Утвержден

РДЦП.10001-02-УД

Подп. и дата	
Инв. № дубл	
Взам. инв. №	
Подп. и дата	
Инв. № подл	

ПРОГРАММНЫЙ КОМПЛЕКС «СРЕДСТВА ВИРТУАЛИЗАЦИИ «БРЕСТ»

РДЦП.10001-02

Руководство пользователя.

Оперативное обновление 3.3.3

Бюллетень № 2025-1804BR02

Листов 148

2025

Литера $О_1$

АННОТАЦИЯ

Настоящий документ является руководством пользователя программного изделия «Программный комплекс «Средства виртуализации «Брест» (ПК СВ «Брест») РДЦП.10001-02 (далее по тексту — ПК СВ) и предназначен для разработчика и администратора виртуальной машины.

Документ содержит описания:

- создания шаблонов ВМ;
- настройки конфигураций шаблонов ВМ;
- создания ВМ;
- настройки конфигураций ВМ;
- работы с виртуальной машиной.

Документ не охватывает порядок установки, развертывания и администрирования ПК СВ и предназначен для использования совместно с эксплуатационными документами согласно ведомости РДЦП.10001-02 20 01 «Программный комплекс «Средства виртуализации «Брест». Ведомость эксплуатационных документов».

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ

1.1. ПК СВ предназначен для управления средой виртуализации, создание и защита которой обеспечивается средствами операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 очередное обновление 1.7 (далее по тексту — ОС СН).

1.2. В ПК СВ входят следующие программные компоненты серверной части:

- сервер виртуализации — для возможности создания виртуальных машин посредством эмуляции аппаратного обеспечения;
- сервер управления — для возможности управления через веб-интерфейс, из командной строки (консольный интерфейс) и с помощью XML-RPC API.

В качестве клиентской части ПК СВ может выступать средство вычислительной техники, с которого выполняется подключение к серверу управления или виртуальной машине (ВМ).

В качестве дополнительных программных компонентов (не входят в состав ПК СВ) выступают:

- хранилище — система, предназначенная для хранения образов дисков виртуальных машин;
- контроллер домена — служба, обеспечивающая аутентификацию пользователей в рамках единого пространства пользователей (не используется в сервисном режиме работы ПК СВ).

1.3. ПК СВ предоставляет следующие возможности:

- создание ВМ, их образов и шаблонов;
- формирование среды выполнения ВМ;
- управление конфигурацией ВМ с помощью графического и консольного интерфейсов;
- централизованное управление средой виртуализации.

Классы решаемых задач приведены в документе РДЦП.10001-02 31 01 «Программный комплекс «Средства виртуализации «Брест». Описание применения».

1.4. ПК СВ функционирует только под управлением ОС СН, имеющей сертификат соответствия ФСТЭК России № 2557, и совместно с ней обеспечивает выполнение следующих функций безопасности информации в соответствии с требованиями по безопасности информации к средствам виртуализации[1)] :

- доверенная загрузка виртуальных машин;
- контроль целостности;
- регистрация событий безопасности;

[1)] Утверждены приказом ФСТЭК России от 27.10.2022 № 187.

- управление доступом;
- резервное копирование;
- управление потоками информации;
- защита памяти;
- ограничение программной среды;
- идентификация и аутентификация пользователей.

Функция централизованного управления (администрирования) виртуальными машинами и взаимодействием между ними реализуется собственными средствами ПК СВ.

Реализация перечисленных функций безопасности основана на основных положениях, изложенных в документе РДЦП.10001-02 97 01 «Программный комплекс «Средства виртуализации «Брест». Руководство по КСЗ».

1.5. ПК СВ интегрирован с комплексом средств защиты информации ОС СН и дополнительно обеспечивает выполнение следующих функций безопасности:

- дискреционное и мандатное управление доступом к ВМ и образам ВМ, в том числе при межпроцессном и сетевом взаимодействии, включая взаимодействие между ВМ по протоколам стека IPv4 и IPv6 в условиях мандатного управления доступом и доступ субъектов к файлам-образам и экземплярам функционирующих ВМ;
- создание кластеров высокой доступности с общим хранилищем, обеспечивающих отказоустойчивое функционирование ВМ посредством миграции ВМ между узлами кластера;
- обновление программного обеспечения ПК СВ с использованием штатных средств ОС СН.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ

2.1. Принципы безопасной работы

ПК СВ функционирует только под управлением ОС СН на максимальном уровне защищенности («Смоленск») или усиленном уровне защищенности («Воронеж»). При этом допускается развертывание ПК СВ в сервисном режиме на компьютерах под управлением ОС СН, функционирующей на базовом уровне защищенности («Орел»).

Для обеспечения корректного функционирования ПК СВ необходимо установить программное обеспечение оперативного обновления ОС СН бюллетень № 2025-0319SE17 (оперативное обновление 1.7.7), при установке выбрать ядро `linux-5.15-generic`.

Принцип безопасной работы основан на соблюдении следующих условий:

- соблюдение условий по безопасной установке ПК СВ в соответствии с РДЦП.10001-02 97 01;
- соблюдение условий безопасности среды функционирования в соответствии с РДЦП.10001-02 97 01;
- настройка функций безопасности в соответствии с РДЦП.10001-02 97 01;
- функционирование ПК СВ должно осуществляться, основываясь на принципах ролевого управления доступом.

Назначение ролей и полномочий выполняются в ОС СН под учетной записью администратора ОС СН с высоким уровнем целостности. Пользователи с ролью администратора ВМ включены в группу `brestusers`. Пользователи с ролью разработчика ВМ включены в группу, название которой определяется администратором ОС СН. Для группы, в которую входит пользователи, предоставляются полномочия USE в отношении хранилищ и виртуальных сетей, а также полномочия CREATE и MANAGE в отношении шаблонов ВМ. Полномочия предоставляются в соответствии с РДЦП.10001-02 97 01. Иных пользовательских настроек не требуется.

С учетом роли пользователя определены следующие типы событий безопасности, связанные с доступными пользователю функциями:

- успешные и неуспешные попытки аутентификации;
- доступ к ВМ;
- создание ВМ;
- изменение конфигураций ВМ.

2.2. Требования к техническим средствам

2.2.1. Требования сервера управления

Минимальные рекомендуемые характеристики компьютера для развертывания службы сервера управления приведены в таблице 1.

Таблица 1

Ресурсы	Минимальная рекомендуемая конфигурация
Оперативная память	4 ГБ
Центральный процессор	2 процессорных ядра с поддержкой SMT
Объем диска	100 ГБ
Сетевой интерфейс	от 1 Гбит/с

Максимальное количество серверов виртуализации (компьютеров, на которых установлена и инициализирована служба сервера виртуализации), которым можно управлять с помощью одного экземпляра сервера управления, зависит от производительности и масштабируемости инфраструктуры ПК СВ и главным образом от системы хранения данных. Не рекомендуется использовать один экземпляр сервера управления для управления более чем 500 серверами виртуализации.

Сервер управления (компьютер, на котором установлена и инициализирована служба сервера управления) должен иметь сетевое соединение со всеми серверами виртуализации и, по возможности, доступ к хранилищам данных (как локальным, так и сетевым). Для обеспечения надежности инфраструктуры ПК СВ рекомендуется использовать как минимум две сети (соответственно, требуется два сетевых интерфейса):

1) сервисная сеть — используется службой сервера управления для обеспечения доступа к серверам виртуализации с целью управления и мониторинга гипервизоров и перемещения файлов образов;
2) сеть экземпляров — обеспечивает возможность сетевого подключения к виртуальным машинам через различные серверы виртуализации.

Кроме того, может потребоваться третий сетевой интерфейс для обеспечения доступа к сети хранения данных.

Для базовой установки службы сервера управления требуется не более 150 МБ.

2.2.2. Требования сервера виртуализации

Минимальные рекомендуемые характеристики компьютера для развертывания службы сервера виртуализации приведены в таблице 2.

Таблица 2

Ресурсы	Минимальная рекомендуемая конфигурация
Оперативная память	8 ГБ
Центральный процессор	4 процессорных ядра
Объем диска	100 ГБ
Сетевой интерфейс	от 1 Гбит/с

На объектах эксплуатации рекомендуется рассчитывать характеристики компьютеров исходя из ожидаемой нагрузки (характеристики ВМ, требования ПО внутри гостевых ОС, сетевой трафик, объем данных). При этом следует учитывать следующие особенности:

1) процессорная архитектура x86-64 должна обеспечивать аппаратную поддержку виртуализации (технологии Intel VT, AMD-V);

2) центральный процессор (ЦП) — без последующих дополнительных нагрузок каждый модуль ЦП, закрепленный за одной ВМ, должен соответствовать физическому ядру ЦП в случае, если необходимо минимизировать конкуренцию ВМ за процессорные ядра. Например, при нагрузке в 40 виртуальных машин с двумя ЦП каждая, потребуются 80 физических ЦП. При этом 80 физических ЦП могут распределяться по различным серверам виртуализации: 10 компьютеров с восемью ядрами каждый или пять компьютеров с 16 ядрами каждый. При необходимости последующих дополнительных нагрузок архитектуру ЦП можно планировать заранее с помощью элементов CPU и VCPU: CPU определяет физические ЦП, закрепленные за виртуальными машинами, а VCPU — виртуальные ЦП, передаваемые гостевой операционной системой;

3) оперативная память — рекомендуется всегда предусматривать резерв 10 % по ресурсам, потребляемым гипервизором. Например, для нагрузки в 40 виртуальных машин с 2 ГБ оперативной памяти каждая необходимо около 90 ГБ физической памяти (с учетом ресурса оперативной памяти, потребляемой гипервизором). Например, пять компьютеров с 24 ГБ оперативной памяти каждый предоставят по 22 ГБ памяти, поэтому они смогут выдержать планируемую нагрузку.

В каждом сервере виртуализации в зависимости от конфигурации хранилища и сети может быть установлено до четырех сетевых интерфейсов: для сети экземпляров (приватной и/или публичной), сервисной сети и сети хранения данных.

2.3. Требования безопасности

ПК СВ может функционировать в двух режимах:

1) в сервисном режиме все ВМ запускаются от имени непривилегированного поль-

зователя. Идентификация и аутентификация пользователей основываются на использовании механизма PAM, реализованного в ОС СН. При этом аутентификация осуществляется с помощью локальной БД пользователей (файл /etc/passwd) и локальной БД пользовательских паролей (файл /etc/shadow);

2) в дискреционном режиме обеспечивается функционирование защищенной среды виртуализации, в том числе дискреционное и мандатное управление доступом к ВМ. В таком режиме ВМ запускаются от имени доменного пользователя, авторизовавшегося в ПК СВ. Для работы в дискреционном режиме необходимо, чтобы все компьютеры, на которых развернуты программные компоненты ПК СВ, входили в один домен FreeIPA или ALD Pro.

Режим функционирования устанавливается на этапе развертывания ПК СВ. После установки и инициализации программных компонент переключение режимов функционирования ПК СВ не предусмотрено.

Создание и защита среды виртуализации обеспечиваются встроенными средствами ОС СН, интегрированными с подсистемой безопасности PARSEC, предназначенной для реализации функций ОС СН по защите информации от несанкционированного доступа:

- модулем ядра KVM, который использует аппаратные возможности архитектуры x86-64 по виртуализации процессоров;
- средствами эмуляции аппаратного обеспечения на основе QEMU;
- сервером виртуализации на основе libvirt.

В ПК СВ конфигурации виртуального оборудования виртуальных машин хранятся в защищенной СУБД PostgreSQL из состава ОС СН, сертифицированные функции которой обеспечивают идентификацию и аутентификацию пользователей, и управление доступом к хранимой информации. Таким образом, при выполнении любого запроса пользователя к конфигурации ВМ осуществляется дискреционное управление доступом на основе установленных пользователю прав. Для каждой выполняемой операции производится проверка наличия права у пользователя на выполнение данной конкретной операции.

При развертывании ПК СВ дополнительная настройка целостности конфигурации виртуального оборудования не требуется.

3. ВЫПОЛНЕНИЕ ПРОГРАММЫ

3.1. Инструменты управления ПК СВ

3.1.1. Инструменты командной строки

Для управления функциональными элементами ПК СВ можно воспользоваться инструментами командной строки, перечисленными в таблице 3.

Таблица 3

Инструмент командной строки	Описание
onecluster	управление кластерами ПК СВ
onedatastore	управление хранилищами
onedb	инструмент для миграции БД
onegroup	управление группами пользователей ПК СВ
onehook	управление хуками, применяемыми в ПК СВ
onehost	управление серверами виртуализации ПК СВ
oneimage	управление образами дисков виртуальных машин (ВМ)
onemarket	управление магазином приложений ПК СВ
onemarketapp	управление приложением из магазина приложений
onetemplate	управление шаблонами ВМ
oneuser	управление пользователями ПК СВ
onevm	управление виртуальными машинами
onevmgroup	управление группами ВМ
onevnet	управление сетями

ВНИМАНИЕ! Для управления функциональными элементами ПК СВ посредством инструментов командной строки необходимо на компьютере, на котором развернут сервер управления, войти в ОС СН под учетной записью разработчика (администратора) ВМ.

Для того чтобы получить подробное описание использования какого-либо инструмента командной строки, необходимо выполнить команду:

`<наименование_инструмента> -h`

3.1.2. Веб-интерфейс ПК СВ

Для подключения к веб-интерфейсу ПК СВ необходимо в браузере Mozilla Firefox перейти по адресу: `https://<полное_доменное_имя>/`,

где `<полное_доменное_имя>` — полное доменное имя компьютера, на котором развернута служба сервера управления.

Примечание. Подключение к веб-интерфейсу ПК СВ можно осуществлять с любого компьютера, имеющего сетевой доступ к серверу управления.

В сервисном режиме работы ПК СВ на открывшейся странице «Брест» необходимо:

- в поле «Логин» ввести имя учетной записи разработчика (администратора) ВМ, заданный администратором ПК СВ;
- в поле «Пароль» ввести пароль учетной записи разработчика (администратора) ВМ;
- нажать на кнопку **[Войти]**.

В дискреционном режиме работы ПК СВ применяется доменная аутентификация. В связи с этим на открывшейся странице «Брест» необходимо:

- в открывшемся окне авторизации ввести имя и пароль доменной учетной записи разработчика (администратора) ВМ, заданный администратором ПК СВ;
- на странице «Брест» нажать на кнопку **[Войти]**.

Примечание. Если подключение к веб-интерфейсу ПК СВ производится с компьютера, на котором развернут сервер управления, и под учетной записью пользователя, зарегистрированного в ПК СВ, то автоматически будут использованы аутентификационные параметры, которые использовались для входа в ОС СН.

3.2. Управление образами

В хранилище образов размещаются файлы, которые могут являться образами дисков с установленной ОС (загрузочных дисков) или образами дисков с различными данными, используемыми в виртуальных машинах. Эти образы могут использоваться несколькими виртуальными машинами одновременно, а также быть общими для различных пользователей ПК СВ.

3.2.1. Типы образов

Существует шесть типов образов, три из которых могут использоваться в качестве дисков ВМ. С помощью команды `oneimage chtype` можно изменить тип существующего образа.

Типы образов, размещенные в хранилище образов и доступные для использования в качестве дисков ВМ:

1) `OS` — образ загрузочного диска (с установленной ОС). Каждый шаблон ВМ должен определять один диск, ссылающийся на образ данного типа;

2) `CDROM` — образ представляет данные только для считывания. В каждом шаблоне ВМ может использоваться только один образ данного типа;

3) `DATABLOCK` — образ блока данных, является образом диска с различными данными, используемыми в виртуальных машинах. Эти образы можно создавать из уже существующих образов дисков или в качестве пустого диска.

Типы образов, которые размещены в хранилище файлов и ядер, и не могут исполь-

зоваться в качестве дисков ВМ:

1) KERNEL — незашифрованный файл, который используется в качестве ядра (параметр OS/KERNEL_DS для ВМ);

2) RAMDISK — незашифрованный файл, который используется в качестве дискового ресурса, размещенного в оперативной памяти (параметр OS/INITRD_DS для ВМ);

3) CONTEXT — незашифрованный файл, который нужно добавить в контекстный CD-ROM (параметр CONTEXT/FILES_DS для ВМ).

3.2.2. Состояния образов

Перечень возможных состояний образов приведен в таблице 4.

Таблица 4

Состояние	Сокращение наименования состояния	Описание
LOCKED	lock	Файл образа создается или копируется в хранилище
LOCKED_USED	lock	Файл непостоянного образа создается или копируется в хранилище, а ВМ ожидают
LOCKED_USED_PERS	lock	Аналогично LOCKED_USED для постоянных образов
READY	rdy	Образ готов к применению
USED	used	Непостоянный образ, используемый, как минимум, одной ВМ
USED_PERS	used	Постоянный образ, используемый ВМ. Не может использоваться новыми ВМ
DISABLED	disa	Образ отключен владельцем, не может использоваться новыми ВМ
ERROR	err	Ошибка в работе файловой системы. Сообщение об ошибке можно посмотреть с помощью команды oneimage show в информации образа
DELETE	dele	Образ удаляется из хранилища данных
CLONE	clon	Образ клонируется

3.2.3. Создание образа

3.2.3.1. Общие сведения

В хранилище можно создать образ на основе имеющегося файла или создать образ пустого блока данных, например, для создания ВМ с последующей установкой ОС.

При создании образа пустого блока данных дополнительно требуется указать размер образа.

При создании образа на основе имеющегося файла, исходный файл необходимо поместить на дисковый ресурс, который в настройках хранилища указан в качестве

разрешенного источника (параметр SAFE_DIRS).

3.2.3.2. Создание образа в интерфейсе командной строки

Для создания образа можно воспользоваться инструментом командной строки oneimage, указав команду create. Перечень параметров для создания образа приведен в таблице 5.

Таблица 5

Параметр	Описание
--datastore <хранилище>	Название хранилища образов или хранилища файлов и ядер, в котором разместить новый образ
--name <имя>	Название нового образа
--description <описание>	Описание нового образа
--type <тип>	Тип нового образа: OS, CDROM, DATABLOCK, KERNEL, RAMDISK
--persistent	Флаг, который указывает, будет ли образ постоянным
--prefix <префикс>	Префикс (условное наименование) драйвера шины диска. Возможные значения: - hd — для устройства IDE; - sd — для устройства SCSI; - vd — для устройства Virtio
--target <устройство>	Устройство, к которому будет подключен диск
--path <путь>	Путь имеющегося файла образа, на основе которого создается образ в хранилище
--source <источник>	Используемый ресурс. Применяется для образов, создаваемых не из файла, а, например, на основе имеющегося блочного устройства
--size <размер>	Размер в МБ. Используется для образов типа DATABLOCK

ВНИМАНИЕ! Для образа типа CDROM не допускается использовать драйвер Virtio в качестве шины диска (префикс vd).

Примеры:

1. Создание в хранилище образов, установленном по умолчанию (с наименованием default), образа типа CDROM из файла установочного диска ОС СН, размещенного в каталоге /var/tmp/:

а) выполнить команду:

```
oneimage create --datastore default --name td-alse17 --type CDROM \
    --path /var/tmp/td-alse17.iso   \
    --description "Технологический установочный диск ОС СН 1.7"
```

Пример вывода после выполнения команды:

```
ID: 4
```

б) удостовериться в том, что образ готов к применению (параметр STATE имеет значение rdy), для этого выполнить команду:

```
oneimage show <идентификатор_образа>
```

Пример вывода после выполнения команды oneimage show 4:

```
IMAGE 4 INFORMATION
ID : 4
NAME : td-alse17
USER : oneadmin
GROUP : brestadmins
LOCK : None
DATASTORE : default
TYPE : CDROM
REGISTER TIME : 07/10 19:43:20
PERSISTENT : No
SOURCE : /var/lib/one//datastores/1/ce3c55d1b1737f5c365644dc7ea31335
PATH : /var/tmp/td-alse17.iso
FORMAT : raw
SIZE : 3.8G
STATE : rdy
RUNNING_VMS : 0
```

2. Создание в хранилище образов, установленном по умолчанию (с наименованием default), образа пустого блока данных, размером 12 ГБ:

а) выполнить команду:

```
oneimage create --datastore default --name os-alse17  \
   --type DATABLOCK --format qcow2 --prefix vd --persistent \
   --size 12288 --description "Загрузочный диск ОС СН 1.7"
```

В представленной выше команде были установлены следующие параметры образа:

- формат — qcow2;
- в качестве драйвера диска выбран VirtIO (префикс vd);
- образ помечен как «постоянный», необходимо для последующей установки ОС.

Пример вывода после выполнения команды:

```
ID: 5
```

б) удостовериться в том, что образ готов к применению (параметр STATE имеет значение rdy), для этого выполнить команду:

```
oneimage show <идентификатор_образа>
```

Пример вывода после выполнения команды oneimage show 5:

```
IMAGE 5 INFORMATION
ID : 5
```

```
NAME : os-alse17
USER : oneadmin
GROUP : brestadmins
LOCK : None
DATASTORE : default
TYPE : DATABLOCK
REGISTER TIME : 07/10 20:09:05
PERSISTENT : Yes
SOURCE : /var/lib/one//datastores/1/3fe0664610de3870cbdd9ba24d6a9132
FORMAT : qcow2
SIZE : 12G
STATE : rdy
RUNNING_VMS : 0
```

3.2.3.3. Создание образа в веб-интерфейсе ПК СВ

Для создания образа необходимо выполнить следующие действия:

1) в веб-интерфейсе ПК СВ в меню слева выбрать пункт «Хранилище — Образы»;

2) на открывшейся странице «Образы» нажать на кнопку **[+]** и в открывшемся меню выбрать пункт «Создать» (см. рис. 1)

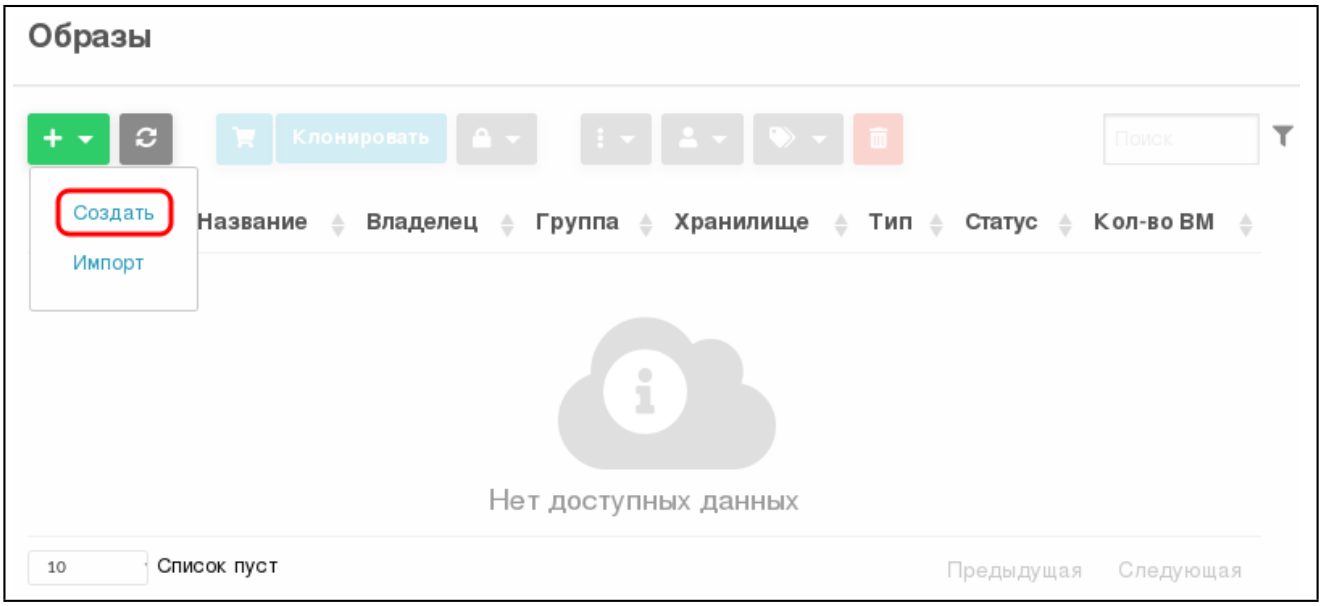

Рис. 1

3) на открывшейся странице «Укажите параметры нового образа» задать параметры образа и нажать на кнопку **[Создать]**.

Примечание. Для образа типа `CDROM` по умолчанию используется драйвер шины диска IDE (префикс `hd`).

ВНИМАНИЕ! Для образа типа `CDROM` не допускается использовать драйвер Virtio в качестве шины диска (префикс `vd`).

При загрузке файла исходного образа через веб-интерфейс ПК СВ выполняется

следующая последовательность действий:

1) клиент браузера загружает весь файл исходного образа на сервер во временный каталог;

2) служба `oned` регистрирует образ во время настройки пути к данному временному файлу;

3) служба `oned` копирует файл образа в хранилище образов;

4) временный файл удаляется и пользователю возвращается запрос (появляется сообщение об успешной загрузке образа).

Примечание. В случае загрузки файлов большого размера, больше 1 ГБ, и в зависимости от используемых аппаратных средств для завершения копирования в хранилище образов может потребоваться много времени. Поскольку запрос на загрузку должен оставаться в состоянии ожидания до успешного завершения копирования (чтобы безопасно удалить временный файл), могут возникнуть паузы при работе Ajax и/или задержка ответа от сервера. Это может привести к ошибкам или запуску повторной загрузки.

Примеры:

1. Создание в хранилище образов, установленном по умолчанию (с наименованием `default`), образа типа `CDROM` из файла установочного диска ОС СН, размещенного в каталоге `/var/tmp/`:

а) в веб-интерфейсе ПК СВ в меню слева выбрать пункт «Хранилище — Образы»;

б) на открывшейся странице «Образы» нажать на кнопку **[+]** и в открывшемся меню выбрать пункт «Создать»;

в) на открывшейся странице «Укажите параметры нового образа»:

- в поле «Название» задать наименование образа установочного носителя,
- в выпадающем списке «Тип» выбрать значение `CD-ROM только для чтения`;
- в секции «Расположение образа» установить флаг «Загрузить»,
- нажать на кнопку **[Обзор...]** (см. рис. 2).

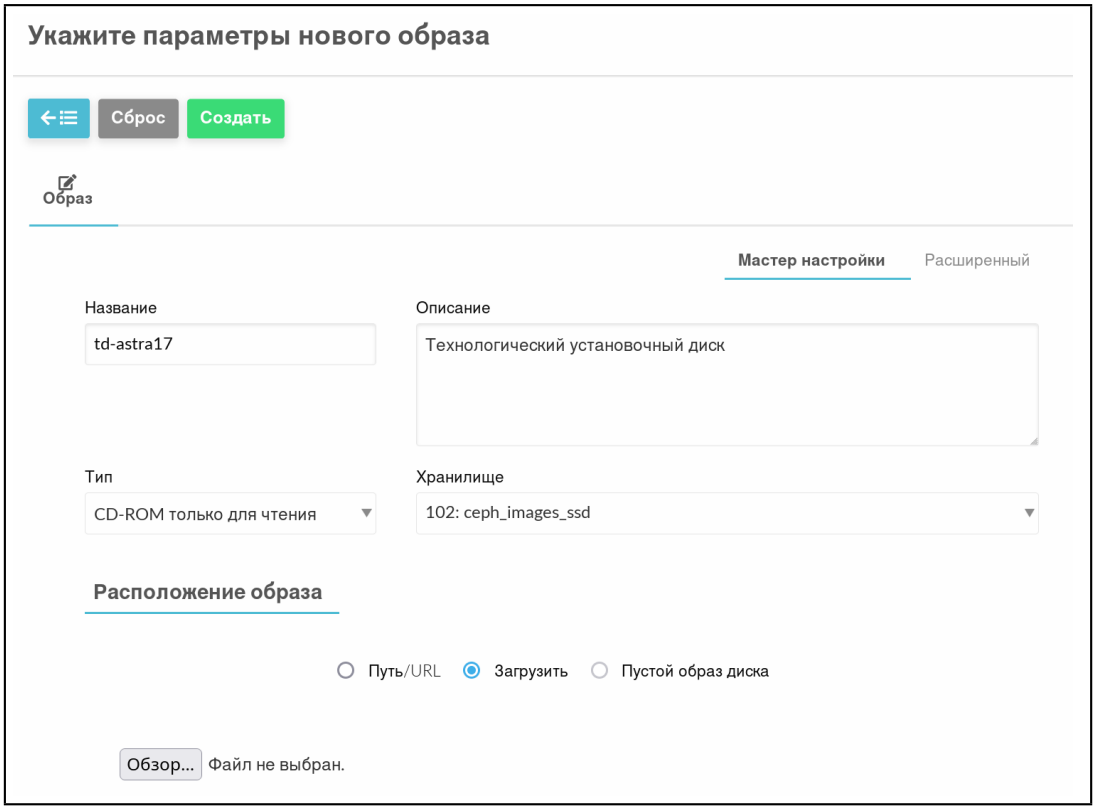

Рис. 2

г) в открывшемся окне «Выгрузка файла» выбрать ISO-файл образа установочного носителя и на кнопку **[Открыть]**;

д) на странице «Укажите параметры нового образа» нажать на кнопку **[Создать]**. После этого на открывшейся странице «Образы» отобразится процесс загрузки образа в облако (см. рис. 3)

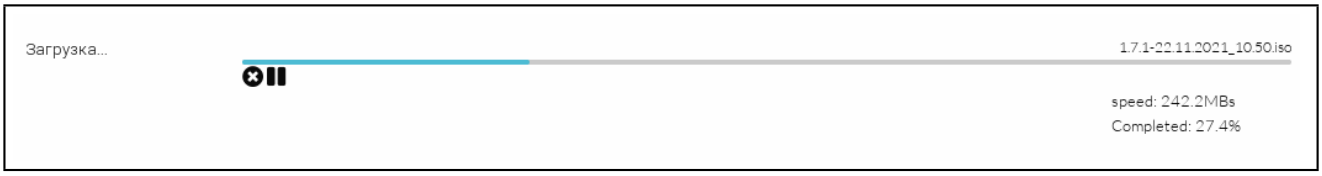

Рис. 3

е) после окончания загрузки образа в хранилище необходимо дождаться момента, когда для загруженного образа в поле «Статус» значение `ЗАБЛОКИРОВАНО` изменится на `ГОТОВО`. Для обновления страницы можно воспользоваться кнопкой **[Обновить]** (см. рис. 4)

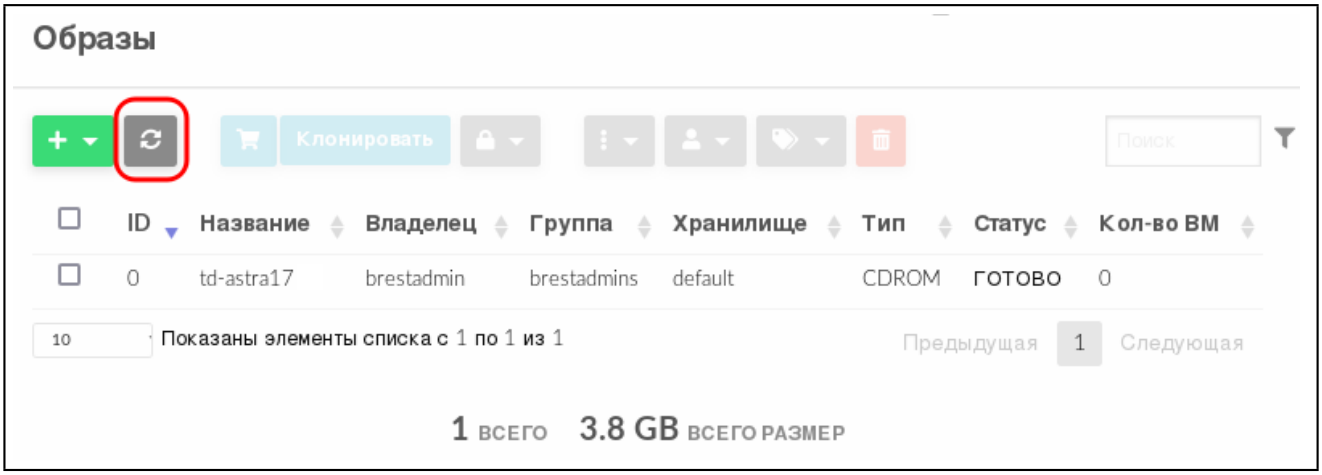

Рис. 4

2. Создание в хранилище образов, установленном по умолчанию (с наименованием `default`), образа пустого блока данных, размером 12 ГБ:

а) в веб-интерфейсе ПК СВ в меню слева выбрать пункт «Хранилище — Образы»;

б) на открывшейся странице «Образы» нажать на кнопку **[+]** и в открывшемся меню выбрать пункт «Создать»;

в) на открывшейся странице «Укажите параметры нового образа» (см. рис. 5):

1) в поле «Название» задать наименование образа диска ВМ,

2) в выпадающем списке «Тип» выбрать значение `Общий блок данных хранилища`,

3) если планируется в дальнейшем использовать этот образ в качестве загрузочного (с установленной ОС), необходимо в выпадающем списке «Этот образ является постоянным» выбрать значение `Да`,

4) в секции «Расположение образа» установить флаг «Пустой образ диска»,

5) в появившемся поле «Размер» задать требуемый размер образа;

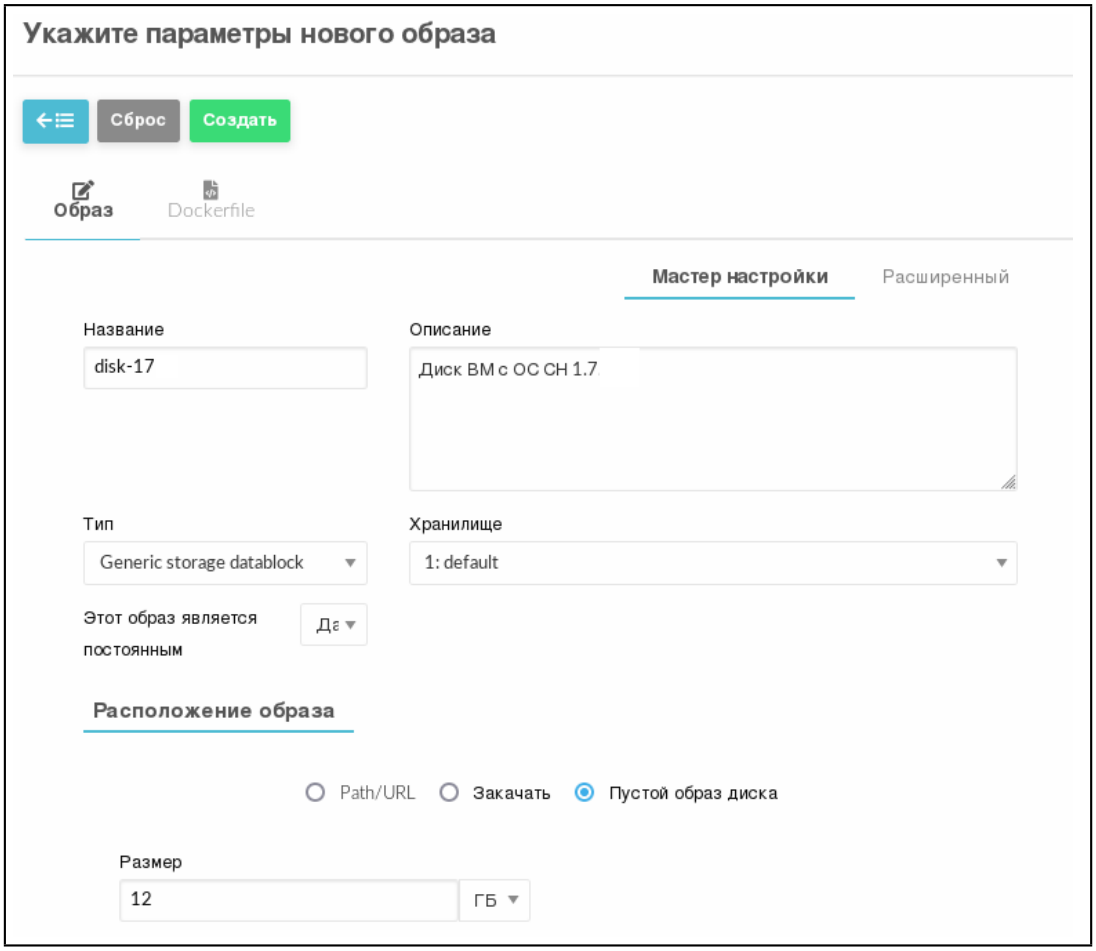

Рис. 5

г) на странице «Укажите параметры нового образа» раскрыть секцию «Расширенные настройки», в выпадающем списке «Шина» выбрать необходимый драйвер диска, например, `Virtio`, в выпадающем списке «Формат» выбрать значение `qcow2` (см. рис. 6)

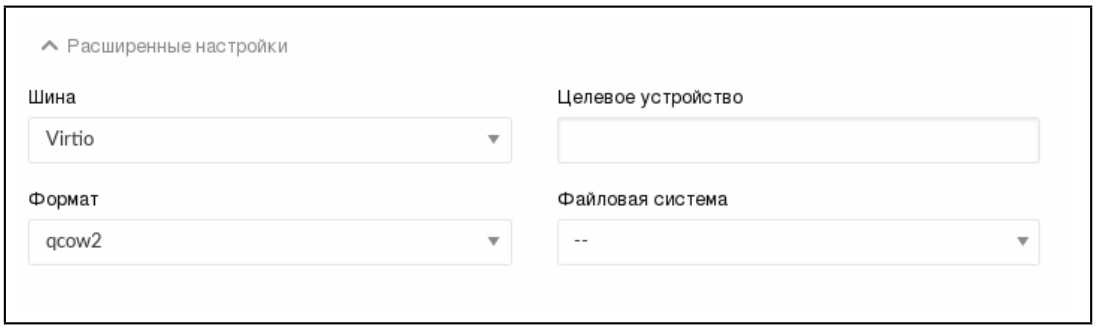

Рис. 6

д) на странице «Укажите параметры нового образа» нажать на кнопку **[Создать]**. После этого на открывшейся странице «Образы» необходимо удостовериться в том, что созданный образ имеет статус `ГОТОВО` (см. рис. 7)

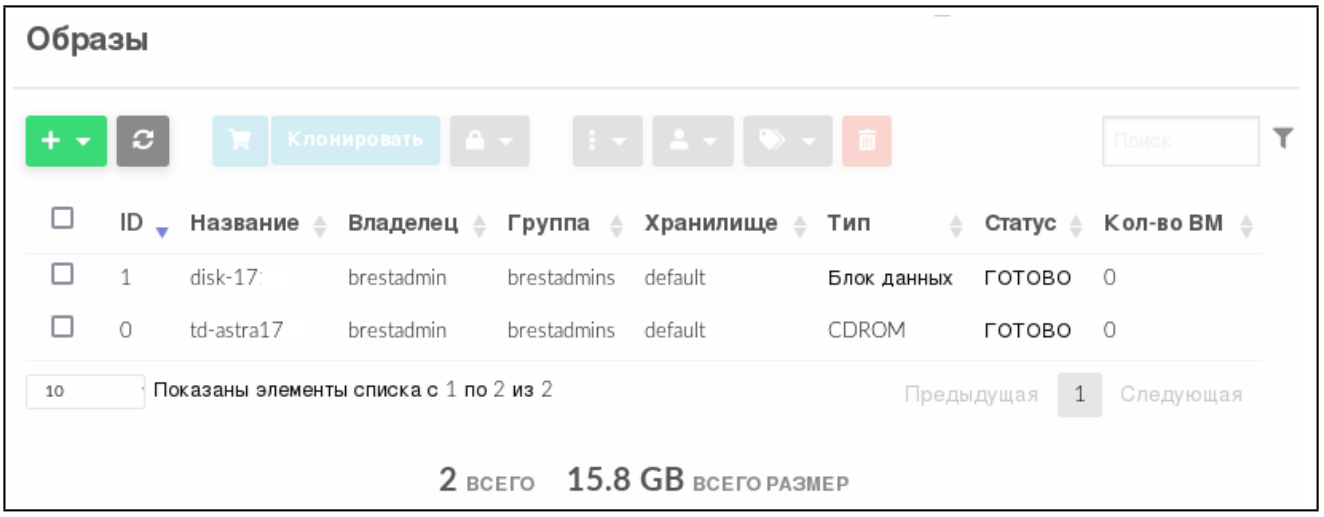

Рис. 7

3.2.4. Клонирование образов

3.2.4.1. Общие сведения

Существующие образы можно клонировать в новый, что актуально при создании резервной копии образа перед его изменением или для получения частной постоянной копии образа, который используется другими пользователями.

ВНИМАНИЕ! Нельзя клонировать постоянные образы со снимками. Для этого пользователю нужно сначала очистить его от снимков в соответствии с 3.2.8.

