
- Все FC-адаптеры должны иметь идентичные версии прошивки.
- Все FC-адаптеры должны иметь идентичную программную конфигурацию и поддерживать режим работы point-to-point.

c. Настройка LUN на СХД:

- Настройка доступа хоста (инициатора) к LUN (ресурсу) – «маскирование таргетов».

  Подробнее в документе «Руководство администратора RAIDIX 5.3.1».

- Настройка типа доступа хоста (инициатора) к LUN (ресурсу) – «маскирование инициаторов».

  Подробнее в документе «Руководство администратора RAIDIX 5.3.1».

d. Настройка хоста (инициатора).

Подробнее в этом документе в разделах конкретных ОС.

- Для SRP (InfiniBand):

a. Управление OpenSM

Подробнее в документе «Руководство администратора RAIDIX 5.3.1».

b. Настройка LUN на СХД:

- Настройка доступа хоста (инициатора) к LUN (ресурсу) – «маскирование таргетов».

  Подробнее в документе «Руководство администратора RAIDIX 5.3.1».

- Настройка типа доступа хоста (инициатора) к LUN (ресурсу) – «маскирование инициаторов».

  Подробнее в документе «Руководство администратора RAIDIX 5.3.1».

c. Настройка хоста (инициатора).

Подробнее в этом документе в разделах конкретных ОС.

Linux

Настройка multipath на Linux

> Для настройки multipath на ОС Linux необходимы права суперпользователя.

> Файл конфигурации multipath также применим к протестированным платформам виртуализации Proxmox VE.

Чтобы настроить mpath на Linux с инициатором:

- Установите следующие пакеты в зависимости от вашей ОС:
  - `multipath-tools` и `open-iscsi` для ALT Linux, Astra Linux или Ubuntu Linux;
  - `device-mapper-multipath` и `iscsi-initiator-utils` для RHEL или Oracle UEK Linux.
- Создайте файл `/etc/multipath.conf` следующего содержания:

```
defaults {
            fast_io_fail_tmo                    5
            features                        "0"
            no_path_retry                   10
            path_checker                    tur
            polling_interval                5
            prio                            alua
            user_friendly_names             yes

            #For Proxmox VE 8.2 or ALT OS
            #find_multipaths                    on
}

devices {
            device {
                        detect_checker       no
                        detect_prio          no
                        failback             immediate
                        no_path_retry        12
                        path_grouping_policy "group_by_prio"
                        path_selector        "round-robin 0"
                        path_checker         "tur"
                        prio                 "alua"
                        product              ".*"
                        rr_min_io            100
                        rr_weight            "uniform"
                        vendor               "Raidix"

                        #For initiators with scsi_dh_alua
                        #hardware_handler    "1 alua"
            }
            device {
                        detect_checker          no
                        detect_prio          no
                        failback             immediate
                        no_path_retry        30
                        path_checker         directio
                        path_grouping_policy "group_by_prio"
                        path_selector        "round-robin 0"
                        prio                 ana
                        product              "Raidix"
                        rr_min_io            100
                        rr_weight            "uniform"
                        uid_attribute        ID_WWN
                        vendor               "NVME"
            }
}
```

- Если ОС с инициатором – CentOS 7.0, Red Hat 7 или загружен модуль scsi_dh_alua, то раскомментируйте строку «hardware_handler» (уберите #).
- Если ОС с инициатором – RHEL 7.4-7.9 или CentOS 7.4-7.9, измените название всех опций `detect_checker` на `detect_path_checker`.
- Если ОС с инициатором – ALT или платформа виртуализации Proxmox VE 8.2, раскомментируйте строку «find_multipaths» (уберите #).
- При большом количестве объектов в системе увеличьте время ожидания для выполнения failover.

  Время ожидания равно произведению значений опций `polling_interval` и `no_path_retry` из конфигурационного файла `multipath.conf`. Определить оптимальное время ожидания можно только экспериментально. Рекомендуем ориентироваться на следующие значения: если в системе от 100 LUN, то установите для `no_path_retry` значение **40**.

- Запустите сервис `multipath`:

```
# systemctl start multipathd.service
```

Чтобы посмотреть информацию о multipath-устройствах, выполните

```
# multipath -ll
```

В результате будут выведены параметры multipath-устройства.

Пример вывода параметров multipath-устройства для SC-системы:

```
root@flexpro13:~# multipath -ll
mpathh (235354432423643 46) dm-0 Raidix,lun0
size=8.7T features='1 queue_if_no_path' hwhandler='1 alua' wp=rw
`-+- policy='round-robin 0' prio=50 status=active
  |- 15:0:0:2 sdc 8:32  active ready running
  |- 16:0:0:2 sdg 8:96  active ready running
  |- 15:0:1:2 sdd 8:48  active ready running
  `- 16:0:1:2 sdh 8:112 active ready running
```

Пример вывода параметров multipath-устройства для DC-системы:

```
root@flexpro13:~# multipath -ll
mpathh (235354432423643 46) dm-0 Raidix,lun0
size=8.7T features='1 queue_if_no_path' hwhandler='1 alua' wp=rw
|-+- policy='round-robin 0' prio=50 status=active
| |- 15:0:0:2 sdc 8:32  active ready running
| |- 16:0:0:2 sdg 8:96  active ready running
| |- 15:0:1:2 sdd 8:48  active ready running
| `- 16:0:1:2 sdh 8:112 active ready running
`-+- policy='round-robin 0' prio=1 status=enabled
  |- 16:0:3:2 sdj 8:144 active ghost running
  |- 15:0:3:2 sdf 8:80  active ghost running
  |- 16:0:2:2 sdi 8:128 active ghost running
  `- 15:0:2:2 sde 8:64  active ghost running
```

Настройка соединения по iSCSI или iSER для Linux

Для управления соединением iSCSI и iSER вы можете использовать **iscsiadm**.

Для включения iSER в качестве транспортного протокола добавьте опцию `-I iser` при вызове iscsiadm.

> При работе с двухпортовыми адаптерами NVIDIA VPI не используйте конфигурацию, при которой один порт работает в режиме Ethernet, а другой – в режиме InfiniBand.

> Версия семейства (или серии) адаптера, используемого в качестве таргета, должна быть не ниже версии семейства (или серии) адаптера, используемого в качестве инициатора.

Убедитесь, что в системе RAIDIX создан LUN, он добавлен в iSCSI-таргет и для таргета настроено маскирование. Тогда:

> Номер порта по умолчанию: 3260.

- Чтобы обнаружить iSCSI-таргет:

```
# iscsiadm -m discovery -t sendtargets -p <IP_address>:<port>
```

- Чтобы подключить таргет:

```
# iscsiadm -m node -l -p <IP_address>:<port> --targetname <target_iqn>
```

- Чтобы просмотреть активные iSCSI-сессии:

```
# iscsiadm -m session
```

- Чтобы отключить iSCSI-таргет:

```
# iscsiadm -m node --targetname <target_iqn> -p <IP_address>:<port> --logout
```

Пример настройки одностороннего режима CHAP

> Это пример настройки режима CHAP, а не рекомендуемый способ.

Чтобы настроить односторонний режим CHAP между СХД и хостом:

1. На СХД создайте пользователя CHAP.
2. На хосте в файл `/etc/iscsi/iscsid.conf` добавьте:
   a. в строку `node.session.auth.username` имя пользователя CHAP СХД;
   b. в строку `node.session.auth.password` пароль пользователя CHAP СХД.
3. На СХД создайте таргет iSCSI, если он ещё не создан.
4. На таргете выберите односторонний режим CHAP.

Пример настройки двустороннего режима CHAP

> Это пример настройки режима CHAP, а не рекомендуемый способ.

Чтобы настроить двусторонний режим CHAP между СХД и хостом:

1. На СХД создайте пользователя CHAP.
2. На хосте в файл `/etc/iscsi/iscsid.conf` добавьте:
   a. в строку `node.session.auth.username` имя пользователя CHAP СХД;
   b. в строку `node.session.auth.password` пароль пользователя CHAP СХД;
   c. в строку `node.session.auth.username_in` имя пользователя CHAP хоста;
   d. в строку `node.session.auth.password_in` пароль пользователя CHAP хоста.
3. На СХД создайте таргет iSCSI, если он ещё не создан.
4. На таргете выберите двусторонний режим CHAP и добавьте пользователя CHAP хоста.

Настройка соединения по Fibre Channel на Linux

Чтобы обнаружить новое устройство:

1. Если в качестве инициатора адаптеры ATTO:
   - При использовании адаптера Fibre Channel 8 Gb производителя ATTO Technology, загрузите драйвер `celerity8fc.ko`:
     ```
     # insmod celerity8fc.ko initiator_mode=1
     ```
   - При использовании адаптера Fibre Channel 16 Gb производителя ATTO Technology, загрузите драйвер `celerity16fc.ko`:
     ```
     # insmod celerity16fc.ko initiator_mode=1
     ```
   - При использовании адаптера производителя ATTO Technology с более низкой скоростью, загрузите драйвер `celerityfc.ko`:
     ```
     # insmod celerityfc.ko initiator_mode=1
     ```
2. Выполните
   ```
   # echo '- - -' > /sys/class/scsi_host/<host_fc>/scan
   ```
   где <host_fc> - номер порта FC-адаптера, настроенного для получения ресурса СХД. Вы можете определить номер порта через команду `$ lsscsi -H`. Например, для адапртеров QLogic нужной номер будет в строке с *qla2xxx*.
3. Чтобы увидеть устройство в общем списке устройств:
   - если multipath не используется: `$ lsscsi`;
   - если multipath настроен: `$ multipath -ll`.

Настройка соединения по SRP (InfiniBand) для Linux

Протокол SRP (SCSI RDMA Protocol) реализует преимущества функций RDMA и уменьшения нагрузки на ядро, предоставляемые архитектурой InfiniBand.

Чтобы настроить соединение по SRP:

> При работе с двухпортовыми адаптерами NVIDIA VPI не используйте конфигурацию, при которой один порт работает в режиме Ethernet, а другой – в режиме InfiniBand.

> Версия семейства (или серии) адаптера, используемого в качестве таргета, должна быть не ниже версии семейства (или серии) адаптера, используемого в качестве инициатора.

1. Установите актуальную версию OFED или убедитесь, что она установлена.

   OFED (OpenFabrics Enterprise Distribution) – это программное обеспечение с открытым исходным кодом для приложений, работающих по RDMA.

   MLNX_OFED (Mellanox OpenFabrics Enterprise Distribution for Linux) – это набор программного обеспечения Virtual Protocol Interconnect (VPI), используемый во всех решениях сетевых адаптеров Mellanox.

   Вы можете скачать MLNX_OFED на *официальном сайте Nvidia*. Подробнее в *официальной документации Nvidia*.

   Чтобы проверить наличие OFED на системе, выполните

   ```
   # ofed_info
   ```

2. Настройте multipath (подробнее в главе *Настройка multipath на Linux (стр. 6)*).

ESXi

Специфика работы ESXi

При настройке блочного доступа к ESXi учитывайте следующие особенности работы ESXi:

- ESXi работает только с размером блока 512 Б. Создавайте LUN (в случае ERA RAID - и RAID) с этим размером блока.
- Подключение по iSCSI поддерживается только через программный инициатор. Аппаратные инициаторы (как зависимые, так и независимые) не поддерживаются.
- Для сетевых интерфейсов iSCSI скоростью 10 Гб/с и выше значение MTU должно быть 9000.
- Для настройки multipath рекомендуем использовать политику Round Robin.
- В VMware vSphere официально поддерживается только политика Round Robin.
- Рекомендации по настройкам для производительности и отказоустойчивости см. в главе *Рекомендации для ESXi (стр. 14)*.

Настройка multipath на ESXi

> Для настройки multipath рекомендуем использовать политику Round Robin.

В этой главе представлена следующая информация:

1. Создание настроек multipath с помощью шаблона multipath (конфигурации SATP (аббр. Storage Array Type Policy)).

   Это стандартный способ настройки multipath на ESXi-хосте.

2. Редактирование настроек multipath через шаблон multipath.

3. Персональная настройка multipath для устройств через NMP PSP (аббр. Native Multipathing Plug-in & Path Selection Plug-in).

   Вы можете настроить multipath для каждого устройства отдельно через NMP. Настройки записываются в Device Custom Config устройства, не требуют перезагрузки ESXi-хоста и имеют больший приоритет, чем конфигурация SATP. Этот способ требует, чтобы соединение с СХД уже было настроено и ESXi-хосту были доступны предоставленные СХД устройства.

Создание шаблона multipath (конфигурации SATP) RAIDIX

Чтобы создать шаблон multipath:

1. На ESXi-хосте включите ESXi Shell и SSH или убедитесь, что они включены.
2. Создайте SATP-конфигурацию:

```
# esxcli storage nmp satp rule add -V Raidix -P VMW_PSP_RR -s VMW_SATP_ALUA -O <NMP_OPTIONS>
```

   где

   <NMP_OPTIONS> - опции NMP. Например, для iops: параметр `iops=1` задаёт политику, а параметры `policy=iops;iops=1` задают приоритет для этой политики среди всех возможных политик.

3. Перезагрузите ESXi-хост:

```
# reboot
```

Изменение или удаление шаблона multipath (конфигурации SATP) RAIDIX

Чтобы изменить или удалить шаблон multipath:

1. Проверьте существующие шаблоны RAIDIX:

```
# esxcli storage nmp satp rule list | grep Raidix
```

2. Удалите существующий шаблон конфигурации SATP:

```
# esxcli storage nmp satp rule remove -V Raidix -P VMW_PSP_RR -s VMW_SATP_ALUA -O <NMP_OPTIONS>
```

3. Задайте новый шаблон:

```
# esxcli storage nmp satp rule add -V Raidix -P VMW_PSP_RR -s VMW_SATP_ALUA -O <NMP_OPTIONS>
```

   где

   <NMP_OPTIONS> - опции NMP. Например, для iops: параметр `iops=1` задаёт политику, а параметры `policy=iops;iops=1` задают приоритет для этой политики среди всех возможных политик.