ВНИМАНИЕ! Клонирование нельзя применить к образам типов KERNEL, RAMDISK и CONTEXT.

3.2.4.2. Клонирование образа в интерфейсе командной строки

Для клонирования образа в интерфейсе командной строки необходимо выполнить команду:

```
oneimage clone <идентификатор_образа> <наименование_нового_образа>
```

Пример

Клонирование образа блока данных с идентификатором «6»:

1) выполнить команду:

```
oneimage clone 6 another-os-alse17
```

Пример вывода после выполнения команды:

```
ID: 7
```

2) удостовериться в том, что образ готов к применению (параметр `STATE` имеет значение `rdy`), для этого выполнить команду:

```
oneimage show <идентификатор_образа>
```

Пример вывода после выполнения команды `oneimage show 7`:

```
IMAGE 7 INFORMATION
ID : 7
NAME : another-os-alse17
USER : oneadmin
GROUP : brestadmins
LOCK : None
DATASTORE : default
TYPE : DATABLOCK
REGISTER TIME : 07/10 21:12:40
PERSISTENT : Yes
SOURCE : /var/lib/one//datastores/1/e84a22fb590908a94f50e3dd06495c95
PATH : /var/lib/one//datastores/1/3fe0664610de3870cbdd9ba24d6a9132
FORMAT : qcow2
SIZE : 12G
STATE : rdy
RUNNING_VMS : 0
```

Также возможно клонировать образ в другое хранилище данных. Новое хранилище данных должно быть совместимо с текущим, т.е. иметь те же самые драйвера передачи данных (параметр `DS_MAD`). Для этого необходимо выполнить команду:

```
oneimage clone <идентификатор_образа> <наименование_нового_образа> \
   --datastore <наименование_нового_хранилища>
```

3.2.4.3. Клонирование образа в веб-интерфейсе ПК СВ

Для клонирования образа в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

1) в меню слева выбрать пункт «Хранилище — Образы»;
2) на открывшейся странице «Образы» выбрать образ, который необходимо клонировать;
3) на открывшейся странице образа нажать на кнопку **[Клонировать]** (см. рис. 8)

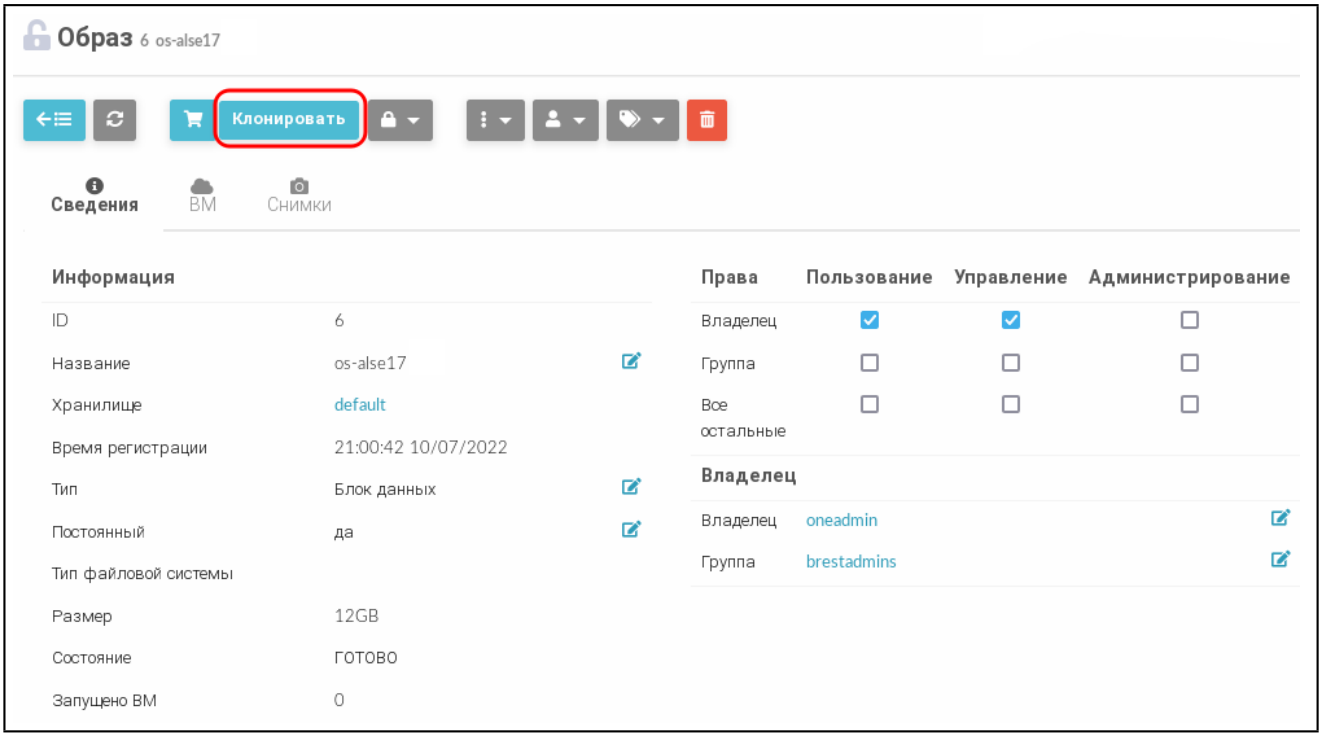

Рис. 8

4) на открывшейся странице «Клонировать образ» задать наименование нового образа. Если необходимо клонировать образ в другое хранилище, необходимо раскрыть секцию «Расширенные настройки» и выбрать новое хранилище образов (см. рис. 9)

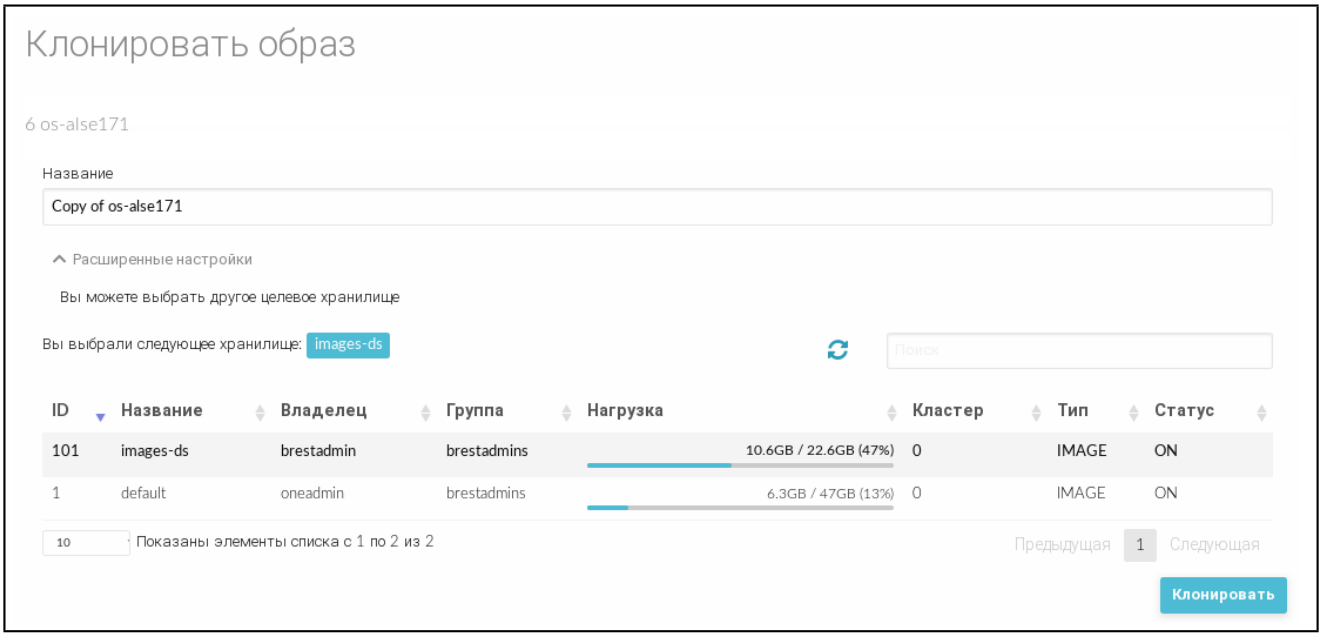

Рис. 9

5) на странице «Клонировать образ» нажать на кнопку **[Клонировать]**.

3.2.5. Отображение доступных образов

3.2.5.1. В интерфейсе командной строки

Для отображения образов, имеющихся в хранилище, в интерфейсе командной строки возможно использовать команду `oneimage list` или настроить непрерывное отображение образов при помощи команды `oneimage top`. Для получения полной информации об образе необходимо использовать команду

`oneimage show <идентификатор_образа>`

Пример

Вывод после выполнения команды `oneimage show 1`:

```
IMAGE 1 INFORMATION
ID : 1
NAME : td-alse17
USER : brestadmin
GROUP : brestadmins
LOCK : None
DATASTORE : default
TYPE : CDROM
REGISTER TIME : 07/18 16:18:44
PERSISTENT : No
SOURCE : /var/lib/one//datastores/1/5c31df1e4e28a9969e4c1a84f77c9c28
PATH : /var/tmp/4093640704-171-22112021_1050iso
FORMAT : raw
SIZE : 3.8G
STATE : rdy
RUNNING_VMS : 0

PERMISSIONS
OWNER : um-
GROUP : ---
OTHER : ---

IMAGE TEMPLATE
DEV_PREFIX="hd"
```

3.2.5.2. В веб-интерфейсе ПК СВ

Для отображения образов, имеющихся в хранилище, в веб-интерфейсе ПК СВ необходимо в меню слева выбрать пункт «Хранилище — Образы».

Для просмотра параметров конкретного образа в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

1) в меню слева выбрать пункт «Хранилище — Образы»;

2) на открывшейся странице «Образы» выбрать необходимый образ. После этого откроется страница с параметрами выбранного образа (вкладка «Сведения») — см. рис. 10

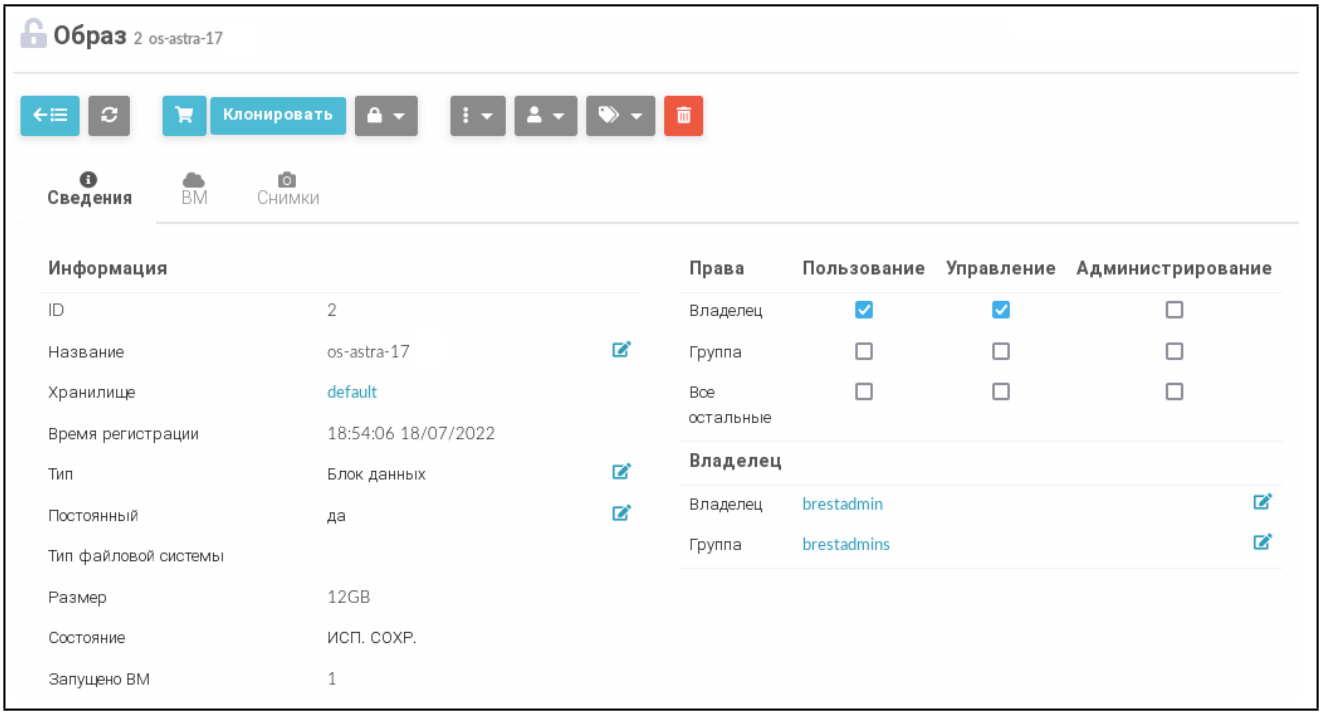

Рис. 10

3.2.6. Общие образы

Пользователи могут предоставлять общий доступ к своим образам другим пользователям в своей группе или всем пользователям ПК СВ в соответствии с установленными полномочиями.

3.2.6.1. Управление доступом к образу в интерфейсе командной строки

Управление доступом осуществляется с помощью команды `oneimage chmod` путем настройки битов прав доступа.

Примеры:

1. Предоставление всем пользователям группы общего доступ к образу 0 путем настройки бита прав типа USE для GROUP:

а) просмотр установленных разрешений, пример вывода после выполнения команды `oneimage show 0`:

```
...
PERMISSIONS
OWNER : um-
GROUP : ---
OTHER : ---
...
```

б) изменение установленных разрешений: `oneimage chmod 0 640`;

в) просмотр новых установленных разрешений, пример вывода после выполнения команды `oneimage show 0`:

```
...
PERMISSIONS
OWNER : um-
GROUP : u--
OTHER : ---
...
```

2. Предоставление всем пользователям группы прав типа USE и MANAGE на образ 0, а остальным пользователям — только права типа USE:

а) изменение установленных разрешений: `oneimage chmod 0 664`;

б) просмотр новых установленных разрешений, пример вывода после выполнения команды `oneimage show 0`:

```
...
PERMISSIONS
OWNER : um-
GROUP : um-
OTHER : u--
...
```

3.2.6.2. Управление доступом к образу в веб-интерфейсе ПК СВ

Для просмотра полномочий, установленных для образа, необходимо в меню слева выбрать пункт «Хранилище — Образы» и на открывшейся странице «Образы» выбрать необходимый образ. На открывшейся странице образа (вкладка «Сведения») будут отображены разрешения, установленные для образа.

Пример

Просмотр установленных разрешений для образа с идентификатором 2 (см. рис. 11).

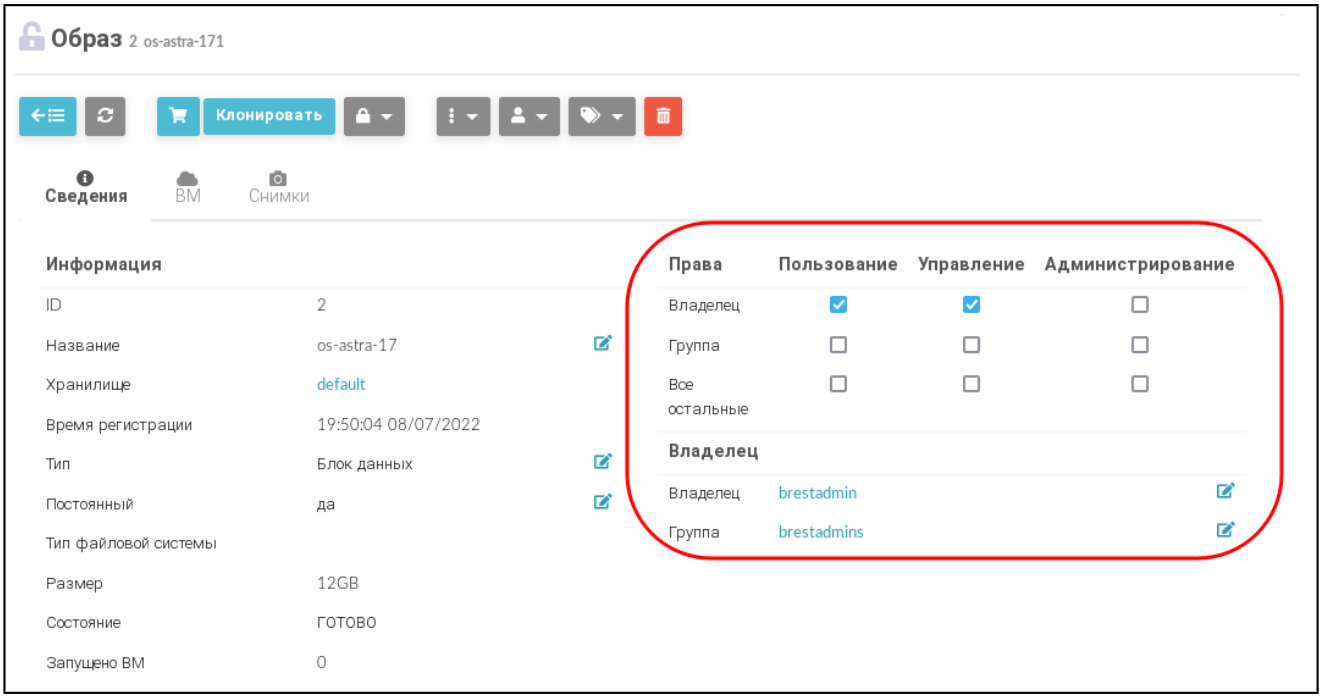

Рис. 11

В представленном примере в отношении образа с идентификатором 2 владелец `brestadmin` имеет полномочия типа USE и MANAGE. Другие пользователи не имеют полномочий в отношении данного образа.

Для изменения полномочий необходимо на странице образа во вкладке «Сведения» установить/снять соответствующие флаги.

3.2.7. Присвоение образам атрибута «постоянный»

ВНИМАНИЕ! Допускается изменение атрибута «постоянный»/«непостоянный» только образов, которые находятся в состоянии READY (ГОТОВО).

3.2.7.1. В интерфейсе командной строки

Для присвоения образу атрибута «постоянный»/«непостоянный» в интерфейсе командной строки используется команда:

```
oneimage persistent / nonpersistent <идентификатор_образа>
```

В качестве идентификатора образа можно указать перечень идентификаторов, разделенных запятыми или диапазон идентификаторов (в качестве разделителя используются две точки — «..»).

3.2.7.2. В веб-интерфейсе ПК СВ

Для присвоения образу атрибута «постоянный»/«непостоянный» в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

1) в меню слева выбрать пункт «Хранилище — Образы»;
2) на открывшейся странице «Образы»:
   a) выбрать необходимые образы,

б) нажать кнопку изменения атрибутов образ и в открывшемся меню выбрать пункт «Сделать постоянным» / «Сделать непостоянным» (см. рис. 12).

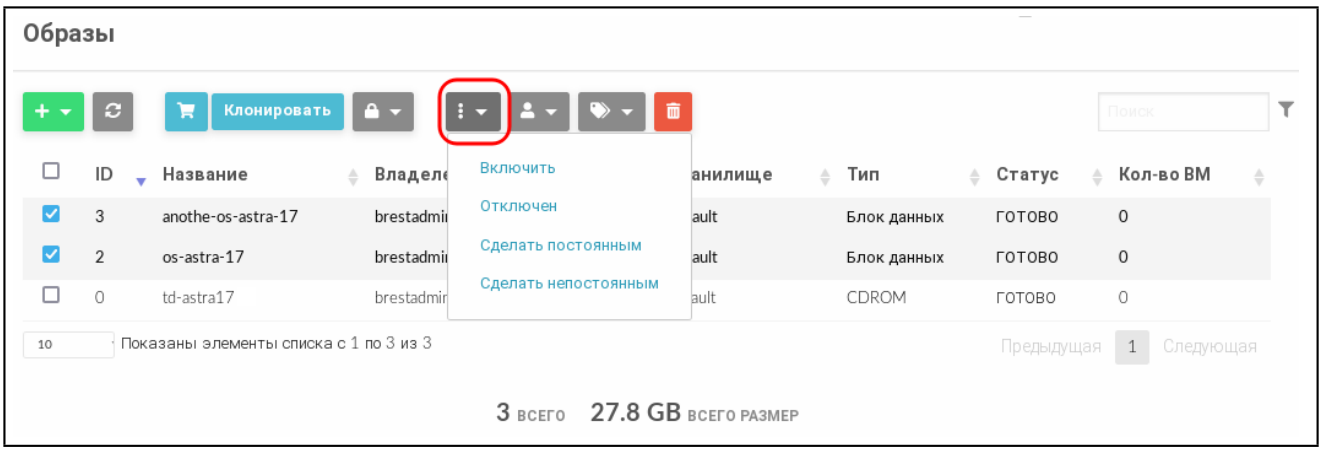

Рис. 12

3.2.8. Управление снимками в постоянных образах

Постоянные образы могут иметь снимки состояния, создаваемые пользователем во время работы ВМ, которая использует данный постоянный образ (см. 3.4.4). Снимки состояния постоянного образа сохраняются после удаления ВМ.

3.2.8.1. В интерфейсе командной строки

Ниже представлены команды, которые позволяют пользователю напрямую управлять снимками.

Для возвращения состояния образа к состоянию, сохраненному в заданном снимке, используется команда:

```
oneimage snapshot-revert <идентификатор_образа> <идентификатор_снимка>
```

Команда удаляет все несохраненные данные.

Для преобразования в образ без снимков используется команда (при этом образ будет приведен в состояние, сохраненное в заданном снимке):

```
oneimage snapshot-flatten <идентификатор_образа> <идентификатор_снимка>
```

Аналогична команде `snapshot-revert` с последующим удалением всех снимков.

Для удаления снимка используется команда:

```
oneimage snapshot-delete <идентификатор_образа> <идентификатор_снимка>
```

Команда будет выполнена только если снимок не является активным и не имеет зависимых элементов.

3.2.8.2. В веб-интерфейсе ПК СВ

Для управления снимками образов в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

1) в меню слева выбрать пункт «Хранилище — Образы»;
2) на открывшейся странице «Образы» выбрать необходимый образ;

3) на странице образа открыть вкладку «Снимки» (см. рис. 13).

Рис. 13

На странице образа во вкладке «Снимки»:

- для преобразования в образ без снимков нажать на кнопку **[Выровнять]**. При этом образ будет возвращен к состоянию, сохраненному в заданном снимке. И все снимки будут удалены;
- для возвращения образа к состоянию, указанному в снимке, необходимо нажать на кнопку **[Откатить]**;
- для удаления снимка состояния образа необходимо нажать на кнопку **[Удалить]**.

3.3. Управление шаблонами виртуальной машины

В ПК СВ виртуальные машины определяются при помощи шаблонов ВМ. Пул шаблонов ВМ позволяет администраторам и пользователям ПК СВ тиражировать экземпляры ВМ. Данные шаблоны могут использоваться несколькими пользователями.

Перечень шаблонов, доступных каждому пользователю, определяется владельцем и зависит от полномочий, установленных в отношении шаблона.

3.3.1. Параметры шаблона ВМ

В ПК СВ параметры шаблона, определяющего ВМ, объединены в следующие группы:

- наименование и производительность ВМ, включает следующие обязательные параметры:
  - `NAME` — наименование шаблона/ВМ (если из шаблона разворачивается несколько экземпляров ВМ, то наименования ВМ будут иметь вид: `<наименование_шаблона>-<идентификатор_ВМ>`),
  - `MEMORY` — объем памяти (в МБ),
  - `CPU` — процент используемой мощности ЦП (в сотых долях). Например, если для ВМ зарезервировано 50% мощности ЦП узла виртуализации, то значение составит «0,5»,
  - `VCPU` — количество виртуальных ЦП;
- блок параметров диска ВМ (`DISK`) обязательно должен содержать параметр `IMAGE`

(наименование образа), а также может содержать такие необязательные параметры, как IMAGE_UNAME (имя владельца образа) или DISK_TYPE (тип образа). Блок параметров DISK указывается для каждого образа, подключаемого к ВМ;

- блок параметров сетевого интерфейса (NIC) обязательно должен содержать параметр NETWORK_ID (идентификатор сети). Кроме того, можно указать те параметры сети, которые необходимо переопределить при создании ВМ (например, IP-адрес или MAC-адрес). Блок параметров NIC указывается для каждого сетевого интерфейса в создаваемой ВМ;
- необязательные блоки параметров, например, средства графического доступа, порядок загрузки, контекстная информация.

3.3.2. Создание шаблонов ВМ

3.3.2.1. В интерфейсе командной строки

Для создания шаблона можно воспользоваться командой onetemplate create, указав в качестве аргументов все обязательные и необязательные параметры шаблона или файл шаблона, в котором эти параметры перечислены.

Примеры:

1. Создание шаблона ВМ с использованием файла, в котором перечислены параметры ВМ:

а) создать файл alse.tmpl следующего содержания:

```
NAME = test-vm
MEMORY = 2048
CPU = "0.25"
DISK = [
IMAGE = "os-astra-17",
IMAGE_UNAME = "brestadmin" ]
DISK = [
IMAGE = "td-astra17",
IMAGE_UNAME = "brestadmin" ]
NIC = [
NETWORK = "virtnetwork",
NETWORK_UNAME = "brestadmin",
SECURITY_GROUPS = "0" ]
OS = [
BOOT = "disk0,disk1" ]
```

б) создать шаблон с использованием файла alse.tmpl:

```
onetemplate create alse.tmpl
```

Пример вывода после выполнения команды:

```
ID: 2
```

в) просмотр перечня шаблонов. Пример вывода после выполнения команды `onetemplate list`:

```
ID   USER      GROUP      NAME     REGTIME
2    oneadmin  brestadm   test-vm  07/18 14:40:22
1    brestadm  brestadm   ALSE-17 07/18 12:45:38
```

2. Создание шаблона ВМ с указанием параметров в качестве аргумента команды:

а) выполнить следующую команду:

```
onetemplate create --name test-vm2 --memory 2048 --cpu "0.25" \
--disk "anothe-os-astra-17" --nic Public
```

Пример вывода после выполнения команды:

```
ID: 3
```

б) просмотр перечня шаблонов. Пример вывода после выполнения команды `onetemplate list`:

```
ID   USER      GROUP      NAME     REGTIME
2    oneadmin  brestadm   test-vm2 07/18 14:50:27
2    oneadmin  brestadm   test-vm  07/18 14:40:22
1    brestadm  brestadm   ALSE-17 07/18 12:45:38
```

3.3.2.2. В веб-интерфейсе ПК СВ

Для того чтобы создать шаблон ВМ в веб-интерфейсе ПК СВ, необходимо выполнить следующие действия:

1) в меню слева выбрать пункт «Шаблоны — ВМ»;

2) на открывшейся странице «Шаблоны ВМ» нажать кнопку **[+]** и в открывшемся меню выбрать пункт «Создать»;

3) на открывшейся странице «Создать шаблон ВМ» во вкладке «Общие» (см. рис. 14) в поле «Название» задать наименование шаблона, в секции «Гипервизор» установить соответствующий флаг (например, `KVM`) и указать основные параметры ВМ (память, процессор и т.п.);

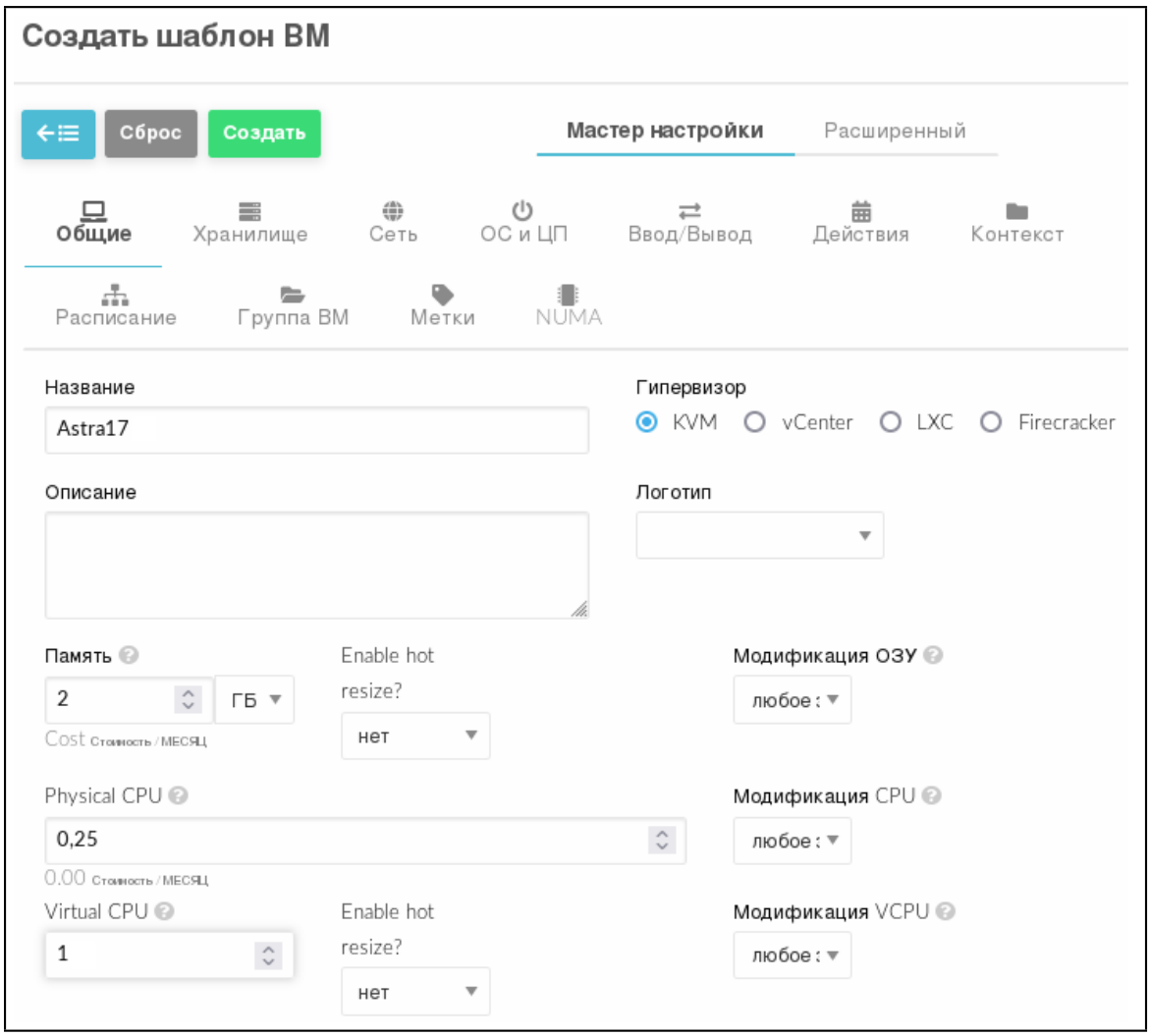
Создать шаблон ВМ
Сброс
Создать
Мастер настройки
Расширенный
Общие
Хранилище
Сеть
ОС и ЦП
Ввод/Вывод
Действия
Контекст
Расписание
Группа ВМ
Метки
NUMA
Название
Astra17
Гипервизор
KVM
vCenter
LXC
Firecracker
Описание
Логотип
Память
2
ГБ
Cost Стоимость / МЕСЯЦ
Enable hot resize?
нет
Модификация ОЗУ
любое
Physical CPU
0,25
0.00 Стоимость / МЕСЯЦ
Модификация CPU
любое
Virtual CPU
1
Enable hot resize?
нет
Модификация VCPU
любое

Рис. 14

4) на странице «Создать шаблон ВМ» во вкладке «Хранилище» (см. рис. 15):

а) для `Диска 0` указать загрузочный диск ВМ;

б) если необходимо подключить CDROM, то в левом поле нажать кнопку **[+]** и для `Диска 1` указать соответствующий образ;

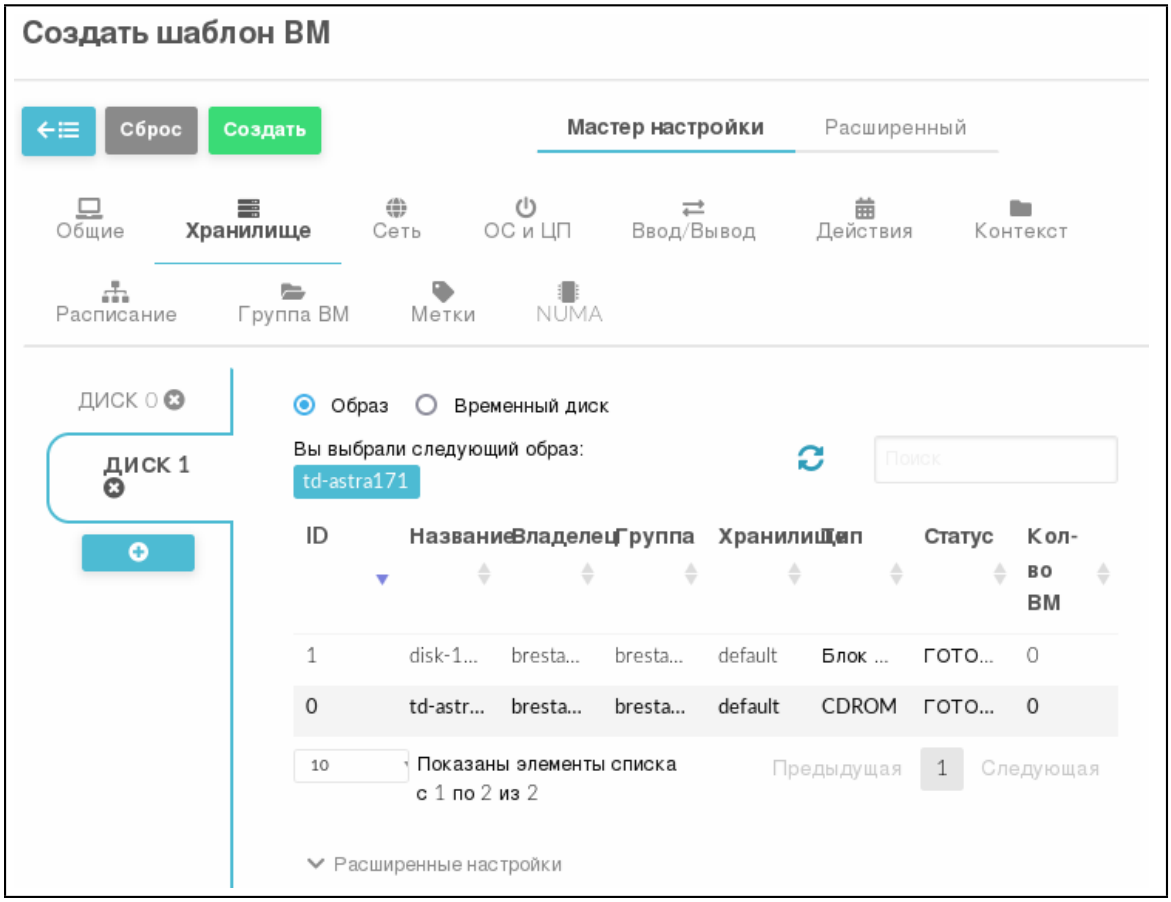

Рис. 15

5) на странице «Создать шаблон ВМ» во вкладке «Сеть» (см. рис. 16) указать виртуальную сеть, к которой будут подключены ВМ;

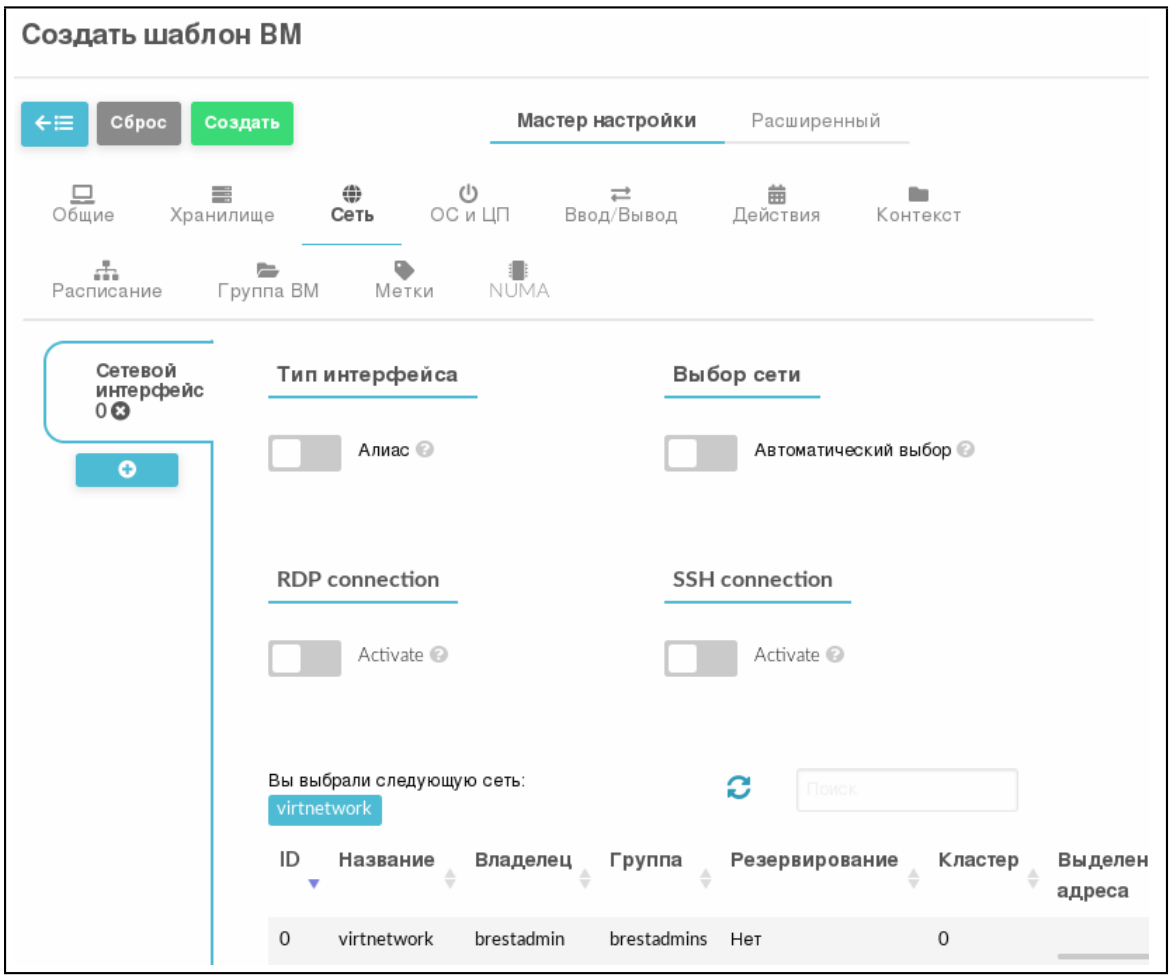

Рис. 16

6) на странице «Создать шаблон ВМ» во вкладке «ОС и ЦП»:

а) в секции «Загрузка» (см. рис. 17) определить очередность использования образов при загрузке ОС;

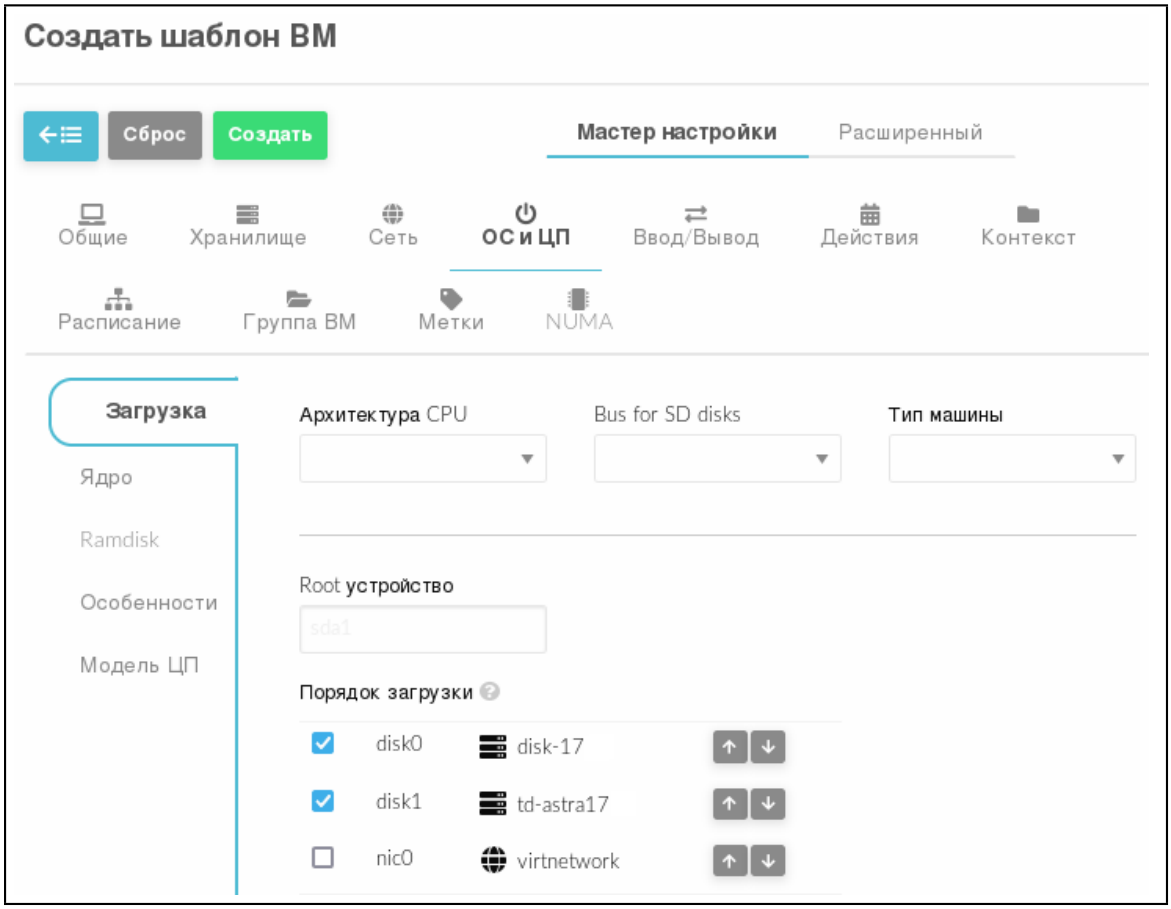

Рис. 17

б) для обеспечения функционирования контекстуализации, в секции «Особенности» (см. рис. 18) в выпадающем списке `Гостевой агент QEMU` выбрать значение `Да`;

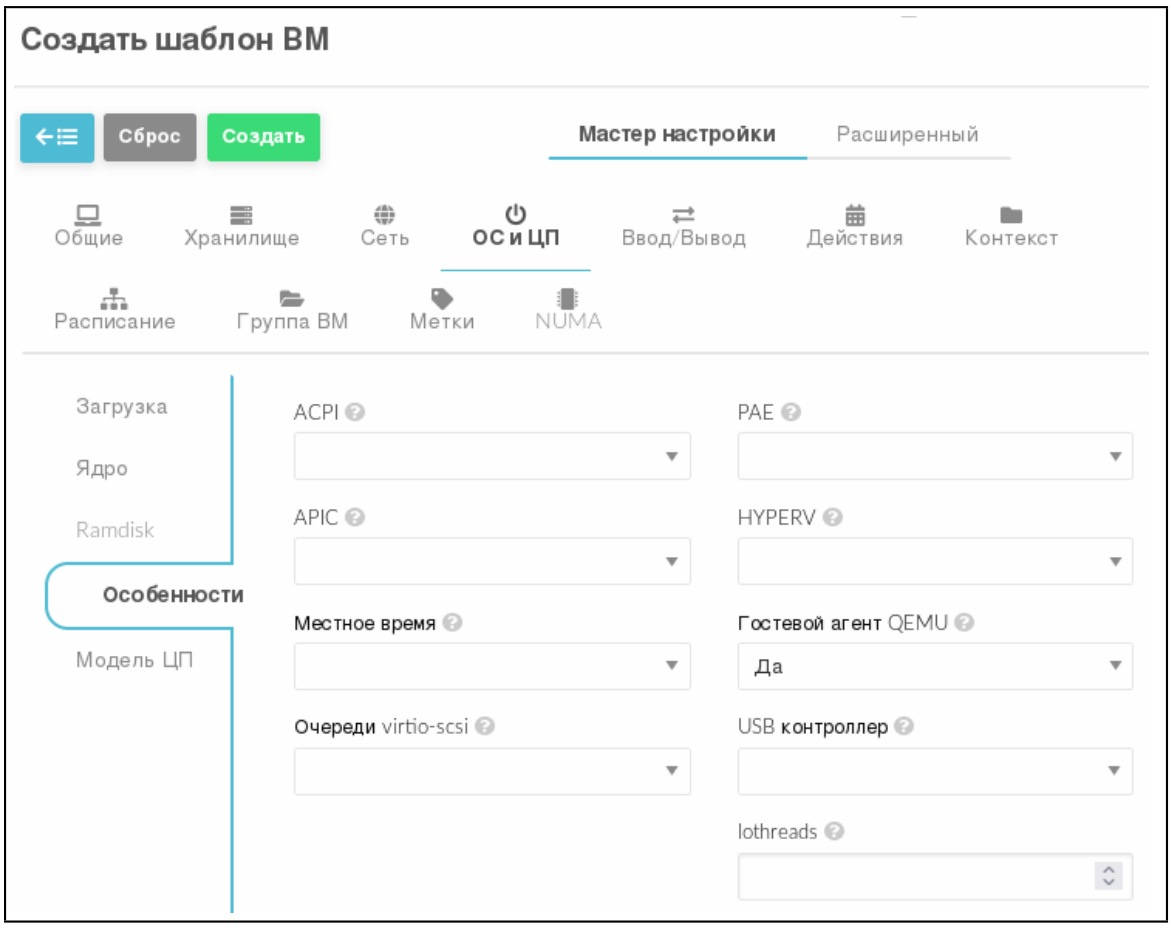

Рис. 18

7) на странице «Создать шаблон ВМ» нажать кнопку **[Создать]**. После этого на открывшейся странице «Шаблоны ВМ» отобразится созданный шаблон (см. рис. 19).

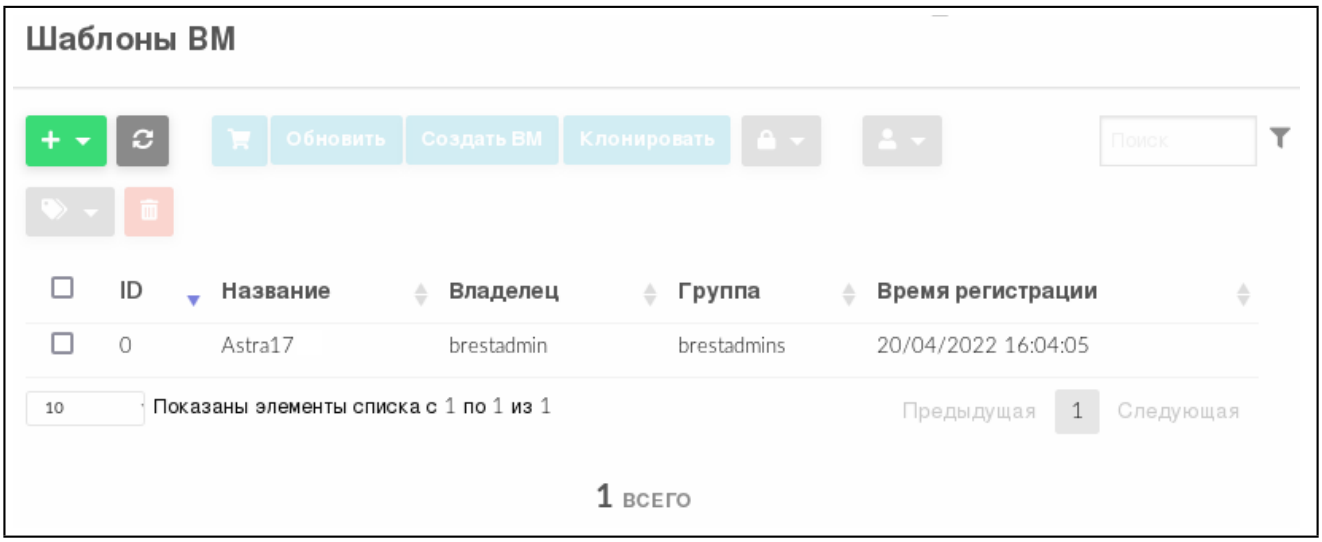

Рис. 19

3.3.3. Отображение доступных шаблонов и просмотр информации о шаблоне

3.3.3.1. В интерфейсе командной строки

Для отображения шаблонов, доступных пользователю, необходимо использовать команду `onetemplate list`. Пример вывода после выполнения команды:

```
ID USER     GROUP    NAME      REGTIME
2  oneadmin brestadm test-vm2  07/18 18:58:19
1  oneadmin brestadm test-vm   07/18 18:56:50
0  brestadm brestadm ALSE-17   07/18 16:22:18
```

Для просмотра полной информации о шаблоне необходимо использовать команду:

```
onetemplate show <идентификатор_шаблона>
```

Пример вывода после выполнения команды `onetemplate show 2`:

```
TEMPLATE 2 INFORMATION
ID             : 2
NAME           : test-vm2
USER           : oneadmin
GROUP          : brestadmins
LOCK           : None
REGISTER TIME  : 07/18 18:58:19

PERMISSIONS
OWNER          : um-
GROUP          : u--
OTHER          : ---

TEMPLATE CONTENTS
CPU="0.25"
DISK=[
IMAGE="os-astra-17" ]
HOT_RESIZE=[
CPU_HOT_ADD_ENABLED="NO",
MEMORY_HOT_ADD_ENABLED="NO" ]
INPUTS_ORDER=""
MEMORY="2048"
MEMORY_UNIT_COST="MB"
NIC=[
NETWORK="virtnetwork",
NETWORK_UNAME="brestadmin",
SECURITY_GROUPS="0" ]
```

3.3.3.2. В веб-интерфейсе ПК СВ

Для отображения шаблонов, доступных пользователю, в веб-интерфейсе ПК СВ необходимо в меню слева выбрать пункт «Шаблоны — ВМ». На открывшейся странице «Шаблоны ВМ» будет отображена таблица шаблонов (см. рис. 20).

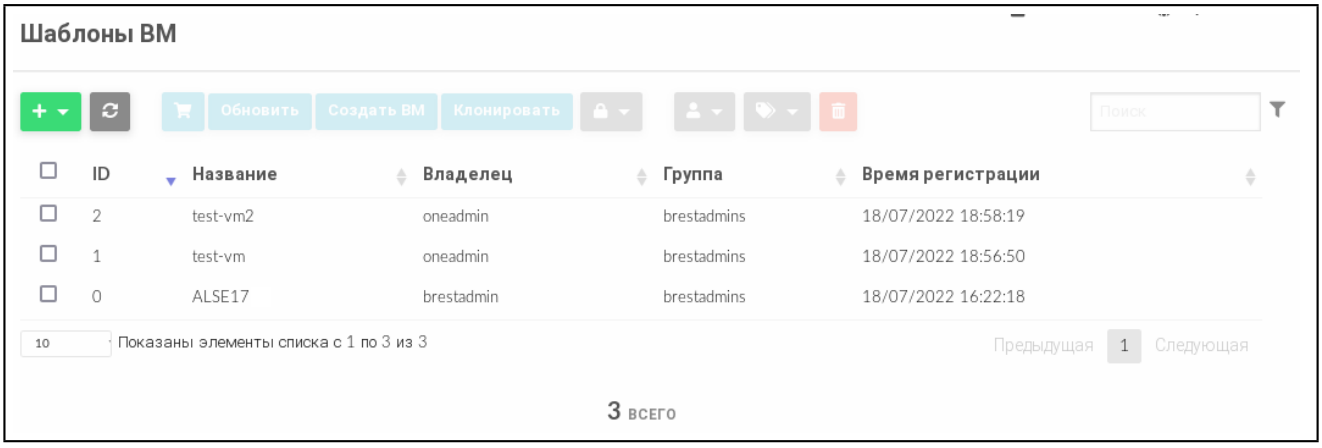

Рис. 20

Для просмотра информации о конкретном шаблоне необходимо на странице «Шаблоны ВМ» выбрать необходимый шаблон. После этого откроется страница шаблона (вкладка «Сведения») — см. рис. 21.

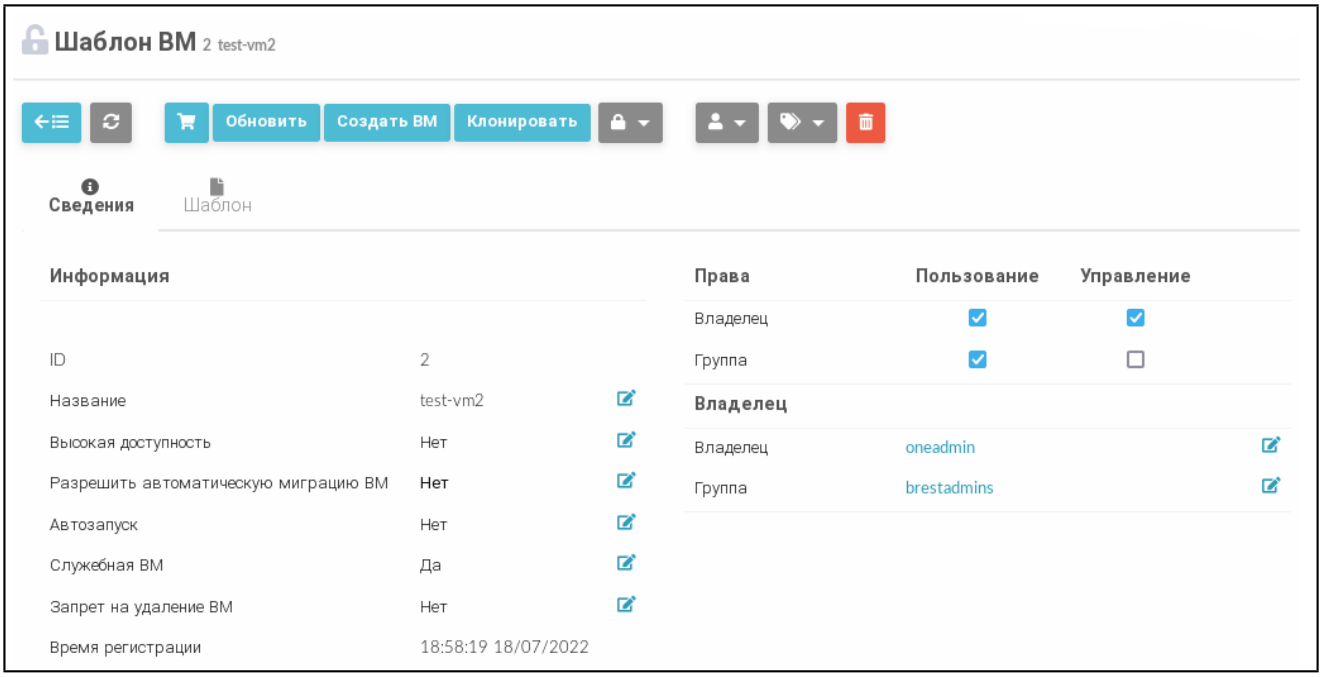

Рис. 21

3.3.4. Изменение параметров шаблона

3.3.4.1. В интерфейсе командной строки

Для изменения параметров шаблона необходимо использовать команду

```
onetemplate update <идентификатор_шаблона> [<файл_параметров>]
```

где `<файл_параметров>` — файл в котором перечислены параметры ВМ, заменяющие значения, которые были ранее определены в шаблоне. Если файл параметров не указан, то после ввода команды откроется текстовый редактор `Vim` для редактирования шаблона ВМ.

3.3.4.2. В веб-интерфейсе ПК СВ

Чтобы изменить параметры шаблона, в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

1) в меню слева выбрать пункт «Шаблоны — ВМ» и на открывшейся странице «Шаблоны ВМ» выбрать необходимый шаблон;

2) на открывшейся странице «Шаблон ВМ» нажать кнопку **[Обновить]**;

3) на открывшейся странице «Изменить шаблон ВМ» внести необходимые изменения и нажать кнопку **[Обновить]**.

3.3.5. Клонирование шаблонов

3.3.5.1. В интерфейсе командной строки

Клонировать существующий шаблон возможно с помощью команды:

```
onetemplate clone <идентификатор_шаблона> <наименование_нового_шабона>
```

При использовании аргумента `--recursive` будут клонированы все образы, указанные в шаблоне (параметр `IMAGE`).

Примеры:

1. Клонирование шаблона с идентификатором 0, а также образов, указанных в этом шаблоне:

```
onetemplate clone 0 clone_template --recursive
```

Пример вывода после выполнения команды:

```
VM ID: 4
```

2. Просмотр перечня образов. Пример вывода после выполнения команды `oneimage list`:

```
ID USER     GROUP    NAME                    DATASTORE  SIZE  TYPE PER
4  oneadmin brestadm clone_template-disk-1   default    3.8G  CD    No
3  oneadmin brestadm clone_template-disk-0   default     12G  DB   Yes
2  brestadm brestadm os-astra-17            default     12G  DB   Yes
1  brestadm brestadm td-alse17              default    3.8G  CD    No
0  brestadm brestadm os-alse17              default     12G  DB   Yes
```

3.3.5.2. В веб-интерфейсе ПК СВ

Для клонирования шаблона, в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

1) в меню слева выбрать пункт «Шаблоны — ВМ» и на открывшейся странице «Шаблоны ВМ» выбрать необходимый шаблон;

2) на открывшейся странице «Шаблон ВМ» нажать кнопку **[Клонировать]**;

3) на открывшейся странице «Клонировать шаблон ВМ»:

   а) задать наименование нового шаблона,

б) нажать кнопку **[Клонировать]** или на кнопку **[Клонировать с образами]**, если также необходимо клонировать все образы, указанные в шаблоне.

3.3.6. Общие шаблоны

Пользователи могут предоставлять общий доступ к своим шаблонам другим пользователям в своей группе или всем пользователям в ПК СВ, указав соответствующие полномочия.

3.3.6.1. В интерфейсе командной строки

Изменить установленные полномочия можно при помощи команды `chmod` с указанием идентификатора шаблона и числового кода полномочий.

Примеры:

1. Исходное состояние, пример вывода после выполнения команды `onetemplate show 0`:

```
...
PERMISSIONS
OWNER          : um-
GROUP          : u--
OTHER          : ---
```

2. Установка полномочий в отношении шаблона с идентификатором 0:
   - владельцу установить биты USE и MANAGE (разрешить применение и управление);
   - пользователям группы установить биты USE и MANAGE;
   - остальным пользователям установить бит USE.

Для этого необходимо выполнить команду:

```
onetemplate chmod 0 664
```

Просмотр установленных полномочий, пример вывода после выполнения команды `onetemplate show 0`:

```
...
PERMISSIONS
OWNER : um-
GROUP : um-
OTHER : u--
```

3. Установка полномочий в отношении шаблона с идентификатором 0:
   - владельцу установить биты USE и MANAGE (разрешить применение и управление);
   - пользователям группы установить бит USE;
   - остальным пользователям установить бит USE.

Для этого необходимо выполнить команду:

```
onetemplate chmod 0 644
```

Просмотр установленных полномочий, пример вывода после выполнения команды `onetemplate show 0`:

```
...
PERMISSIONS
OWNER : um-
GROUP : u--
OTHER : u--
```

4. Установка полномочий в отношении шаблона с идентификатором 0:
   - владельцу установить биты USE и MANAGE (разрешить применение и управление);
   - пользователям группы снять все биты (отозвать все полномочия);
   - остальным пользователям установить биты USE, MANAGE и ADMIN (разрешить применение, управление и администрирование).

Для этого необходимо выполнить команду:

```
onetemplate chmod 0 607
```

Просмотр установленных полномочий, пример вывода после выполнения команды `onetemplate show 0`:

```
...
PERMISSIONS
OWNER : um-
GROUP : ---
OTHER : uma
```

Кроме того, аргумент команды `--recursive`, выполнит действие по изменению полномочий в отношении каждого образа, указанного в шаблоне (параметр `IMAGE`).

3.3.6.2. В веб-интерфейсе ПК СВ

Для просмотра полномочий, установленных в отношении шаблона, необходимо перейти на страницу этого шаблона (вкладка «Сведения»).

Пример

Просмотр полномочий, установленных в отношении шаблона с идентификатором 0 (см. рис. 22).

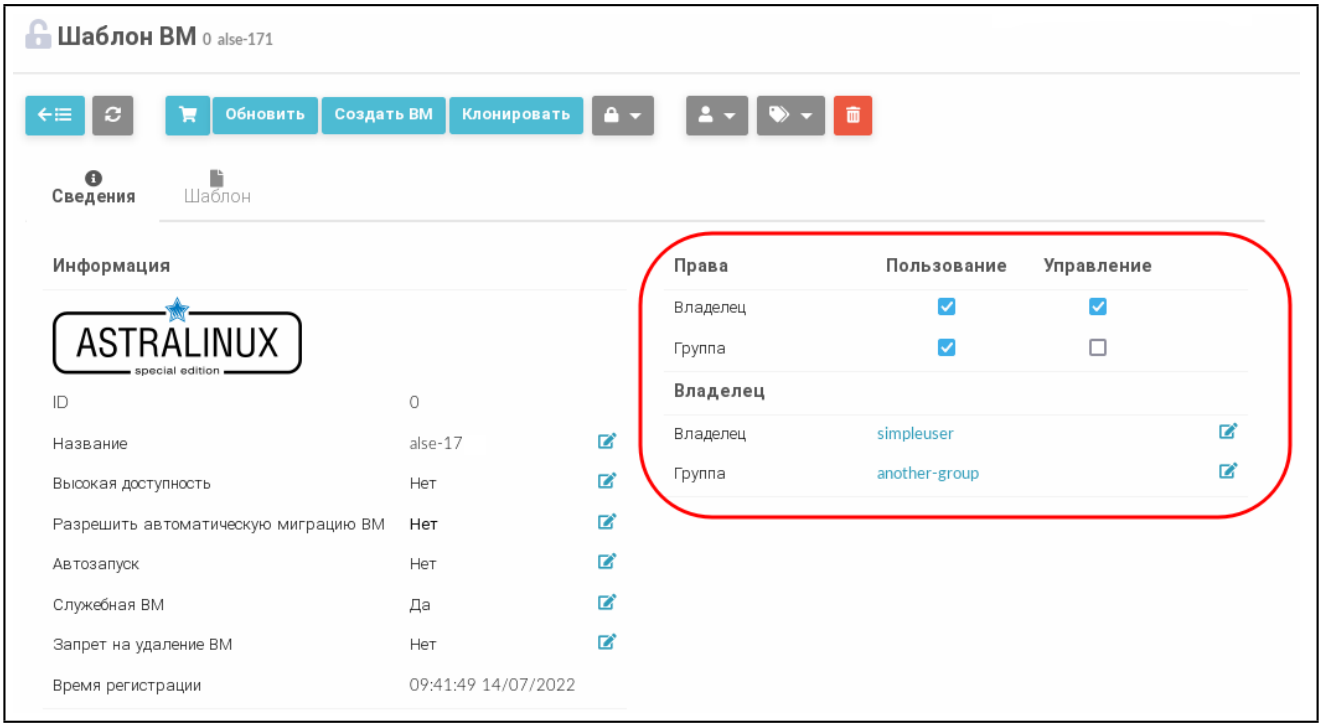

Рис. 22

В представленном примере в отношении шаблона 0 владелец `simpleuser` имеет полномочия типа USE и MANAGE. Пользователи в группе `another-group` имеют полномочия типа USE, другие пользователи не имеют полномочий в отношении данного шаблона.

Для изменения полномочий необходимо на странице шаблона во вкладке «Сведения» установить/снять соответствующие флаги.

3.3.7. Удаление шаблонов

3.3.7.1. В интерфейсе командной строки

Для удаления шаблона необходимо выполнить команду:

```
onetemplate delete <идентификатор_шаблона>
```

В качестве идентификатора шаблона можно указать перечень идентификаторов, разделенных запятыми или диапазон идентификаторов (в качестве разделителя используются две точки — «..»).

Кроме того, при указании аргумента команды `--recursive` будет удален каждый образ, указанный в шаблоне (параметр `IMAGE`).

3.3.7.2. В веб-интерфейсе ПК СВ

Для удаления шаблона в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

1) в меню слева выбрать пункт «Шаблоны — ВМ»;

2) на открывшейся странице «Шаблоны ВМ» отметить необходимые шаблоны и нажать кнопку **[Удалить]** (см. рис. 23);

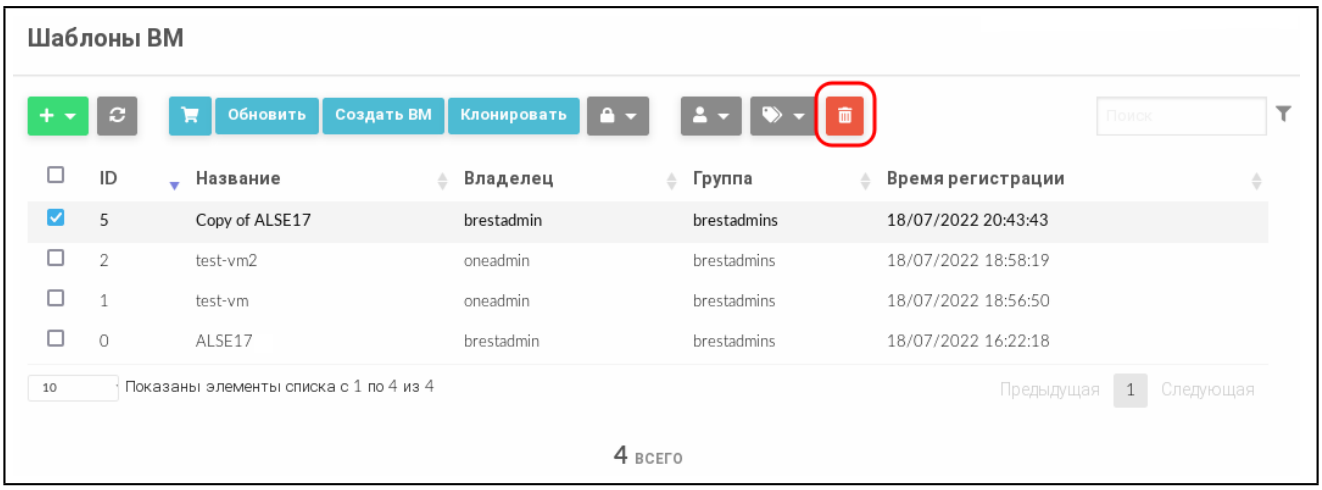

Рис. 23

3) в открывшемся окне нажать кнопку **[Удалить]** или **[Удалить все образы]**, если также необходимо удалить все образы, указанные в шаблоне. (см. рис. 24).

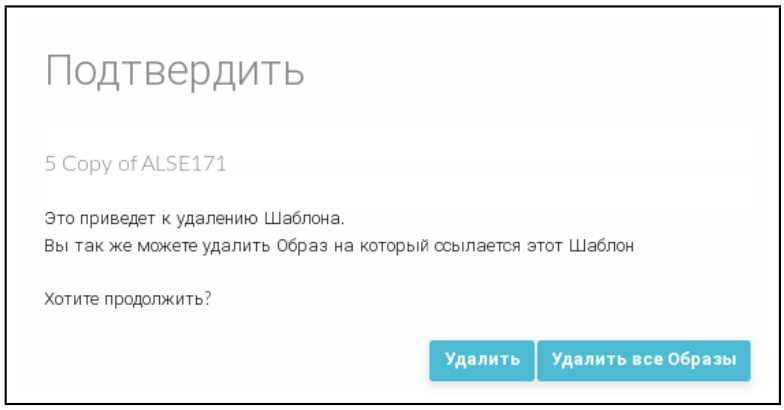

Рис. 24

3.3.8. Развертывание ВМ из шаблона

3.3.8.1. В интерфейсе командной строки

Для развертывания ВМ из шаблона можно воспользоваться командой:

`onetemplate instantiate <идентификатор_шаблона> [<файл_параметров>]`

где `<файл_параметров>` — файл в котором перечислены параметры ВМ, заменяющие значения, которые были определены в шаблоне. Кроме того, возможно вместо файла параметров в команде в качестве аргумента указывать новые значения параметров.

Примеры:

1. Развертывание ВМ из шаблона с идентификатором 2, при этом для ВМ будет выделено 3 ГБ оперативной памяти (в шаблоне установлено 2 ГБ):

```
onetemplate instantiate 2 --memory 3072
```

Пример вывода после выполнения команды:

```
VM ID: 1
```

2. Просмотр перечня ВМ. Пример вывода после выполнения команды `onevm list`:

```
ID USER     GROUP     NAME        STAT  CPU   MEM HOST            TIME
1  oneadmin brestadm  test-vm-1   prol  0.25  3G  172.16.1.210    0d 00h00
```

С помощью аргумента `--multiple <количество_ВМ>` можно создать более одного экземпляра одновременно. При этом наименования ВМ будут иметь вид: `<наименование_шаблона>-<идентификатор_ВМ>`

Пример

Развертывание двух ВМ из шаблона с идентификатором 0:

```
onetemplate instantiate 0 --multiple 2
```

3.3.8.2. В веб-интерфейсе ПК СВ

Для развертывания ВМ из шаблона в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

1) в меню слева выбрать пункт «Шаблоны — ВМ»;
2) на открывшейся странице «Шаблоны ВМ» выбрать необходимый шаблон;
3) на открывшейся странице «Шаблон ВМ» нажать кнопку **[Создать ВМ]** (см. рис. 25);

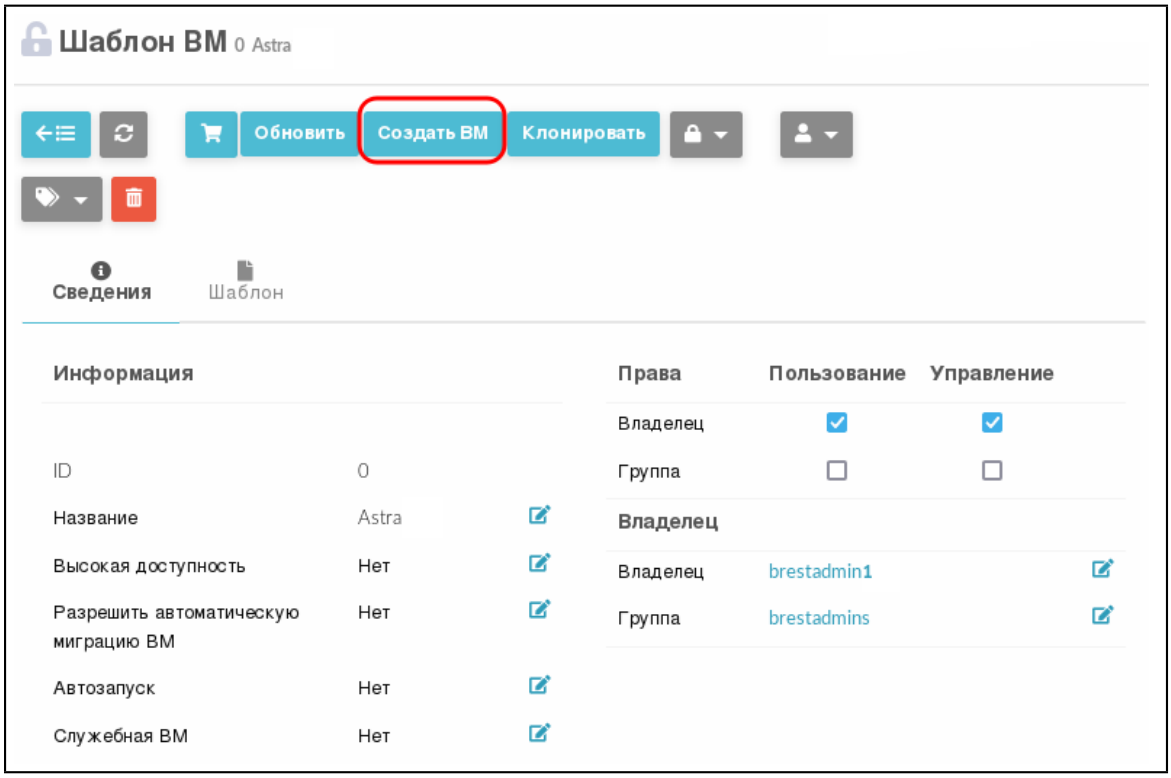

Рис. 25

4) на открывшейся странице «Создать ВМ» в поле «Имя ВМ» задать наименование и количество экземпляров ВМ и нажать кнопку **[Создать ВМ]** (см. рис. 26);

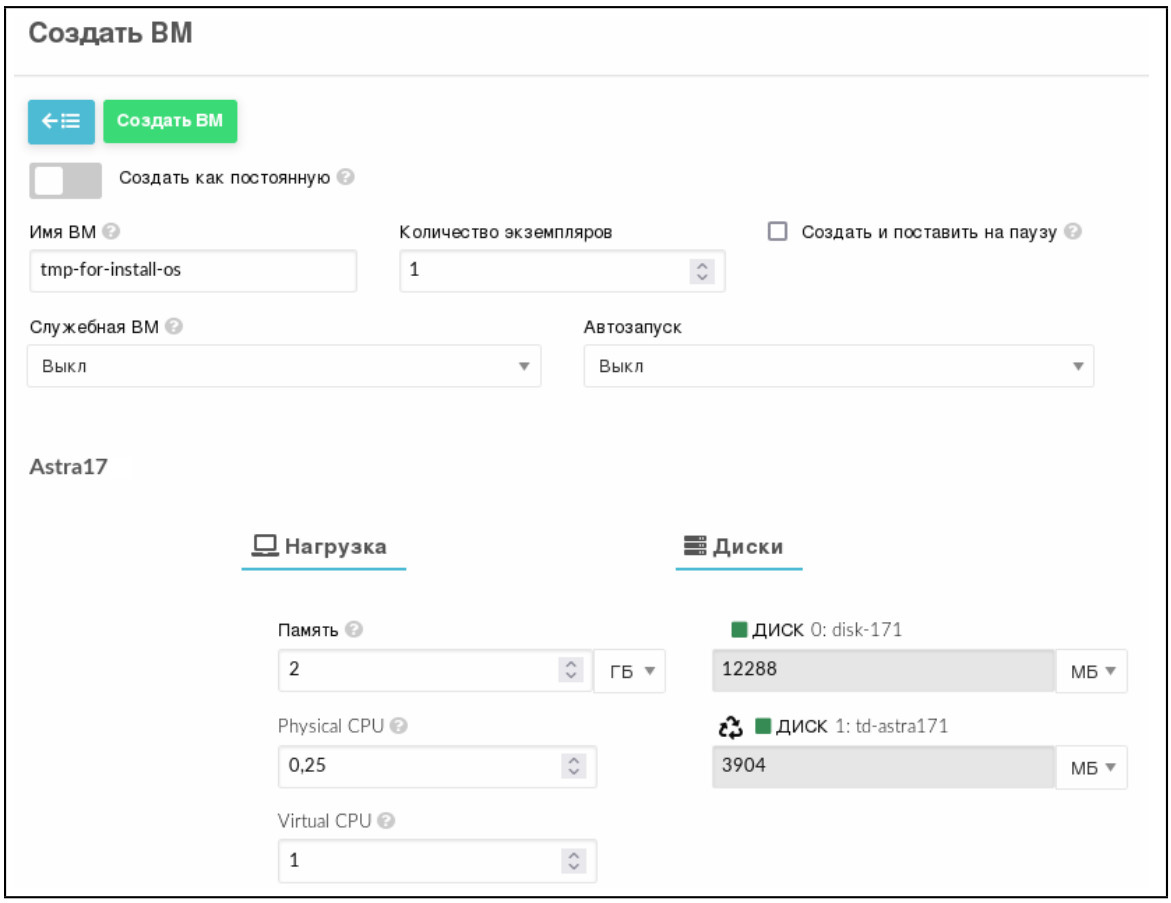

Рис. 26

ВНИМАНИЕ! Если при создании ВМ указать только один сервер виртуализации для развертывания, в шаблон ВМ будет добавлена опция `SCHED_REQUIREMENTS` с идентификатором указанного сервера. Планировщик, в таком случае, будет использовать для планирования только указанный сервер (например, при выполнении команды `onevm resched ID_VM`).

В случае указания нескольких серверов виртуализации для развертывания ВМ, при работе планировщика будут использоваться только указанные в списке сервера. Если при создании ВМ сервер виртуализации для развертывания не указан, планировщик будет учитывать все сервера виртуализации в заданном кластере.

5) в веб-интерфейсе в меню слева выбрать пункт «Экземпляры ВМ — ВМ» и дождаться пока в поле «Статус» для созданной на предыдущем шаге ВМ значение `Инициализация` не изменится на `ВЫКЛЮЧЕНО` (промежуточные значения: `Ожидание` и `Пролог`). Для обновления значения статуса можно воспользоваться кнопкой **[Обновить]** (см. рис. 27).

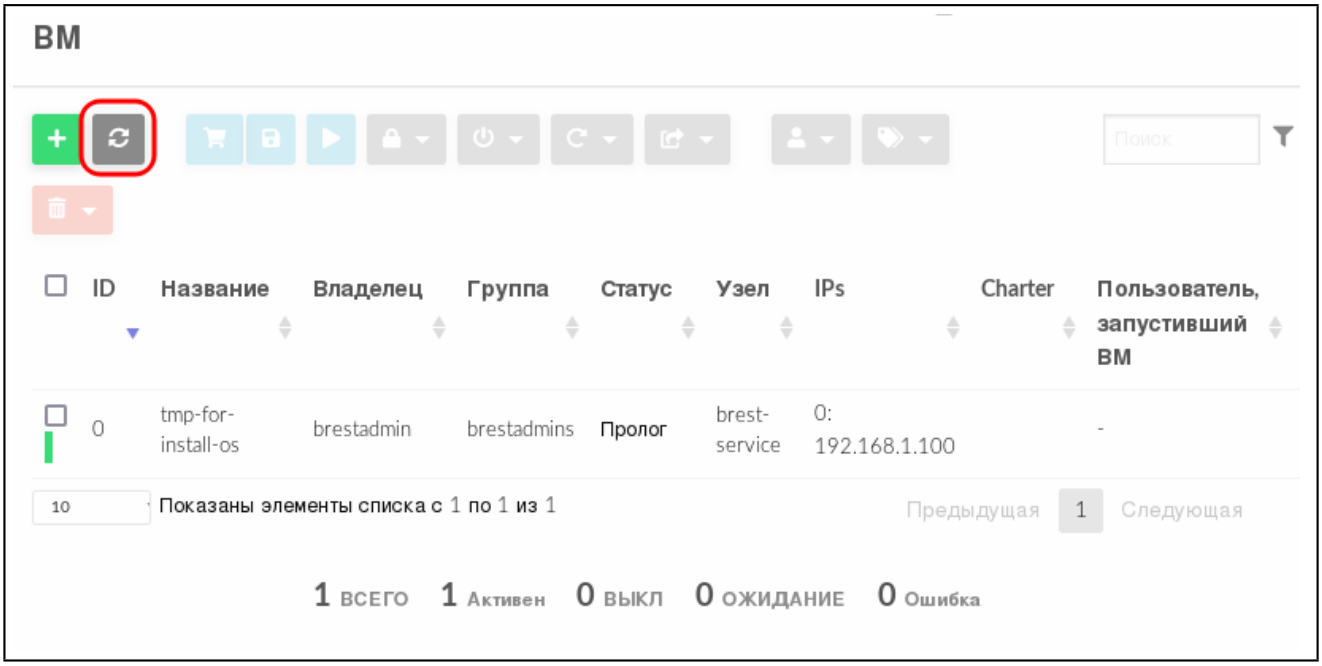

Рис. 27

3.4. Управление экземплярами ВМ

3.4.1. Статус и жизненный цикл виртуальной машины

В процессе функционирования экземпляру ВМ присваивается один из статусов, описание которых приведено в таблице 6.