   Полный синтаксис команды для задания шаблона:

```
# esxcli storage nmp satp rule add -V <VENDOR_NAME> -P <VMW_PSP_POLICY> -s <VMW_SATP_SATP> -o <"OPTIONS"> -c
 <CLAIM_OPTIONS> -O <NMP_OPTIONS>
```

4. Перезагрузите ESXi-хост:

```
# reboot
```

Настройка multipath для устройств RAIDIX через NMP

Чтобы настроить multipath через NMP:

1. Установите политику PSP Round Robin для устройств RAIDIX:

```
for i in `esxcfg-scsidevs -c | grep Raidix | awk '{print $1}'`; do esxcli storage nmp device set --device $i --psp
 VMW_PSP_RR; done
```

2. Установите политику NMP для каждого устройства через его `eui`.

   Существует 4 типа политик NMP для RoundRobin:

   - default – стандартный набор правил:

```
# esxcli storage nmp psp roundrobin deviceconfig set --type=default --useano=0 --device=<eui.xxxxxxxx>
```

   - iops – набор правил с приоритетом на количествово операций:

```
# esxcli storage nmp psp roundrobin deviceconfig set --type=iops --iops=<num> --device=<eui.xxxxxxxx>
```

     <num> – значение для параметра `iops`. Например, 1.

   - bytes – набор правил с приоритетом на количествово передаваемых данных:

```
# esxcli storage nmp psp roundrobin deviceconfig set --type=bytes --bytes=<num> --device=<eui.xxxxxxxx>
```

     <num> – значение для параметра `bytes`. Например, 1024.

   - latency – набор правил с приоритетом на время отклика:

```
# esxcli storage nmp psp roundrobin deviceconfig set --type=latency --latency-eval-time=<time>
 --num-sampling-cycles=<cycles> --device=<eui.xxxxxxxx>
```

     <time> – значение для параметра `latency-eval-time`. Например, 3000.
     <cycles> – значение для параметра `num-sampling-cycles`. Например, 16.

Вы можете установить политику NMP для всех устройств RAIDIX одновременно с установкой политики PSP:

```
for i in `esxcfg-scsidevs -c | grep Raidix | awk '{print $1}'`; do esxcli storage nmp device set --device $i --psp
 VMW_PSP_RR; esxcli storage nmp psp roundrobin deviceconfig set <nmp> --device=$i; done
```

где

<nmp> – политика NMP для RoundRobin (например, для iops: `--type=iops --iops=1000`).

Подключение по iSCSI

> Подключение по iSCSI поддерживается только через программный инициатор. Аппаратные инициаторы (как зависимые, так и независимые) не поддерживаются.

> Для сетевых интерфейсов iSCSI скоростью 10 Гб/с и выше значение MTU должно быть 9000.

Вы можете выполнить подключение ESXi-хоста к СХД по iSCSI двумя способами:

- через веб-интерфейс ESXi;
- через vSphere.

Подключение через веб-интерфейс ESXi

Чтобы выполнить подключение и получить ресурсы СХД через iSCSI:

1. Включите iSCSI:
   a. Откройте **Storage > Adapters**.
   b. Выберите виртуальный сетевой адаптер (iSCSI Software Adapter) из списка и кликните **Configure iSCSI**.
   c. Для параметра **iSCSI enabled** выберите **Enabled**.
2. При необходимости, настройте параметры аутентификации CHAP в соответствии с настройками СХД.
3. Добавьте таргеты и iSCSI-порталы, настроенные для блочного доступа на СХД, в секции **Static Targets** с помощью **Add static target**.

   > Убедитесь, что вы добавили таргеты пассивных путей вместе с активными. Убедитесь, что IQN таргетов заданы согласно стандарту именования IQN.

   > Убедитесь, что вы не добавили адрес основного интерфейса СХД.

4. Сохраните настройки, кликнув **SAVE CONFIGURATION**.
5. В разделе **Storage** во вкладке **Adapters** кликните **Rescan**.
6. Проверьте подключение, открыв вкладку **Devices**.

Подключение через vSphere

Чтобы выполнить подключение и получить ресурсы СХД через iSCSI, на каждом ESXi-хосте:

1. Добавьте виртуальный сетевой адаптер:
   a. В левой верхней части окна интерфейса выберите ESXi-хост из списка.
   b. Откройте **Configure**.
   c. В секции **Storage** выберите **Storage Adapters**.
   d. Опционально: если iSCSI-адаптер отсутствует в списке, добавьте его при помощи **ADD SOFTWARE ADAPTER > Add iSCSI adapter**.
2. Добавьте таргеты:
   a. Выберите адаптер *vmhbaxx* модели *iSCSI Software Adapter*.
   b. Ниже откройте вкладку **Static Discovery**.
   c. Добавьте таргеты и iSCSI-порталы, настроенные для блочного доступа на СХД, используя **ADD**.

      > Убедитесь, что вы добавили таргеты пассивных путей вместе с активными. Убедитесь, что IQN таргетов заданы согласно стандарту именования IQN.

      > Убедитесь, что вы не добавили адрес основного интерфейса СХД.

3. При необходимости, настройте параметры аутентификации CHAP в соответствии с настройками СХД, в секции **Authentication** кликнув **Edit**.
4. Кликните **RESCAN ADAPTER**, затем **RESCAN STORAGE**.
5. Проверьте состояние подключения, открыв вкладку **Devices**.
6. Проверьте состояние путей, открыв вкладку **Paths**.

Подключение по FC

Вы можете выполнить подключение ESXi-хоста к СХД по FC двумя способами:

- через веб-интерфейс ESXi;
- через веб-интерфейс vCenter.

Подключение через веб-интерфейс ESXi

Чтобы выполнить подключение и получить ресурсы СХД через FC:

1. Откройте **Storage > Adapters**.
2. Выберите сетевой адаптер.
3. Кликните **Rescan**.
4. Проверьте подключение, открыв вкладку **Devices**.

Подключение через vShpere

Чтобы выполнить подключение и получить ресурсы СХД через FC:

1. В левой верхней части окна интерфейса выберите ESXi-хост из списка.
2. Откройте **Configure**.
3. В секции **Storage** выберите **Storage Adapter**.
4. Выберите сетевой адаптер.
5. Кликните **Rescan Adapter**.
6. Проверьте подключение, открыв вкладку **Devices**.

Рекомендации для ESXi

В главе представлены рекомендации по настройкам ESXi, влияющим на производительность и отказоустойчивость гипервизора. Рекомендации отсортированы по следующим тематическим секциям:

- *Повреждение данных VMware ESX Datastore (VMFS) (стр. 14)*;
- *Транспорт FC QLogic (Marvell) (стр. 15)*;
- *Общие рекомендации (стр. 18)*.

Повреждение данных VMware ESX Datastore (VMFS)

В секции представлены известные сценарии, при которых возможно повреждение данных VMFS, и рекомендации по их избежанию. При подозрении на повреждение обратитесь в службу поддержки VMware.

Сценарии и рекомендации:

1. При одновременном использовании LUN несколькими хостами ESXi:
   a. Во время продолжительных операций на RAID со стороны СХД, влияющих на уменьшение производительности (например, реконструкция RAID, переключение контроллеров, исправление SDC, высокая нагрузка на RAID), рекомендуем не мигрировать ресурсы между хостами, не создавать снэпшоты и бэкапы, а также отключить ATS HB.

      Если хост ESXi не может обновить метаданные на томе дольше 15 секунд, то из-за специфики ATS HB остальные хосты будут считать, что блокировка тома тем хостом неактуальна.

   b. При высокой нагрузке на СХД ошибки CAW (Compare And Write) со статусом MISCPOMPARE на ESXi-хосте могут указывать на то, что хосты не могут согласованно использовать пространство одного тома.

      Пример ошибки:

```
Cmd 0x89 to dev "eui.xxxx" failed H 0x0 D 0x2 P 0x0 Valid sense data: 0xe 0x1d 0x0
```

c. Некорректная работа DSswitch (vSphere Distributed Switch) может привести к ошибкам соединения между хостами и vCenter (получение хостом некорректного статуса «Not Responding») и повлечь миграцию ресурсов в кластере ESXi.

   Пример ошибки:

```
Hostd[2100937]: [Originator@6876 sub=Statssvc.Vapi.HTTPService.HttpConnection] HTTP Connection read failed
 while waiting for further requests; <io_obj p:0x000000a458ac4888, h:-1, <TCP '127.0.0.1 : 9131'>, <TCP
 '127.0.0.1 : 56712'>>, N7Vmacore16TimeoutExceptionE(Operation timed out: Stream: <io_obj p:0x000000a458ac4888,
 h:-1, <TCP '127.0.0.1 : 9131'>, <TCP '127.0.0.1 : 56712'>>, duration: 00:00:49.404834 (hh:mm:ss.us))
```

d. Ошибки в работе адаптеров инициаторов (например, «false hang»), могут сильно снижать производительность и провоцировать некорректное срабатывание передачи ресурсов между хостами в кластере ESXi.

   Пример ошибки:

```
igbn: igbn_CheckRxHang:1414: vmnic1: false hang detected on RX queue 0
```

2. Лучшая практика перед установкой или обновлением ESXi – отключение от хоста общего хранилища.

Транспорт FC QLogic (Marvell)

В секции представлены настройки, рекомендованные при работе с инициатором ESXi, которые могут быть использованы для решения и минимизации проблем, возникающих при использовании FC Qlogic (Marvell) в качестве транспорта данных между ESXi и СХД под управлением RAIDIX.

Рекомендации подобраны под систему, в которой в качестве транспорта инициатора используется QLogic (Marvell) FC, а для синхронизации – Mellanox IB SRP.

Для корректной работы ESXi с Generic RAID отключите VAAI.

При работе ESXi с DC-системой не перезагружайте одновременно оба узла СХД.

Из-за механизма *Permanent Device Loss* (PDL) на ESXi, устройства, что находятся удалённо, и не отвечают более 10 минут, не будут восстановлены, когда таргет будет снова их отдавать.

Чтобы на ESXi восстановить доступ к таким устройствам, вы можете использовать один из способов:

- Перерегистрируйте ВМ или перемонтируйте datastore, использующие такие устройства.
- Перезагрузите ESXi-хост.

1. В случаях потери физических путей от инициатора при использовании Fibre Channel в качестве транспорта во время длительных переездов используйте `bus_reset` вместо `lun_reset` (используемый по умолчанию) и `target_reset`.

```
# esxcfg-advcfg -s 0 /Disk/UseLunReset
# esxcfg-advcfg -s 0 /Disk/UseDeviceReset
```

2. При использовании конфигурации с 64 LUN рекомендуется установить значение `port_down_retry` 160 и выше.

```
# esxcli system module parameters set -p qlport_down_retry=160 -m qlnativefc
```

3. При использовании RDM-дисков рекомендуется запретить использование INQUIRY из кэша ESXi во избежание проблем с нестабильностью из-за неактуальных данных INQUIRY из кэша ESXi (подробнее см. на *сайте VMware*).

```
# esxcli storage core device inquirycache set --device device id --ignore true
```

4. При длительных переездах рекомендуется установить порог для LSOM, при котором *transient error* в 64 команды (либо 0) будет расцениваться как постоянное состояние.

```
# esxcfg-advcfg -s 64 /LSOM/lsomDeviceNeedsRepairCount
```

5. Для сохранения активности путей при возникновении *transient error* рекомендуется запретить переключение на пути с меньшим количеством ошибок.

```
# esxcfg-advcfg -s 0 /NmpManageDegradedPaths
# esxcfg-advcfg -s 0 /HppManageDegradedPaths
```

6. При достижении порога *transient error* в 20% рекомендуется убрать переключение статуса пути в *degraded*.

```
# esxcfg-advcfg -s 0 /Misc/NmpDegradedPathThresholdPer
# esxcfg-advcfg -s 0 /Misc/HppDegradedPathThresholdPer
```

7. Для получения ESXi актуального статуса путей рекомендуется установить повторный опрос о выходе из *transient error* в 3 секунды (по умолчанию: 20 секунд).

```
# esxcfg-advcfg -s 3 /Nmp/NmpSatpAluaCmdRetryTime
```

8. Для сохранения производительности при повышенной нагрузке рекомендуется включить алгоритм адаптивной длины очереди при возникновении *Queue full detected* и *Task set full*.

```
# esxcfg-advcfg -s 32 /Disk/QFullSampleSize
# esxcfg-advcfg -s 16 /Disk/QFullThreshold
```

9. При повторяющихся потерях доступа к устройствам без восстановления рекомендуется сократить *reset period* (по умолчанию: 30 секунд).

```
# esxcfg-advcfg -s 10 /Disk/ResetPeriod
```

   При сохранении проблемы вы можете вручную отключить обработку *All-Paths-Down* (APD) (подробнее см. на *сайте VMware*).

```
# esxcfg-advcfg -s 0 /Misc/APDHandlingEnable
```

10. При кратковременном падении производительности всех путей после отключения одного пути рекомендуется включить `Action_OnRetryErrors` (подробнее см. на *сайте VMware*) и применить `reset_on_attempted_reserve` (подробнее см. на *сайте VMware*) для инициации *failover*. Для применения изменений потребуется перезагрузка ESXi-хоста:

```
# esxcli storage nmp satp rule add -V <vendor_name> -P VMW_PSP_RR -s VMW_SATP_ALUA -o "enable_action_OnRetryErrors
 reset_on_attempted_reserve"
# esxcli storage core claimrule load
# reboot
```

    где `<vendor_name>` – имя вендора СХД (имя можно увидеть, выполнив на СХД команду `$ rdcli -V`, в конце строки вывода).

   При сохранении проблемы рекомендуется удалить и добавить правило повторно без применения `reset_on_attempted_reserve`:

```
# esxcli storage nmp satp rule remove -V <vendor_name> -P VMW_PSP_RR -s VMW_SATP_ALUA -o
 "enable_action_OnRetryErrors reset_on_attempted_reserve"
# esxcli storage nmp satp rule add -V <vendor_name> -P VMW_PSP_RR -s VMW_SATP_ALUA -o enable_action_OnRetryErrors
```

где `<vendor_name>` – имя вендора СХД (имя можно увидеть, выполнив на СХД команду `$ rdcli -V`, в конце строки вывода).

Заданные настройки будут применяться по умолчанию для всех существующих и новых устройств.

11. Во избежание падения производительности рекомендуем задать значение 100 или 200 для *iops* или 1024 или 2048 для *bytes* в настройках *NativeMultipathPlugin* (подробнее см. на *сайте VMware*) для смены пути.

    Задать значение *iops*:

    ```
    # esxcli storage nmp psp roundrobin deviceconfig set --type=iops --iops=<100or200> --device=eui.<LUN_number>
    ```

    где `<100or200>` – значение IOPS, `<LUN_number>` – номер устройства.