Таблица 6

Статус	Сокращенное название статуса	Описание
INIT	init	Внутренний статус инициализации после создания ВМ, этот статус не виден пользователям
PENDING	pend	Ожидается выделение ресурсов виртуализации для запуска ВМ. ВМ остается в этом статусе, пока не будет развернута планировщиком или пользователем при помощи команды `onevm deploy`
HOLD	hold	Разработчик ВМ поставил ВМ на удержание, она не доступна для развертывания в автоматическом режиме, пока не будет разблокирована. Однако ее можно развернуть вручную
ACTIVE	см. таблицу 7	ВМ запущена и находится в одном из состояний жизненного цикла (см. таблицу 7)
STOPPED	stop	ВМ остановлена. Снимок состояния ВМ (файл `checkpoint`) было сохранен и перенесен вместе с образами дисков в хранилище образов. Ресурсы сервера виртуализации (ЦПУ и память) освобождаются

Окончание таблицы 6

Статус	Сокращенное название статуса	Описание
SUSPENDED	susp	Аналогично статусу STOPPED, но снимок состояния ВМ (файл `checkpoint`) и образы дисков остаются на сервере виртуализации, чтобы позже возобновить на нем работу ВМ (т.е. нет необходимости перепланировать ВМ). Ресурсы сервера виртуализации (ЦПУ и память) не освобождаются
DONE	done	ВМ удалена. ВМ в этом статусе отображается при использовании команды `onevm list`, но информация о ВМ останется в БД. Информацию о удаленной ВМ можно получить с помощью команды `onevm show`
POWEROFF	poff	Аналогичен статусу SUSPENDED, но снимок состояния ВМ (файл `checkpoint`) не сохраняется. Образы дисков остаются на сервере виртуализации для последующего запуска ВМ. Ресурсы сервера виртуализации (ЦПУ и память) не освобождаются. ВМ получает этот статус после завершения работы гостевой ОС, установленной на этой ВМ
UNDEPLOYED	unde	ВМ выключена. Аналогичен статусу STOPPED, но снимок состояния ВМ (файл `checkpoint`) не сохраняется. Образы дисков переносятся в хранилище образов. ВМ может быть запущена позже. Ресурсы сервера виртуализации (ЦПУ и память) освобождаются
CLONING	clon	ВМ ожидает завершение операции клонирования образов дисков (хотя бы один образ диска все еще находится в состоянии `lock`)
CLONING_FAILURE	fail	В процессе клонирования ВМ произошла ошибка (хотя бы один образ диска перешел в состояние `error`)

После запуска жизненный цикл ВМ включает состояния, приведенные в таблице 7.

Таблица 7

Состояние	Сокращенное название состояния	Описание
LCM_INIT	init	ВМ находится в состоянии инициализации, этот внутренний статус и не виден пользователям
PROLOG	prol	Происходит перенос файлов ВМ (образы диска и файл `checkpoint`) на сервер виртуализации, на котором ВМ будет запущена
BOOT	boot	ПК СВ ожидает, пока сервер виртуализации создаст ВМ

Продолжение таблицы 7

Состояние	Сокращенное название состояния	Описание
RUNNING	runn	ВМ находится в работе (данное состояние включает фазы загрузки и отключения ВМ). Состояние ВМ контролируется драйвером виртуализации
MIGRATE	migr	ВМ мигрирует с одного сервера виртуализации на другой без выключения
SAVE_STOP	save	Система сохраняет файлы ВМ после завершения какой-либо операции
SAVE_SUSPEND	save	Система сохраняет файлы ВМ после приостановки какой-либо операции
SAVE_MIGRATE	save	Система сохраняет файлы ВМ для «холодной» миграции (перемещение выключенных ВМ)
PROLOG_MIGRATE	migr	Передача файлов во время «холодной» миграции (перемещение выключенных ВМ)
PROLOG_RESUME	prol	Передача файлов после возобновления действия (связан с статусом STOPPED)
EPILOG_STOP	epil	Передача файлов в хранилище образов
EPILOG	epil	Система очищает сервер виртуализации, который использовался для запуска ВМ, кроме того, образы постоянных дисков перемещаются обратно в хранилище образов
SHUTDOWN	shut	Система отправила сигнал ACPI для выключения ВМ и ожидает, пока процесс выключения завершится. Если по истечении времени ожидания ВМ не выключится, система будет считать, что ОС виртуальной машины проигнорировала сигнал ACPI, а статус ВМ изменится на RUNNING вместо DONE
CLEANUP_RESUBMIT	clea	Очистка после действия удаления/восстановления ВМ
UNKNOWN	unkn	Не удалось определить статус ВМ, она находится в неизвестном состоянии
HOTPLUG	hotp	Выполняется операция подключения/отсоединения диска

Продолжение таблицы 7

Состояние	Сокращенное название состояния	Описание
SHUTDOWN_POWEROFF	shut	Система отправила на ВМ сигнал ACPI о завершения работы и ожидает его выполнения. Если за время ожидания ВМ не исчезнет, система будет считать, что ОС виртуальной машины проигнорировала сигнал ACPI, и статус ВМ будет изменен на RUNNING, вместо POWEROFF
BOOT_UNKNOWN	boot	Система ожидает, пока сервер виртуализации создаст ВМ (связан с статусом UNKNOWN)
BOOT_POWEROFF	boot	Система ожидает, пока сервер виртуализации создаст ВМ (связан с статусом POWEROFF)
BOOT_SUSPENDED	boot	Система ожидает, пока сервер виртуализации создаст ВМ (связан с статусом SUSPENDED)
BOOT_STOPPED	boot	Система ожидает, пока сервер виртуализации создаст ВМ (связан с статусом STOPPED)
CLEANUP_DELETE	clea	Очистка после действия удаления
HOTPLUG_SNAPSHOT	snap	Выполняется снимок состояния
HOTPLUG_NIC	hotp	Выполняется операция подключения/отсоединения сетевого интерфейса
HOTPLUG_SAVEAS	hotp	Выполняется операция сохранения на диске
HOTPLUG_SAVEAS_POWEROFF	hotp	Выполняется операция сохранения на диске (связан с статусом POWEROFF)
HOTPLUG_SAVEAS_SUSPENDED	hotp	Выполняется операция сохранения на диске (связан с статусом SUSPENDED)
SHUTDOWN_UNDEPLOY	shut	Система отправила на ВМ сигнал ACPI для завершения работы и ожидает его выполнения. Если за время ожидания ВМ не будет удалена, система будет считать, что ОС виртуальной машины проигнорировала сигнал ACPI, и статус ВМ будет изменен на RUNNING, вместо UNDEPLOYED
EPILOG_UNDEPLOY	epil	Система очищает сервер виртуализации, который использовался для запуска ВМ, кроме того, образы постоянных дисков перемещаются обратно в хранилище образов

Продолжение таблицы 7

Состояние	Сокращенное название состояния	Описание
PROLOG_UNDEPLOY	prol	Передача файлов после возобновления действия (связан с статусом UNDEPLOY)
BOOT_UNDEPLOY	boot	Система ожидает, пока сервер виртуализации создаст ВМ (связан с статусом UNDEPLOY)
HOTPLUG_PROLOG_POWEROFF	hotp	Передача файлов для подключения к диску при отключении питания
HOTPLUG_EPILOG_POWEROFF	hotp	Передача файлов при отсоединении диска от источника питания
BOOT_MIGRATE	boot	Система ожидает, пока сервер виртуализации создаст ВМ (в результате «холодной» миграции)
BOOT_FAILURE	fail	Сбой при переводе в состояние BOOT
BOOT_MIGRATE_FAILURE	fail	Сбой при переводе в состояние BOOT_MIGRATE
PROLOG_MIGRATE_FAILURE	fail	Сбой при переводе в состояние PROLOG_MIGRATE
PROLOG_FAILURE	fail	Сбой при переводе в состояние PROLOG
EPILOG_FAILURE	fail	Сбой при переводе в состояние EPILOG
EPILOG_STOP_FAILURE	fail	Сбой при переводе в состояние EPILOG_STOP
EPILOG_UNDEPLOY_FAILURE	fail	Сбой при переводе в состояние EPILOG_UNDEPLOY
PROLOG_MIGRATE_POWEROFF	migr	Передача файлов во время «холодной» миграции (связан с статусом POWEROFF)
PROLOG_MIGRATE_POWEROFF_FAILURE	fail	Сбой при переводе в состояние PROLOG_MIGRATE_POWEROFF
PROLOG_MIGRATE_SUSPEND	migr	Передача файлов во время «холодной» миграции (связан с статусом SUSPEND)
PROLOG_MIGRATE_SUSPEND_FAILURE	fail	Сбой при переводе в состояние PROLOG_MIGRATE_SUSPEND
BOOT_UNDEPLOY_FAILURE	fail	Сбой при переводе в состояние BOOT_UNDEPLOY
BOOT_STOPPED_FAILURE	fail	Сбой при переводе в состояние BOOT_STOPPED
PROLOG_RESUME_FAILURE	fail	Сбой при переводе в состояние PROLOG_RESUME

Окончание таблицы 7

Состояние	Сокращенное название состояния	Описание
PROLOG_UNDEPLOY_FAILURE	fail	Сбой при переводе в состояние PROLOG_UNDEPLOY
DISK_SNAPSHOT_POWEROFF	snap	Выполняется снимок состояния диска (связан с статусом POWEROFF)
DISK_SNAPSHOT_REVERT_POWEROFF	snap	Выполняется восстановление снимка состояния диска (связан с статусом POWEROFF)
DISK_SNAPSHOT_DELETE_POWEROFF	snap	Выполняется удаление снимка состояния диска (связан с статусом POWEROFF)
DISK_SNAPSHOT_SUSPENDED	snap	Выполняется снимок состояния диска (связан с статусом SUSPENDED)
DISK_SNAPSHOT_REVERT_SUSPENDED	snap	Выполняется восстановление снимка состояния диска (связан с статусом SUSPENDED)
DISK_SNAPSHOT_DELETE_SUSPENDED	snap	Выполняется удаление снимка состояния диска (связан с статусом SUSPENDED)
DISK_SNAPSHOT	snap	Выполняется снимок состояния диска (связан с статусом RUNNING)
DISK_SNAPSHOT_DELETE	snap	Выполняется удаление снимка состояния диска (связан с статусом RUNNING)
PROLOG_MIGRATE_UNKNOWN	migr	Передача файлов во время «холодной» миграции (связан с статусом UNKNOWN)
PROLOG_MIGRATE_UNKNOWN_FAILURE	fail	Сбой при переводе в состояние PROLOG_MIGRATE_UNKNOWN
DISK_RESIZE	dsrz	Изменение размера диска, когда ВМ находится в состоянии RUNNING
DISK_RESIZE_POWEROFF	dsrz	Изменение размера диска, когда ВМ находится в статусе POWEROFF
DISK_RESIZE_UNDEPLOYED	dsrz	Изменение размера диска, когда ВМ находится в статусе UNDEPLOYED
HOTPLUG_NIC_POWEROFF	hotp	Выполняется операция подключения/отсоединения сетевого интерфейса (связан с статусом POWEROFF)
HOTPLUG_RESIZE	hotp	Выполняется изменение размера vCPU и памяти с помощью HotPlug
HOTPLUG_SAVEAS_UNDEPLOYED	hotp	Выполняется операция сохранения на диске (связан с статусом UNDEPLOYED)
HOTPLUG_SAVEAS_STOPPED	dsrz	Выполняется операция сохранения на диске (связан с статусом STOPPED)

Информацию о том, какой статус (параметр «STATE») имеет ВМ и в каком состоянии (параметр «LCM_STATE») она находится, можно получить выполнив команду `onevm show` (см. 3.4.2.1) или в веб-интерфейсе ПК СВ на странице ВМ во вкладке «Сведения» (см. 3.4.3.1).

Примечание. Значения параметра «LCM_STATE» устанавливаются только когда ВМ находится в статусе ACTIVE.

3.4.2. Управление экземплярами ВМ в интерфейсе командной строки

3.4.2.1. Отображение существующих ВМ

Для отображения существующих ВМ необходимо использовать команду `onevm list`. Пример вывода после выполнения команды:

```
ID USER     GROUP     NAME        STAT  CPU  MEM HOST          TIME
1  oneadmin brestadm  test-vm-1   poff  0.25  3G 172.16.1.210  0d 14h53
```

Кроме того, можно использовать команду `onevm top` для непрерывного отображения ВМ.

Для просмотра полной информации о ВМ необходимо использовать команду:

```
onevm show <идентификатор_ВМ>
```

Пример вывода после выполнения команды `onevm show 1`:

```
VIRTUAL MACHINE 1 INFORMATION
ID                  : 1
NAME                : test-vm-1
USER                : oneadmin
GROUP               : brestadmins
STATE               : POWEROFF
LCM_STATE           : LCM_INIT
LOCK                : None
RESCHED             : No
HOST                : 172.16.1.210
CLUSTER ID          : 0
CLUSTER             : default
START TIME          : 07/18 19:05:39
END TIME            : -
DEPLOY ID           : 3b4d40f7-55c0-4ba6-9bcf-2e627c744179

VIRTUAL MACHINE MONITORING
ID                  : 1
TIMESTAMP           : 1658214069
```

```
PERMISSIONS
OWNER                : um-
GROUP                : ---
OTHER                : ---
```

3.4.2.2. Удаление экземпляров ВМ

Удаление экземпляра ВМ из любого состояния выполняется командой:

```
onevm terminate <идентификатор_ВМ>
```

В качестве идентификатора ВМ можно указать перечень идентификаторов, разделенных запятыми или диапазон идентификаторов (в качестве разделителя используются две точки — «..»).

Команда `onevm terminate` корректно отключает и удаляет работающие ВМ, отправляя сигнал ACPI. После отключения ВМ освободятся ресурсы (образы, сети и др.), которые использовались ВМ, сервер виртуализации будет очищен, а постоянный диск с будет перемещен в хранилище образов.

Если по истечении определенного времени после выполнения команды `onevm terminate` ВМ все еще работает, т.е. ОС виртуальной машины игнорирует сигналы ACPI, служба сервера управления снова присвоит ВМ статус RUNNING.

Если экземпляр ВМ находится в статусе RUNNING, для завершения его работы в команде можно указать аргумент `--hard`. В этом случае экземпляр ВМ будет удален незамедлительно. Следует использовать данный аргумент команды, если ВМ не поддерживает ACPI.

3.4.2.3. Приостановка экземпляров ВМ

Существует два способа временно остановить выполнение ВМ: с сохранением состояния и без сохранения. Для приостановки ВМ используются следующие команды:

- `onevm suspend` — краткосрочная приостановка: состояние ВМ, в том числе выделенные ресурсы, сохраняется на задействованном сервере виртуализации. При возобновлении работы приостановленной ВМ выполняется ее незамедлительное развертывание на том же сервере виртуализации;
- `onevm poweroff` — долгосрочная приостановка: корректно выключает электропитание работающей ВМ, отправляя сигнал ACPI, при этом состояние ВМ не сохраняется. Возобновление работы ВМ осуществляется на том же сервере виртуализации. Использование с командой аргумента `--hard` позволяет незамедлительно отключить электропитание ВМ. Использование данной опции актуально, если ВМ не поддерживает ACPI.

Примечание. В случае запуска процедуры выключения в ОС виртуальной машины, в ПК СВ состояние ВМ также будет установлено как POWEROFF.

Возможно запланировать долгосрочную приостановку. В этом случае ресурсы сервера виртуализации, которые использовала ВМ, будут освобождены, а сервер виртуализации очищен. Любой диск будет сохранен в хранилище образов. Следующие команды применяются при необходимости сохранить выделенные ресурсы сети и памяти, например, IP-адреса, постоянные образы диска:

- `undeploy` — корректно выключает работающую ВМ, отправляя сигнал ACPI. Диски ВМ перемещаются в хранилище образов. При возобновлении ВМ, развертывание которой было отменено, она перейдет в состояние ожидания, а планировщик выберет место для ее повторного развертывания;
- `undeploy --hard` — аналогично команде `undeploy`, но работающая ВМ удаляется незамедлительно;
- `stop` — аналогично команде `undeploy`, но также сохраняется состояние ВМ для последующего возобновления;
- `resume` — возобновляет работу ВМ при успешной остановки или приостановки их работы, а также ВМ, развертывание которых было отменено или электропитание которых было отключено.

3.4.2.4. Перезагрузка экземпляров ВМ

Для перезагрузки ВМ используются следующие команды:

- `reboot` — корректная перезагрузка работающей ВМ, отправляя сигнал ACPI;
- `reboot --hard` — принудительная перезагрузка работающей ВМ, актуально, если ВМ не поддерживает ACPI.

3.4.2.5. Отсрочка развертывания экземпляров ВМ

Возможно отсрочить развертывание ожидающей ВМ, например, после ее создания или возобновления, используя команду `hold`. Команда переводит ВМ в состояние удержания. Планировщик не будет выполнять развертывание ВМ, находящейся в состоянии удержания. Также можно создавать ВМ непосредственно на удержании с помощью команд `onetemplate instantiate -hold` или `onevm create -hold`.

Возобновление развертывания ВМ осуществляется с помощью команды `release`. Команда разблокирует ВМ, находящуюся на удержании, и переведет ее в состояние ожидания. Возможно автоматически разблокировать ВМ, запланировав выполнение данной команды.

3.4.3. Управление экземплярами ВМ в веб-интерфейсе ПК СВ

3.4.3.1. Отображение существующих ВМ

Для отображения существующих ВМ в веб-интерфейсе ПК СВ необходимо в меню слева выбрать пункт «Экземпляры ВМ — ВМ». На открывшейся странице «ВМ» будет отображена таблица экземпляров ВМ (см. рис. 28)

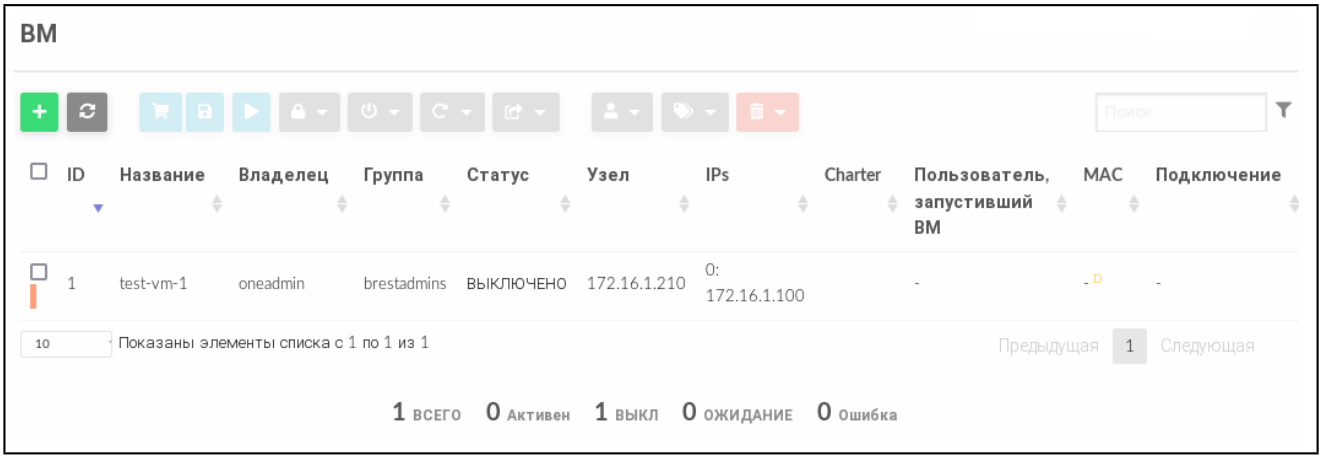

Рис. 28

Для просмотра полной информации о ВМ необходимо на странице «ВМ» выбрать необходимую ВМ. После этого откроется страница виртуальной машины (вкладка «Сведения») (см. рис. 29).

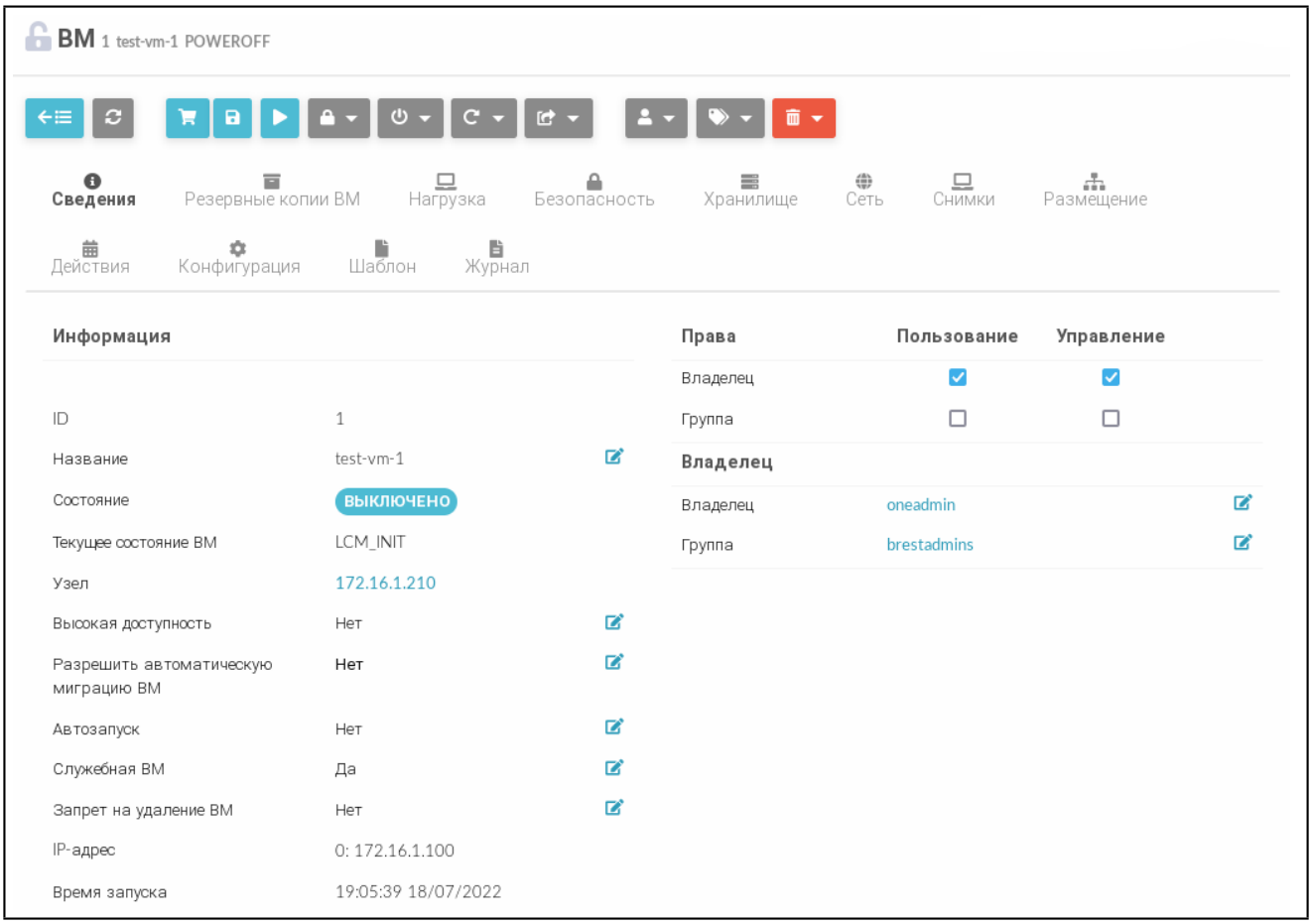

Рис. 29

3.4.3.2. Завершение работы и приостановка экземпляров ВМ

Для завершения работы экземпляра ВМ или его приостановки в веб-интерфейсе ПК СВ используется кнопка **[Управление питанием]**, после нажатия на которую откроется меню действий (см. рис. 30):

- Приостановить работу ВМ — краткосрочная приостановка: состояние ВМ, в том числе выделенные ресурсы, сохраняются на задействованном сервере виртуализации. При возобновлении работы приостановленной ВМ выполняется ее незамедлительное развертывание на том же сервере виртуализации;
- Остановить — корректно выключает работающую ВМ, отправляя сигнал ACPI. Диски ВМ перемещаются в хранилище образов, при этом сохраняется состояние ВМ. Возобновление работы ВМ осуществляется на любом доступном сервере виртуализации;
- Отключить питание — долгосрочная приостановка: корректно выключает работающую ВМ, отправляя сигнал ACPI, при этом состояние ВМ не сохраняется. Возобновление работы ВМ осуществляется на том же сервере виртуализации;
- Отключить питание немедленно — незамедлительно отключить электропитание ВМ. Использование данной опции актуально, если ВМ не поддерживает ACPI;
- Отменить размещение — корректно выключает работающую ВМ, отправляя сигнал ACPI. Диски ВМ перемещаются в хранилище образов, при этом состояние ВМ не сохраняется. Возобновление работы ВМ осуществляется на любом доступном сервере виртуализации;
- Отменить размещение немедленно — аналогично команде Отменить размещение, но работающая ВМ удаляется незамедлительно.

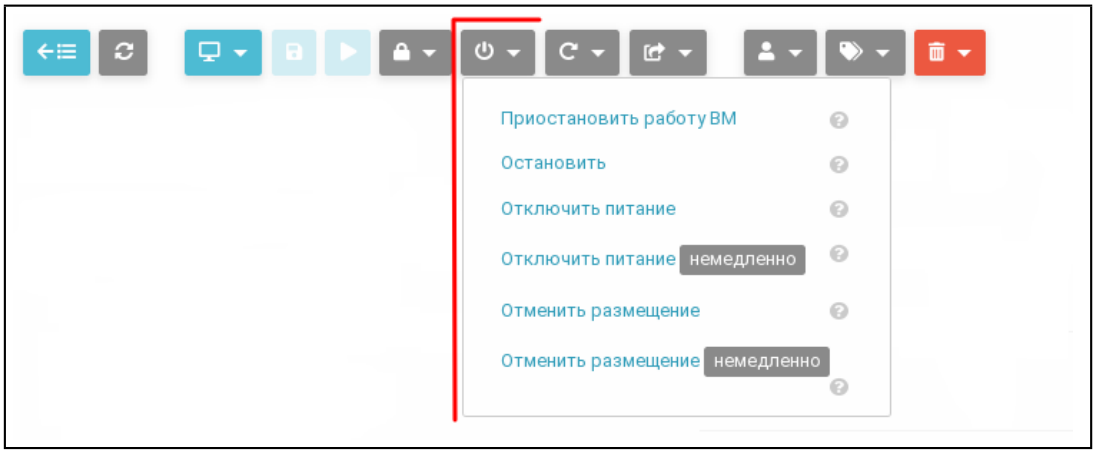

Рис. 30

3.4.3.3. Перезагрузка экземпляров ВМ

Для перезагрузки ВМ в веб-интерфейсе ПК СВ используется кнопка **[Перезагрузка]**, после нажатия на которую откроется меню действий (см. рис. 31):

- Перезагрузить — корректная перезагрузка работающей ВМ, отправляя сигнал ACPI;
- Перезагрузить немедленно — принудительная перезагрузка работающей ВМ, актуально, если ВМ не поддерживает ACPI.

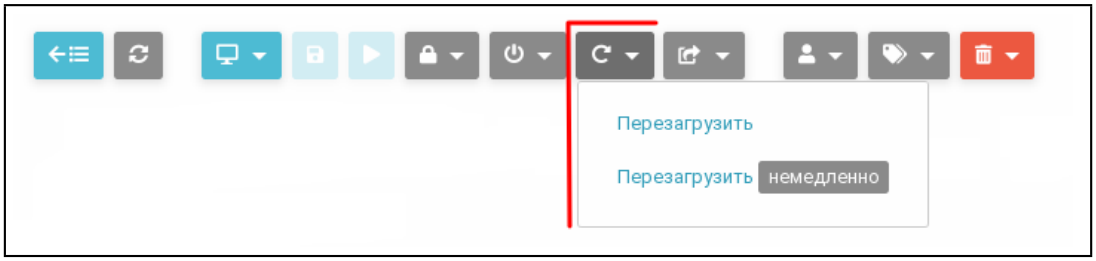

Рис. 31

3.4.3.4. Отсрочка развертывания экземпляров ВМ

Для управления блокировкой ВМ в веб-интерфейсе ПК СВ используется кнопка **[Блокировка]**, после нажатия на которую откроется меню действий (см. рис. 32):

- `Заблокировать` — переводит ВМ в состояние удержания;
- `Разблокировать` — разблокировать ВМ, находящуюся на удержании.

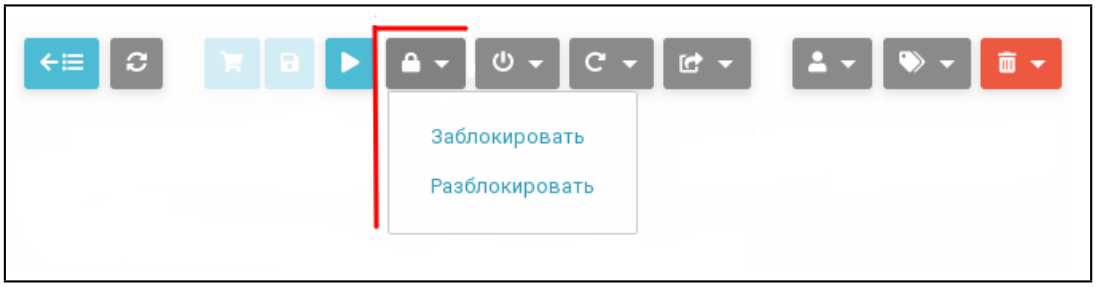

Рис. 32

3.4.3.5. Удаление экземпляров ВМ

Для удаления экземпляров ВМ в веб-интерфейсе ПК СВ используется кнопка **[Уничтожить]**, после нажатия на которую откроется меню действий (см. рис. 33):

- `Уничтожить` — корректно завершить работу и удалить ВМ, отправляя сигнал ACPI. Если по истечении определенного времени после выполнения команды ВМ все еще работает, т.е. ОС виртуальной машины игнорирует сигналы ACPI, служба сервера управления снова присвоит ВМ статус RUNNING;
- `Уничтожить немедленно` — удалить ВМ незамедлительно. Следует использовать данную команду, если ВМ не поддерживает ACPI.

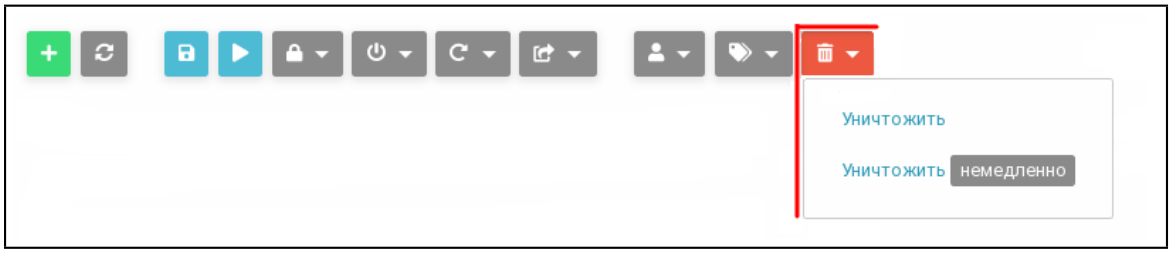

Рис. 33

3.4.4. Снимки дисков ВМ

Снимки организованы с применением древовидной структуры, т.е. у каждого снимка есть родительский элемент, за исключением первого снимка, чьим родительским элементом

является снимок с идентификатором «-1».

Пользователь может вернуть состояние диска к последнему сделанному снимку в любое время. Последний сделанный снимок или снимок, к которому вернулся пользователь, является активным снимком. Активный снимок выступает в качестве родительского элемента для следующего снимка. Снимки, которые не являются активными и не имеют дочерних элементов, можно удалять.

ВНИМАНИЕ! Возможность создавать снимки дисков ВМ зависит от используемой в системном хранилище технологии хранения и драйвера передачи данных. Например, в драйвере хранилища LVM_LVM не поддерживается создание снимка состояния диска.

3.4.4.1. Управление снимками дисков в интерфейсе командной строки

Для создания снимка состояния диска необходимо выполнить команду:

```
onevm disk-snapshot-create <идентификатор_ВМ> \
<идентификатор_диска_ВМ> <наименование_снимка>
```

Для возвращения диска к состоянию, заданному в снимке, необходимо выполнить команду:

```
onevm disk-snapshot-revert <идентификатор_ВМ> \
<идентификатор_диска_ВМ> <идентификатор_снимка>
```

Команда будет выполнена только в том случае, если ВМ находится в состоянии POWEROFF или SUSPENDED.

Снимки являются неизменяемыми, поэтому пользователь может вернуться к снимку неограниченное количество раз.

Для удаления снимка необходимо выполнить команду:

```
onevm disk-snapshot-delete <идентификатор_ВМ> \
<идентификатор_диска_ВМ> <идентификатор_снимка>
```

Команда удалит снимок только в том случае, если он не активен и не имеет дочерних элементов.

3.4.4.2. Управление снимками дисков в веб-интерфейсе ПК СВ

Для создания снимка состояния диска ВМ в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

1) в меню слева выбрать пункт «Экземпляры ВМ — ВМ»;
2) на открывшейся странице «ВМ» выбрать необходимую виртуальную машину;
3) на странице виртуальной машины открыть вкладку «Хранилище» и в строке необходимого диска нажать кнопку **[Snapshot]** (см. рис. 34);

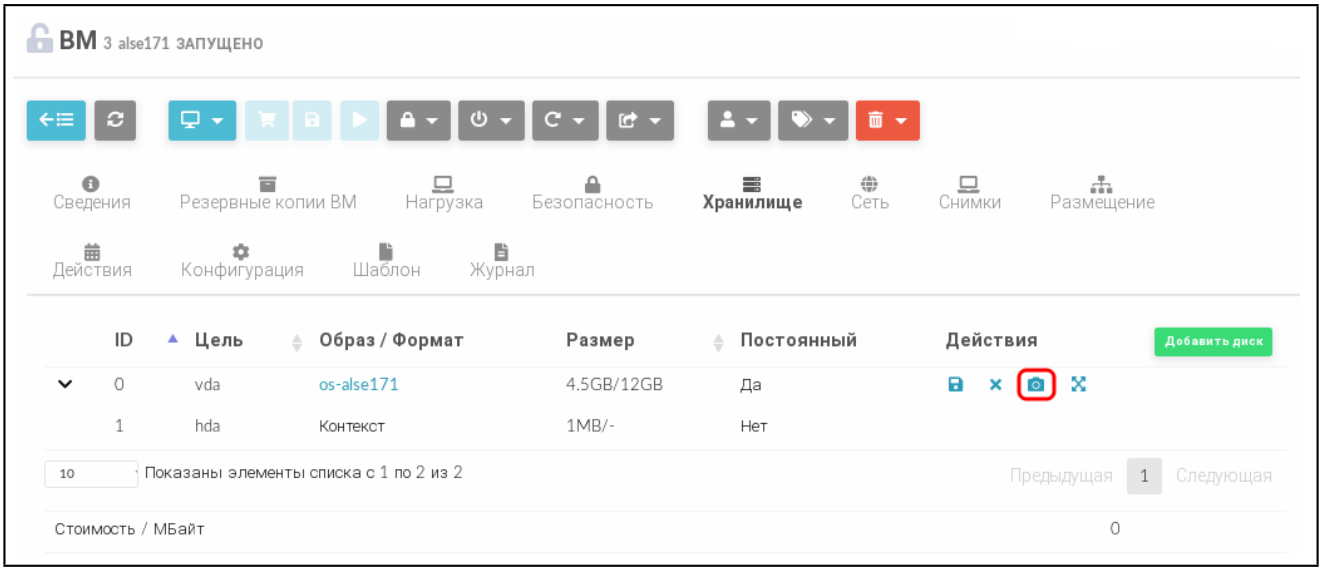

Рис. 34

4) в открывшемся окне «Снимок диска» задать наименование снимка и нажать кнопку **[Сделать снимок]** (см. рис. 35).

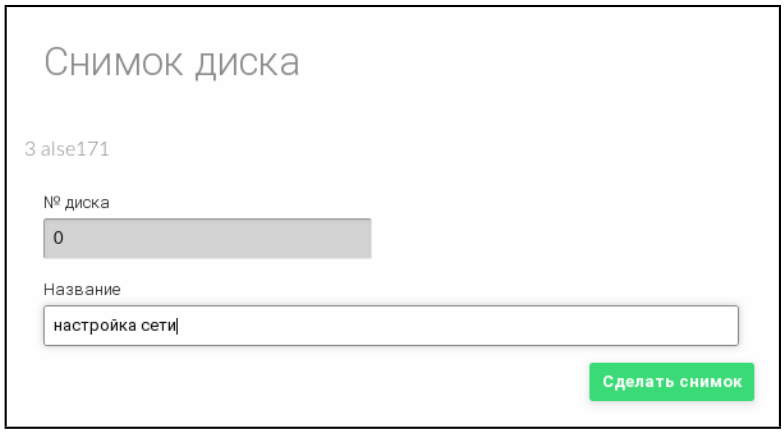

Рис. 35

На странице виртуальной машины во вкладке «Хранилище» (после остановки ВМ) — см. рис. 36:

- для возвращения диска к состоянию, указанному в снимке, необходимо отметить соответствующий снимок и нажать кнопку **[Откатить]**;
- для удаления снимка состояния диска необходимо отметить соответствующий снимок и нажать кнопку **[Удалить]**.

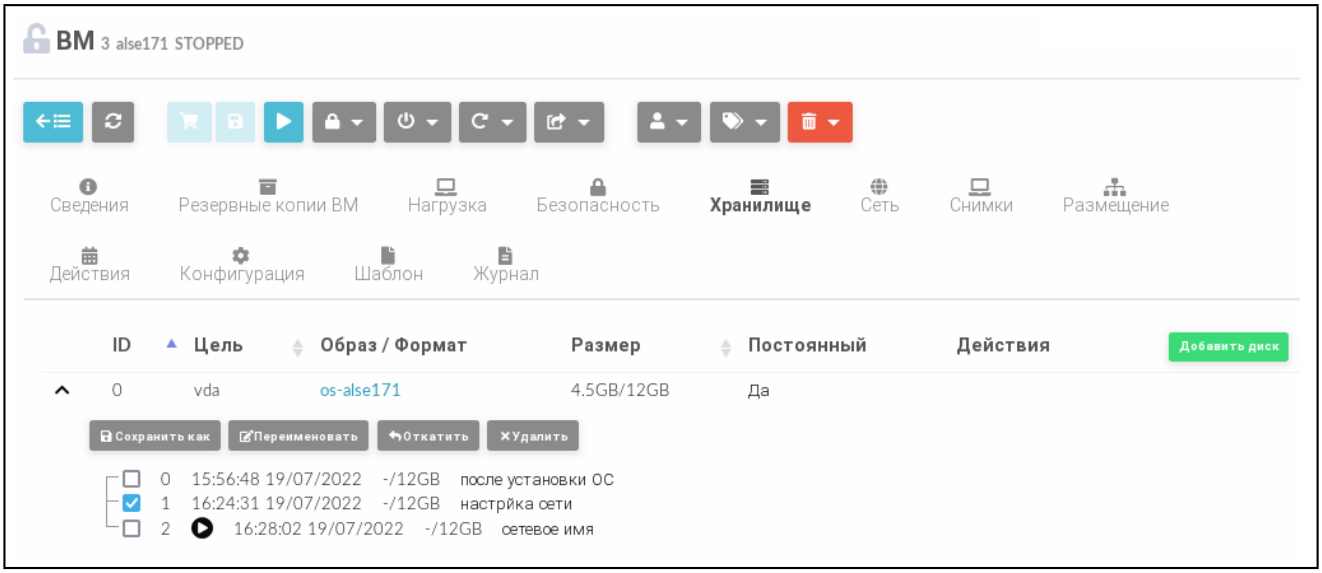

Рис. 36

Кроме того, на странице виртуальной машины во вкладке `Хранилище` можно переименовать снимок состояния диска ВМ. Для этого необходимо отметить соответствующий снимок и нажать кнопку **[Переименовать]**. В открывшемся окне необходимо задать новое наименование снимка и нажать кнопку **[Переименовать]**.

3.4.5. Экспорт диска ВМ

Любой диск ВМ можно экспортировать в новый образ, если ВМ находится в состоянии RUNNING, POWEROFF или SUSPENDED.

3.4.5.1. В интерфейсе командной строки

Для экспорта диска ВМ необходимо выполнить команду:

```
onevm disk-saveas  <идентификатор_ВМ> <идентификатор_диска_ВМ> \
<наименование_нового_образа>
```

По умолчанию выполняется экспорт текущего состояния диска. При необходимости можно указать идентификатор снимка диска, который нужно использовать как источник для экспорта. Для этого необходимо выполнить команду:

```
onevm disk-saveas  <идентификатор_ВМ> <идентификатор_диска_ВМ> \
<наименование_нового_образа> --snapshot <идентификатор_диска>
```

ВНИМАНИЕ! Это действие не синхронизируется с гипервизором. Если ВМ находится в состоянии RUNNING, перед созданием снимка необходимо убедиться, что диск размонтирован, синхронизирован или приостановлен.