    Задать значение bytes:

    ```
    # esxcli storage nmp psp roundrobin deviceconfig set --type=bytes --bytes=<1024or2048> --device=eui.<LUN_number>
    ```

    где `<1024or2048>` – значение bytes, `<LUN_number>` – номер устройства.

    Если в системе присутствует большое количество LUN и отсутствуют LUN других СХД, использующих атрибут eui, вы можете задать значения с помощью скрипта.

    Скрипт для *iops*:

    ```
    # for i in `esxcfg-scsidevs -c | grep Raidix | awk '{print $1}'`; do esxcli storage nmp psp roundrobin deviceconfig
     set --type=iops --iops=<100or200> --device=$i; done
    ```

    где `<100or200>` – значение IOPS.

    Скрипт для *bytes*:

    ```
    # for i in `esxcfg-scsidevs -c | grep Raidix | awk '{print $1}'`; do esxcli storage nmp psp roundrobin deviceconfig
     set --type=bytes --bytes=<1024or2048> --device=$i; done
    ```

    где `<1024or2048>` – значение bytes.

    Заданные настройки можно сохранить как значения по умолчанию для всех существующих и новых устройств. Для этого удалите созданное правило SATP (если было создано) и создайте новое правило с рекомендуемым значением для *iops* или для *bytes*:

    Удаление правила SATP:

    ```
    # esxcli storage nmp satp rule remove -V <vendor_name> -P VMW_PSP_RR -s VMW_SATP_ALUA -o
     "enable_action_OnRetryErrors reset_on_attempted_reserve"
    ```

    где `<vendor_name>` – имя вендора СХД (имя можно увидеть, выполнив на СХД команду `$ rdcli -V`, в конце строки вывода).

    Новое правило со значением *iops*:

    ```
    # esxcli storage nmp satp rule add -V <vendor_name> -P VMW_PSP_RR -s VMW_SATP_ALUA -o "enable_action_OnRetryErrors
     reset_on_attempted_reserve" -c tpgs_on -O iops=<100or200>
    ```

    где `<vendor_name>` – имя вендора СХД (имя можно увидеть, выполнив на СХД команду `$ rdcli -V`, в конце строки вывода); `<100or200>` – значение IOPS.

    Новое правило со значением *bytes*:

    ```
    # esxcli storage nmp satp rule add -V <vendor_name> -P VMW_PSP_RR -s VMW_SATP_ALUA -o "enable_action_OnRetryErrors
     reset_on_attempted_reserve" -c tpgs_on -O bytes=<1024or2048>
    ```

    где `<vendor_name>` – имя вендора СХД (имя можно увидеть, выполнив на СХД команду `$ rdcli -V`, в конце строки вывода); `<1024or2048>` – значение bytes.

12. Обнаружение LUN, отданных по FC QLogic.

    Информация на сайте VMware: *kb.vmware.com*.

Если LUN не отображаются при сканировании устройств через ESXi GUI, попробуйте один из способов ниже:

- Проверьте правила маскирования в ПО RAIDIX.
- Просканируйте устройства через ESXi CLI:

```
# esxcli storage core adapter rescan --all
```

- Выполните принудительное перелогирование (FLOGI) на каждом порту используемых в ESXi адаптеров:

```
# esxcli storage san fc reset -A vmhba<X>
```

Посмотреть список адаптеров можно с помощью команды

```
# esxcli storage core adapter device list
```

- Перезагрузите ESXi-хост.

Общие рекомендации

1. Обработка ситуаций с уменьшением производительности в DC.

   Если ВМ на ESXi выполняет I/O медленно или с прерываниями, и при этом на DC-системе RAIDIX отсутствует синхронизация кэшей между контроллерами (например, после перезагрузки узла), выполните следующие действия:

   a. Проверьте логи ESXi в `/var/log/vmkernel.log` на наличие сообщений

   ```
   Device <eui.###> performance has deteriorated. I/O latency increased from average value of <val1> to <val2>
   ```

   b. Если собщения присутствуют, отключите функцию «Сквозная запись без синхронизации» на СХД RAIDIX.

2. Обработка переполнения очереди на канале транспорта.

   Включите адаптивную глубину очереди на ESXi, если в логах ESXi в `/var/log/vmkernel.log` есть строки

   - для iSCSI:

   ```
   ScsiDeviceIO: 4124: Cmd(0x45d90ed478c8) 0x28, CmdSN 0x800e000a from world 2120104 to dev "eui.3034343446303039"
    failed H:0x0 D:0x28 P:0x0
   ```

   где после «failed» код ответа «D:0x28» означает, что операция отклонена, очередь операций к выполнению полностью переполнена (Device Status - "TASK_SET_FULL").

   - для FC:

   ```
   vmhba5(31:0.1): C0:T0:L1 - FCP command status: 0x15-0x828 (0x0) portid=0000e8 oxid=0x171 cdb=2a00f2 len=32768
    rspInfo=0x0 resid=0x8000 fwResid=0x8000 host status = 0x0 device status = 0x28
   ```

   где для «FCP command status:» значение «0x828» означает, что операция отклонена, очередь операций к выполнению полностью переполнена (Device Status - "QUEUE FULL").

   Чтобы включить адаптивную глубину очереди, выполните

   ```
   # esxcfg-advcfg -s 32 /Disk/QFullSampleSize
   # esxcfg-advcfg -s 16 /Disk/QFullThreshold
   ```

3. ESXi после корректного удаления LUN и создания нового может продолжить определять новый LUN как удалённый, что влечёт за собой повреждение данных.

   Проблема возникает из-за неправильной работы механизма PDL в некоторых версиях ESXi. Для избежания проблемы необходимо вручную выполнять рескан путей на адаптере при любом изменении LUN на системе (подробнее на *сайте VMware*).

Если проблема уже возникла:

- Отмонтируйте datastore и снимите с регистрации ВМ, которые использовали LUN.
- Выполните рескан адаптеров:

```
# esxcli storage core adapter rescan --all
```

Если проблема сохраняется после рескана, перезагрузите адаптер, на котором отображался удалённый LUN:

```
# esxcli storage san fc reset -A vmhbaX
```

4. При удалении RAID без нагрузки, LUN продолжают отображаться на ESXi.

   Проблема возникает при использовании ESXi версии выше 7.0.3g, когда удалённые LUN были обнаружены ESXi или были добавлены в datastore или ВМ, где сохранилась информация о них (подробнее на *сайте VMware*).

   При возникновении проблемы удалите информацию о LUN:

   - Перемонтируйте datastore и снимите с регистрации ВМ, которые использовали LUN.
   - Перезагрузите адаптер, на котором отображался удалённый LUN:

     ```
     # esxcli storage san fc reset -A vmhbaX
     ```

   - Выполните рескан адаптеров:

     ```
     # esxcli storage core adapter rescan --all
     ```

   - Проверьте, что пути удалённого LUN не отображаются:

     ```
     # esxcfg-mpath -b
     ```

   Для избежания проблемы используйте на инициаторе конфигурацию Active-Passive SATP вместо ALUA:

   - Удалите правило ALUA:

     ```
     # esxcli storage nmp satp rule remove -V <vendor_name> -P VMW_PSP_RR -s VMW_SATP_ALUA
     ```

   - Добавьте правило Active-Passive SATP:

     ```
     # esxcli storage nmp satp rule add -V <vendor_name> -P VMW_PSP_RR -s VMW_SATP_DEFAULT_AP -c tpgs_on
     ```

5. На ESXi версий 8.0, 8.0 U1, 8.0 U2 возникают проблемы с запуском ВМ на базе Linux версии 5.18 и выше.

   Проблемы актуальны для ВМ с технологией *Fault Tolerance* и включённой поддержкой *VMCI DMA datagrams*.

   Для избежания проблем отключите поддержку *VMCI DMA datagrams* на ВМ (подробнее см. *на сайте Broadcom*). Отключение поддержки доступно через:

   - ESXi-хост;
   - vCenter.

   На ESXi-хосте:

   a. В конфигурационном файле ВМ (*.vmx) добавьте строку:

      ```
      vmci.dmaDatagramSupport = FALSE
      ```

   b. Обновите конфигурационный файл.

В интерфейсе vCenter:

В разделе **Advanced Parameters** ВМ добавьте параметр **vmci.dmaDatagramSupport** со значением **FALSE** и сохраните изменения.

6. Если после замены компонентов, смены имени таргета, обновления драйверов или замены кабелей ESXi перестал видеть часть Datastore, но LUN, на котором расположен Datastore, доступен, выполните следующие действия:

   a. Проверьте логи ESXi `/var/vmkernel.log` на наличие сообщений типа:

   ```
   vmkwarning: cpu20:2100869)WARNING: VMKAPICore: 1824: unable to validate header
   LVM: 8445: Device eui.64784a3271307365:1 detected to be a snapshot:
   LVM: 8452: queried disk ID: <type 1, len 12, lun 3, devType 0, scsi 0, h(id) 42832082591475764905>
   ```

   b. Проверьте, видны ли сигнатуры несмонтированных LUN:

   ```
   # esxcfg-volume -l
   ```

   c. Смонтируйте LUN одним из способов:

   - Для временного монтирования, только в текущей сессии и до следующего перезапуска ESXi:

     ```
     # esxcfg-volume -M <UUID/Name>
     ```

   - Для постоянного монтирования до следующего перезапуска (Non-persistent Mode):

     ```
     # esxcli storage vmfs snapshot mount -n -l  <Datastore_name>
     ```

   - Для постоянного монтирования с сохранением после перезагрузки (Persistent Mode):

     ```
     # esxcli storage vmfs snapshot mount -l  <Datastore_name>
     ```

     Сигнатура VMFS не изменяется.

   - Для монтирования с изменением сигнатуры VMFS (Resignature):

     ```
     # esxcli storage vmfs snapshot resignature -l  <Datastore_name>
     ```

     Или используйте UUID:

     ```
     # esxcli storage vmfs snapshot resignature -u  <Datastore_UUID>
     ```

     VMware рекомендует менять сигнатуру LUN во избежание проблем в будущем. Однако смена сигнатуры может привести к ситуации, когда в системе один LUN ассоциируется с двумя сигнатурами. Данные при этом остаются целостными (подробнее см. *на сайте Broadcom*).

7. Если на ESXi-хосте появляются логи об ошибках миграции ресурсов и резервации файлов, проверьте наличие функции vMotion на сетевом интерфейсе, используемом для блочного доступа к СХД, и видимость на этом интерфейсе соседнего ESXi-хоста.

   Пример логов:

   ```
   2025-09-26T13:29:02.573Z Wa(180) vmkwarning: cpu46:2189032)WARNING: DLX: 4551: Sleep and recheck lock completes
    with POLL_NO_LOCK_CHANGE_WAIT on LUN_6, no lock change has happened, status: Not found
   2025-09-26T13:35:50.279Z Wa(180) vmkwarning: cpu33:2190036)WARNING: Swap: 3691: Failed to initialize swap file
    '/vmfs/volumes/68cb1bee-dbb56395-7b78-bceca0eb6f0c/THICK_SEQ_4/vmx-THICK_SEQ_4-a8078cda2e14bdf7fc2f1c30b08544b20eb
   e583f3872d827a3cd2f878c0c5952-2.vswp' : B
   2025-09-26T13:35:53.698Z Wa(180) vmkwarning: cpu27:2189673)WARNING: DLX: 4551: Sleep and recheck lock completes
    with POLL_NO_LOCK_CHANGE_WAIT on LUN_6, no lock change has happened, status: Not found
   2025-09-26T13:40:40.667Z Wa(180) vmkwarning: cpu17:2190815)WARNING: DLX: 4551: Sleep and recheck lock completes
    with POLL_NO_LOCK_CHANGE_WAIT on LUN_6, no lock change has happened, status: Not found
   ```

Дополнительно проверьте логи на наличие подобных сообщений:

```
)WARNING: VMotionUtil: 5261: 9182711570002500502 S: stream thread failed to connect to the remote host <4.4.4.7>:
 The ESX hosts failed to connect over the VMotion network
WARNING: Migrate: 257: 9182711570002500502 S: Failed: The ESX hosts failed to connect over the VMotion network
 (0xbad010b) @0x4200334d67b3
WARNING: Migrate: 7074: 9182711570002500502 S: Migration considered a failure by the VMX.  It is most likely a
 timeout, but check the VMX log for the true error.
WARNING: MigrateNet: 1953: 9182711570067514772 S: failed to connect to remote host <4.4.4.7> from host <4.4.4.5>:
 Timeout.
WARNING: VMotionUtil: 5261: 9182711570067514772 S: stream thread failed to connect to the remote host <4.4.4.7>:
 The ESX hosts failed to connect over the VMotion network
WARNING: Migrate: 257: 9182711570067514772 S: Failed: The ESX hosts failed to connect over the VMotion network
 (0xbad010b) @0x4200334d67b3
WARNING: Migrate: 7074: 9182711570067514772 S: Migration considered a failure by the VMX.  It is most likely a
 timeout, but check the VMX log for the true error.
WARNING: VMotion: 6787: 9182711572658739042 D: Opening swap file took 78ms. Status: Success
```

В этом примере адрес 4.4.4.7 второго ESXi-хоста виден первому через коммутатор, который используется для блочного доступа к СХД.

Функция vMotion требует для своей работы выделенного канала между ESXi-хостами. Не используйте в качестве канала для vMotion канал для блочного доступа к СХД.

Чтобы проверить функцию vMotion на интерфейсе:

a. На каждом ESXi-хосте через vCenter в свойствах vSwitch выберите коммутатор, используемый для блочного доступа к СХД.
b. В свойствах коммутатора убедитесь, что vMotion выключена на интерфейсе, используемом для блочного доступа к СХД.

8. Для полной производительности рекомендуем использовать "толстый" тип диска ВМ (англ. «Thick provisioned») с полным занулением (англ. «Eager zeroed»).

   При использовании «тонких» дисков (англ. «Thin provisioned») может быть потеря производительности при первичном обращении к блоку диска. Аналогичная потеря может быть при использовании "ленивого" зануление (англ. «Lazy zeroed»).

Windows

Специфика работы Windows

При настройке блочного доступа к Windows учитывайте следующие особенности работы Windows:

- Рекомендуем всегда включать синхронизацию PR, если в качестве инициаторов используются кластеры Windows или Hyper-V.

  Подробнее о синхронизации Persistent reservation в главе Синхронизация Persistent Reservations *(стр.)* или документе «Руководство администратора RAIDIX 5.3.1».

Установка MPIO

> Настройка описана на примере Windows Server 2022. На других версиях Windows Server настройка аналогична.

Для работы с multipath-устройствами на Windows Server установите «Multipath I/O» (MPIO):

1. Откройте **Server Manager**.

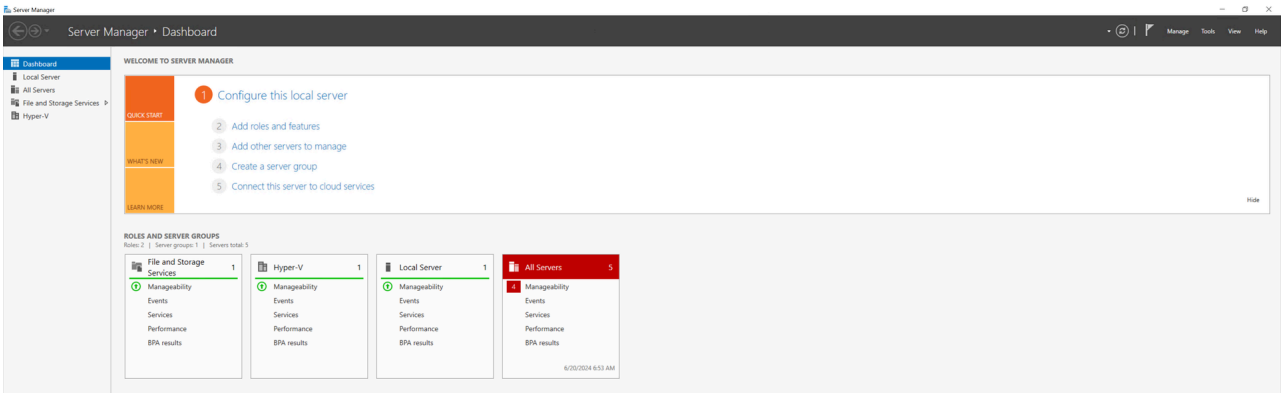

Рис. 1. Окно Windows Server Manager

2. Во вкладке **Dashboards > QUICK START** кликните **Add roles and features**.
3. В открывшемся окне **Add Roles and Features Wizard** кликните **Next >**.
4. На шаге **Installation Type** выберите **Role-based or feature-based installation** и кликните **Next >**.

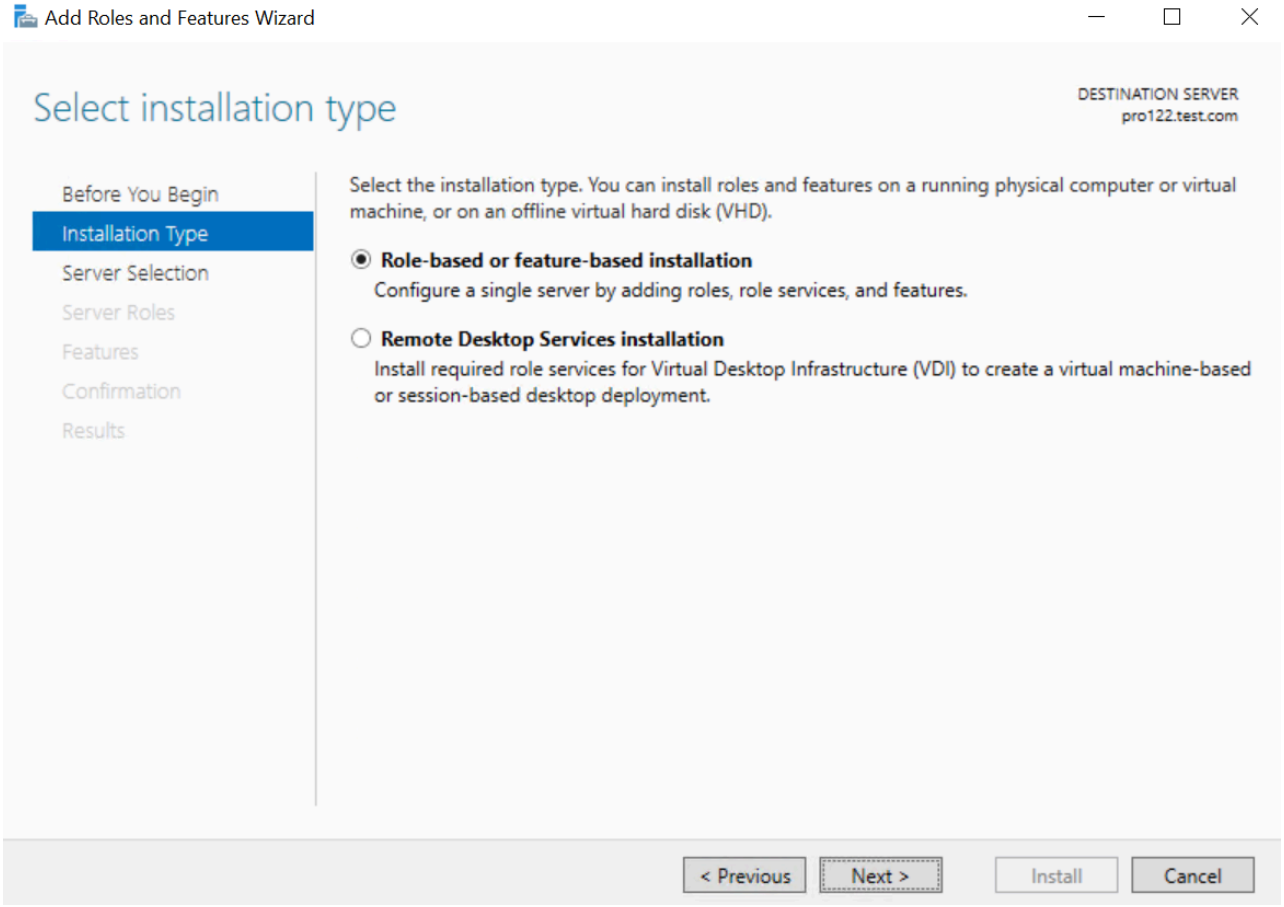

Рис. 2. Шаг Installation Type

5. На шаге **Server Selection** выберите имя настраиваемого сервера и кликните **Next >**.

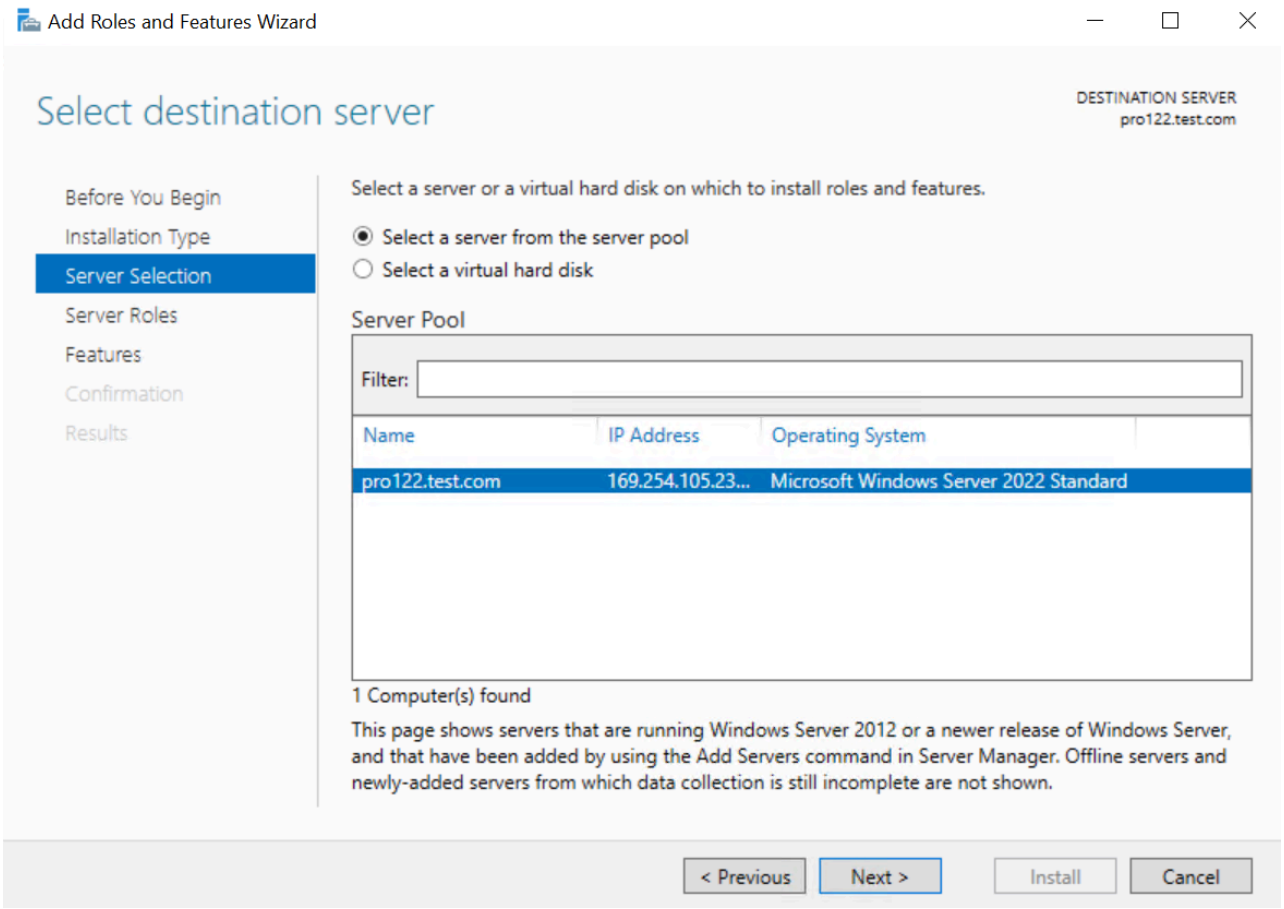

Рис. 3. Шаг Server Selection - имя сервера

6. На шаге **Server Roles** выберите **File and Storage Services** и кликните **Next >**.

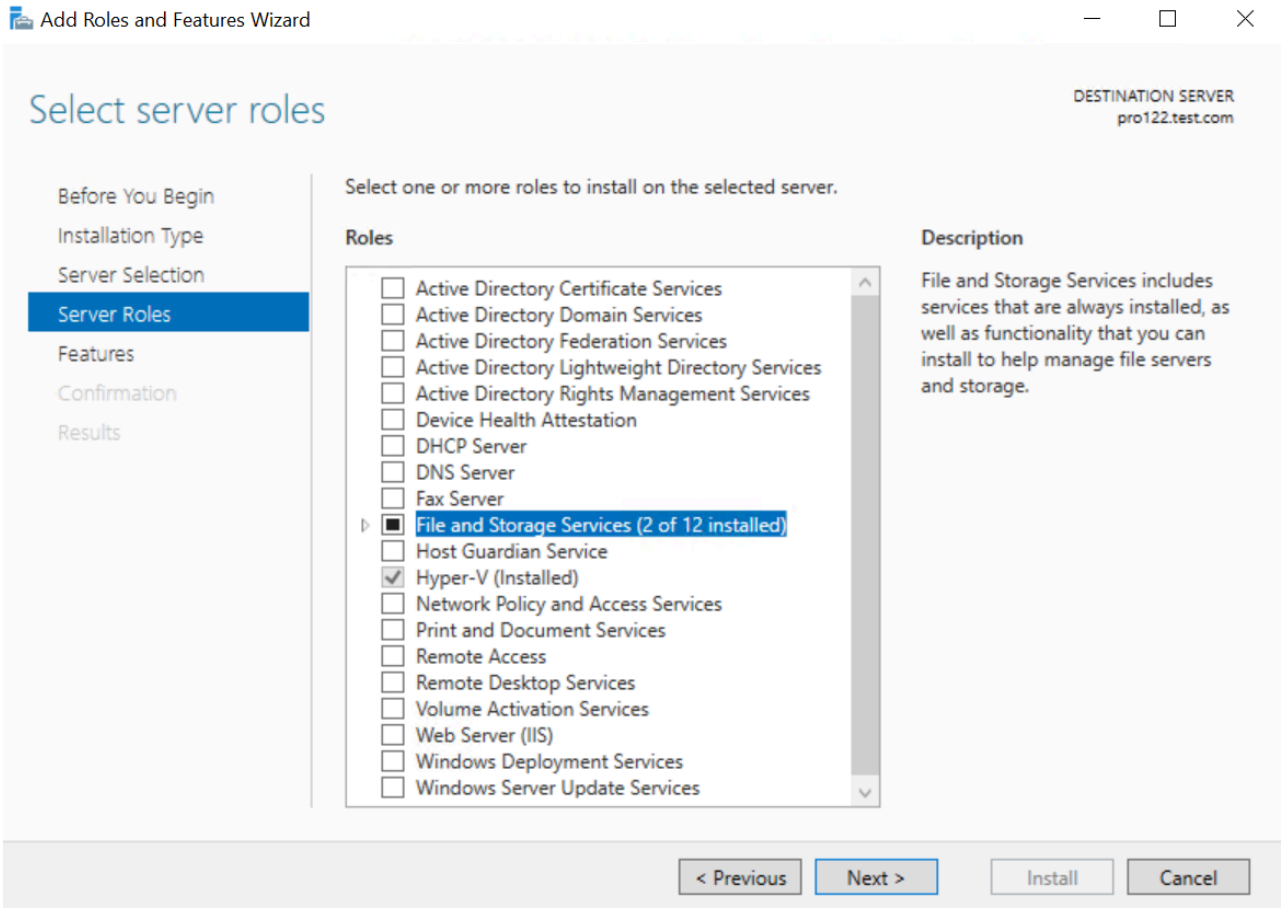

Рис. 4. Шаг Server Roles - File and Storage Services

7. На шаге **Select Features** выберите **Multipath I/O** и кликните **Install**.