3.4.5.2. В веб-интерфейсе ПК СВ

Для экспорта диска ВМ в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

1) в меню слева выбрать пункт «Экземпляры ВМ — ВМ»;
2) на открывшейся странице «ВМ» выбрать необходимую виртуальную машину;

3) на странице виртуальной машины открыть вкладку «Хранилище» и в строке необходимого диска нажать кнопку **[Сохранить как]** (см. рис. 37);

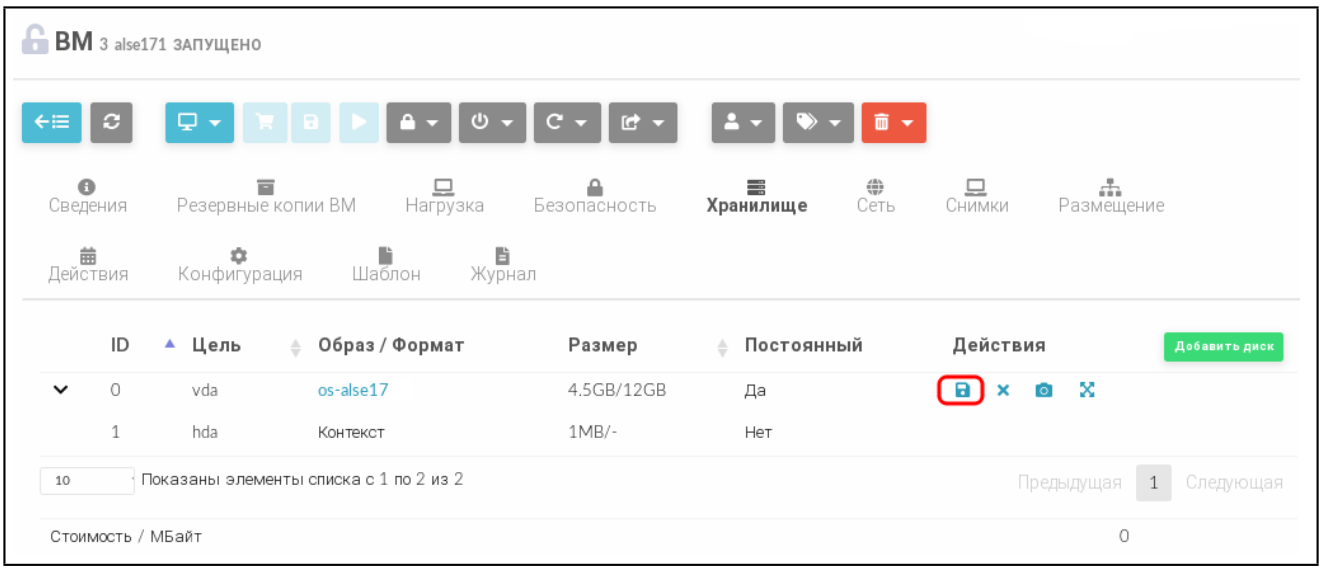

Рис. 37

4) в открывшемся окне «Сохранить диск как» задать наименование нового образа и нажать кнопку **[Сохранить как]** (см. рис. 38).

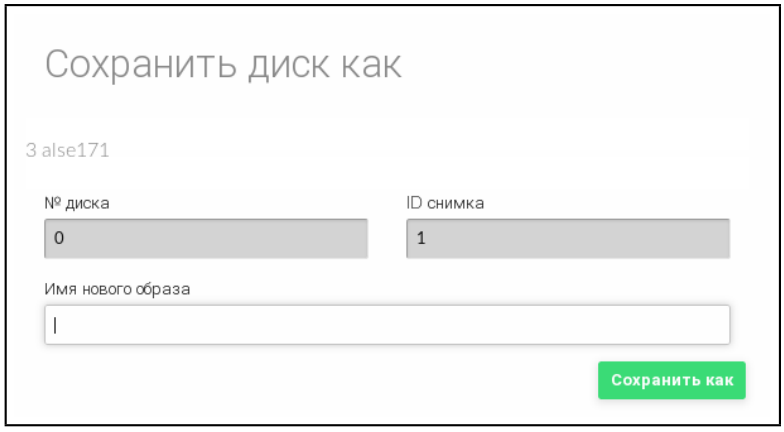

Рис. 38

Если необходимо указать определенный снимок диска, который нужно использовать как источник для экспорта, на странице виртуальной машины во вкладке «Хранилище» необходимо отметить соответствующий снимок и нажать кнопку **[Сохранить как]** (см. рис. 36).

3.4.6. Изменение размера дисков ВМ

Увеличение объема дисков, выделенных для ВМ, возможно выполнить во время развертывания ВМ из шаблона.

Настройка выполняется путем установки значения для параметра диска `SIZE`. Если заданное значение параметра будет превышать изначальный размер образа, будет увеличен размер контейнера диска перед запуском ВМ. Для того чтобы в ОС виртуальной машины

в автоматическом режиме были применены изменения локальной файловой системы, необходимо использовать пакеты контекстуализации.

3.4.6.1. В интерфейсе командной строки

Чтобы изменить объем диска, выделяемого для ВМ при развертывании, можно воспользоваться файлом параметров, указав в нем новое значение.

Примеры:

1. Подготовить файл с параметрами `disk.txt`:

```
DISK = [
IMAGE_ID = 2,
SIZE = 20480
]
```

В представленном примере для диска ВМ, создаваемом на основе образа с идентификатором 2, будет установлен объем 20 ГБ (размер образа — 12 ГБ).

2. Развернуть ВМ на основе шаблона с наименованием `alse17` и с использованием файла параметров `disk.txt`:

```
onetemplate instantiate alse17 disk.txt
```

Пример вывода после выполнения команды:

```
VM ID: 3
```

3. Просмотреть информацию о ВМ, пример вывода после выполнения команды `onevm show 3`:

```
VIRTUAL MACHINE 3 INFORMATION
ID                  : 3
NAME                : alse17-3
USER                : oneadmin
GROUP               : brestadmins
STATE               : PENDING
LCM_STATE           : LCM_INIT
LOCK                : None
RESCHED             : No
START TIME          : 07/20 10:56:01
END TIME            : -
DEPLOY ID           : -
...
VM DISKS
ID DATASTORE  TARGET   IMAGE              SIZE    TYPE   SAVE
0  default    vda      copy-os-alse17   -/20G   file   NO
```

Также новое значение объема диска можно указывать в виде аргумента в команде развертывания ВМ из шаблона.

Пример

Развернуть ВМ на основе шаблона с наименованием `alse17`, при этом для диска ВМ, создаваемом на основе образа с идентификатором 2, будет установлен объем 20 ГБ:

```
onetemplate instantiate alse17 --disk 2:size=20480
```

3.4.6.2. В веб-интерфейсе ПК СВ

Чтобы изменить объем диска, выделяемого для ВМ, при развертывании из шаблона в веб-интерфейсе ПК СВ необходимо на странице «Создать ВМ» в секции «Диски» задать новое значение (см. рис. 39)

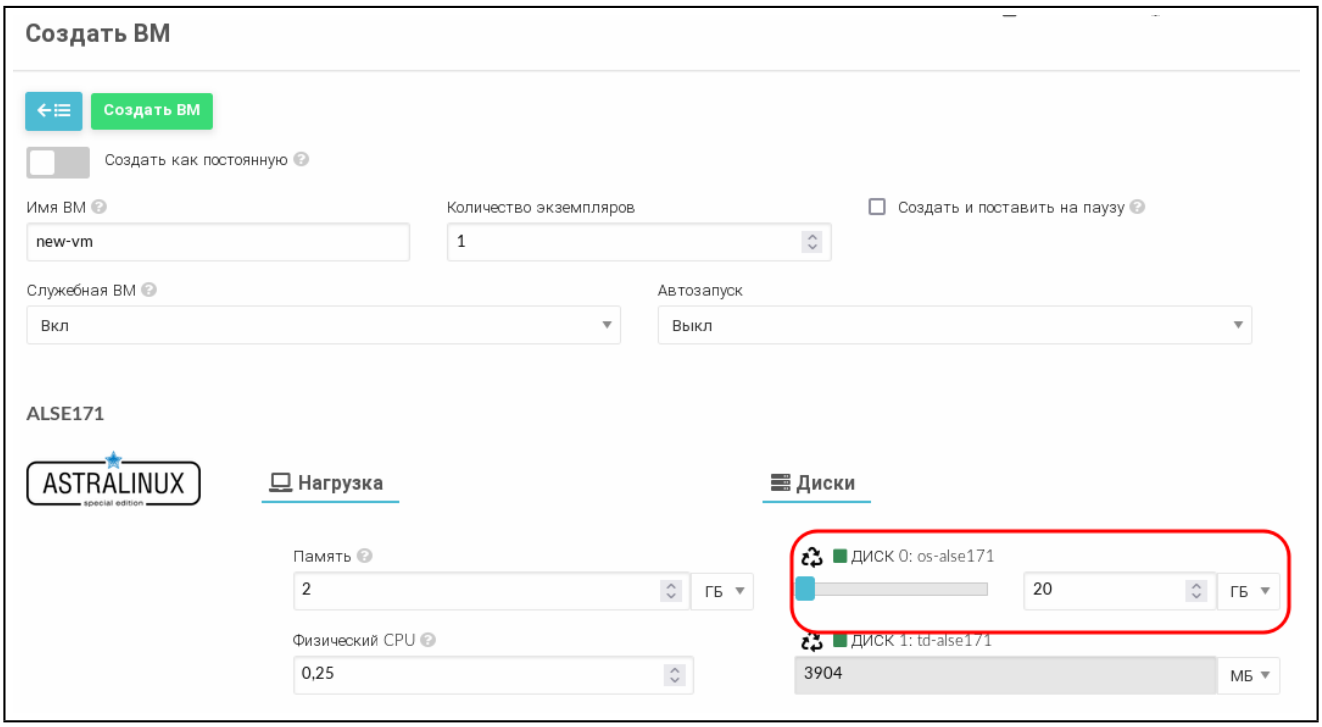

Рис. 39

3.4.7. Клонирование ВМ

Шаблон или экземпляр ВМ можно копировать в новый шаблон ВМ. Это копия сохранит все изменения, внесенные в диски ВМ после того, как работа экземпляра была завершена. Шаблон является частным и будет отображаться только для владельца.

Существует два способа создания постоянной частной копии ВМ:

- реализовать шаблон в качестве постоянного;
- сохранить существующий экземпляр ВМ как шаблон.

При реализации шаблона в качестве постоянного выполняется его рекурсивное клонирование — создается частная постоянная копия каждого образа диска.

ВНИМАНИЕ! Энергозависимые диски не могут быть постоянными, поэтому их со-

держимое будет потеряно в случае прекращения работы ВМ. Клонированный шаблон ВМ будет содержать определение для пустого энергозависимого диска.

При сохранении ВМ в качестве шаблона выполняется клонирование исходного шаблона ВМ с заменой дисков на снимки текущих дисков. Если для экземпляра ВМ выполнялось перераспределение ресурсов, будет использоваться текущая производительность. Новые клонированные образы можно дополнительно сделать постоянными, установив атрибут `--persistent` (см. 3.2.7). Сетевые интерфейсы (блок параметров `NIC`) также будут перезаписаны на полученные от экземпляра ВМ.

ВНИМАНИЕ! Перед тем как сохранить ВМ в качестве постоянного шаблона, эту ВМ необходимо выключить.

3.4.7.1. В интерфейсе командной строки

Для реализации шаблона в качестве постоянного в команде инициализации ВМ из шаблона используется аргумент `--persistent`.

Примеры:

1. Развернуть ВМ из шаблона с наименованием `alse17` и на его основе создать постоянный шаблон с наименованием `my_vm`:

```
onetemplate instantiate alse17 --persistent --name my_vm
```

Пример вывода после выполнения команды:

```
VM ID: 4
```

2. Просмотреть перечень имеющихся шаблонов, пример вывода после выполнения команды `onetemplate list`:

```
ID USER      GROUP      NAME             REGTIME
2  oneadmin  brestadm   my_vm            07/20 12:21:42
1  brestadm  brestadm   Copy of alse17  07/20 10:49:49
0  brestadm  brestadm   alse17          07/19 17:49:33
```

3. Просмотреть перечень имеющихся ВМ, пример вывода после выполнения команды `onevm list`:

```
ID USER     GROUP     NAME       STAT  CPU   MEM  HOST        TIME
4  oneadmin brestadm  my_vm      runn  0.25  2G   oneserver   0d 00h07
2  oneadmin brestadm  alse17-2  poff  0.25  2G   oneserver   0d 01h35
```

Чтобы сохранить ВМ в качестве постоянного шаблона, необходимо выполнить команду:

```
onevm save <идентификатор/наименование_ВМ> \
<наименование_нового_шаблона> --persistent
```

3.4.7.2. В веб-интерфейсе ПК СВ

Для реализации шаблона в качестве постоянного, при развертывании ВМ из этого шаблона, в веб-интерфейсе ПК СВ необходимо на странице «Создать ВМ» установить флаг

«Создать как постоянную» (см. рис. 40).

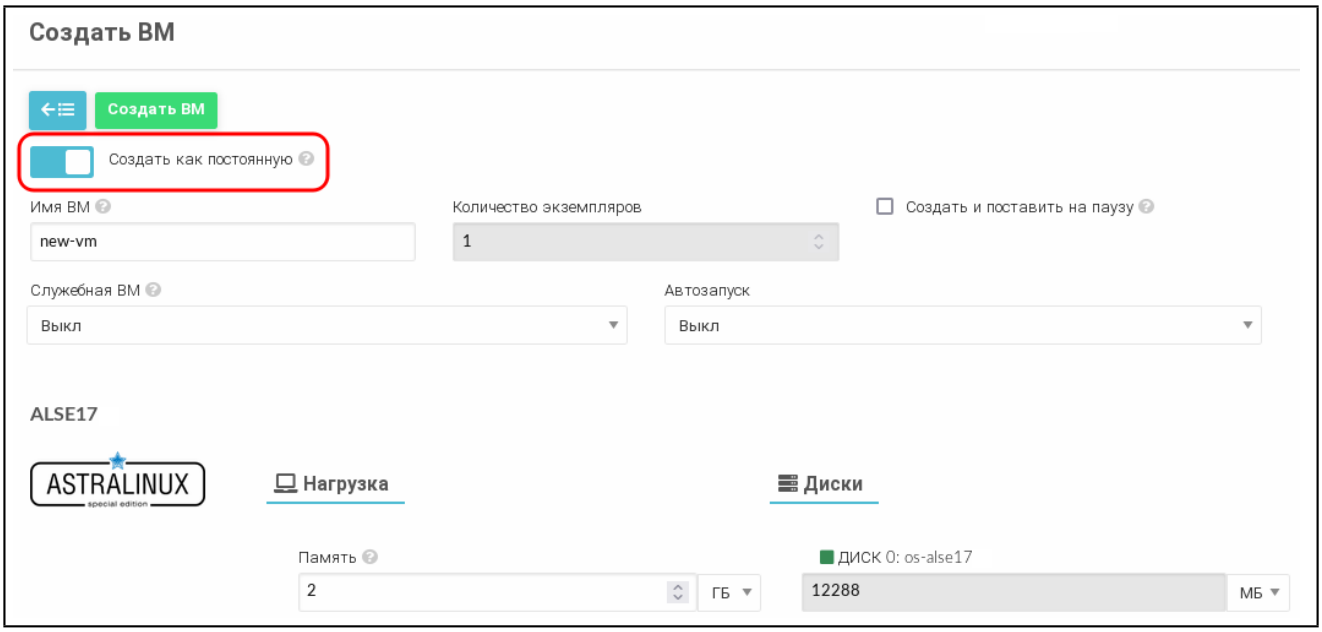

Рис. 40

Чтобы сохранить ВМ в качестве постоянного шаблона, в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

1) на странице выключенной ВМ нажать кнопку **[Сохранить как]** (см. рис. 41);

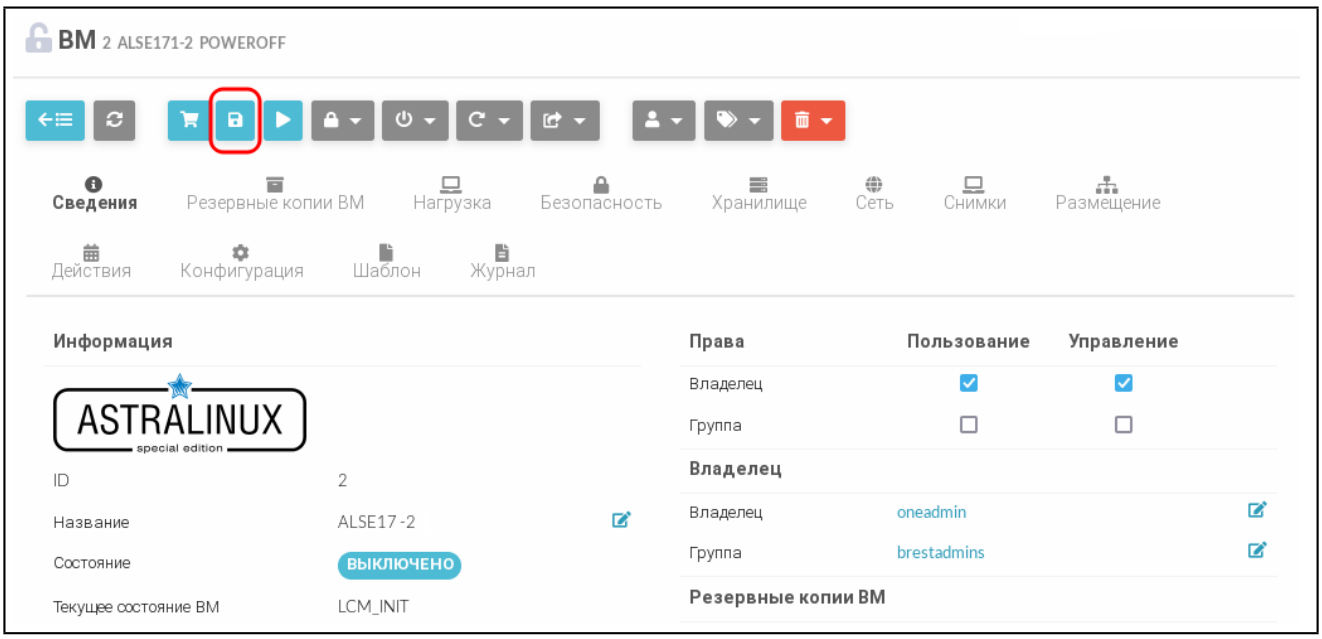

Рис. 41

2) в открывшемся окне «Сохранить как шаблон» (см. рис. 42):
   а) задать наименование нового шаблона,
   б) установить флаг «Сделать новый образ постоянным»,
   в) нажать кнопку **[Сохранить как шаблон]**.

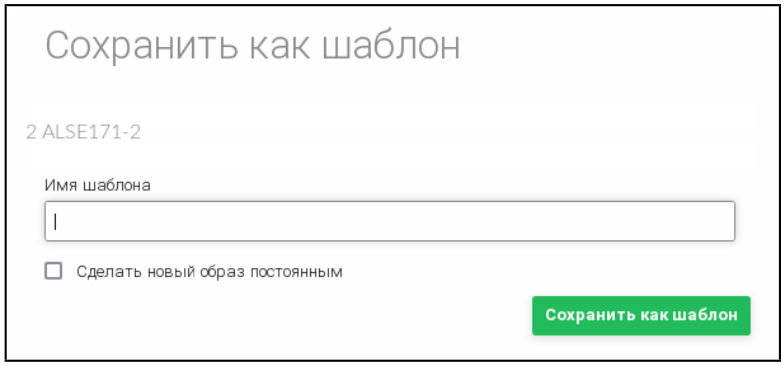

Рис. 42

3.4.8. Управление полномочиями для ВМ

В ПК СВ реализован механизм полномочий на основе правил ACL, предназначенный для администраторов. Не является нарушением условий эксплуатации, когда пользователь (или разработчик) ВМ может открыть доступ к экземпляру ВМ для других пользователей, разрешить им просматривать и использовать ВМ.

3.4.9. Планирование действий

Пользователи могут запланировать выполнение одного или нескольких действий ВМ в определенные дату и время.

ВНИМАНИЕ! В дискреционном режиме функционирования ПК СВ можно запланировать только создание резервной копии ВМ (`backup`).

3.4.9.1. В интерфейсе командной строки

Использование совместно с командами `onevm` аргумента `--schedule` позволяет отложить выполнение действий до определенного времени.

Примеры:

1. 22 сентября (в 00:00) приостановить работу ВМ с идентификатором «0»:

```
onevm suspend 0 --schedule "09/22"
```

Пример вывода после выполнения команды:

```
VM 0: suspend scheduled at 2022-09-22 00:00:00 +0300
```

2. Восстановить работу ВМ с идентификатором «0» в 14:15 22 сентября:

```
onevm resume 0 --schedule "09/23 14:15"
```

Пример вывода после выполнения команды:

```
VM 0: resume scheduled at 2022-09-23 14:15:00 +0300
```

3. Просмотреть информацию о ВМ, пример вывода после выполнения команды `onevm show 0`:

```
VIRTUAL MACHINE 0 INFORMATION
ID                  : 0
NAME                : one-0
```

```
[...]

SCHEDULED ACTIONS
ID ACTION   ARGS     SCHEDULED
0  suspend  -        09/20 00:00
1  resume   -        09/23 14:15
```

Для периодического выполнения действий дополнительно указываются следующие аргументы:

- `weekly` (еженедельно) — указывается диапазон дней недели, в которые необходимо выполнять запланированное действия. Допустимые значения: [0,6], где 0 — воскресенье, 6 — суббота;
- `monthly` (ежемесячно) — указывается диапазон дней месяца, в которые необходимо выполнять запланированное действия. Допустимые значения: [1,31];
- `yearly` (ежегодно) — указывается диапазон дней года, в которые необходимо выполнять запланированное действия. Допустимые значения: [0,365];
- `hourly` (ежечасно) — указывается диапазон часов недели, в которые необходимо выполнять запланированное действия. Допустимые значения: [0,168] (168 часов — 1 неделя).

Аргумент `end` определяет окончание выполнения периодических действий. Может принимать значения:

- `число` — выполнение запланированного действия прекращается после указанного количества повторений;
- `дата` — выполнение запланированного действия прекращается после достижения указанной даты.

Примеры:

1. Примеры команд:

```
onevm suspend 0 --schedule "10/01" --weekly "1,5" --end 5
onevm resume 0 --schedule "10/03 14:15" --weekly "2,6" --end 5
onevm snapshot-create 0 --schedule "10/03" --hourly 5 --end "12/25"
```

2. Пример вывода после выполнения команды `onevm show 0`:

```
VIRTUAL MACHINE 0 INFORMATION
ID                  : 0
NAME                : one-0

[...]
```

```
SCHEDULED ACTIONS
ID           ACTION  ARGS   SCHEDULED  REPEAT        END
0          suspend   -   10/27 00:00
1           resume   -   10/28 14:15
2          suspend   -   10/01 00:00   Weekly 1,5    After 5 times
3           resume   -   10/03 14:15   Weekly 2,6    After 5 times
4 snapshot-create   -   10/03 00:00   Each 5 hours  On 12/25/22
```

Запланированные действия можно удалить, используя команду:

```
onevm delete-chart <идентификатор/наименование_ВМ> <идентификатор_действия>
```

Кроме того, запланированные действия можно отредактировать, для этого используется команда:

```
onevm update-chart <идентификатор/наименование_ВМ> <идентификатор_действия>
```

После ввода команды откроется текстовый редактор `Vim` для редактирования запланированного действия.

Пример

Редактирование запланированного действия с идентификатором «1» для ВМ с идентификатором «0»:

```
onevm update-chart 0 1
```

Пример вывода после выполнения команды:

```
ACTION="resume"
ID="1"
TIME="1663931700"
```

Примечание. В параметре `TIME` дата и время указаны в формате Unix-времени.

3.4.9.2. В веб-интерфейсе ПК СВ

Чтобы запланировать выполнение одного или нескольких действий ВМ в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

1) в меню слева выбрать пункт «Экземпляры ВМ — ВМ»;

2) на открывшейся странице «ВМ» выбрать необходимую виртуальную машину;

3) на странице виртуальной машины открыть вкладку «Действия» и нажать кнопку **[Добавить действие]**;

4) на открывшейся странице внести необходимые настройки и нажать кнопку **[Добавить]** (см. рис. 43.

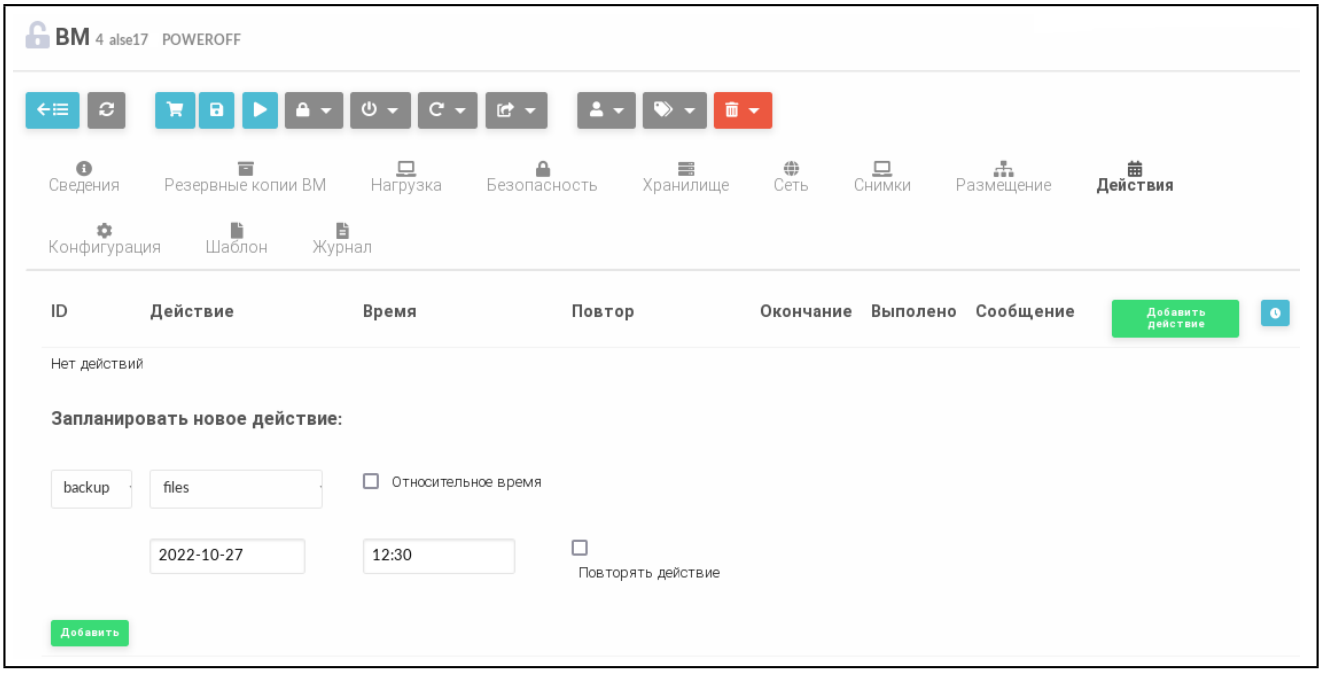

Рис. 43

3.4.10. Доступ к рабочему столу ВМ в веб-интерфейсе ПК СВ

Если ВМ поддерживает VNC или Spice и находится в состоянии RUNNING, то во вкладке просмотра ВМ отображается иконка доступа к рабочему столу ВМ (см. рис. 44).

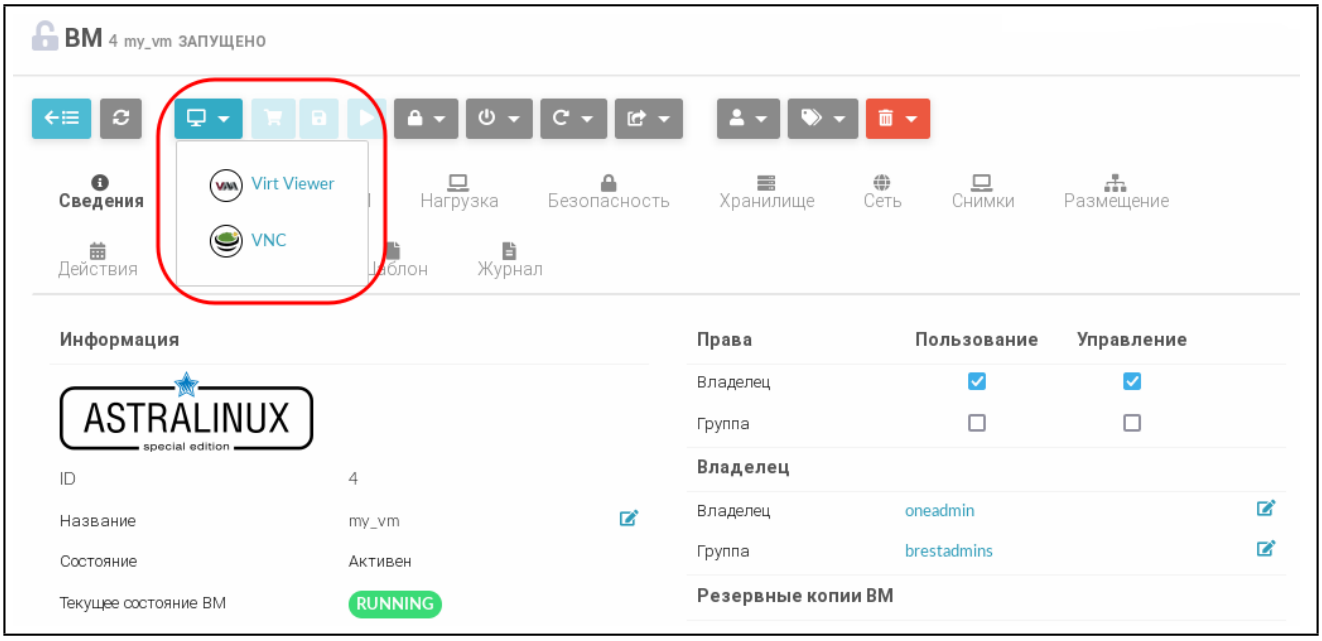

Рис. 44

При появлении в браузере firefox панели с предупреждением нажать кнопку **[Настройки]** и выбрать пункт `Разрешить всплывающие окна` (см. рис. 45).

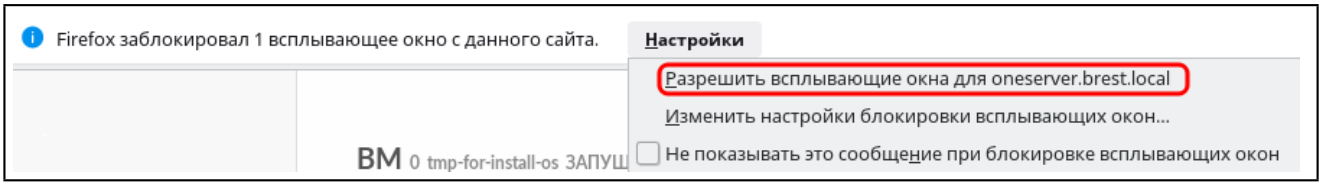

Рис. 45

После этого откроется страница с подключенным удаленным рабочим столом ВМ (см. рис. 46).

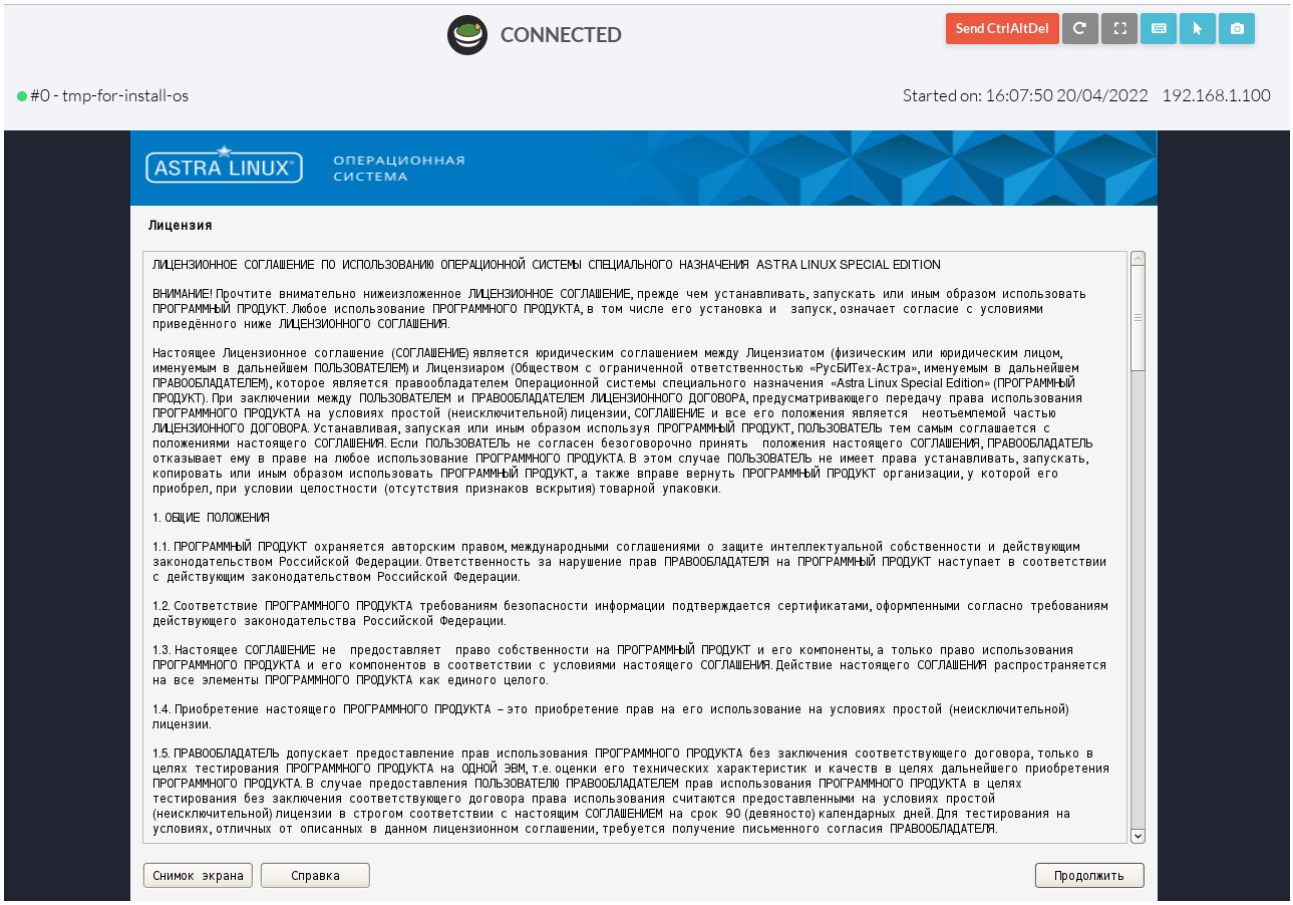

Рис. 46

3.4.11. Резервное копирование и восстановление экземпляра ВМ

3.4.11.1. Особенности резервного копирования экземпляра ВМ в ПК СВ

При выполнении резервного копирования в автоматическом режиме выполняются следующие операции:

1) на сервере управления в каталоге `/var/tmp/one-dump` создается каталог `<идентификатор_ВМ>_<метка_времени>`, где `<метка_времени>` записывается в формате UNIX времени длиной 13 цифр (с указанием миллисекунд).

Примечание. Если для обеспечения отказоустойчивости сервера управления применяется технология Raft, то все предварительные операции выполняются в локальном каталоге `/var/tmp/one-dump` сервера управления, выполняющего функцию лидера;

2) в каталог <идентификатор_ВМ>_<метка_времени> копируются образы дисков ВМ, а также файлы, описывающие конфигурацию ВМ:

- файлы с наименованием вида «disk<номер>», которые являются копиями дисков ВМ. Цифра после префикса «disk» соответствует номеру диска, указанному в шаблоне;
- файлы с наименованием вида «disk<номер>.tmpl», в которых указаны тип и префикс соответствующего образа диска;
- файлы с наименованием вида «disk<номер>.target», в которых указан идентификатор эмулируемого дискового устройства, в качестве которого подключается соответствующий образ диска;
- файл «boot», в котором указано наименование образа загрузочного диска;
- файл «vm.template», в котором указаны значения параметров контекста, настройки графического подключения к ВМ, значения параметров вычислительных ресурсов и идентификатор исходного шаблона ВМ;

Примечание. Если системное хранилище построено на базе файловой технологии хранения с использованием драйверов Shared и Qcow2 или на базе программно-определяемой технологии хранения Ceph, то размер файла «disk<номер>» будет определяться фактическим объемом данных, размещенных в образе диска ВМ. Если системное хранилище построено на базе блочной технологии хранения с использованием LVM, то размер файла «disk<номер>» будет соответствовать размеру образа диска ВМ;

3) все вышеуказанные файлы упаковываются в архив вида <наименование_ВМ>_<дата-время>.tar.gz

Примечание. Данная операция может занимать продолжительное время, особенно для образов дисков в формате RAW, т.к. в этом случае необходимо удалить «нулевые блоки» в процессе резервного копирования для уменьшения размера образа;

4) сформированный архив перемещается в хранилище файлов, а все вышеуказанные файлы уничтожаются.

ВНИМАНИЕ! Если для обеспечения отказоустойчивости сервера управления применяется технология Raft, хранилище файлов должно быть построено на базе файловой технологии хранения. При этом должна использоваться общая (распределенная) файловая система. Каталог хранилища файлов должен быть доступен для всех экземпляров сервера управления.

3.4.11.2. Создание резервной копии ВМ

Чтобы создать резервную копию ВМ, необходимо выполнить следующие действия:

1) в веб-интерфейсе ПК СВ в меню слева выбрать пункт «Экземпляры ВМ — ВМ» и на открывшейся странице «ВМ» выбрать необходимую виртуальную машину;

2) выключить ВМ, если она была включена;

3) на странице выключенной ВМ нажать кнопку **[Управление размещением]** и в открывшемся меню выбрать пункт «Резервная копия» (см. рис. 47);

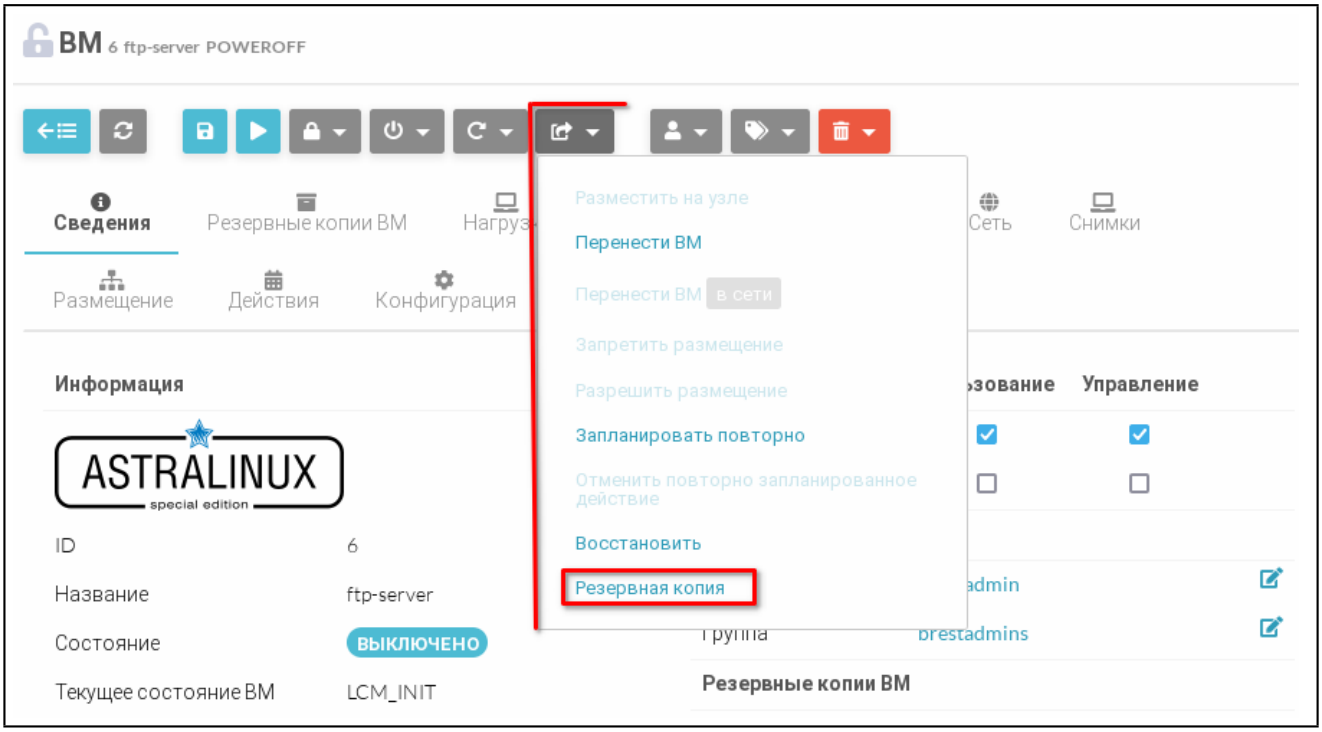

Рис. 47

4) в открывшемся окне «Резервная копия ВМ» (см. рис. 48):

а) в поле «Название» задать наименование резервной копии.

ВНИМАНИЕ! Не допускается использование одинаковых наименований резервных копий. Если в хранилище файлов уже имеется резервная копия с таким наименованием (в том числе для другого экземпляра ВМ), операция резервного копирования не будет выполнена;

б) выбрать хранилище файлов, в котором будет размещен архив резервной копии;

в) нажать кнопку **[Резервная копия]**.

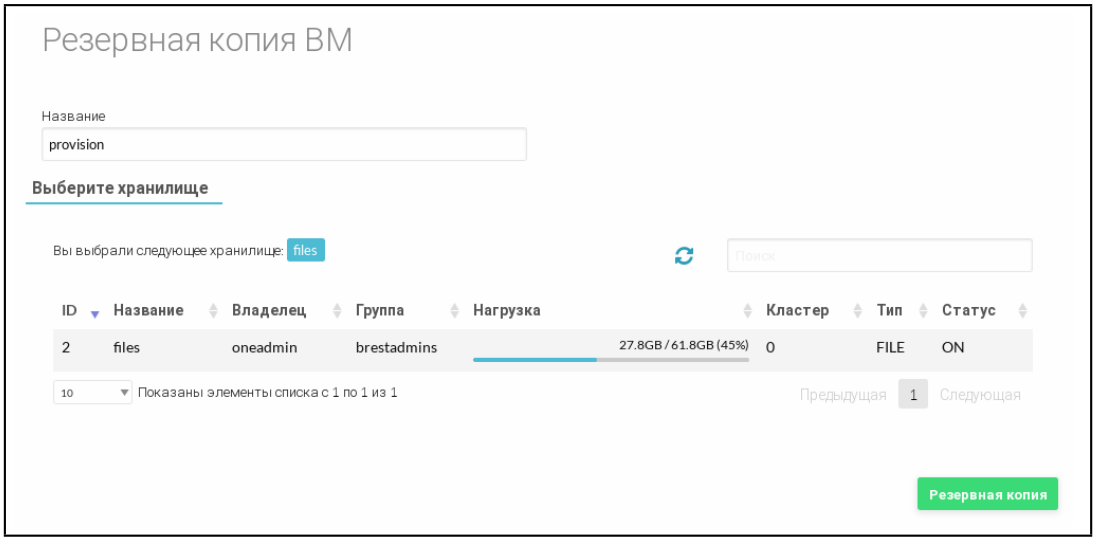

Рис. 48

3.4.11.3. Отображение резервных копий экземпляра ВМ

Для отображения существующих резервных копий ВМ необходимо на странице этой виртуальной машины открыть вкладку «Резервные копии ВМ» (см. рис. 49).

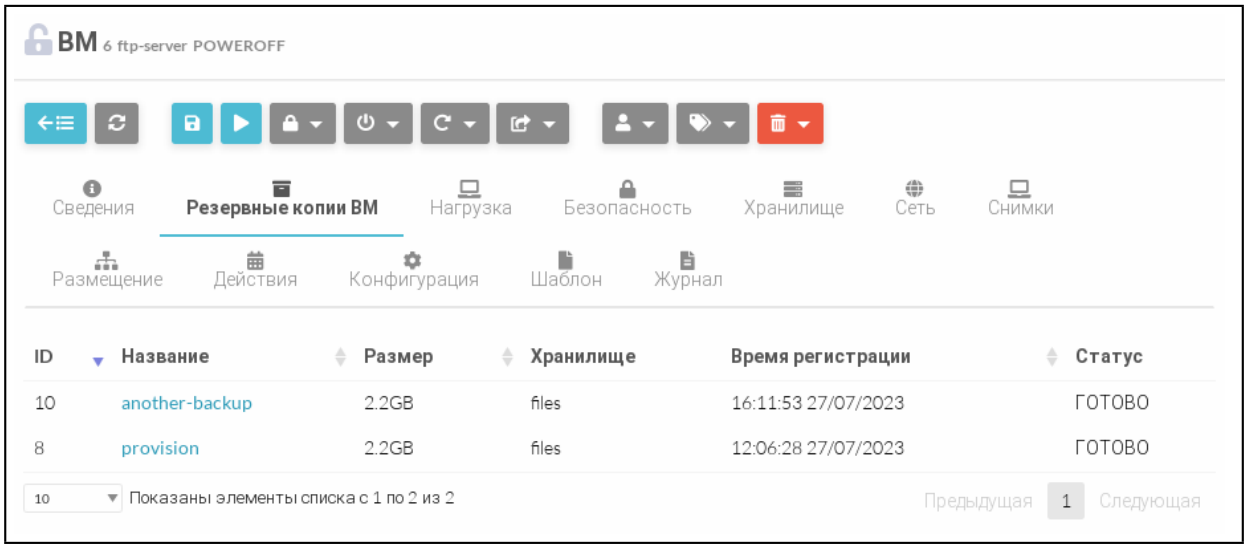

Рис. 49

Для просмотра полной информации о резервной копии ВМ необходимо нажать на соответствующую ссылку в поле «Название». После этого откроется страница «Резервная копия» (см. рис. 50).

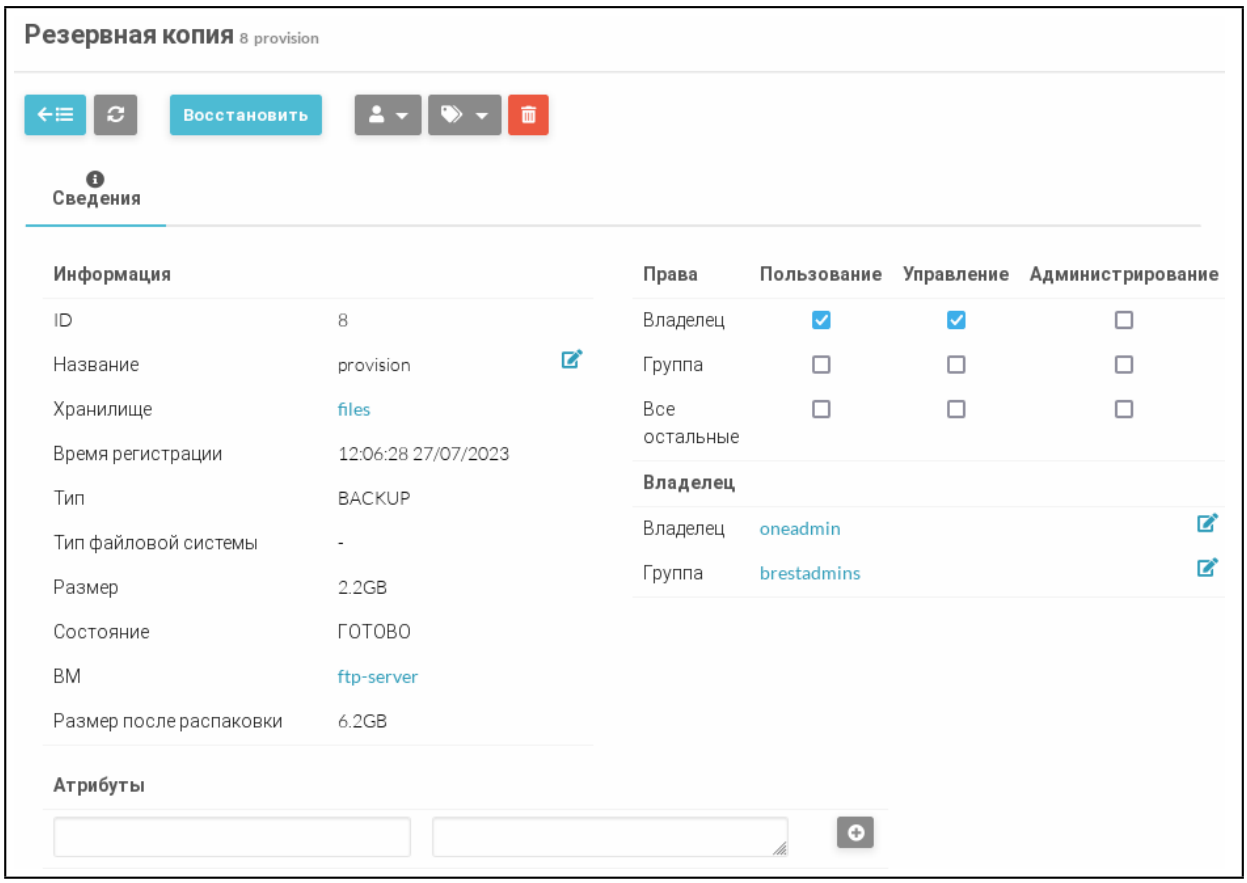

Рис. 50

3.4.11.4. Отображение всех резервных копий, имеющихся в ПК СВ

Для отображения всех существующих резервных копий ВМ необходимо в веб-интерфейсе ПК СВ в меню выбрать «Хранилище — Резервные копии ВМ». На открывшейся странице «Резервные копии ВМ» будет отображена таблица резервных копий ВМ (см. рис. 51)

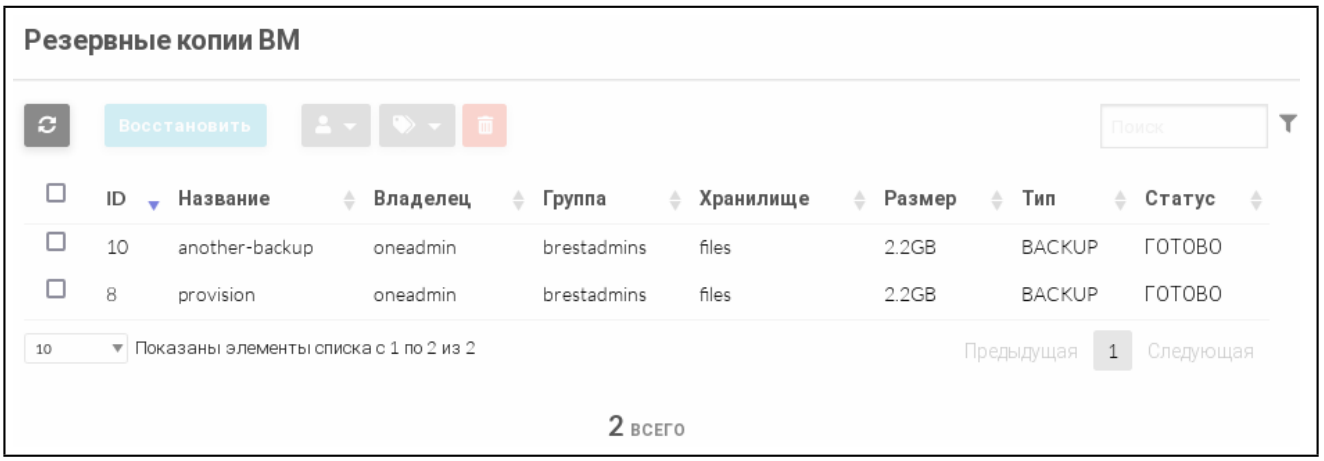

Рис. 51

Для просмотра полной информации о резервной копии ВМ необходимо нажать на соответствующую строку таблицы. После этого откроется страница «Резервная копия» (см. рис. 50).

3.4.11.5. Восстановление ВМ из резервной копии

Для восстановления ВМ из резервной копии необходимо выполнить следующие действия:

1) в веб-интерфейсе ПК СВ в меню слева выбрать пункт «Хранилище — Резервные копии ВМ» и на открывшейся странице «Резервные копии ВМ» выбрать необходимую резервную копию;
2) на странице «Резервная копия» нажать кнопку **[Восстановить]**;
3) в открывшемся окне «Восстановление резервной копии» (см. рис. 52):
   а) в поле «Имя восстанавливаемой машины» задать наименование ВМ;
   б) выбрать системное хранилище, в котором будут размещена ВМ;
   в) нажать кнопку **[Восстановить]**.

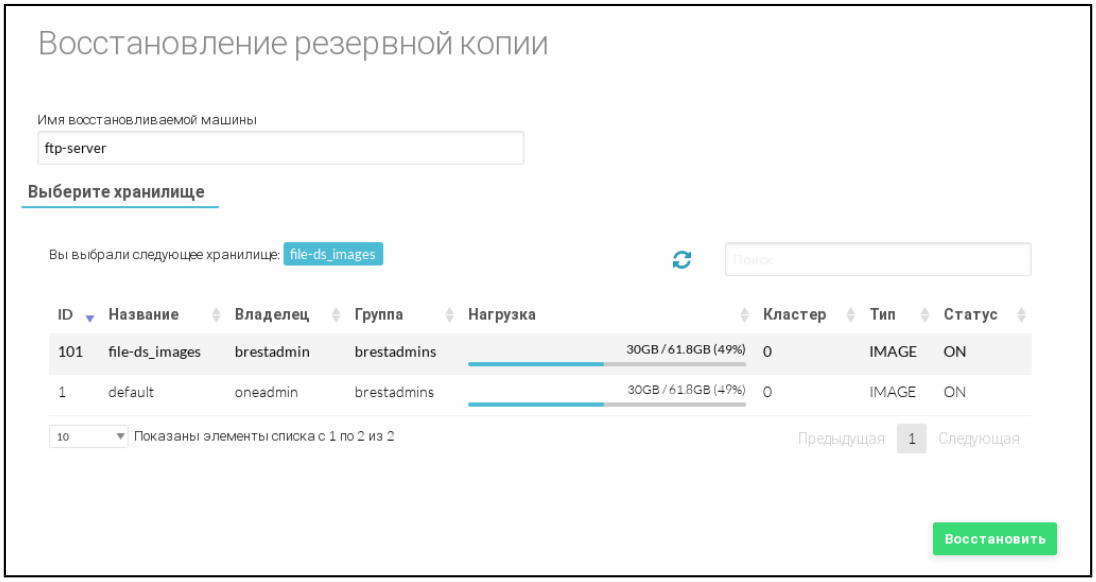

Рис. 52

4) в веб-интерфейсе в меню слева выбрать пункт «Экземпляры ВМ — ВМ» и дождаться пока в поле «Статус» для восстановленной ВМ значение `Инициализация` не изменится на `ВЫКЛЮЧЕНО` или `ЗАПУЩЕНО`, в зависимости от настроек ВМ. Для обновления значения статуса можно воспользоваться кнопкой **[Обновить]**.

3.5. Пользовательские сети

3.5.1. Общие сведения

Пользовательская сеть — это подсеть существующей виртуальной сети, предназначенная для использования конкретным пользователем (группой пользователей). Для создания пользовательской сети используется операция резервирования IP-адресов адресного пространства (диапазона адресов) виртуальной сети.

Примечание. Для пользователя (группы пользователей) в отношении виртуальной сети, в адресном пространстве которой планируется создать пользовательскую сеть,

администратором ПК СВ должны быть установлены полномочия типа USE (применение).

3.5.2. Управление пользовательскими сетями в интерфейсе командной строки

3.5.2.1. Создание пользовательской сети

Для создания пользовательской сети используется команда:

```
onevnet reserve <виртуальная_сеть> -n <пользовательская_сеть> -s <размер>
```

где:

- <виртуальная_сеть> — наименование или идентификатор виртуальной сети, адресное пространство которой необходимо использовать;
- <пользовательская_сеть> — наименование создаваемой пользовательской сети;
- <размер> — количество IP-адресов адресного пространства виртуальной сети, которое необходимо зарезервировать для пользовательской сети.

Пользовательская сеть отобразится в перечне виртуальных сетей, доступных пользователю (группе пользователей).

Кроме того, при создании пользовательской сети можно указать диапазон адресов (Address Ranges — AR), в котором необходимо зарезервировать IP-адреса. Для этого используется аргумент команды `-a <идентификатор_AR>`.

Также при создании пользовательской сети можно указать начальный IP-адрес. Для этого используется аргумент команды `-i <начальный_IP-адрес>`.

Пример

1) просмотреть перечень доступных виртуальных сетей. Пример вывода после выполнения команды `onevnet list`:

```
ID USER      GROUP     NAME     CLUSTERS  BRIDGE  LEASES
1  brestadm  brestadm  Private  0         onebr1      10
```

2) просмотреть перечень доступных диапазонов адресов виртуальной сети Private. Пример вывода после выполнения команды `onevnet show Private`:

```
...
ADDRESS RANGE POOL
AR 0
SIZE           : 51
LEASES         : 0
RANGE    FIRST                              LAST
MAC      02:00:0a:00:00:96     02:00:0a:00:00:c8
IP       10.0.0.150                  10.0.0.200
```

```
AR 1
SIZE           : 20
LEASES         : 0
RANGE                FIRST                   LAST
MAC      02:00:0a:00:00:c8     02:00:0a:00:00:db
IP              10.0.0.200            10.0.0.219
```

3) создать пользовательскую сеть с наименованием MyVNET, в которой будет 10 IP-адресов, зарезервированных из адресного пространства с идентификатором «1» виртуальной сети Private, при этом первый IP-адрес будет иметь значение 10.0.0.210:

```
onevnet reserve Private -n MyVNET -s 10 -a 1 -i 10.0.0.210
```

Пример вывода после выполнения команды:

```
Reservation VNET ID: 8
```

4) просмотреть перечень виртуальных сетей. Пример вывода после выполнения команды `onevnet list`:

```
ID USER      GROUP     NAME     CLUSTERS  BRIDGE  LEASES
8  brestadm  brestadm  MyVNET   0         onebr1       0
1  brestadm  brestadm  Private  0         onebr1      10
...
```

В представленном примере отмечено, что 10 IP-адресов адресного пространства виртуальной сети Private зарезервировано (параметр `LEASES`).

3.5.2.2. Порядок использования пользовательской сети

Порядок использования пользовательской сети такой же, как и при использовании виртуальной сети.

Для подключения ВМ к сети достаточно указать название или идентификатор сети в шаблоне ВМ (блок параметров `NIC`).

Примеры:

1. Для определения ВМ с сетевым интерфейсом, подключенным к сети MyVNET, добавить в шаблон строку:

```
NIC = [ NETWORK = "MyVNET" ]
```

2. При использовании идентификатора сети добавить в шаблон строку:

```
NIC = [ NETWORK_ID = 8]
```

ВМ также получит свободный адрес из любого адресного диапазона сети. Возможно запросить определенный адрес, указав параметры `IP` или `MAC` в блоке параметров `NIC`.

Пример

Подключить ВМ к сети MyVNET с присвоением ей IP-адреса 10.0.0.213:

```
NIC = [
```

```
NETWORK = "MyVNET",
IP = 10.0.0.213
]
```

3.5.2.3. Удаление пользовательской сети

Для удаления пользовательской сети используется команда:

```
onevnet delete <идентификатор/наименование_сети>
```

После удаления пользовательской сети зарезервированные IP-адреса будут автоматически разблокированы и доступны для использования.

3.5.2.4. Снятие резервирования IP-адресов пользовательской сети

Для снятия резервирования IP-адресов без удаления пользовательской сети используется команда:

```
onevnet free <идентификатор/наименование_сети> <идентификатор_AR>
```

Если в пользовательскую сеть не был добавлен дополнительный диапазон адресов (AR), то необходимо указывать идентификатор диапазона адресов, который установлен по умолчанию и имеет значение «0».

ВНИМАНИЕ! В результате выполнения команды `onevnet free` будет удален указанный диапазон адресов. Для добавления диапазона адресов пользователь должен обладать полномочиями типа ADMIN (администрирование) в отношении пользовательской сети.

Примечание. Если в пользовательской сети для какого-либо адреса был установлен запрет на использование (командой `onevnet hold`), то перед снятием резервирования диапазона адресов необходимо разблокировать эти адреса командой `onevnet release`.

3.5.3. Управление пользовательскими сетями в веб-интерфейсе ПК СВ

3.5.3.1. Создание пользовательской сети

Для создания пользовательской сети в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

1) в меню слева выбрать пункт меню «Сеть — Вирт.сети» и на открывшейся странице «Вирт.сети» выбрать сеть, адресное пространство которой необходимо использовать;
2) на открывшейся странице виртуальной сети нажать кнопку **[+]**, а затем в открывшемся меню выбрать пункт «Зарезервировано»;
3) на открывшейся странице «Резервирование из Виртуальной сети» (см. рис. 53):
   а) указать количество IP-адресов адресного пространства виртуальной сети, которое необходимо зарезервировать для пользовательской сети;
   б) задать наименование создаваемой пользовательской сети;
   в) нажать кнопку **[Зарезервировано]**;

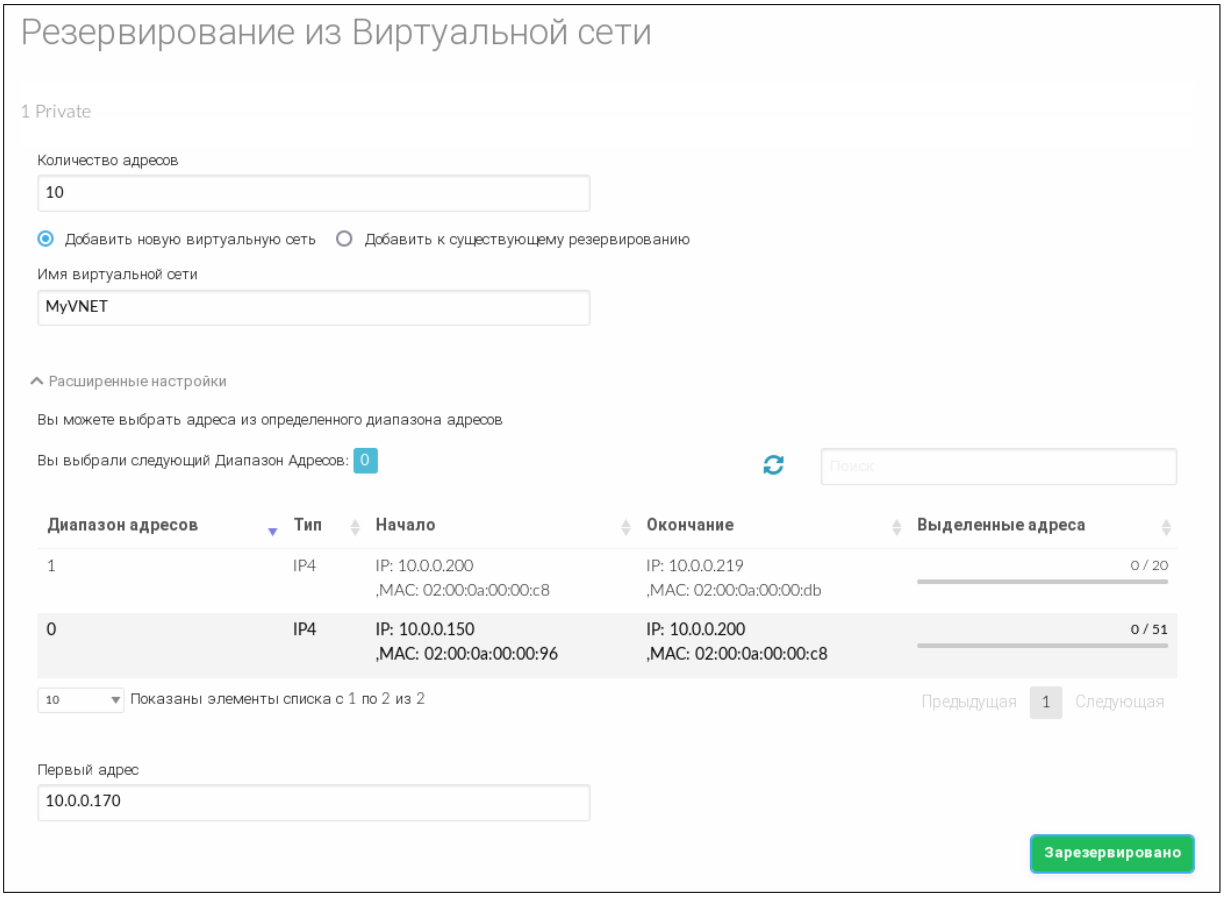

Рис. 53

4) кроме того, в секции «Расширенные настройки» (см. рис. 53) дополнительно можно указать:

- диапазон адресов виртуальной сети, в котором необходимо зарезервировать IP-адреса;
- начальный IP-адрес.

3.5.3.2. Порядок использования пользовательской сети

Порядок использования пользовательской сети такой же, как и при использовании виртуальной сети.

Для подключения создаваемых экземпляров ВМ к сети в веб-интерфейсе ПК СВ достаточно выбрать необходимую сеть в шаблоне ВМ (вкладка «Сеть») — см. рис. 54.

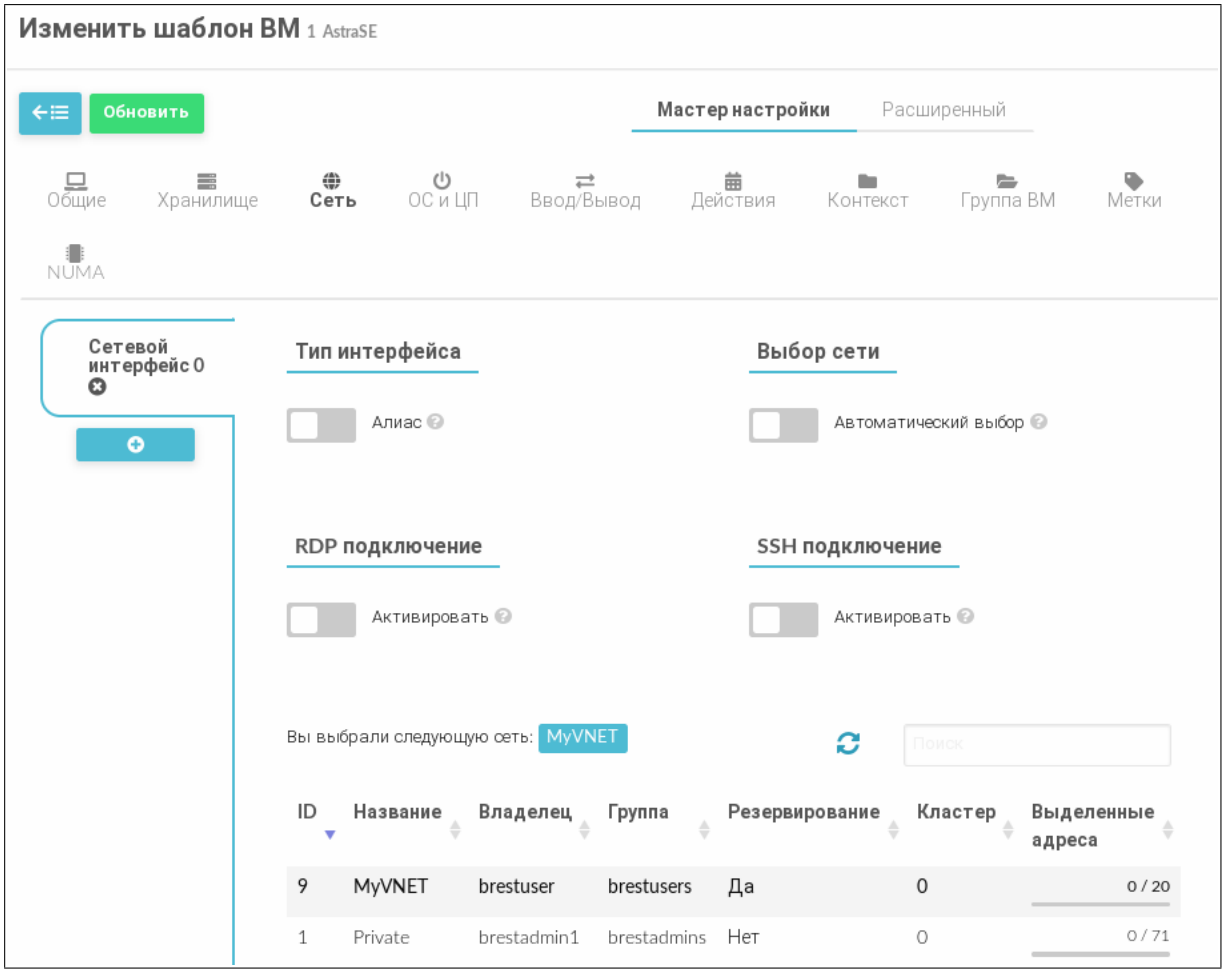

Рис. 54

ВМ получит свободный адрес из любого адресного диапазона сети.

При создании экземпляра ВМ в веб-интерфейсе ПК СВ в секции «Сеть» возможно задать определенный IP-адрес (см. рис. 55).

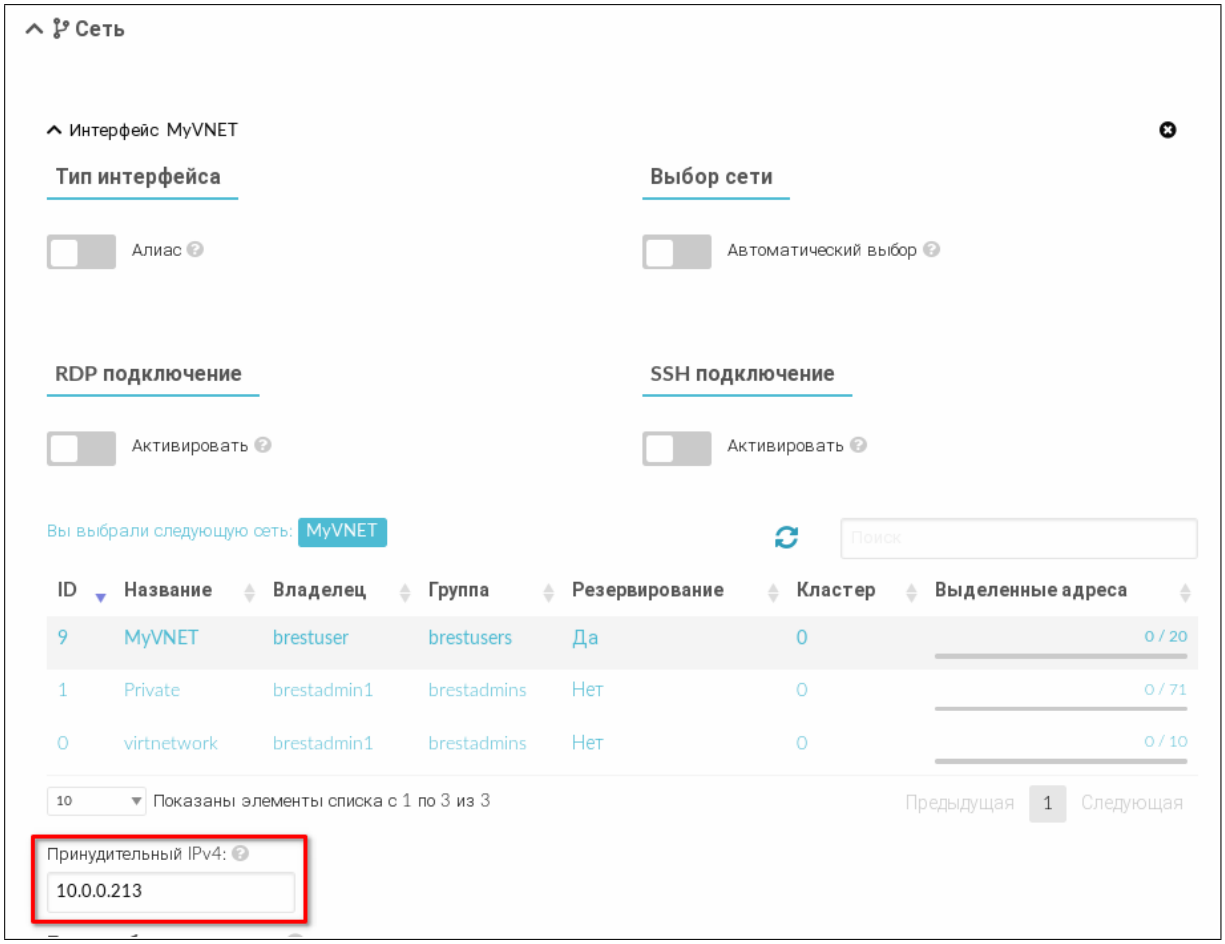

Рис. 55

3.5.3.3. Добавление IP-адресов в пользовательскую сеть

Для добавления IP-адресов в пользовательскую сеть необходимо выполнить следующие действия:

1) в веб-интерфейсе ПК СВ в меню слева выбрать пункт меню «Сеть — Вирт.сети» и на открывшейся странице «Вирт.сети» выбрать сеть, адресное пространство которой было использовано при создании пользовательской сети;

2) на открывшейся странице виртуальной сети нажать кнопку **[+]**, а затем в открывшемся меню выбрать пункт «Зарезервировано»;

3) на открывшейся странице «Резервирование из Виртуальной сети» (см. рис. 56):

   а) указать количество IP-адресов адресного пространства виртуальной сети, которое необходимо зарезервировать для пользовательской сети;

   б) установить флаг «Добавить к существующему резервированию»;

   в) выбрать имеющуюся пользовательскую сеть;

   г) нажать кнопку **[Зарезервировано]**;

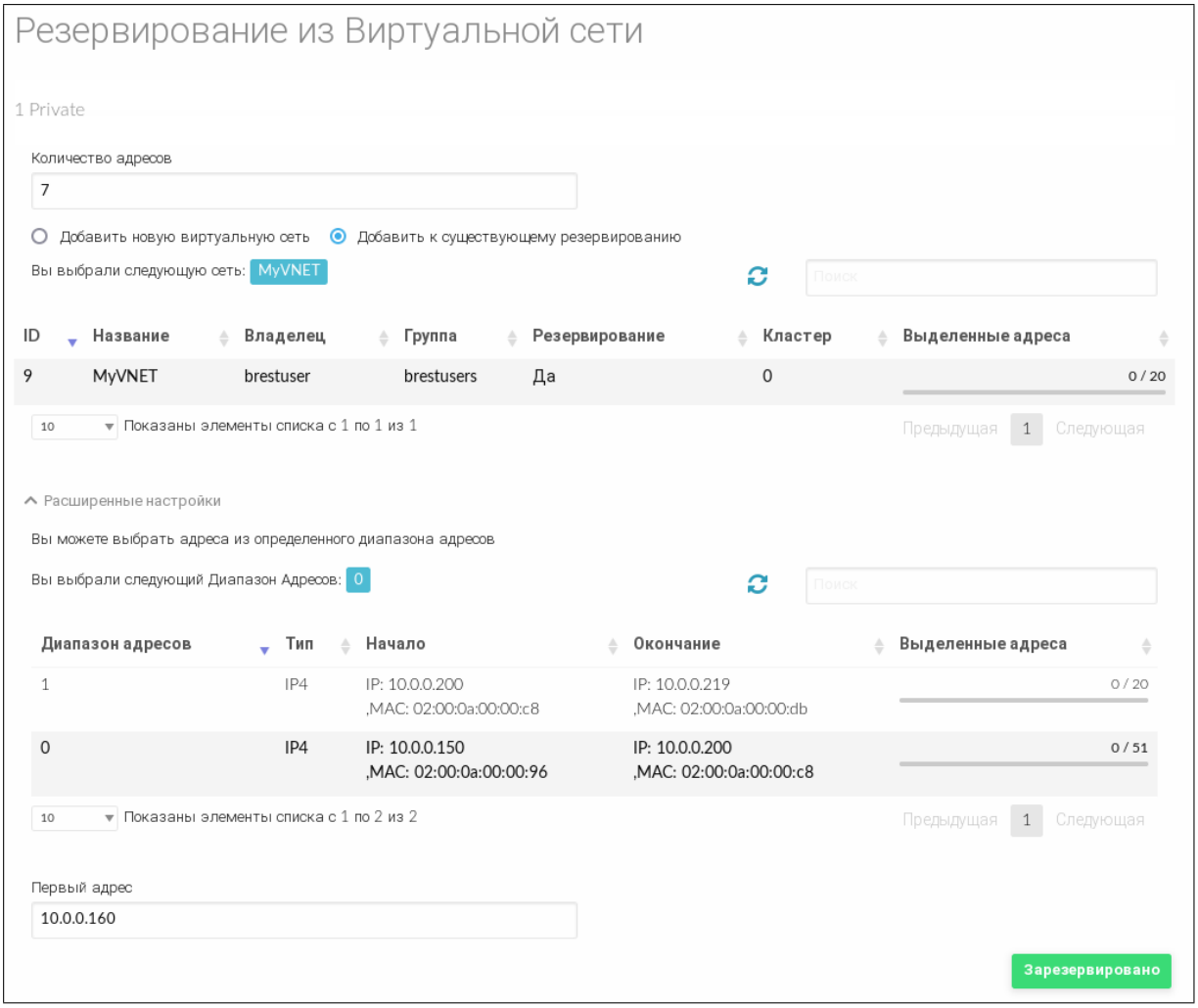

Рис. 56

4) кроме того, в секции «Расширенные настройки» (см. рис. 56) дополнительно можно указать:

- диапазон адресов виртуальной сети, в котором необходимо зарезервировать IP-адреса;
- начальный IP-адрес.

3.5.3.4. Снятие резервирования IP-адресов пользовательской сети

ВНИМАНИЕ! Для снятия резервирования IP-адресов пользователь должен обладать полномочиями типа ADMIN (администрирование) в отношении пользовательской сети.

Для снятия резервирования IP-адресов в пользовательской сети необходимо выполнить следующие действия:

1) в веб-интерфейсе ПК СВ в меню слева выбрать пункт меню «Сеть — Вирт.сети» и на открывшейся странице «Вирт.сети» выбрать пользовательскую сеть;

2) на открывшейся странице пользовательской сети открыть вкладку «Адреса»;

3) во вкладке «Адреса» (см. рис. 57):

а) выбрать диапазон адресов, IP-адреса которого необходимо разблокировать;

б) нажать кнопку **[Удалить]**;

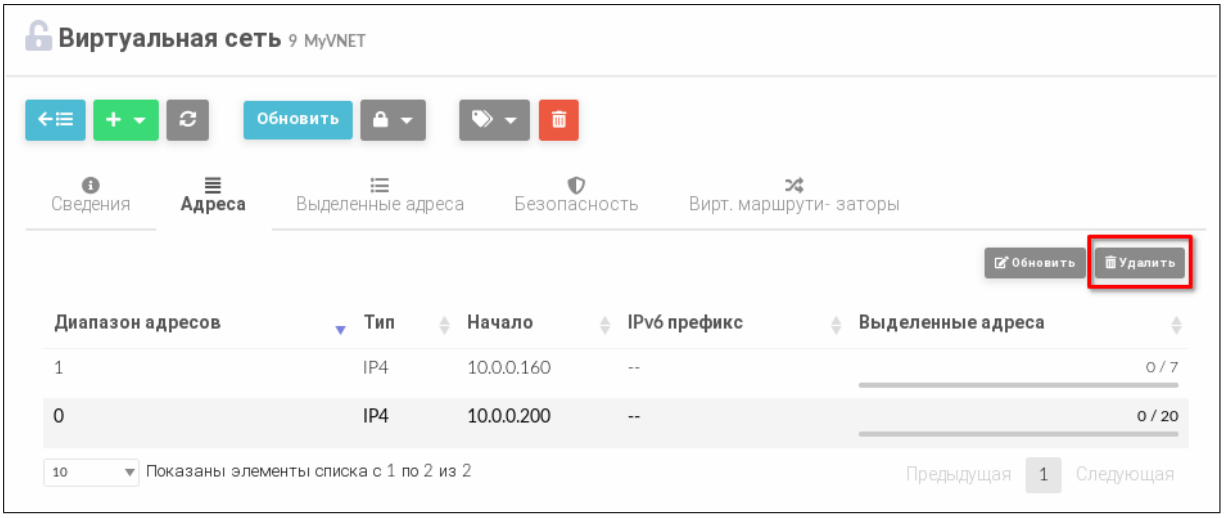

Рис. 57

4) в открывшемся окне «Подтвердить» нажать кнопку **[ОК]** (см. рис. 58).

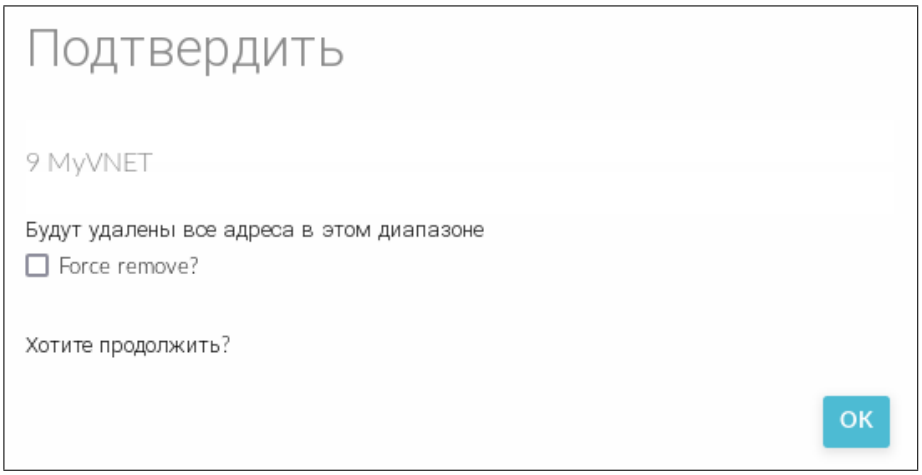

Рис. 58

3.5.3.5. Удаление пользовательской сети

Для удаления пользовательской сети необходимо выполнить следующие действия:

1) в веб-интерфейсе ПК СВ в меню слева выбрать пункт меню «Сеть — Вирт.сети» и на открывшейся странице «Вирт.сети» выбрать пользовательскую сеть;

2) на открывшейся странице пользовательской сети нажать кнопку **[Удалить]**;

3) в открывшемся окне «Подтвердить» нажать кнопку **[ОК]** (см. рис. 59).