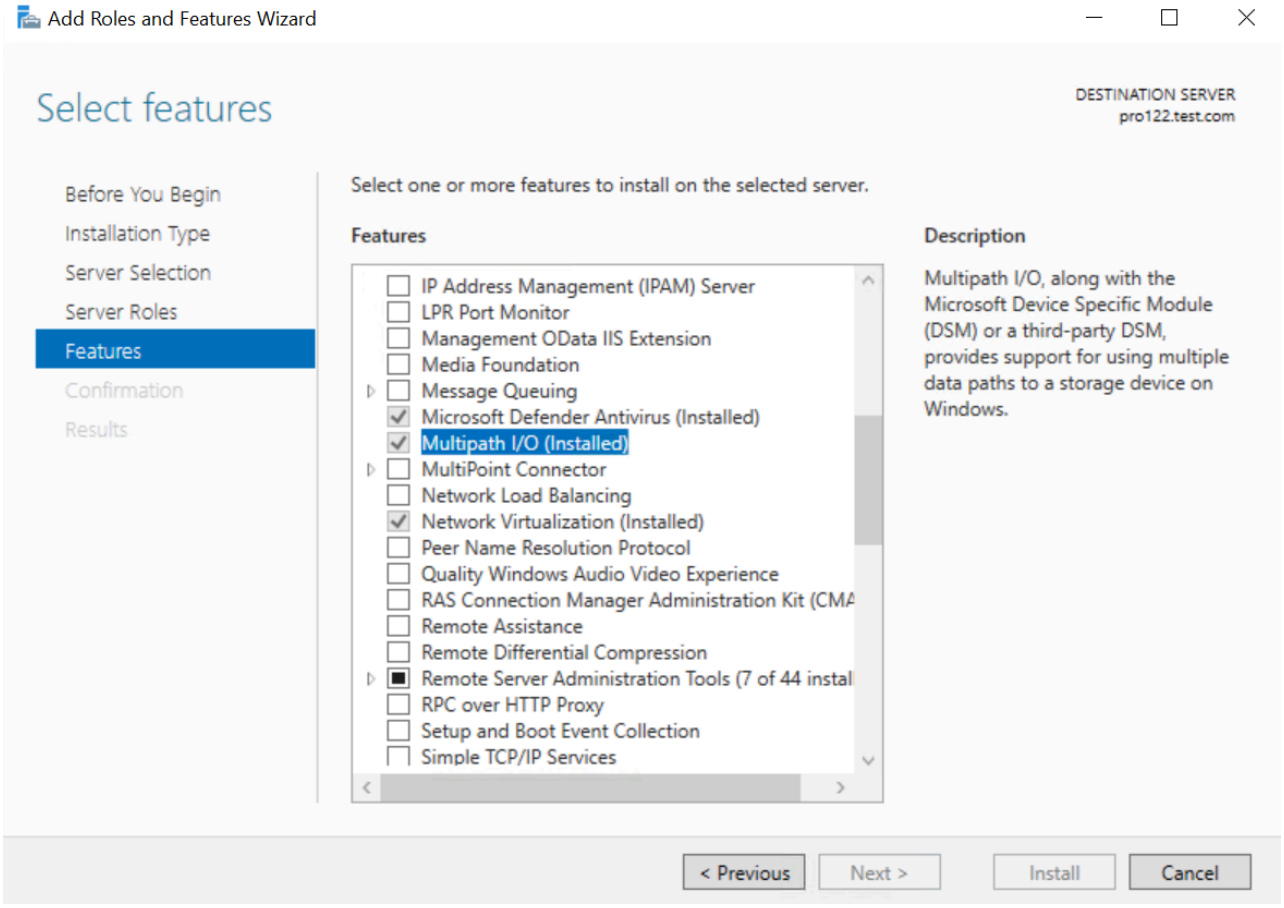

Рис. 5. Шаг Server Roles - Multipath I/O

Настройка FC на Windows Server

> Настройка описана на примере Windows Server 2022. На других версиях Windows Server настройка аналогична.

Чтобы добавить диски и настроить MPIO:

1. Настройка хоста и сети:
   a. Подключите сервер с установленной ОС Windows Server к системе хранения данных RAIDIX.
   b. Проверьте, что установлен драйвер для адаптера.

2. Добавление дисков:

a. Зайдите в панель управления MPIO устройствами (**Start > Administrative Tools > MPIO**).

b. Перед добавлением новых устройств убедитесь, что ранее созданные неиспользуемые MPIO-устройства (не связанные с существующими разделами LUN) удалены. Для этого откройте вкладку **MPIO Devices** и при наличии здесь ранее созданных устройств RAIDIX, удалите их и перезагрузите систему.

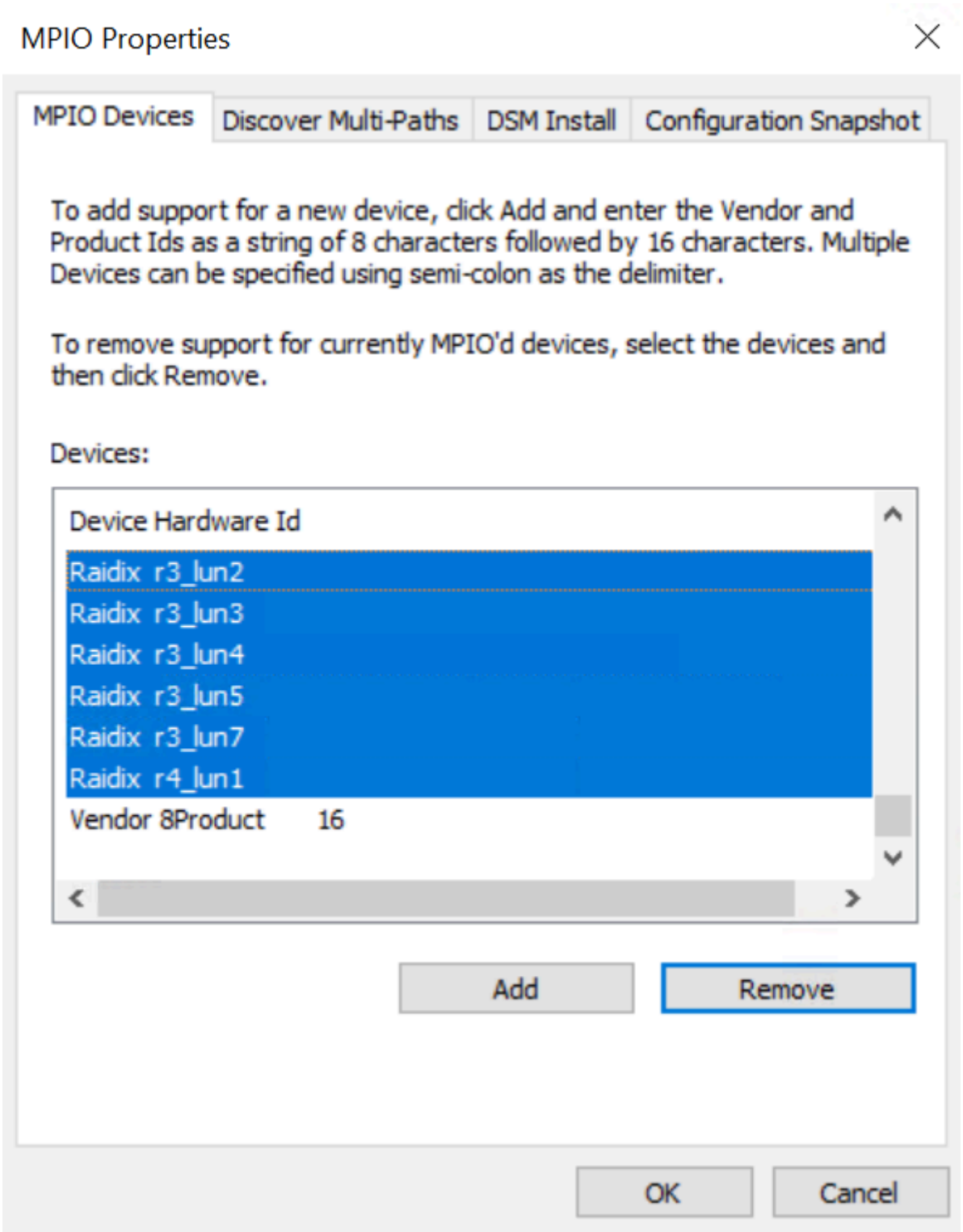

Рис. 6. Ранее добавленный RAIDIX LUN в списке устройств MPIO

c. Откройте вкладку **Discover Multi-Paths**.

d. При настройке подключения с использованием адаптера Fibre Channel QLogic 16Gb на СХД и хосте может возникнуть задержка отображения LUN 15 минут.

В разделе **SPC-3 compliant** убедитесь, что в списке устройств присутствуют добавляемые, и кликните **Add**.

Закройте окно **MPIO Properties**, кликнув **OK**.

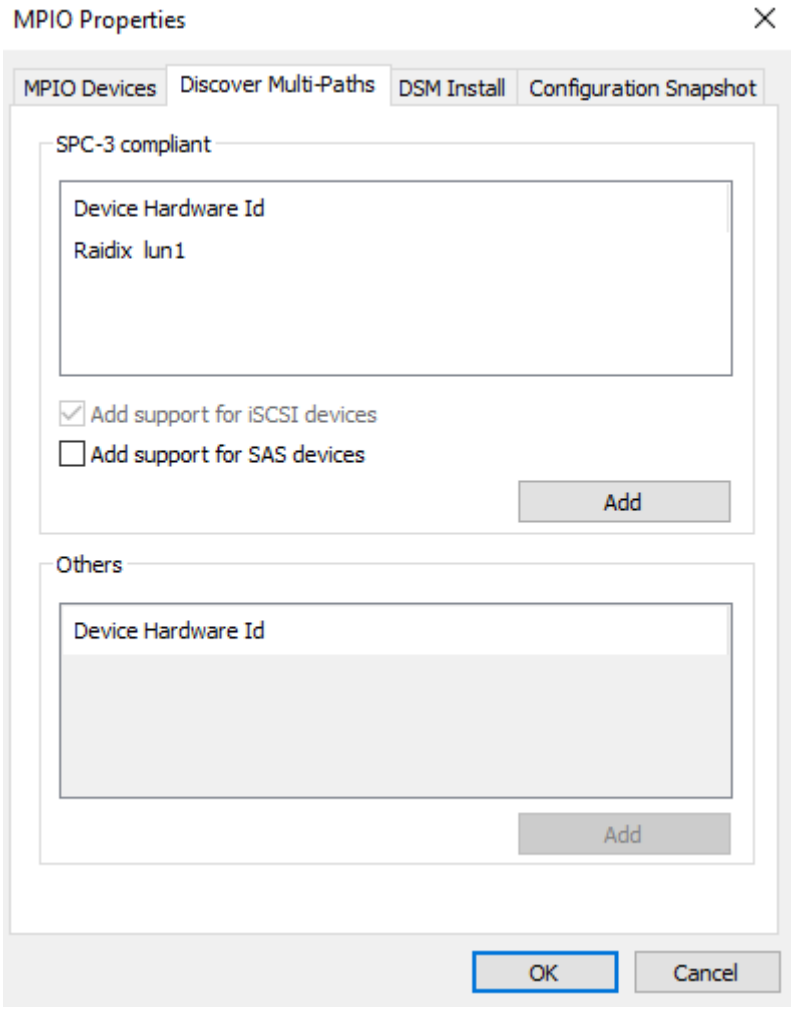

Рис. 7. Окно MPIO-устройств. Добавление устройства

3. Настройка политики MPIO.

   Для каждого добавленного устройства:

a. Откройте окно **Device Manager**, в списке **Disk drives** для добавленного устройства в контекстном меню выберите **Properties**.
b. В открывшемся окне выберите вкладку **MPIO**.
c. В строке **Select the MPIO policy** выберите **Round Robin With Subset**. Кликните **OK**.

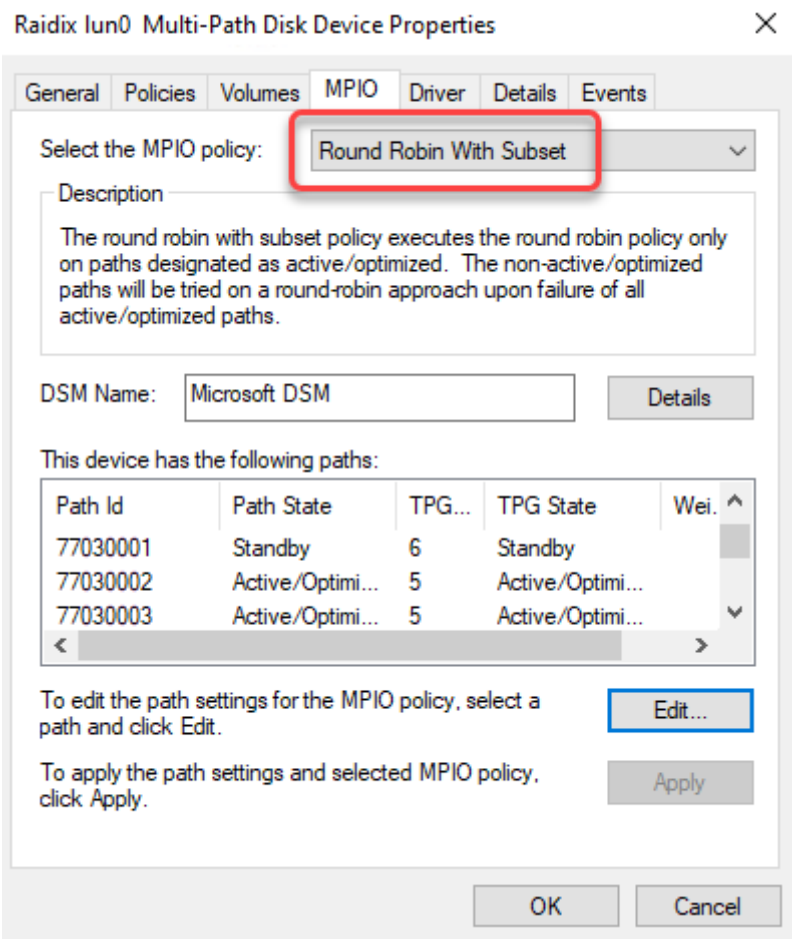

Рис. 8. Определение политики MPIO. Выбрано значение Round Robin With Subset

4. Настройка параметров сканирования путей:

> Значения параметров выбираются в зависимости от системы (см. на docs.microsoft-.com *параметры MPIO* и *таймаут дисков*).

a. Откройте PowerShell (`cmd` # `powershell`).
b. Задайте значения для следующих параметров:
   i. Retry Count.
   ii. PDO Remove Period.
   iii. Retry Interval.
   iv. TimeOut Value.

Например, так:

```
> Set-MPIOSetting -NewRetryCount 5 -NewPDORemovePeriod 60 -NewRetryInterval 10 -NewDiskTimeout 90
```

Настройка iSCSI на Windows Server

> Настройка описана на примере Windows Server 2022. На других версиях Windows Server настройка аналогична.

Чтобы добавить диски и настроить MPIO:

1. Настройка хоста и сети:
   a. Подключите сервер с установленной ОС Windows Server к системе хранения данных RAIDIX.
   b. Проверьте, что установлен драйвер для адаптера.

2. Подключение к таргету:
   a. Откройте окно **Server Manager**.
   b. В меню **Tools** выберите пункт **iSCSI Initiator**.

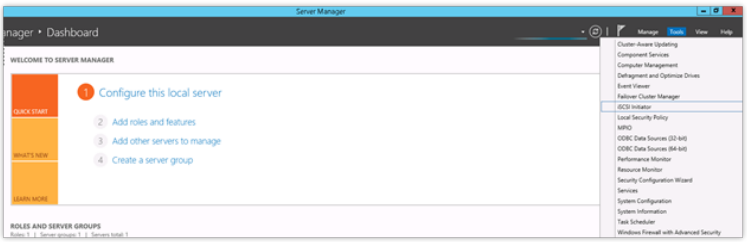

Рис. 9. Server Manager

   c. В открывшемся окне **iSCSI Initiator** перейдите во вкладку **Discovery**. Кликните **Discover Portal**.

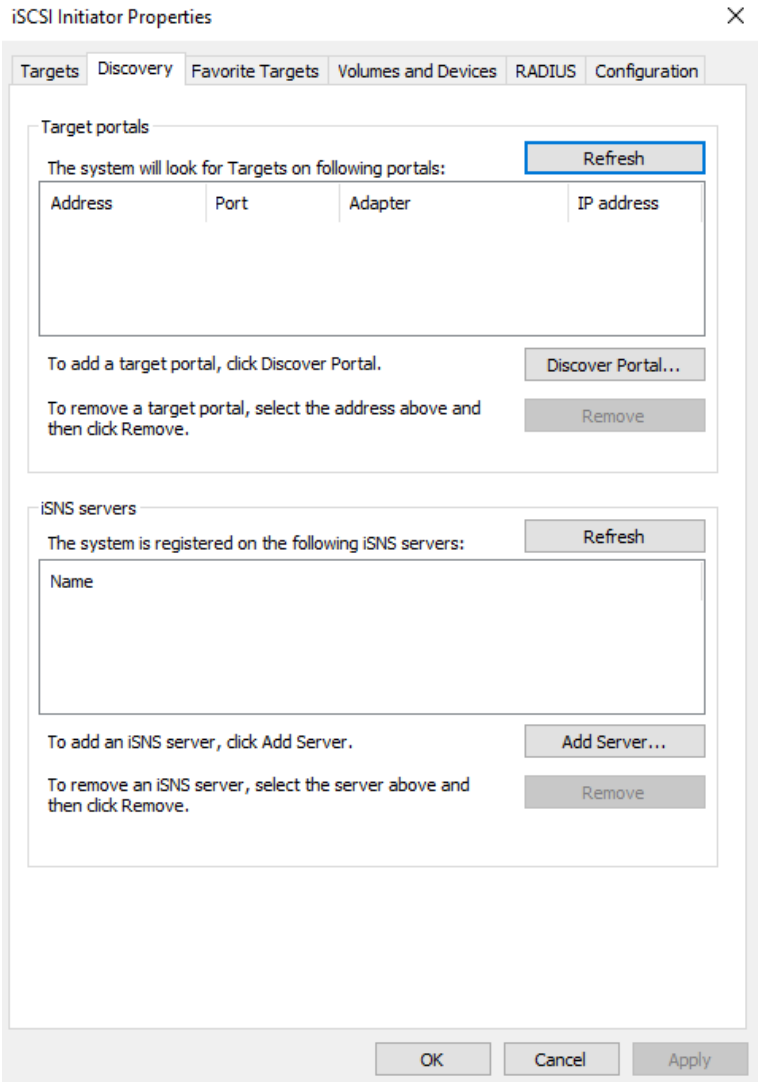

Рис. 10. Окно Initiator Properties

d. В открывшемся окне **Discover Target Portal** введите IP-адрес СХД, который будет использоваться для взаимодействия с таргетом iSCSI (для DC-системы – IP-адрес с первого контроллера) и кликните **OK**. При настройке подключения к DC-системе снова кликните **Discover Portal**, введите IP-адрес со второго контроллера и кликните **OK**. Подробнее о IP-адресах СХД для взаимодействия с таргетом в документе «Руководство администратора RAIDIX 5.3.1», глава «iSCSI».

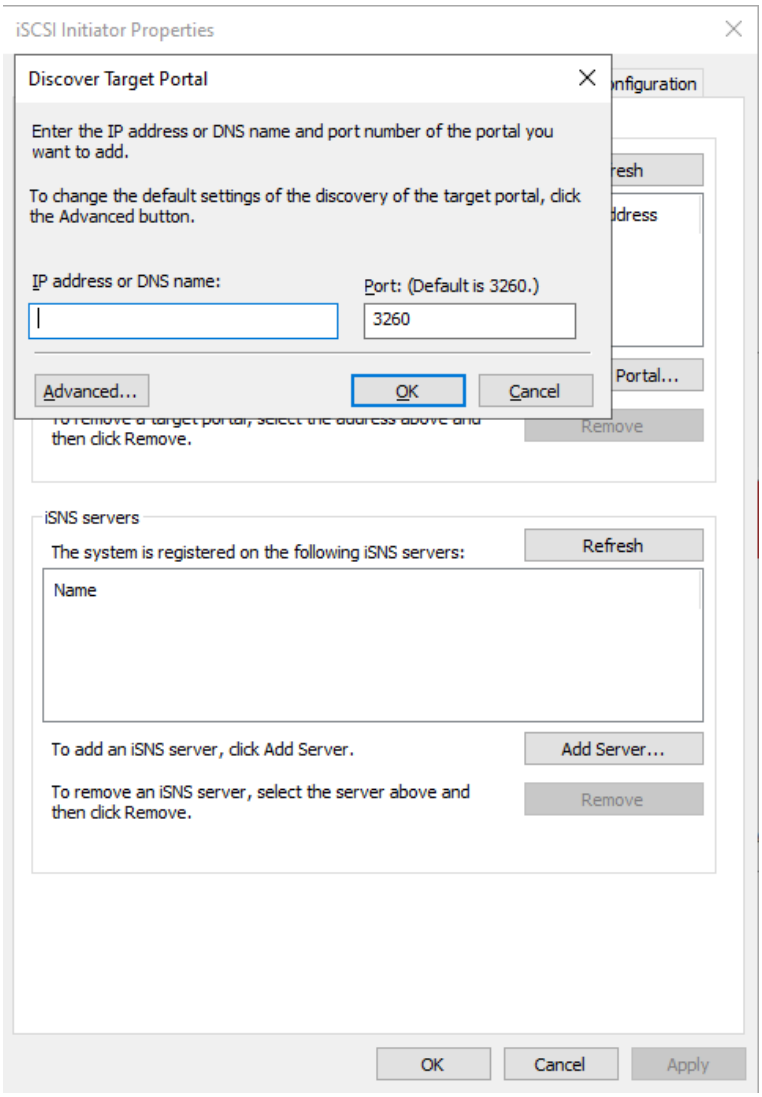

Рис. 11. Поиск таргета

e. Во вкладке **Targets** в поле **Discovered targets** кликните на обнаруженный iSCSI-таргет и кликните **Connect**.

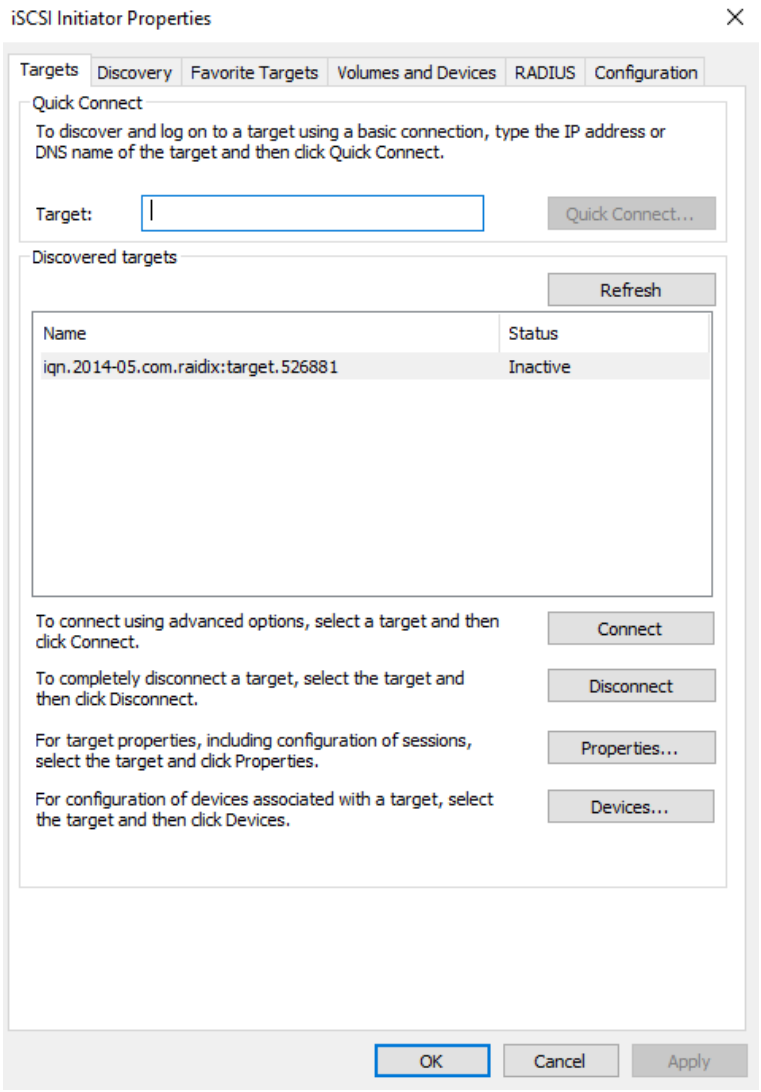

Рис. 12. Обнаруженный iSCSI-таргет

f. В открывшемся окне выберите **Enable Multipath** и кликните **Advanced…**.

g. В открывшемся окне **Advanced Settings** в поле **Target Portal IP** выберите IP-адрес СХД (в DC-режиме – первого контроллера) и кликните **OK**. При работе в DC-режиме снова кликните **Advanced…**, выберите IP-адрес второго контроллера и кликните **OK**.

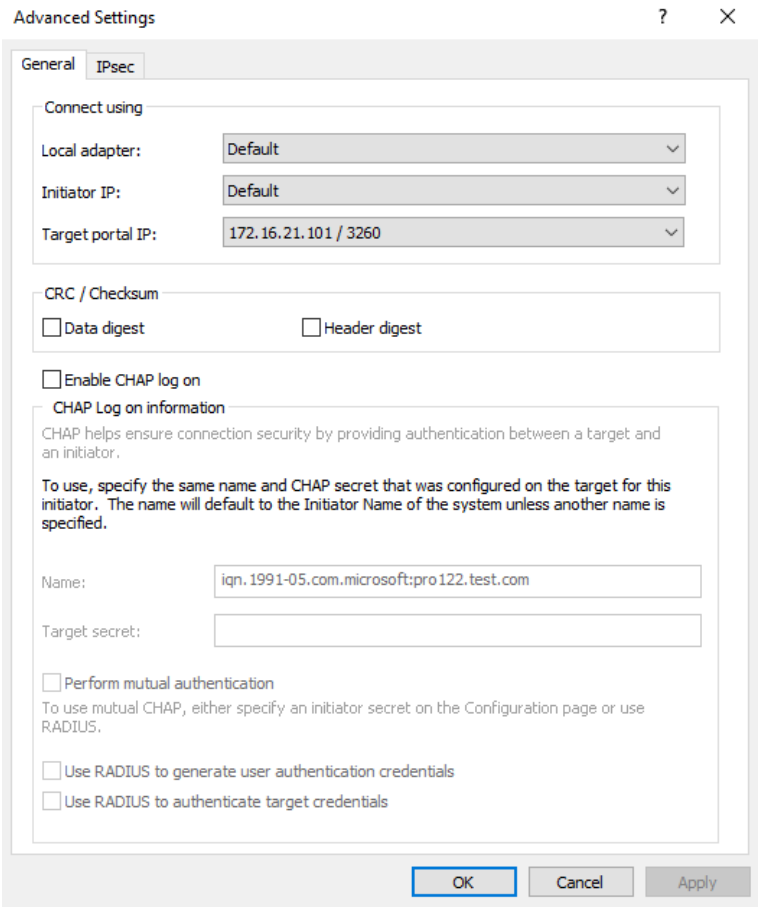

Рис. 13. Окно Advanced Settings

Для улучшения производительности рекомендуем создавать 3 сессии для каждого соединения.

Чтобы проверить сессии, в окне **iSCSI Initiator Properties** во вкладке **Targets** кликните **Properties**.