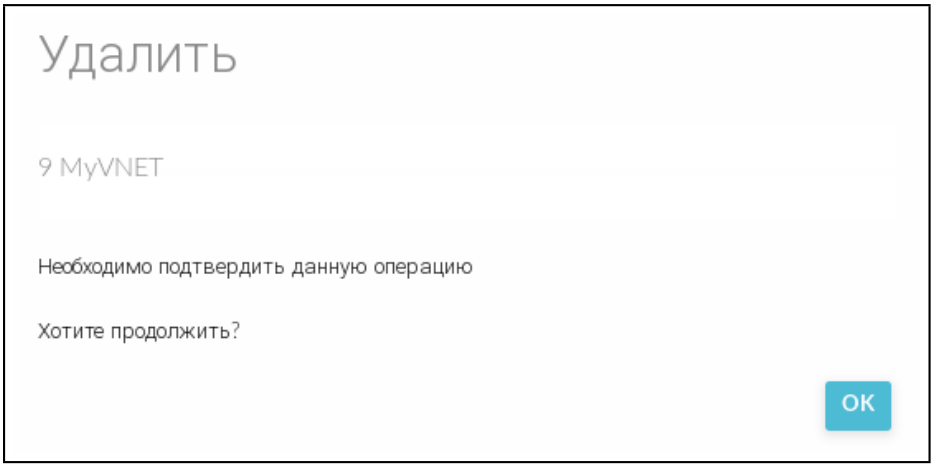

Рис. 59

После удаления пользовательской сети зарезервированные IP-адреса будут автоматически разблокированы и доступны для использования.

3.6. Дополнительная настройка виртуальной машины

3.6.1. Контекстуализация

В ПК СВ применяется контекстуализация для отправки информации на ВМ во время загрузки. Основная задача метода — передача настроек сети и учетных данных на ВМ для ее настройки. Более сложная задача – передача индивидуальных сценариев для загрузки ВМ.

ВНИМАНИЕ! Если в качестве ОС виртуальной машины используется ОС СН, то в ОС этой ВМ должен быть установлен пакет `one-context`, который размещен в расширенном репозитории ОС СН.

В шаблоне ВМ предусмотрен раздел CONTEXT, где можно задать необходимые параметры конфигурации.

Пример

Раздел `CONTEXT` шаблона ВМ

```
CONTEXT = [
   NETWORK = "YES",
   SSH_PUBLIC_KEY = "$USER[SSH_PUBLIC_KEY]",
   START_SCRIPT = "sudo apt install -y ntpdate"
   ]
```

В данном примере задаются следующие настройки ВМ:

- включены сетевые настройки ВМ;
- подключение к ВМ с использованием ssh с пользовательским значением переменной `SSH_PUBLIC_KEY`;
- запуск команды `sudo apt install -y ntpdate` при загрузке ВМ.

3.6.2. Автоматический ввод ВМ в домен через механизм контекста

Механизм контекста позволяет настроить шаблон ВМ таким образом, чтобы при разворачивании ВМ из шаблона, эта ВМ будет автоматически включена в существующий домен FreeIPA/ALD. Для этого необходимо:

1) создать базовую ВМ, на основе которой будет подготовлен шаблон;
2) в базовой ВМ выполнить следующие шаги:
   а) установить ОС СН;
   б) установить пакет `one-context`;
   в) выключить базовую ВМ сохранить ее как постоянный шаблон (см. 3.4.7);
3) в веб-интерфейсе ПК СВ для созданного шаблона выполнить следующие шаги:
   а) на странице шаблона нажать кнопку **[Обновить]**,
   б) на странице «Изменить шаблон ВМ» во вкладке «Контекст» в секции `Опции FreeIPA/ALD` (см. рис. 60) указать параметры контроллера домена:
      - переключатель «Контролер домена» предназначен для выбора типа домена (FreeIPA/ALD),
      - в поле «Доменное имя (REALM)» — указывается наименование домена,
      - в поле «Полное доменное имя сервера (FQDN)» — указывается полное доменное имя контроллера домена FreeIPA/ALD,
      - в поле «IP адрес сервера» — указывается IP-адрес контроллера домена FreeIPA/ALD,
      - в поле «Логин администратора» — указывается имя администратора домена FreeIPA/ALD,
      - в поле «Пароль администратора» — указывается пароль администратора домена FreeIPA/ALD,
      - в поле «Установить префикс для имени ВМ» опционально можно указать префикс, который будет добавляться к имени (hostname) создаваемой ВМ;

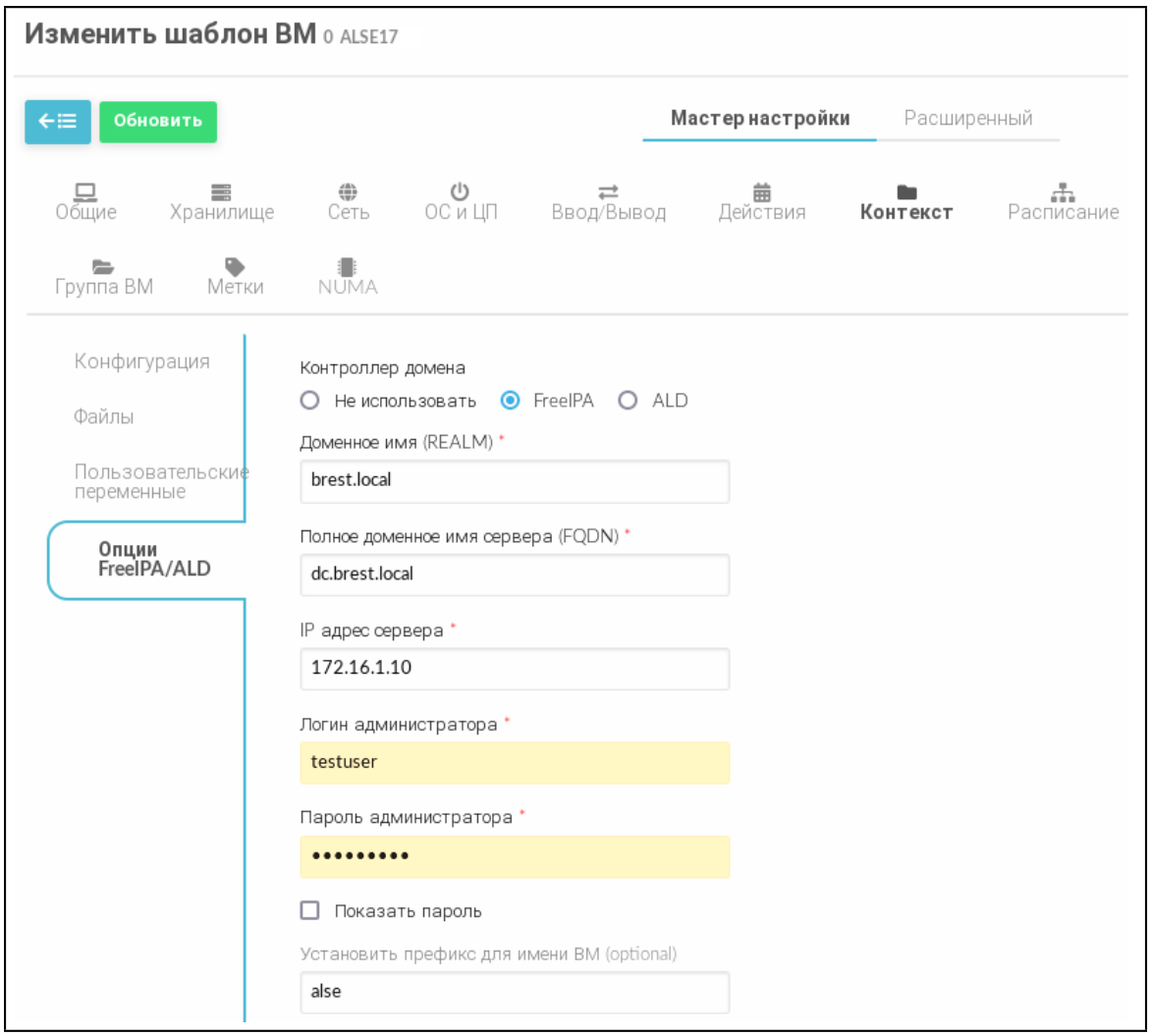

Рис. 60

Примечание. По умолчанию создаваемой ВМ будет присвоено имя вида «one-ID_VM» (например, «one-0.brest.local»). После добавления префикса «PREFIX_-NAME» создаваемой ВМ будет присвоено имя вида «PREFIX_NAME-one-ID_VM» (например, «alse-one-0.brest.local»).

в) на странице «Изменить шаблон ВМ» нажать кнопку **[Обновить]**.

3.7. Подключение устройств к ВМ

3.8. Размещение ВМ с vGPU в ПК СВ

Проброс графического процессора (GPU) в процесс виртуальной машины на узле виртуализации с видеокартой, необходим для запуска виртуальных машин, которые подходят для выполнения графически интенсивных задач и для запуска программного обеспечения, которое не может работать без GPU, например, CAD.

ВНИМАНИЕ! В ПК СВ не поддерживается:

- горячая миграция для ВМ с vGPU;
- горячая перепланировка размещения (rescheduling) для ВМ с vGPU;

- подключение двух и более разных vGPU (разные модели видеокарт) к одной ВМ;

- подключение разных профилей (например Q и B) и и типов профилей (например B1 и B2) к одной ВМ от одной или нескольких видеокарт одной модели; автобалансировка для ВМ с vGPU.

Профили типа A и C тестирования не проходили и не имеют официальной поддержки.

Поддерживаются только видеокарты с встроенным функционалом `vGPU (Time-Slice)` от NVIDIA, `vGPU MIG` от NVIDIA не поддерживается.

Требуется поддержка от аппаратного обеспечения функций SR-IOV и IOMMU.

Требуется использовать ядро ОС СН `linux-5.15-generic`.

Поддерживаются типы профилей vGPU-Q, B.

3.8.1. Использование драйверов NVIDIA

Для корректной работы функций, требующих vGPU на базе программно-аппаратных решений ускорения графических вычислений в средах виртуализации (далее видеокарты с поддержкой vGPU) NVIDIA необходимо, чтобы на серверы виртуализации ПК СВ были установлены драйверы NVIDIA согласно модели видеокарты с поддержкой vGPU.

ВНИМАНИЕ! Данные драйверы не входят в состав сертифицированных на соответствие требованиям по безопасности информации ПК СВ и ОС СН.

После установки драйверов и настройки серверов виртуализации изменяются следующие файлы ПК СВ контрольные суммы которых указаны в файле `gostsums.txt` состава установочного диска и его обновления:

- `/usr/bin/sprof`;
- `/usr/bin/rpcgen`;
- `/usr/bin/gencat`;
- `/usr/lib/x86_64-linux-gnu/libmcheck.a`.

Изменения контрольных сумм не являются нарушением сертифицированных характеристик ПК СВ.

Для проведения контроля целостности данные файлы могут быть исключены из проверки или установлены на контроль с обновленными контрольными суммами.

Назначение файлов, подлежащих изменению:

- `/usr/bin/sprof` — отображает сводку профилирования для общего объекта (общей библиотеки), указанного в качестве первого аргумента командной строки. Сводка профилирования создается с использованием ранее сгенерированных данных профилирования во втором (необязательном) аргументе командной строки;

- `/usr/bin/rpcgen` — инструмент, который генерирует код C для реализации протокола RPC. Входные данные для `rpcgen` — это язык, похожий на C, известный как

RPC Language (язык удаленного вызова процедур);

- /usr/bin/gencat — файл каталога сообщений (обычно *.cat), который команда gencat создает из исходных файлов текстов сообщений (обычно *.msg). Команда gencat объединяет исходные файлы текстов сообщений, указанные параметром SourceFile, в форматированный каталог сообщений, указанный параметром CatalogFile;

- /usr/lib/x86_64-linux-gnu/libmcheck.a — библиотека функции mcheck, которая устанавливает набор отладочных хуков для семейства функций выделения памяти malloc. Эти хуки вызывают определенные проверки согласованности состояния общей массы запросов в памяти. Проверки могут обнаруживать ошибки приложения, такие как освобождение блока памяти более одного раза или повреждение структур данных учета, которые непосредственно предшествуют блоку выделенной памяти.

3.8.2. Подготовка и настройка узла виртуализации

Для подготовки и настройки узла виртуализации необходимо запустить скрипт предварительной настройки узла виртуализации для использования vGPU brest_vgpu_configure: /usr/sbin/brest_vgpu_configure

ВНИМАНИЕ! Скрипт предварительной настройки узла виртуализации для использования vGPU не устанавливает драйвера видеокарты NVIDIA.

3.8.3. Присоединение графического процессора к виртуальной машине

Примечания:

1. После подключения графического процессора необходимо подключиться к ВМ для установки драйвера выбранной видеокарты и активации ее лицензии. Для установки драйвера видеокарты и активации лицензии необходимо обратиться к документации NVIDIA и разработчика ОС, установленной на ВМ.
2. При большом количестве ВМ можно воспользоваться сторонними средствами автоматизации для установки драйверов и активации лицензий.

3.8.3.1. Присоединение графического процессора в веб-интерфейсе

Настройка шаблона ВМ

Для того, чтобы добавить vGPU в шаблон виртуальной машины, необходимо:

1) В веб-интерфейсе ПК СВ в меню слева выбрать «Шаблоны — ВМ».

2) На открывшейся странице «Шаблоны ВМ» нажать кнопку **[+]** и выбрать пункт «Создать».

3) На открывшейся странице «Создать шаблон ВМ» перейти во вкладку «Ввод/Вывод» (см. рис. 61):

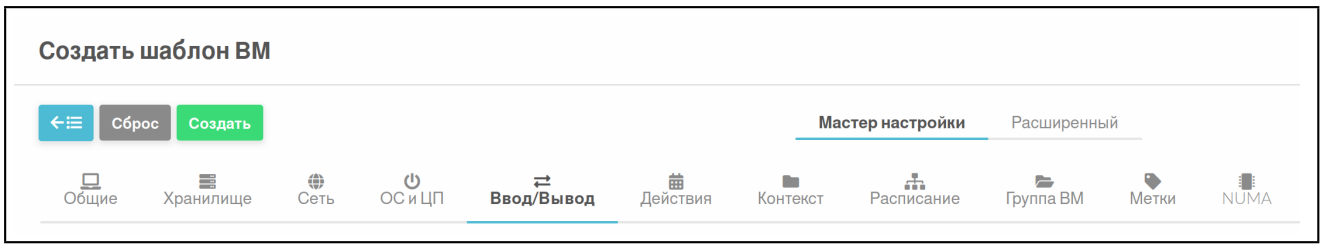

Рис. 61

4) На вкладке «Ввод/Вывод» перейти к разделу «VGPU Devices» и нажать на кнопку **[+]**.

5) Заполнить появившиеся поля:

- «VGPU name» — название видеокарты (значение выбирается из выпадающего списка);
- «VGPU profile» — название готового профиля (значение выбирается из выпадающего списка);
- «Amount» — количество подключаемых виртуальных функций (указывается целочисленное значение) (см. рис. 62):

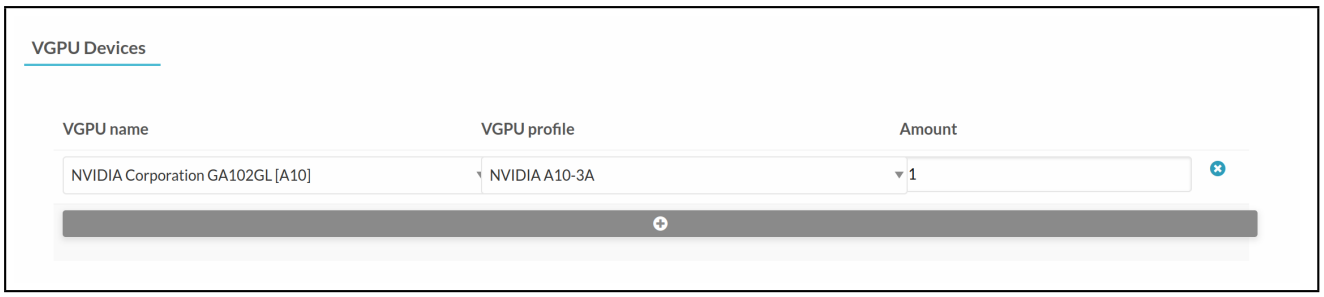

Рис. 62

6) На странице «Создать шаблон ВМ» после заполнения остальных необходимых параметров нажать на кнопку **[Создать]**.

7) После этого на открывшейся странице «Шаблоны ВМ» отобразится созданный шаблон.

8) На странице «Шаблоны ВМ» выбрать созданный шаблон и на открывшейся странице «Шаблон ВМ» нажать на кнопку **[Создать экземпляр]**.

9) На открывшейся странице «Создать ВМ»:

- в поле «Имя ВМ» задать наименование ВМ;
- для параметра «Служебная ВМ» установить значение «Вкл»;
- нажать на кнопку **[Создать экземпляр]**.

Настройка конфигурации ВМ

Для того, чтобы добавить vGPU в виртуальной машине, необходимо изменить конфигурацию виртуальной машины, для этого необходимо:

1) В веб-интерфейсе ПК СВ в меню слева выбрать «Экземпляры ВМ — ВМ».

2) На странице «Экземпляры ВМ — ВМ» выбрать созданную ВМ.

3) На странице «ВМ» перейти на вкладку «Конфигурация» и нажать на кнопку **[Изменить конфигурацию]** (см. рис. 63):

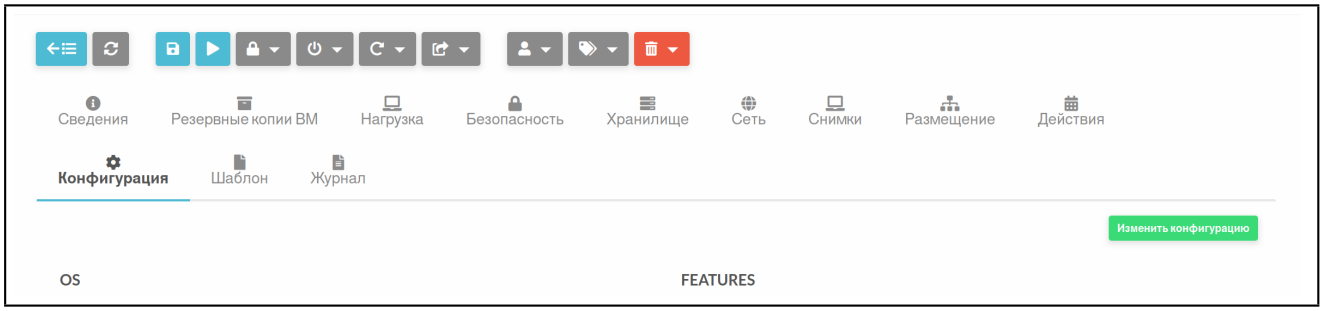

Рис. 63

4) В открывшемся окне «Редактирование конфигурации ВМ» перейти на вкладку «Ввод/Вывод» (см. рис. 64):

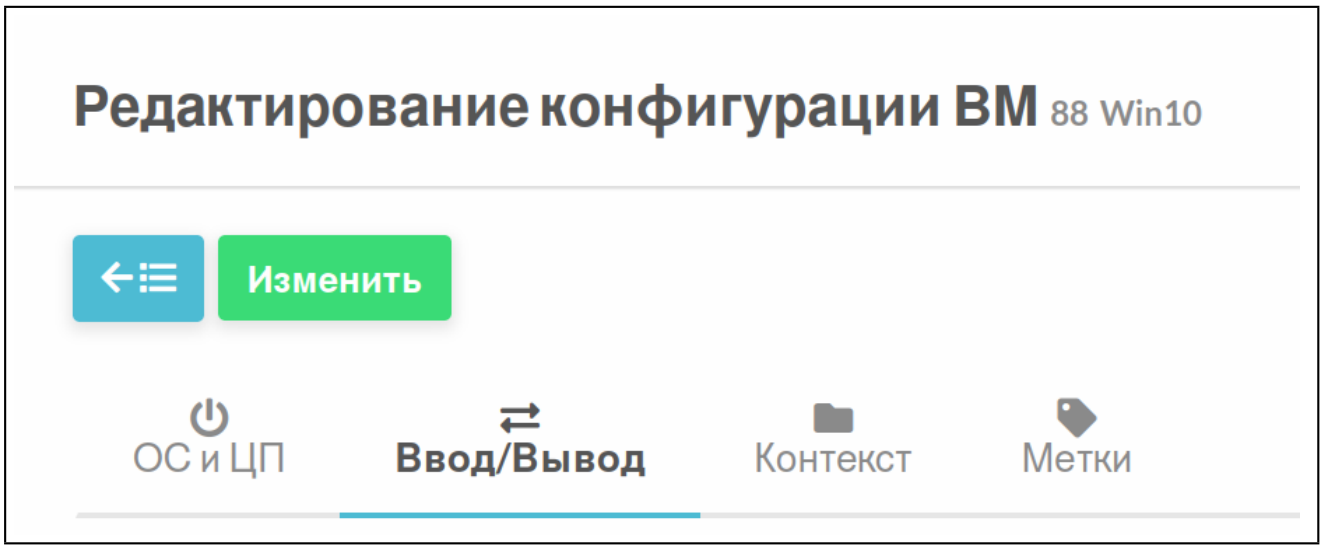

Рис. 64

5) В разделе «VGPU Devices», нажать на кнопку **[+]**, а затем заполнить следующие параметры:

- «VGPU name» — название видеокарты (значение выбирается из выпадающего списка);
- «VGPU profile» — название готового профиля (значение выбирается из выпадающего списка);
- «Amount» — количество подключаемых виртуальных функций (указывается целочисленное значение) (см. рис. 65):

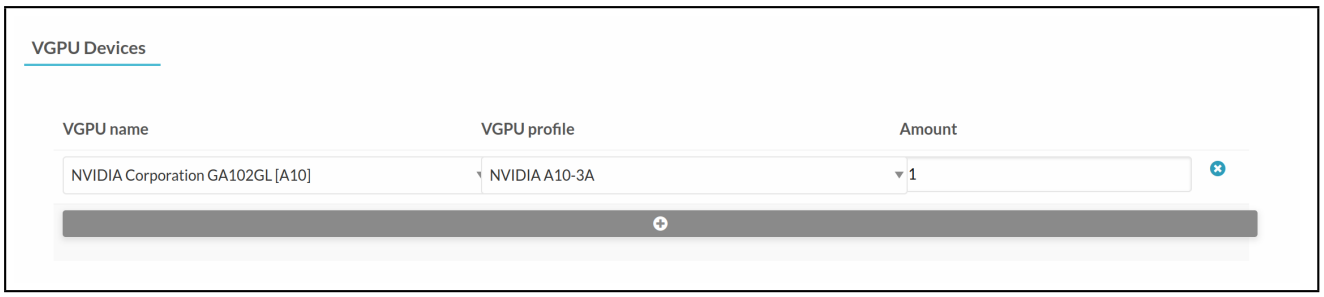

Рис. 65

6) В окне «Редактирование конфигурации ВМ» нажать на кнопку **[Изменить]**.

3.8.3.2. Присоединение графического процессора в интерфейсе командной строки

Для того, чтобы добавить vGPU к виртуальной машине, необходимо на сервере управления (на текущем лидере RAFT), выполнить следующую команду:

```
onevm attach-vgpu <VM_ID> --vgpu_pool <VGPU_POOL_ID> --vgpu_profile <VGPU_PROFILE>
```

где:

- <VM_ID>text — идентификационный номер ВМ;
- <VGPU_POOL_ID> — идентификационный номер присоединяемой видеокарты;
- <VGPU_PROFILE> — название готового профиля;
- <VFS> — количество подключаемых виртуальных функций.

3.8.4. Отсоединение графического процессора от ВМ

3.8.4.1. Удаление графического процессора в веб-интерфейсе

Настройка шаблона ВМ

Для того, чтобы удалить vGPU из шаблона виртуальной машины, необходимо:

1) В веб-интерфейсе ПК СВ в меню слева выбрать «Шаблоны — ВМ».

2) На открывшейся страницы «Шаблоны ВМ» выбрать нужный шаблон из списка.

3) На открывшейся странице «Шаблон ВМ» нажать на кнопку **[Обновить]**.

4) На открывшейся странице «Изменить шаблон ВМ» открыть вкладку «Ввод/Вывод».

5) На открытой вкладке «Ввод/Вывод» перейти к разделу «VGPU Devices» и нажать на кнопку **[x]** справа от параметров удаляемого GPU (см. рис. 66):

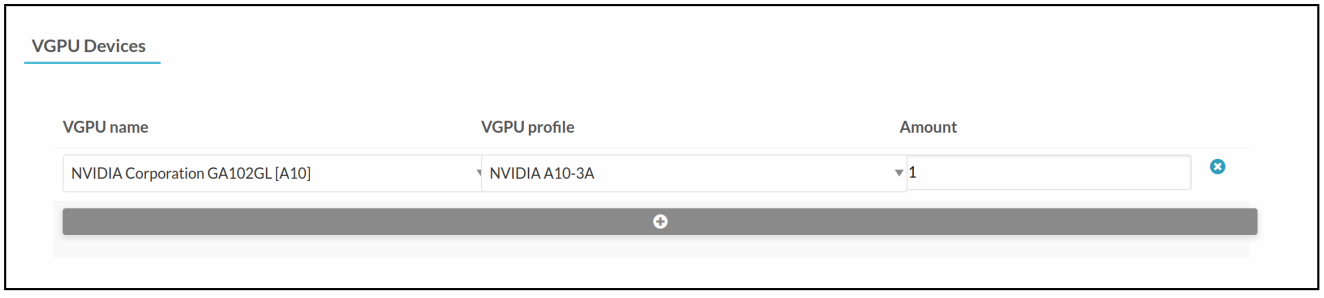

Рис. 66

6) На странице «Изменить шаблон ВМ» после заполнения остальных необходимых параметров нажать на кнопку **[Обновить]**.

Настройка конфигурации ВМ

Для того, чтобы удалить vGPU в виртуальной машине, необходимо изменить конфигурацию виртуальной машины, для этого необходимо:

1) В веб-интерфейсе ПК СВ в меню слева выбрать «Экземпляры ВМ — ВМ».

2) На странице «Экземпляры ВМ — ВМ» выбрать нужную ВМ.

3) На странице «ВМ» перейти на вкладку «Конфигурация» и нажать на кнопку **[Изменить конфигурацию]** (см. рис. 67):

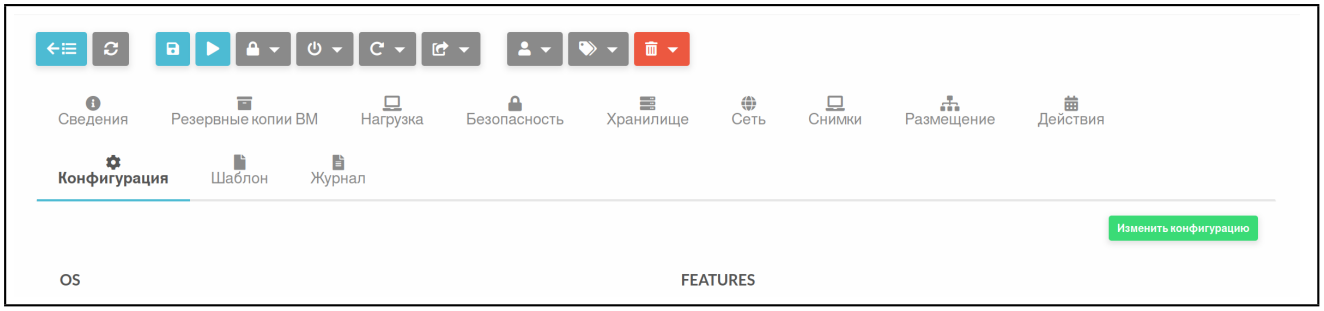

Рис. 67

4) В открывшемся окне «Редактирование конфигурации ВМ» перейти на вкладку «Ввод/Вывод».

5) На открытой вкладке «Ввод/Вывод» перейти к разделу «VGPU Devices» и нажать на кнопку **[x]** справа от параметров удаляемого GPU (см. рис. 68):

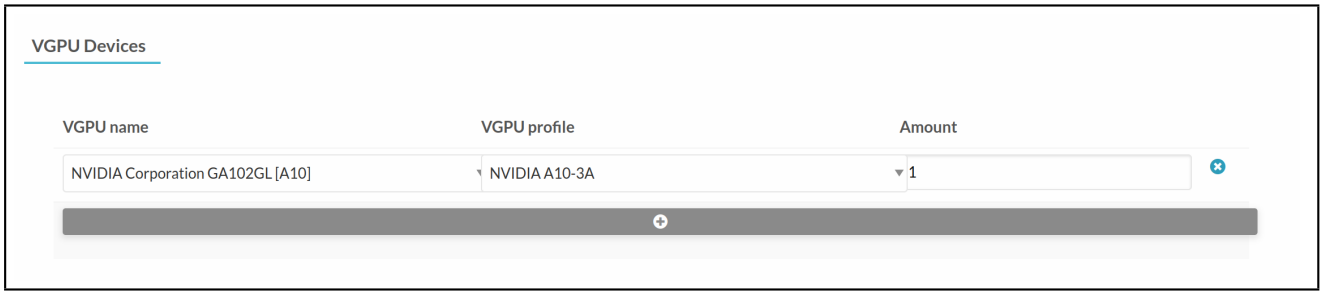

Рис. 68

6) В окне «Редактирование конфигурации ВМ» нажать на кнопку **[Изменить]**.

3.8.4.2. Удаление графического процессора в интерфейсе командной строки

Для того, чтобы удалить vGPU из виртуальной машины, необходимо на сервере управления (на текущем лидере RAFT), выполнить следующую команду:

```
onevm detach-vgpu <VM_ID> <VGPU_POOL_ID>
```

где:

- <VM_ID> — идентификационный номер ВМ;
- <VGPU_POOL_ID> — идентификационный номер присоединяемой видеокарты.

3.9. Удаленное подключение USB-устройств к ВМ по протоколам VNC/SPICE/RDP

В состав дистрибутива ПК СВ входит графическое приложение `brest-usb-redirect`, позволяющее пользователю перенаправить подключенные USB-устройства на виртуальные машины в рамках домена FreeIPA по протоколам VNC, SPICE или RDP.

Для того чтобы обеспечить возможность перенаправить подключенные USB-устройства на ВМ, необходимо выполнить следующие действия:

1) на сервере управления ПК СВ установить пакет `brest-vdi-tools`, для этого в терминале выполнить команду:

```
apt install brest-vdi-tools
```

2) в веб-интерфейсе ПК СВ на странице ВМ, на которую необходимо перенаправить USB-устройство:

а) открыть вкладку «Конфигурация» и нажать кнопку **[Изменить конфигурацию]**;

б) на открывшейся странице «Редактирование конфигурации ВМ» указать один из протоколов удаленного доступа. Для этого:

- при выборе VNC или SPICE — во вкладке «Вод/Вывод» в секции «Средства графического доступа» выбрать необходимый протокол (см. рис. 69),

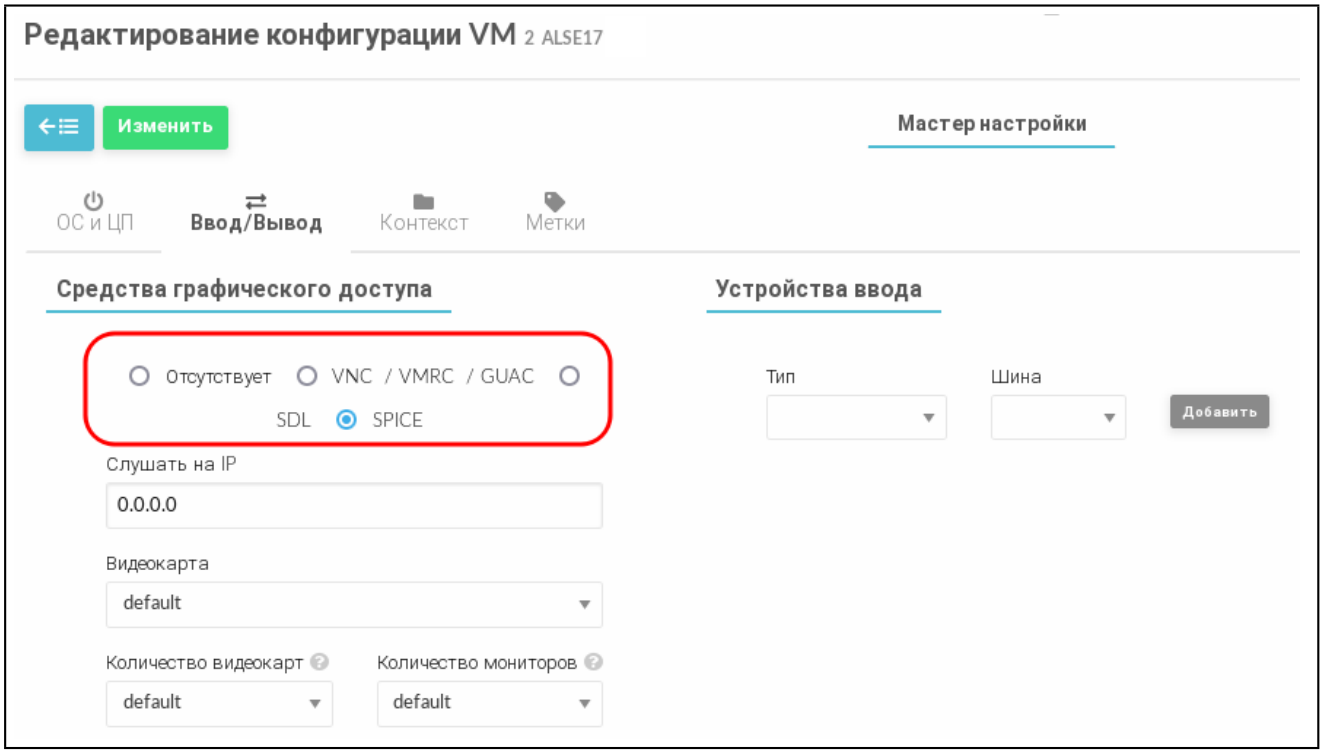

Рис. 69

- при выборе RDP — во вкладке «ОС и ЦП» в секции «Особенности» в

выпадающем списке «Гостевой агент Qemu» выбрать «Да» (см. рис. 70),

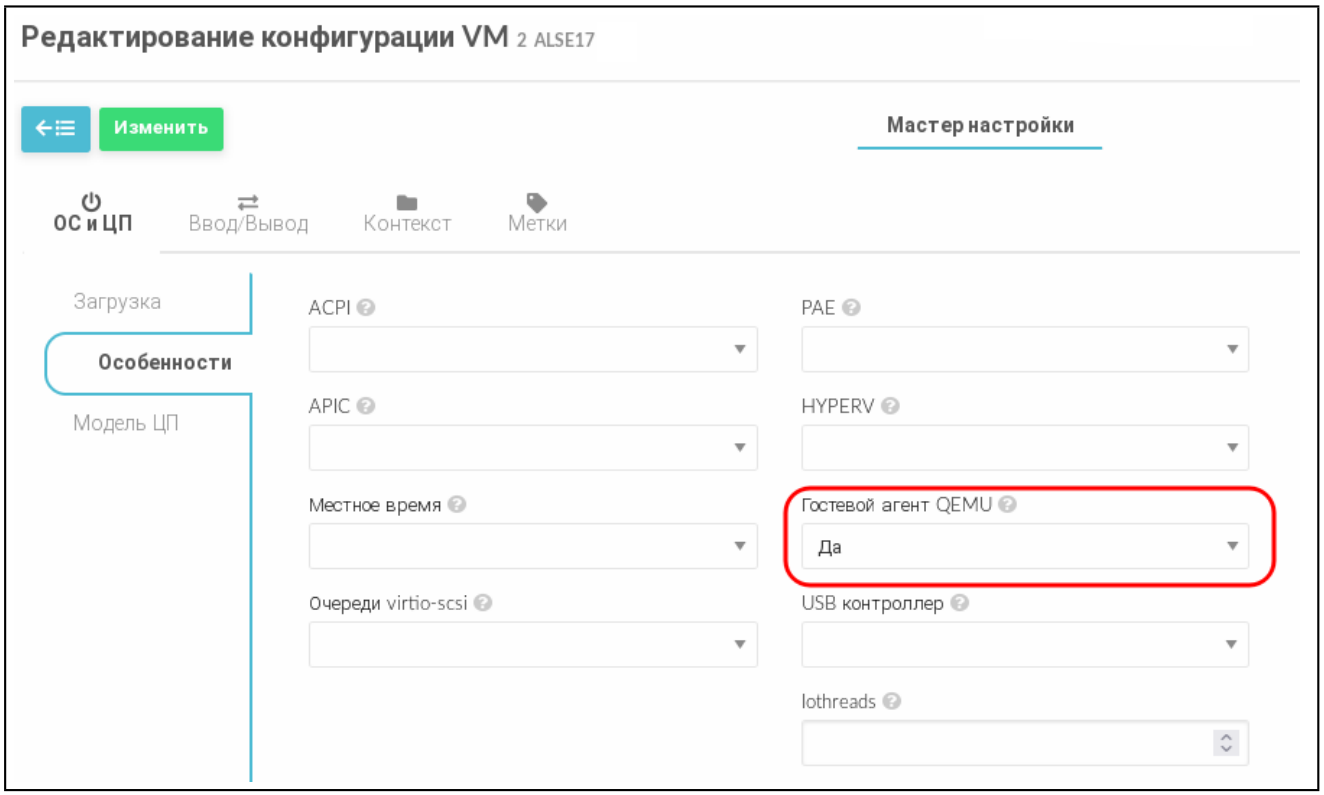

Рис. 70

- при необходимости скорректировать тип USB-контроллера в настройках виртуальной машины, на которую будет перенаправлено USB-устройство (по умолчанию задействован контроллер USB 2.0). Если необходимо перенаправить устройство USB 3.0 и выше, то во вкладке «ОС и ЦП» в секции «Особенности» в выпадающем списке «USB контроллер» выбрать «3.0» (см. рис. 70),

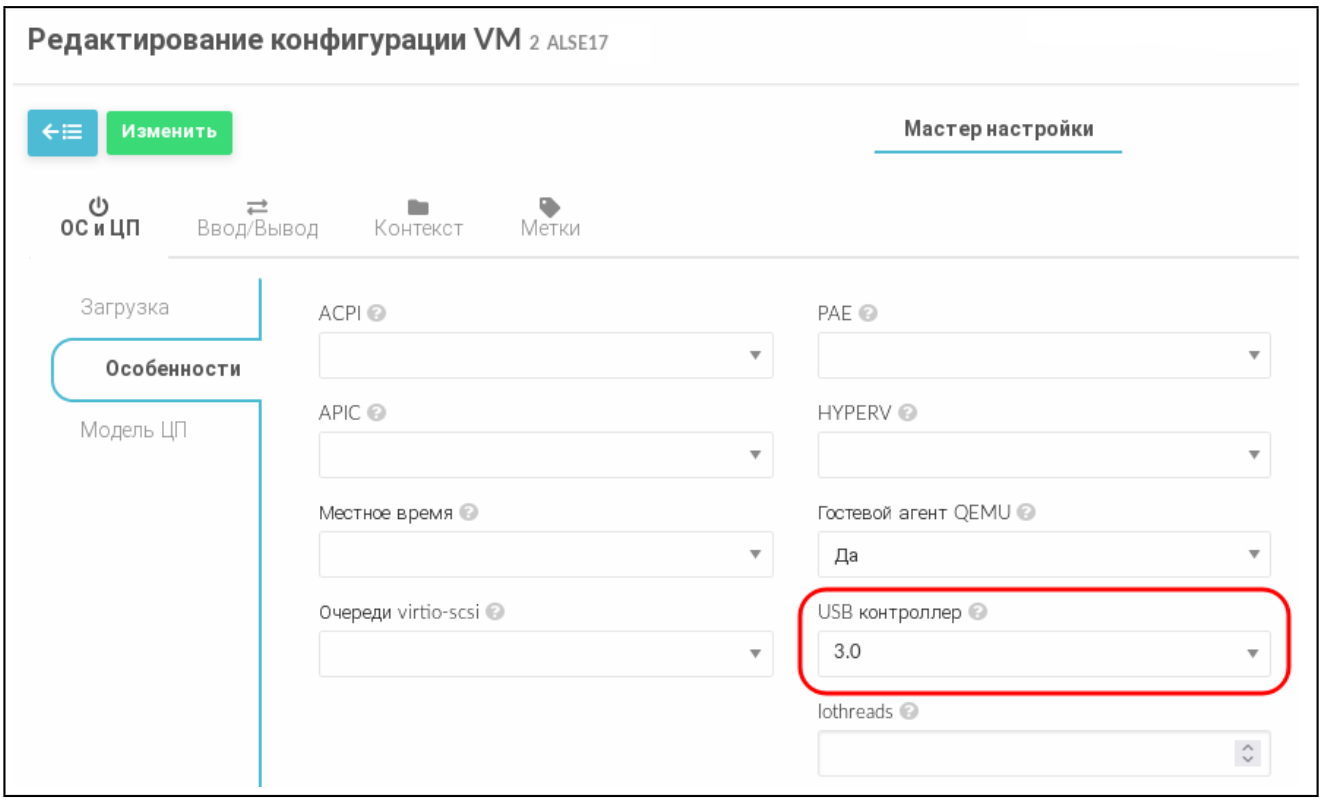

Рис. 71

- на странице «Редактирование конфигурации ВМ» нажать кнопку **[Изменить]**;

3) на виртуальной машине, на которую необходимо перенаправить USB-устройство, следует установить пакеты `qemu-guest-agent`, `xrdp` и `one-context`. Для этого в терминале выполнить команду:

```
apt install qemu-guest-agent xrdp one-context
```

4) на клиентской машине, с которой будут перенаправлены подключенные USB-устройства, должна быть установлена ОС СН. Для перенаправления подключенных USB-устройств необходимо установить пакет `brest-usb-redirect`, выполнив в терминале команду:

```
apt install brest-usb-redirect
```

ВНИМАНИЕ! Клиентская машина должна входить в тот же домен FreeIPA, что и сервер управления ПК СВ.