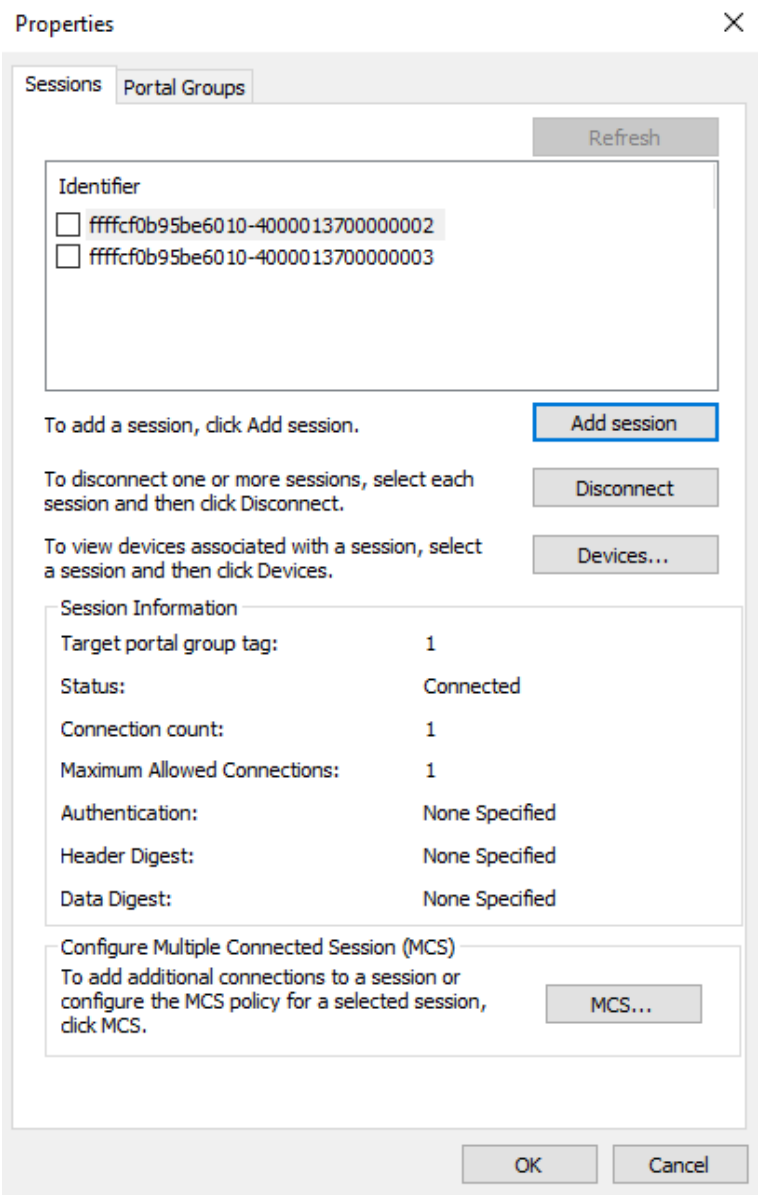

Рис. 14. Просмотр сессий

3. Добавление дисков:

a. Откройте панель управления MPIO-устройствами (**Start > Administrative Tools > MPIO**).

b. Откройте вкладку **Discover Multi-Paths**. Включите **Add Support for iSCSI Devices** и кликните **Add**.

После настройки новые разделы будут автоматически пробрасываться на инициатор, MPIO-устройство будет собираться автоматически.

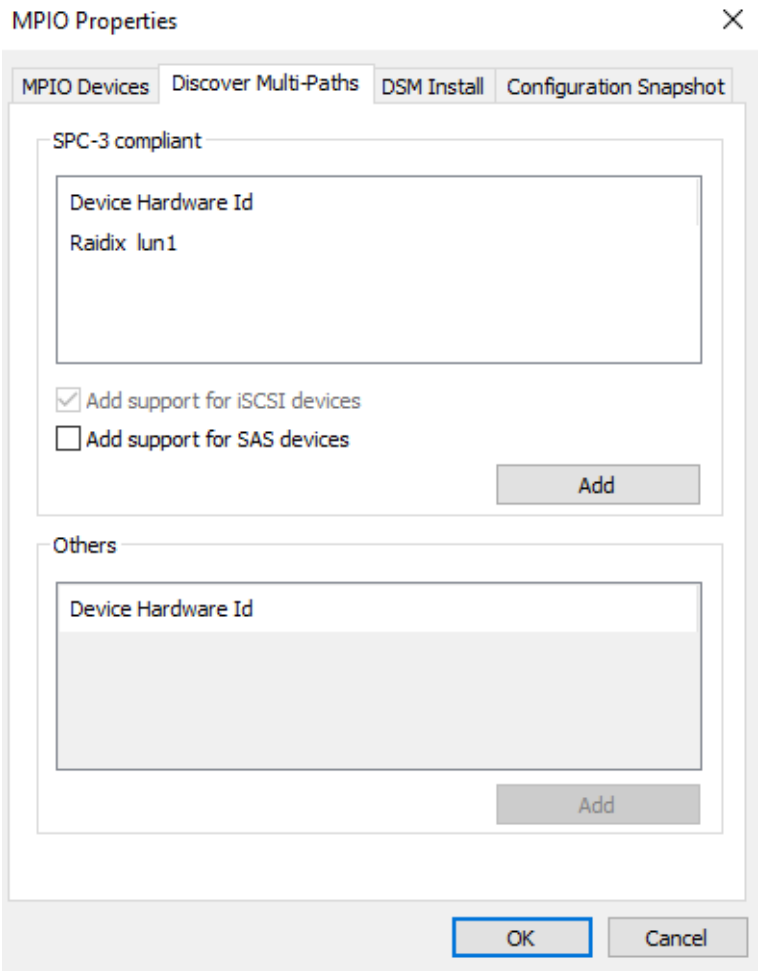

Рис. 15. Настройка multipath

4. Настройка политики MPIO.

Для каждого добавленного устройства:

a. Откройте окно **Device Manager**, в списке **Disk drives** для добавленного устройства в контекстном меню выберите **Properties**.
b. В открывшемся окне выберите вкладку **MPIO**.
c. В строке **Select the MPIO policy** выберите **Round Robin With Subset**. Кликните **OK**.

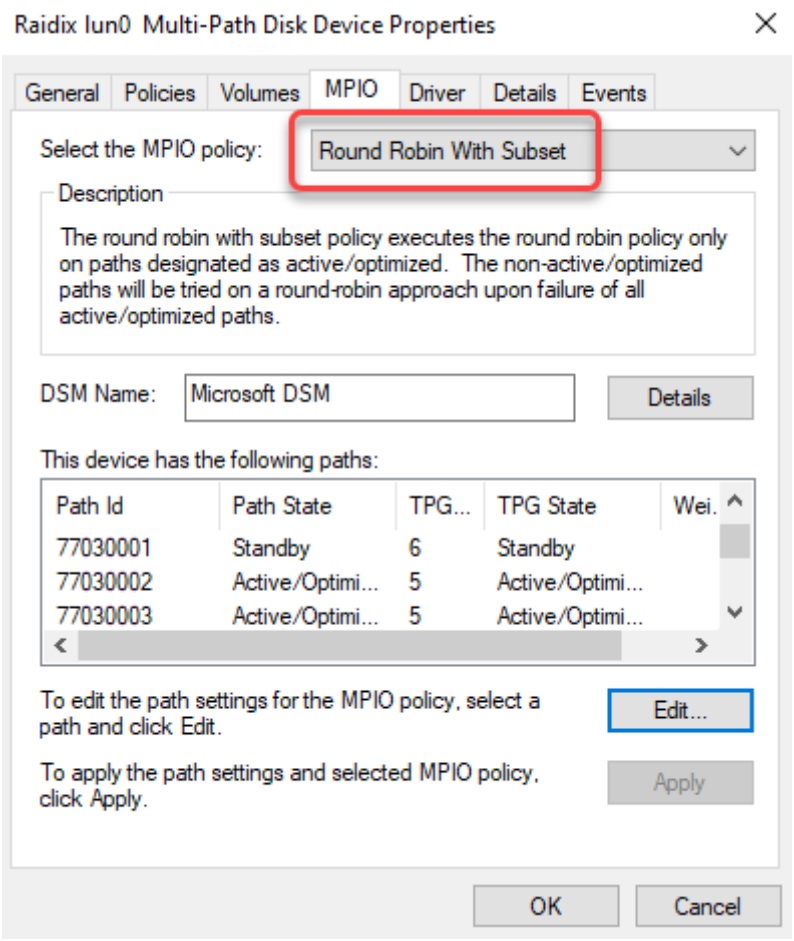

Рис. 16. Определение политики MPIO. Выбрано значение Round Robin With Subset

5. Настройка параметров сканирования путей:

> Значения параметров выбираются в зависимости от системы (см. на docs.microsoft-.com *параметры MPIO* и *таймаут дисков*).

a. Откройте PowerShell (`cmd` # `powershell`).
b. Задайте значения для следующих параметров:
   i. Retry Count.
   ii. PDO Remove Period.
   iii. Retry Interval.
   iv. TimeOut Value.

Например, так:

```
> Set-MPIOSetting -NewRetryCount 5 -NewPDORemovePeriod 60 -NewRetryInterval 10 -NewDiskTimeout 90
```

Отключение от iSCSI-таргета на Windows Server

В связи с особенностями работы Windows Server, для корректного отключения iSCSI-таргета выполните следующее:

> Отключение описано на примере Windows Server 2022. На других версиях Windows Server отключение аналогично.

1. Зайдите в меню **Start** и перейдите в **Disk Management**.
2. Правой кнопкой мыши кликните «Disk X» и выберите **Offline**. Disk X – это RAIDIX LUN.
3. Повторите шаг 2 для всех LUN.
4. Откройте **iSCSI Initiator Properties**, выберите таргет и кликните **Disconnect**.

Если LUN до этого был под нагрузкой, то после клика **Disconnect** отключение может произойти не сразу, а по завершении записи из кэша Windows на LUN.

zVirt

Доступные для zVirt блочные протоколы:

- iSCSI;
- FC.

Инструкции по настройке подключения см. на *официальном сайте zVirt*.

Рекомендации Рэйдикс по настройке zVirt см. в *Специфика работы zVirt (стр. 37)*. Инструкцию по настройке multipath – в главе *Настройка multipath на zVirt (стр. 38)*.

Специфика работы zVirt

> При настройке zVirt ознакомьтесь с требованиями и рекомендациями по настройке от поставщика СХД и на официальном сайте zVirt https://www.orionsoft.ru/zvirt.

При настройке блочного доступа к zVirt учитывайте следующие особенности работы zVirt:

- zVirt работает только с размером блока 512 Б. Создавайте LUN (в случае ERA RAID - и RAID) с этим размером блока.
- Не рекомендуем устанавливать ОС на напрямую проброшенный в ВМ LUN.
- Минимальный размер LUN для подключения к zVirt (в качестве домена хранения) – 10 GiB.

Фильтр дисков через blacklist

Если на хосте с zVirt есть локальные диски помимо системного, *перед настройкой multipath для томов с СХД* добавьте такие диски в blacklist (если хост – часть кластерной системы, то на каждом хосте этой системы):

1. Проверьте список дисков:

```
# lsblk
```

2. Создайте новый файл с любым именем в каталоге `/etc/multipath/conf.d`.
3. В созданный файл добавьте секцию `blacklist`, а в секцию – названия блочных устройств.

   Пример файла с добавленными устройствами */dev/sda*, */dev/sdb*, */dev/nvme0n1*, */dev/nvme1n1*:

```
blacklist {
  devnode "^sd[a-b]"
  devnode "nvme0n1"
  devnode "nvme1n1"
}
```

4. Перезагрузите службу multipath:

```
# systemctl reload multipathd.service
```

5. Убедитесь, что добавленные диски не собираются в multipath-устройста, любой из команд:

```
# lsblk
```

```
# multipath -l
```

Настройка multipath на zVirt

Чтобы настроить multipath на zVirt, выполните (в случае кластерной системы - на каждом контроллере):

> Не меняйте оригинальный `/etc/multipath.conf`.

1. Создайте файл `/etc/multipath/conf.d/raidix-multipath.conf` следующего содержания:

```
defaults {
    fast_io_fail_tmo        5
    features                "0"
    no_path_retry           10
    path_checker            tur
    polling_interval        5
    prio                    alua
}

devices {
    device {
            #For initiators with scsi_dh_alua
            #hardware_handler       "1 alua"
            detect_checker          no
            detect_prio             no
            failback                immediate
            no_path_retry           12
            path_checker            "tur"
            path_grouping_policy    "group_by_prio"
            path_selector           "round-robin 0"
            prio                    "alua"
            product                 ".*"
            rr_min_io               100
            rr_weight               "uniform"
            vendor                  "Raidix"
    }
}
```

2. > Не перезапускайте (restart) службу `multipathd`.

   Примените настройку multipath:

```
# systemctl reload multipathd
```

ROSA Virtualization

Доступные для ROSA Virtualization блочные протоколы:

- iSCSI;
- FC.

Инструкции по настройке подключения см. в *официальной документации ROSA Virtualization*.

Рекомендации Рэйдикс по настройке ROSA Virtualization см. в *Специфика работы ROSA Virtualization (стр. 39)*. Инструкцию по настройке multipath – в главе *Настройка multipath на ROSA Virtualization (стр. 39)*.

Специфика работы ROSA Virtualization

При настройке ROSA Virtualization ознакомьтесь с требованиями и рекомендациями по настройке от поставщика СХД и в *официальной документации ROSA Virtualization*.

При настройке блочного доступа учитывайте следующие особенности работы ROSA Virtualization:

- ROSA Virtualization работает только с размером блока 512 Б. Создавайте LUN (в случае ERA RAID - и RAID) с этим размером блока.
- Минимальный размер LUN для подключения к ROSA Virtualization (в качестве домена хранения) – 10 GiB.

Фильтр дисков через blacklist

Если на системе с ROSA Virtualization есть диски помимо системного, *перед настройкой multipath* добавьте такие диски в blacklist (на каждом контроллере для кластерных систем):

1. Проверьте список дисков:

   ```
   # lsscsi
   ```

2. Определите WWID дисков, для каждого диска выполнив

   ```
   # udevadm info --attribute-walk --name=/dev/sd<letter> | grep wwid
   ```

   где

   `/dev/sd<letter>` – имя диска из списка.

3. Добавьте WWID дисков в файл `/etc/multipath/conf.d/vdsm_blacklist.conf`.

   Пример добавленного WWID диска:

   ```
   # This file is managed by vdsm, do not edit!
   # Any changes made to this file will be overwritten when running:
   # vdsm-tool config-lvm-filter

   blacklist {
       wwid "INTEL_SSDSC2KB019T8_PHYF124301J21P9DGN"
   }
   ```

Настройка multipath на ROSA Virtualization

Для настройки multipath на ROSA Virtualization выполните (на каждом контроллере для кластерных систем):

Не изменяйте оригинальный файл `/etc/multipath.conf`.

1. Создайте файл `/etc/multipath/conf.d/raidix-multipath.conf` следующего содержания:

```
defaults {
         fast_io_fail_tmo        5
         features                "0"
         no_path_retry           10
         path_checker            tur
         polling_interval        5
         prio                    alua
}

devices {
         device {
                 #For initiators with scsi_dh_alua
                 #hardware_handler       "1 alua"
                 detect_checker          no
                 detect_prio             no
                 failback                immediate
                 no_path_retry           12
                 path_checker            "tur"
                 path_grouping_policy    "group_by_prio"
                 path_selector           "round-robin 0"
                 prio                    "alua"
                 product                 ".*"
                 rr_min_io               100
                 rr_weight               "uniform"
                 vendor                  "Raidix"
        }
}
```

2. Примените настройку multipath:

```
# systemctl restart multipathd.service
```

ГЛАВА 3. ФАЙЛОВЫЙ ДОСТУП

Файловое хранилище используется чаще всего для недорогой организации общего доступа к файлам и для систем локального архивирования.

Настройка файлового хранилища состоит из настройки сети, хостов и СХД. Общий план настройки представлен ниже.

Схема настройки файлового доступа

Настройка блочного доступа состоит из следующих этапов:

1. Проверка первичной настройки СХД:
   - ПО RAIDIX установлено;
   - лицензия добавлена;
   - менеджмент-интерфейс настроен;
   - в случае двухконтроллерной системы, включён DC-режим;
   - в случае использования дисковой корзины, она подсоединена к СХД.
2. Предварительная подготовка:
   - Монтаж и настройка сети и сетевого оборудования между клиентом и СХД (сервером).
   - Настройка сети на СХД:
     - *Опционально:* настройка VIP.

       Подробнее о настройке VIP в документе «Руководство администратора RAIDIX 5.3.1».
     - *Опционально:* настройка бонда.

       Подробнее о настройке бонда в документе «Руководство администратора RAIDIX 5.3.1».
3. Настройка СХД и ресурсов:

   Подробнее о кажом шаге см. в документе «Руководство администратора RAIDIX 5.3.1».
   a. *Опционально:* настройка NFS-сервера.
   b. *Опционально:* подключение к службе каталогов.
   c. Создание и настройка общих папок (ресурсов) на СХД.
   d. Создание и/или настройка прав доступа NAS-пользователей.
4. Подключение (монтирование) общей папки (ресурса, сетевого диска, сетевой директории) на клиенте.

   Примеры способов монтирования см. в этом документе в главах для используемых ОС клиентов.

Монтирование общей папки на Linux

NFS

Чтобы смонтировать общую папку NFS:

1. Установите пакет `nfs-common` (для дистрибутивов на основе Debian) или `nfs-utils` (для дистрибутивов на основе RPM) для работы с NFS.
2. Смонтируйте общую папку:

```
# mount <node_ip>:<storage_mount_point> <client_mount_point>
```

`<node_ip>` – IP-адрес сетевого интерфейса (или VIP) на контроллере СХД.
`<storage_mount_point>` – точка монтирования общей папки на СХД: `/mnt/nas/<lun_name>/<share_path>`.
`<client_mount_point>` – точка монтирования на клиенте.

SMB

Чтобы смонтировать общую папку SMB:

> Приведённые команды выполняются от пользователя root. Команды для пользователя с правами суперпользователя см. ниже в примерах.

1. Установите пакет `cifs-utils` для работы с SMB.
2. Смонтируйте общую папку:

```
# mount -o username=<user> //<node_ip>/<share_name> <client_mount_point>
```

`<user>` – пользователь, имеющий доступ к общей папке, от имени которого будет осуществляться доступ.
`<node_ip>` – IP-адрес сетевого интерфейса (или VIP) на контроллере СХД.
`<share_name>` – имя общей папки на СХД.
`<client_mount_point>` – точка монтирования на клиенте.

3. Введите пароль пользователя <user>.

Примеры монтирования на Ubuntu 22.04

> Примеры приведены для выполнения пользователем с правами суперпользователя.

1. Установка пакета `cifs-utils`:

```
# sudo apt-get install cifs-utils
```

2. Монтирование общей папки.

   Если монтирование выполняется с правами суперпользователя, на точку монтирования по умолчанию устанавливаются права 755, а владельцем точки монтирования становится root:root. Чтобы на точку монтирования назначить права, позволяющие выполнять запись в общую папку, при монтировании задайте параметры `file_mode` и `dir_mode` со значениями `0777`. При этом права доступа к общей папке будут определяться через заданные на СХД права доступа пользователя к общей папке.

   Пример команд монтирования от локального пользователя в уже созданную точку монтирования:

   - Параметры объектов NAS на СХД:
     - локальный пользователь **user1**;
     - пароль локального пользователя **123**;
     - путь **/shares/smb**;
     - имя общей папки **smb_a**;
     - адрес интерфейса контроллера **10.10.10.1**;
     - существующая точка монтирования на клиенте **/mnt/new_share**.
   - Команды монтирования:

```
# sudo mount -o username=user1,file_mode=0777,dir_mode=0777 //10.10.10.1/smb_a /mnt/new_share
# 123
```

Пример команд монтирования с гостевым доступом в ещё не созданную точку монтирования:

- Параметры объектов NAS на СХД:
  - пользователь **гость**;
  - путь **/shares/smb**;
  - имя общей папки **smb_b**;
  - адрес интерфейса контроллера **10.10.10.1**;
  - несуществующая точка монтирования на клиенте **/mnt/new_share1**.
- Команды монтирования:

```
# sudo mkdir /mnt/new_share1/
# sudo mount -o username=guest,file_mode=0777,dir_mode=0777 //10.10.10.1/smb_b /mnt/new_share1
```

Пример команд монтирования от доменного пользователя в уже созданную точку монтирования:

- Параметры объектов NAS на СХД:
  - пользователь из AD **user_ad**;
  - пароль пользователя из AD **1234**;
  - имя домена **example.com**;
  - имя общей папки **smb_c**;
  - адрес интерфейса контроллера **10.10.10.1**;
  - существующая точка монтирования на клиенте **/mnt/new_share2**.
- Команды монтирования:

```
# sudo mount -o
 username=user_ad,domain=example.com,file_mode=0777,dir_mode=0777 //10.10.10.1/smb_c /mnt/new_share2
# 1234
```

FTP

Чтобы смонтировать общую папку FTP.

> Приведённые команды выполняются от пользователя root. Команды для пользователя с правами суперпользователя см. ниже в примерах.

1. Установите пакет `curlftpfs` для работы с FTP.
2. Смонтируйте общую папку:

```
# curlftpfs ftp://<user>:<pass>@<node_ip>/<share_name> <client_mount_point>
```

`<user>` – пользователь, имеющий доступ к общей папке, от имени которого будет осуществляться доступ.
`<pass>` – пароль пользователя `<user>`.
`<node_ip>` – IP-адрес сетевого интерфейса (или VIP) на контроллере СХД.
`<share_name>` – имя общей папки на СХД.
`<client_mount_point>` – точка монтирования на клиенте.

Примеры монтирования на Ubuntu 22.04

> Примеры приведены для выполнения пользователем с правами суперпользователя.

1. Установка пакета `curlftpfs`:

```
# apt-get install curlftpfs
```

2. Монтирование общей папки.

   Если монтирование выполняется от имени пользователя с правами суперпользователя, определите права на точку монтирования:

   - если папка требуется только для чтения, то при монтировании необходимо использовать параметр `allow_other`.
   - если папка требуется и для чтения, и для записи, то при монтировании используйте параметры `umask` со значением `000` и `allow_other`.

   При этом права доступа к общей папке будут определяться через заданные на СХД права доступа пользователя к общей папке.

   Пример команды монтирования папки от локального пользователя только для чтения:

   - Параметры объектов NAS на СХД:
     - локальный пользователь **user3**;
     - пароль локального пользователя **12345**;
     - путь **/shares/ftp**;
     - имя общей папки **ftp_a**;
     - адрес интерфейса контроллера **10.10.10.1**;
     - существующая точка монтирования на клиенте **/mnt/new_share4**.
   - Команда монтирования:

```
# sudo curlftpfs -o user=user3:12345,allow_other ftp://10.10.10.1/ftp_a /mnt/new_share4
```

   Пример команды монтирования папки с гостевым доступом для чтения и записи:

   - Параметры объектов NAS на СХД:
     - пользователь **гость**;
     - путь **/shares/ftp**;
     - имя общей папки **ftp_b**;
     - адрес интерфейса контроллера **10.10.10.1**;
     - существующая точка монтирования на клиенте **/mnt/new_share4**.
   - Команда монтирования:

```
# sudo curlftpfs -o allow_other,umask=000 ftp://10.10.10.1/ftp_b /mnt/new_share4
```

AFP

Чтобы смонтировать общую папку AFP.

1. Смонтируйте общую папку:

```
# mount_afp afp://<user>:<pass>@<node_ip>/<share_name> <client_mount_point>
```

   `<user>` – пользователь, имеющий доступ к общей папке, от имени которого будет осуществляться доступ.
   `<pass>` – пароль пользователя `<user>`.
   `<node_ip>` – IP-адрес сетевого интерфейса (или VIP) на контроллере СХД.
   `<share_name>` – имя общей папки на СХД.
   `<client_mount_point>` – точка монтирования на клиенте.

Монтирование общей папки на Windows

Монтирование SMB

Чтобы смонтировать общую папку SMB:

1. Нажмите **Win+E** и выберите **Этот компьютер**.
2. На вкладке **Компьютер** кликните **Подключить сетевой диск**.
3. Выберите любую свободную букву и укажите адрес общей папки:

   ```
   \\<node_ip>\<share_name>
   ```

   `<node_ip>` – IP-адрес сетевого интерфейса (или VIP) на контроллере СХД.
   `<share_name>` – имя общей папки на СХД.
4. Введите пользователя, от имени которого осуществляется подключение общей папки, и пароль.

Монтирование общей папки на zVirt

Для zVirt доступен файловый протокол NFS. В терминах zVirt, создаётся объект «домен хранения».

Особенности NFS и zVirt

При настройке файлового доступа к zVirt учитывайте следующие особенности работы zVirt:

- При работе с NFS по каналам 10 Гб и выше рекомендуем настраивать NFS-папку на СХД (параметр «Клиенты») с указанием IP-адресов используемых интерфейсов.

  Подробнее о настройке NFS см. в документе «Руководство администратора RAIDIX 5.3.1».
- Не рекомендуем размещать критичные ВМ на NFS-хранилищах двухконтроллерной системы. При failover и «перемещении» NFS-папки между контроллерами, ВМ останавливают свою работу до их ручного перезапуска.

Подключение общей папки NFS

В текущей версии ПО RAIDIX поддерживается только анонимный доступ. Для его настройки, на СХД включите параметр **All squash** и укажите ID пользователя/группы. Подробнее о настройке см. в документе «Руководство администратора RAIDIX 5.3.1».

Чтобы подключить на zVirt общую папку NFS в качестве «домена хранения»:

> Подробную инструкцию по настройке см. на *официальном сайте zVirt*.

1. На **Портале администрирования** кликните **Хранилище (Storage) > Домены (Domains)**.
2. Кликните **Новый домен (New Domain)**.
3. Задайте **Имя (Name)** для домена хранения.
4. Примите значения по умолчанию для списков **Центр данных (Data Center)**, **Функция домена (Domain Function)**, **Тип хранилища (Storage Type)**, **Используемый хост (Host)**.
5. Введите **Путь экспорта (Export Path)**, который должен использоваться для домена хранения. Путь экспорта должен иметь следующий формат: `<node_ip>:<mount_point>`, где

   <node_ip> – IP-адрес (или VIP) контроллера СХД;
   <mount_point> – точка монтирования общей папки NFS на СХД: `/mnt/nas/<lun_name>/<share_path>`.
6. Кликните **OK**.

Монтирование общей папки на ROSA Virtualization

Для ROSA Virtualization доступен файловый протокол NFS. В терминах ROSA Virtualization создаётся объект «домен хранилища».

Особенности NFS и ROSA Virtualization

При настройке файлового доступа к ROSA Virtualization учитывайте следующие особенности работы:

- Рекомендуем настраивать NFS-папку на СХД (параметр «Клиенты») с указанием IP-адресов используемых интерфейсов, если вы работаете с NFS по каналам 10 Гб и выше.

  Подробнее о настройке NFS см. в документе «Руководство администратора RAIDIX 5.3.1».

- Не рекомендуем размещать критичные ВМ на NFS-хранилищах DC-систем. При failover и «перемещении» NFS-папки между контроллерами, ВМ останавливают свою работу до ручного перезапуска.

Подключение общей папки NFS

Для подключения на ROSA Virtualization общей папки NFS выполните:

> Подробную инструкцию по настройке см. в *официальной документации ROSA Virtualization*.

1. На **Портале администрирования** выберите **Хранилище > Домены**.
2. Нажмите **Добавить домен**.
3. В окне **Новый домен** укажите **Имя** домена хранилища.
4. Укажите значения для **Дата-центр**, **Функция домена**, **Тип хранилища**, **Хост**.
5. Введите **Путь экспорта**, который должен использоваться для домена хранения. Путь экспорта должен иметь следующий формат: `<node_ip>:<mount_point>`, где

   <node_ip> – IP-адрес (или VIP) контроллера СХД;
   <mount_point> – точка монтирования общей папки NFS на СХД: `/mnt/nas/<lun_name>/<share_path>`.
6. Нажмите **OK**.

ГЛАВА 4. МЕХАНИЗМ SERIAL-OVER-LAN

Механизм Serial-over-LAN (SoL) предоставляет хосту возможность удалённого управления и мониторинга сервера через сетевой интерфейс, используя возможности BMC (Baseboard Management Controller). Использование механизма SoL позволяет хосту взаимодействовать с сервером через удалённую консоль при возникновении неполадок в сети или при отсутствии доступа к веб-интерфейсу BMC.

Требования и особенности работы механизма SoL

На стороне BMC:

- реализация BMC поддерживает механизм SoL;
- поддержка механизма SoL должна быть включена.

По умолчанию реализация механизма Serial-over-LAN использует порт 2200. Если при настройке BMC для SoL был установлен другой порт или порт был изменён, используйте актуальный порт.

На стороне хоста:

- операционная система хоста должна поддерживать механизм SoL;
- хост должен находиться в одной сети с сервером с доступом к BMC.

Для получения доступа к удалённой консоли на хосте:

1. Введите команду

   ```
   $ ssh -p 2200 <user>@<BMC_IP>
   ```

   `<user>` – пользователь, имеющий доступ к BMC, от имени которого будет осуществляться доступ.

   `<BMC_IP>` – IP-адрес интерфейса BMC.

2. Введите пароль пользователя <user>.