Для того чтобы перенаправить подключенное USB-устройство на ВМ, на клиентской машине необходимо выполнить следующие действия:

1) через графический интерфейс запустить приложение (права администратора не требуются): «Пуск — Сеть — Brest Usb Redirect» (см. рис. 72).

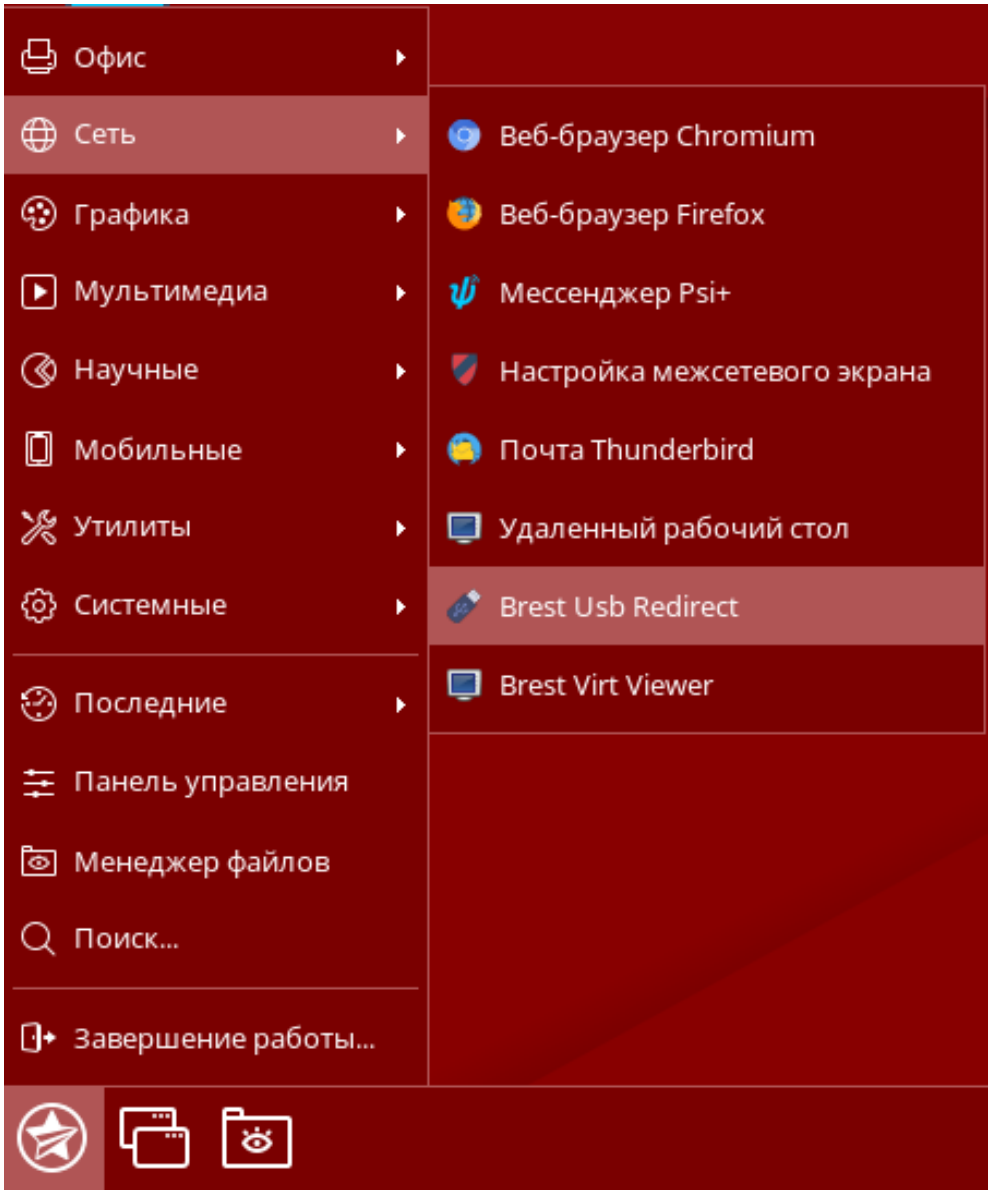

Рис. 72

ВНИМАНИЕ! Учетная запись пользователя, от имени которого запускается графическое приложение `brest-usb-redirect`, должна быть зарегистрирована в том же домене FreeIPA, в который входит сервер управления ПК СВ;

2) в открывшемся окне «Авторизация» (см. рис. 73) указать авторизационные параметры для доступа к виртуальной машине, на которую необходимо перенаправить USB-устройство:

- «Адрес сервера» — полное доменное имя компьютера, на котором установлен сервер виртуализации;
- «Логин» — имя учетной записи пользователя домена, имеющего доступ к виртуальной машине;
- «Пароль» — пароль учетной записи пользователя домена, имеющего доступ к виртуальной машине;

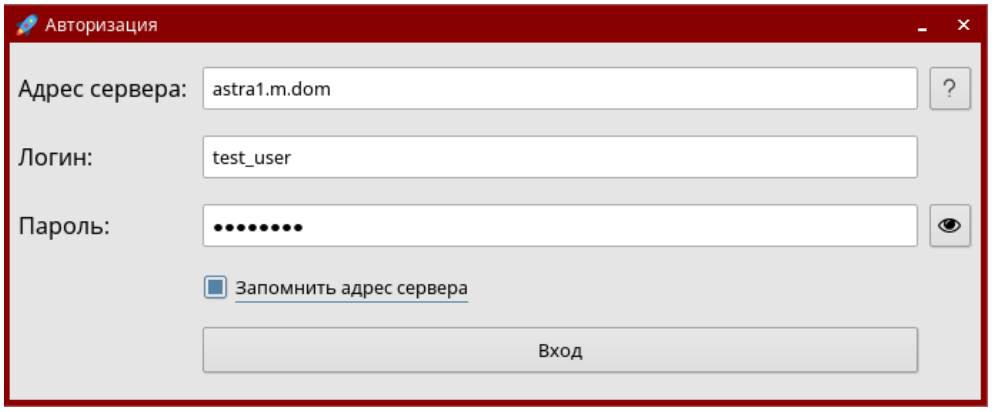

Рис. 73

3) в открывшемся окне «Список виртуальных машин» (см. рис. 74) указать виртуальную машину, на которую необходимо перенаправить USB-устройство.

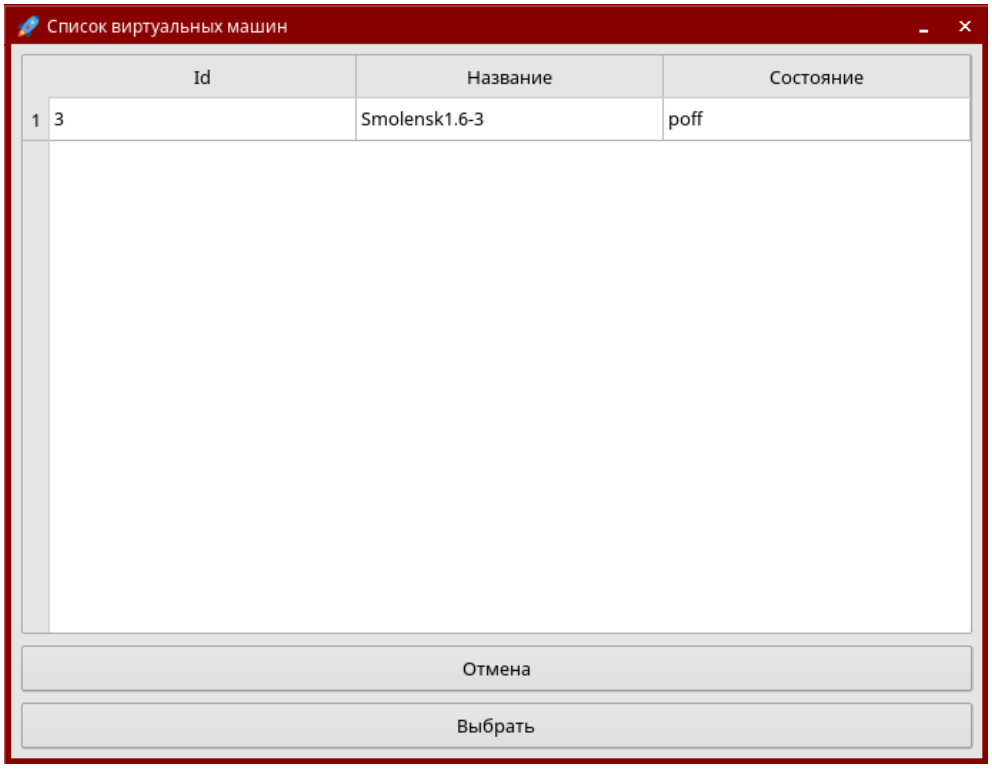

Рис. 74

ВНИМАНИЕ! Виртуальная машина должна входить в тот же домен FreeIPA, что и сервер управления ПК СВ;

4) в открывшемся окне «Список usb-устройств» (см. рис. 75) выбрать одно или несколько USB-устройств, которые необходимо перенаправить;

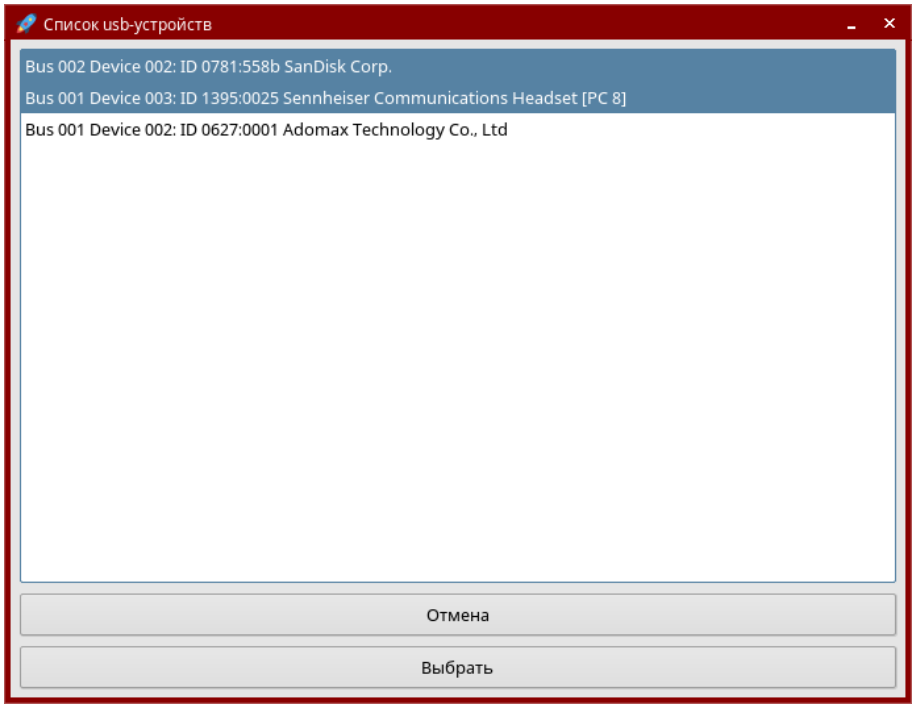

Рис. 75

5) в открывшемся окне «Доступные подключения» (см. рис. 76) выбрать протокол подключения;

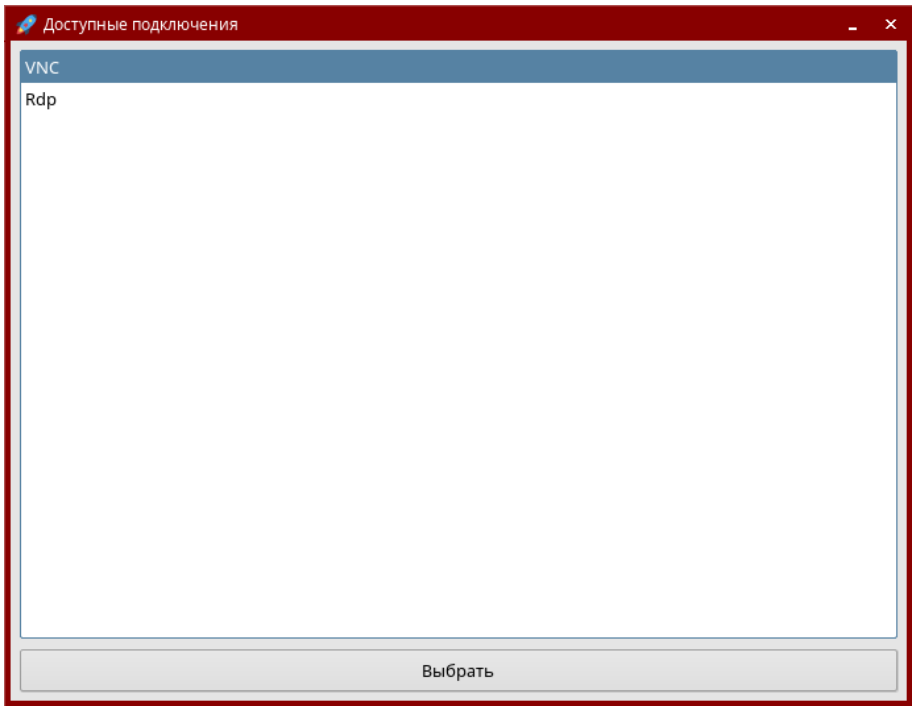

Рис. 76

6) проверить подключение USB-устройства, для этого на ВМ, на которую было перенаправлено USB-устройство, в терминале выполнить команду:

```
lsusb
```

Если подключение прошло успешно, то в результате выполнения команды в выведенном списке доступных USB-устройств будет отображено перенаправляемое

USB-устройство (см. рис. 77).

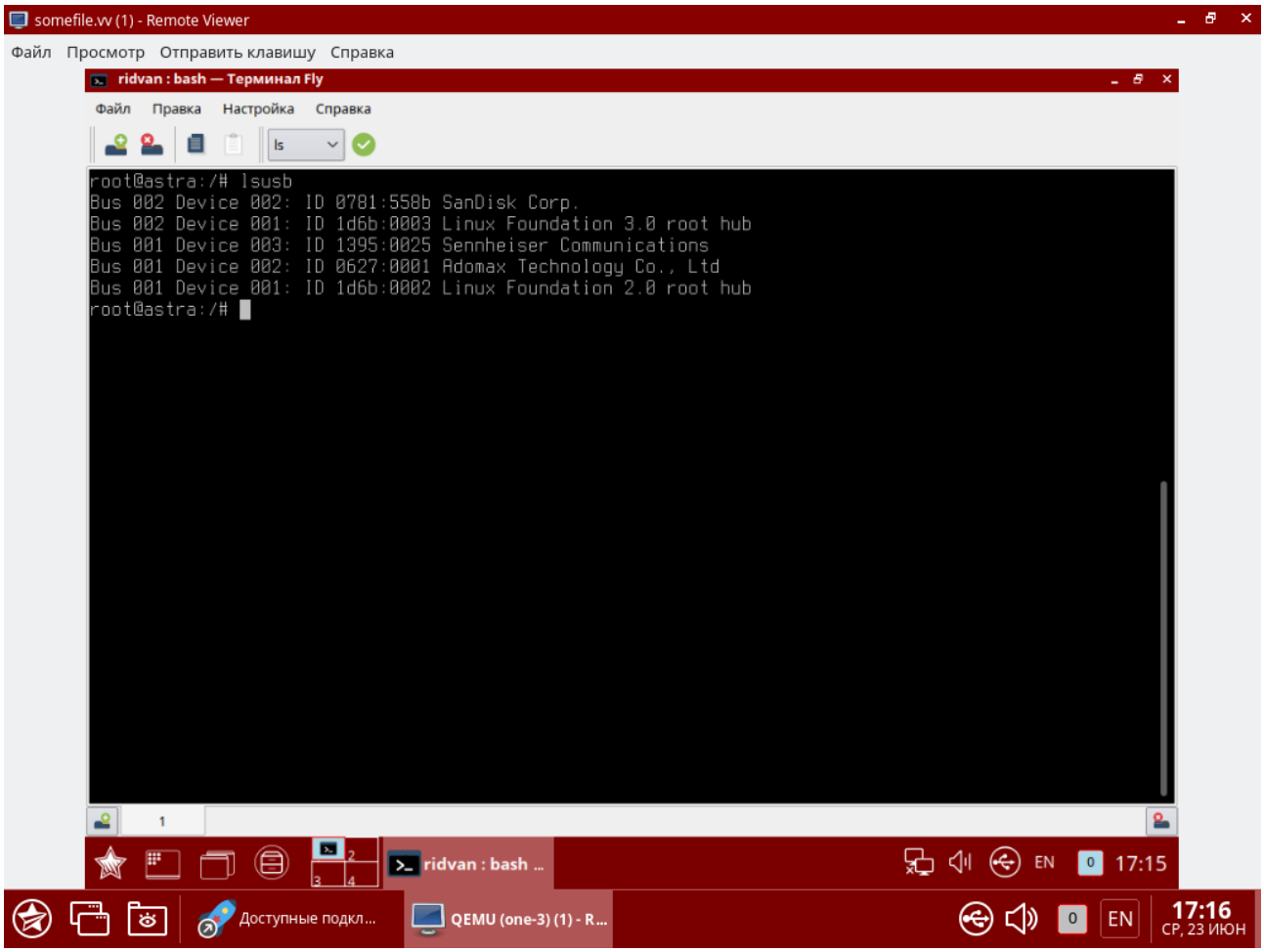

Рис. 77

3.10. Ретрансляция PCI

Устройства PCI серверов виртуализации можно перенаправлять на виртуальные машины.

3.10.1. Требования

Ядро на сервере виртуализации должно поддерживать ввод/вывод MMU. Для процессоров Intel это реализация VT-d, для AMD — AMD-Vi. Кроме того, должна обеспечиваться возможность внесения в черный список любого драйвера, который может получить доступ к PCI-устройству, которое необходимо подключить к виртуальным машинам.

3.10.2. Настройка сервера виртуализации

3.10.2.1. Конфигурация ядра

Конфигурация ядра должна выполняться с учетом необходимости поддержки ввода/вывода MMU и блокировки любых драйверов, которые могут осуществлять доступ к устройствам PCI, предполагаемым для использования в виртуальных машинах. Параметр для подключения ввода/вывода MMU:

```
intel_iommu=on
```

Необходимо также разрешить ядру загружать драйвер vfio-pci и блокировать драйверы для выбранных карт. Например, для графической платы nvidia можно применять следующие параметры:

```
rd.driver.pre=vfio-pci rd.driver.blacklist=nouveau
```

Указанные выше параметры необходимо добавить в конфигурационный файл `/etc/default/grub`:

```
GRUB_CMDLINE_LINUX_DEFAULT="intel_iommu=on rd.driver.pre=vfio-pci rd.driver./
   blacklist=nouveau"
```

3.10.2.2. Загрузка драйвера vfio в initrd

Модули для vfio должны быть добавлены в initrd. Для этого необходимо:

1) в конфигурационный файл `/etc/modules` добавить перечень модулей:

```
pci_stub
vfio
vfio_iommu_type1
vfio_pci
vfio_virqfd
```

2) выполнить команду:

```
update-initramfs -u -k all
```

3.10.2.3. Блокировка драйверов

Блокировка, которая определяется в параметрах ядра, должна вноситься и в настройки системы. Пример файла `/etc/modprobe.d/blacklist.conf` для графической платы nvidia:

```
blacklist nouveau
blacklist lbm-nouveau
options nouveau modeset=0
alias nouveau off
alias lbm-nouveau off
```

Наряду с этой конфигурацией драйвер vfio должен быть загружен с передачей идентификатора карт PCI, которые предполагается подключить к ВМ. Для того что бы узнать идентификатор PCI устройства, необходимо ввести команду:

```
lspci -nn
```

Например, для графической платы nvidia Grid K2 с идентификатором `10de:11bf` в конфигурационный файл `/etc/modprobe.d/blacklist.conf` необходимо добавить следующую строку:

```
options vfio-pci ids=10de:11bf
```

3.10.2.4. Привязка устройств к vfio

Механизм ввода/вывода MMU разделяет устройства PCI на группы для изолирования работы памяти между устройствами и ВМ. Для добавления устройств PCI в vfio и назначения

им группы можно использовать совместно используемые скрипты.

Пример

Скрипт привязывает карту к vfio, прописывается в файле /usr/local/bin/vfio-bind

```
#!/bin/sh
modprobe vfio-pci
for dev in "$@"; do
      vendor=$(cat /sys/bus/pci/devices/$dev/vendor)
      device=$(cat /sys/bus/pci/devices/$dev/device)
      if [ -e /sys/bus/pci/devices/\$dev/driver ]; then
            echo $dev > /sys/bus/pci/devices/$dev/driver/unbind
      fi
      echo $vendor $device > /sys/bus/pci/drivers/vfio-pci/new_id
done
```

Необходимо сделать этот скрипт исполняемым.

Конфигурация прописывается в файле /etc/sysconfig/vfio-bind. Устройства указываются с PCI-адресами. Адреса можно получить командой lspci, добавив в начало домен, как правило, 0000.

```
DEVICES="0000:04:00.0 0000:05:00.0 0000:84:00.0 0000:85:00.0"
```

Приведенный в примере выше скрипт необходимо добавить в автостарт системы. Для этого следует выполнить следующие действия:

1) создать службу, например vfio-bind, сформировав unit-файл /etc/systemd/system/vfio-bind.service, такого содержания:

```
[Unit]
Description=Binds devices to vfio-pci
After=syslog.target
[Service]
EnvironmentFile=-/etc/default/vfio-bind
Type=oneshot
RemainAfterExit=yes
ExecStart=-/usr/local/bin/vfio-bind $DEVICES
[Install]
WantedBy=multi-user.target
```

2) перезагрузить список служб командой:

```
sudo systemctl daemon-reload
```

3) добавить службу vfio-bind в автозагрузку командой:

```
sudo systemctl enable vfio-bind
```

3.10.2.5. Конфигурация qemu

После привязки PCI к vfio необходимо предоставить qemu-доступ к vfio-устройствам для групп, назначенных устройствам PCI. Список устройств PCI и их vfio-группу можно получить с помощью команды:

```
find /sys/kernel/iommu_groups/ -type l
```

Пример

Для карт с группами 45, 46 и 58 в файл `/etc/libvirt/qemu.conf` добавить конфигурацию:

```
cgroup_device_acl = [
"/dev/null", "/dev/full", "/dev/zero", "/dev/random", "/dev/urandom",
"/dev/ptmx", "/dev/kvm", "/dev/kqemu", "/dev/rtc","/dev/hpet",
"/dev/vfio/vfio", "/dev/vfio/45", "/dev/vfio/46", "/dev/vfio/58"
]
```

3.10.3. Настройка драйвера

Единственной необходимой настройкой является фильтр для теста системы мониторинга, который получает список устройств PCI. По умолчанию тест перечисляет все устройств PCI, имеющиеся на сервере виртуализации. Для изменения данного списка можно изменить настройки фильтра в файле `/var/lib/one/remotes/im/kvm-probes.d/pci.rb` и установить список с таким же форматом lspci:

```
# Данная функция содержит фильтры для мониторинга устройств PCI. Формат
# такой же, как lspci, и можно добавить несколько фильтров через запятые.
# Нулевой фильтр обеспечит извлечение всех устройств PCI.
#
# Из раздела помощи lspci:
# -d [<vendor>]:[<device>][:<class>]
#
# Например
#
# FILTER = '::0300' # все карты VGA
# FILTER = '10de::0300' # все карты NVIDIA VGA
# FILTER = '10de:11bf:0300' # только GK104GL [GRID K2]
# FILTER = '8086::0300,::0106' # все карты Intel VGA и любые контроллеры SATA
```

3.10.4. Настройка использования устройств PCI

Основным действием по настройке является просмотр информации о сервере виртуализации в интерфейсе командной строки или в веб-интерфейсе ПК СВ, обнаружение доступных устройств PCI и добавление желаемого устройства в шаблон. Устройства PCI можно добавлять указывая значения параметров `vendor` (производитель), `device` (устрой-

ство) и class (класс). В ПК СВ виртуальная машина будет развернута только на сервере виртуализации с имеющимся устройством PCI. Если таких серверов виртуализации нет, в журнале планировщика появится сообщение об ошибке.

3.10.4.1. В интерфейсе командной строки

Перечень доступных устройств PCI на сервере виртуализации (секция PCI DEVICES) можно просмотреть командой:

```
onehost show <идентификатор_сервера_виртуализации>
```

Пример

Список устройств PCI сервера виртуализации с идентификатором 0, пример вывода после выполнения команды onehost show 0:

```
PCI DEVICES

VM ADDR TYPE NAME
   00:00.0 8086:0a04:0600 Haswell-ULT DRAM Controller
   00:02.0 8086:0a16:0300 Haswell-ULT Integrated Graphics Controller
123 00:03.0 8086:0a0c:0403 Haswell-ULT HD Audio Controller
   00:14.0 8086:9c31:0c03 8 Series USB xHCI HC
   00:16.0 8086:9c3a:0780 8 Series HECI #0
   00:1b.0 8086:9c20:0403 8 Series HD Audio Controller
   00:1c.0 8086:9c10:0604 8 Series PCI Express Root Port 1
   00:1c.2 8086:9c14:0604 8 Series PCI Express Root Port 3
   00:1d.0 8086:9c26:0c03 8 Series USB EHCI #1
   00:1f.0 8086:9c43:0601 8 Series LPC Controller
   00:1f.2 8086:9c03:0106 8 Series SATA Controller 1 [AHCI mode]
   00:1f.3 8086:9c22:0c05 8 Series SMBus Controller
   02:00.0 8086:08b1:0280 Wireless 7260
```

где:

- VM — идентификационный номер ВМ, использующей данное устройство. Не указывается, если это устройство не используется ни одной ВМ;
- ADDR — адрес на шине PCI;
- TYPE (тип) — значения описания устройства, в формате vendor:device:class. Данные значения используются при выборе устройства PCI для перенаправления;
- NAME (имя) — имя устройства PCI.

Для обеспечения перенаправления одного из устройств PCI, в шаблон ВМ необходимо добавить блок параметров PCI, с помощью которого производится выбор устройства для использования. Например, для устройства Haswell-ULT HD Audio Controller:

```
PCI = [
      VENDOR = "8086",
      DEVICE = "0a0c",
```

```
CLASS = "0403"
]
```

Устройство может быть также указано без всех типовых значений. Например, для получения любых портов PCI Express Root Ports в шаблон ВМ можно добавить:

```
PCI = [
CLASS = "0604"
]
```

Для подключения более одного устройства PCI в шаблоне ВМ необходимо добавить дополнительные блоки параметров `PCI`.

3.10.4.2. В веб-интерфейсе ПК СВ

Для отображения доступных устройств PCI сервера виртуализации в веб-интерфейсе ПК СВ необходимо:

1) в меню слева выбрать пункт меню «Инфраструктура — Узлы»;
2) на открывшейся странице «Узлы» открыть вкладку «PCI» (см. рис. 78)

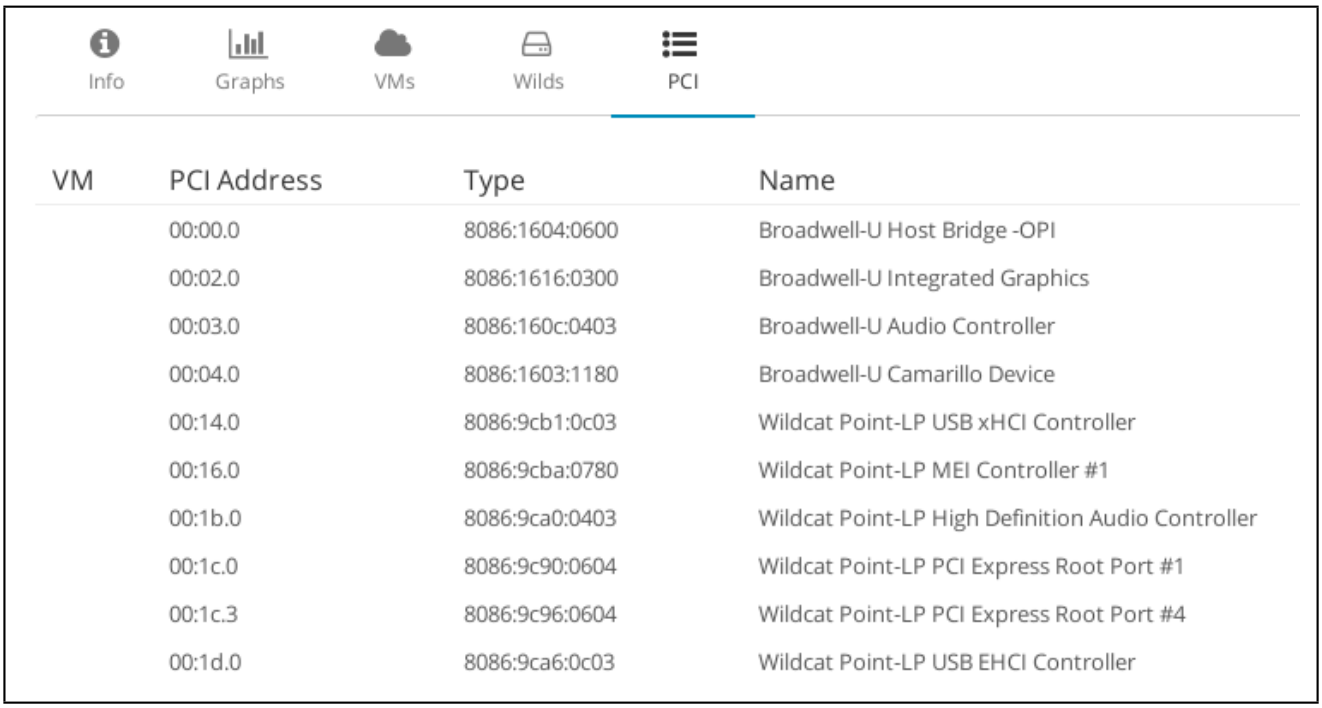

Рис. 78

Для добавления устройства PCI в шаблон ВМ в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

1) в меню слева выбрать пункт меню «Шаблоны — ВМ» и на открывшейся странице «Шаблоны ВМ» выбрать необходимый шаблон;
2) на открывшейся странице «Шаблон ВМ» нажать кнопку **[Обновить]**;
3) на открывшейся странице «Изменить шаблон ВМ» открыть вкладку «Ввод/Вывод» (рис. 79).

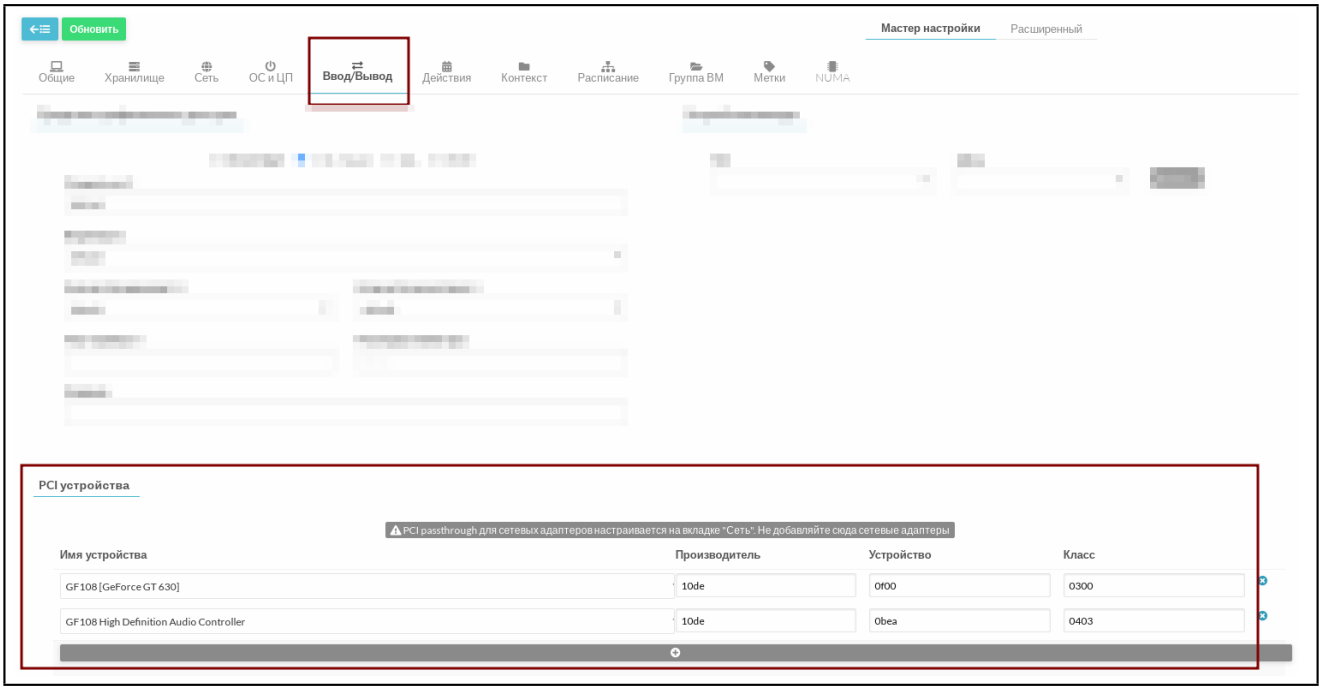

Рис. 79

3.11. Настройка дискреционного и мандатного управление доступом к ВМ

ВНИМАНИЕ! Настройка дискреционного и мандатного управление доступом к ВМ возможно только в дискреционном режиме работы ПК СВ.

Для настройки мандатного контроля целостности, дискреционного и мандатного управления доступом виртуальной машины необходимо в веб-интерфейсе ПК СВ для этой ВМ открыть вкладку «Безопасность» и выполнить следующие действия (см. рис. 80.):

- в секции «Модель PARSEC» в выпадающем списке «Тип» выбрать тип модели мандатного управления доступом (динамический или статический). При выборе статического типа модели в поле «Метка» необходимо задать мандатную метку;
- в секции «Дискреционный контроль доступа» следует:
  - в выпадающем списке «Тип» выбрать тип субъекта (пользователь или группа);
  - в выпадающем списке «Субъект» выбрать соответствующего субъекта (пользователя или группу);
  - в выпадающем списке «Права доступа» выбрать вид операций, разрешенных в отношении ВМ:
    - «Управление» — создание, удаление или изменение конфигурации ВМ, включая управление правами доступа к ней;
    - «Использование» — просмотр свойств, запуск и работа в графической или текстовой консоли ВМ.

ВНИМАНИЕ! Для обеспечения полного доступа к ВМ пользователю должно быть одновременно разрешено выполнение операций вида и «Использование», и

«Управление».

Для добавления разрешенного вида операций необходимо воспользоваться кнопкой **[Добавить]**;

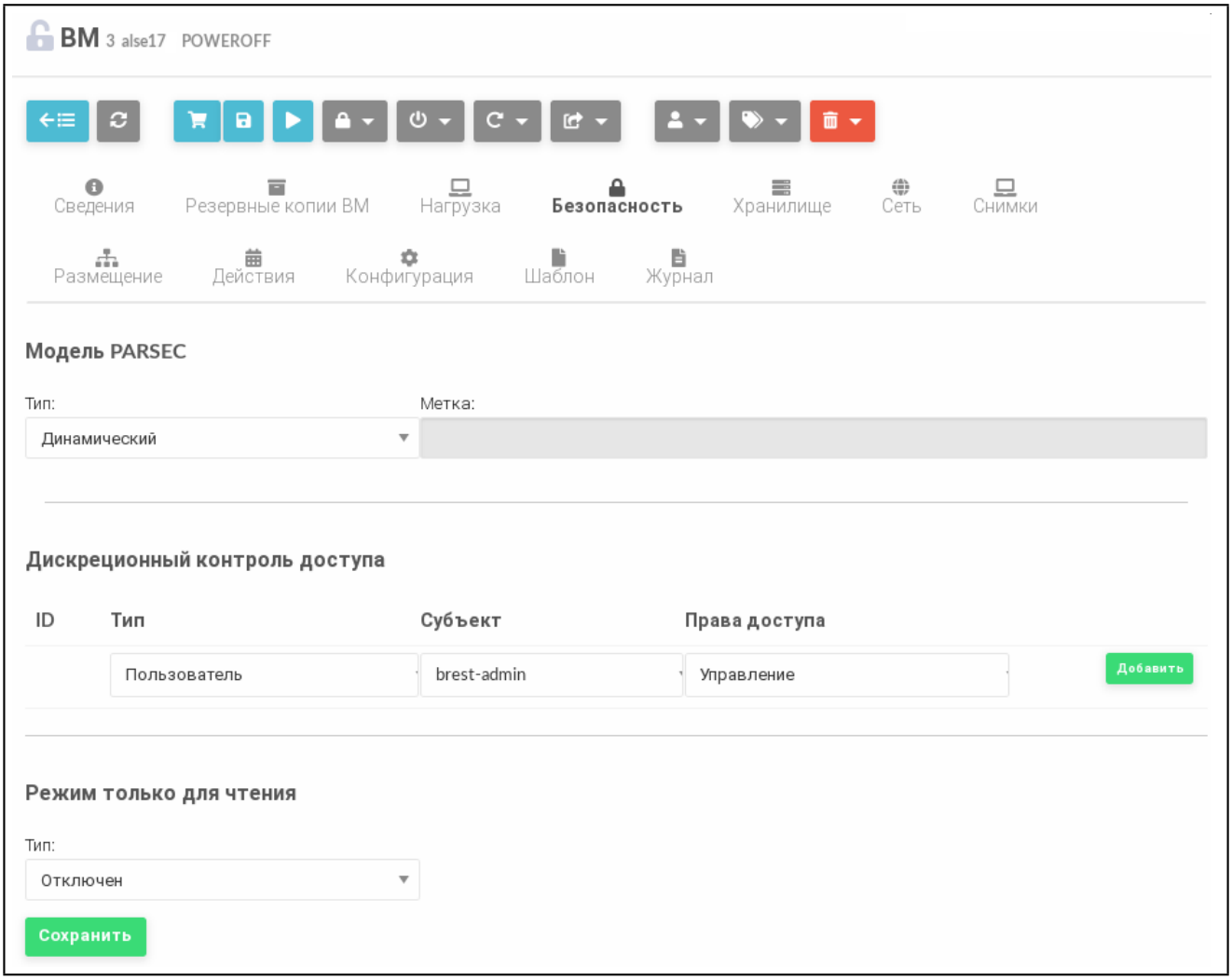

Рис. 80

После внесения изменений необходимо нажать кнопку **[Сохранить]**.

ВНИМАНИЕ! Настройка доступа возможно только при выключенной ВМ.

3.12. Пользовательские сценарии использования МРД и МКЦ

3.12.1. Мандатное разграничение ВМ для групп в одной компании

В рамках работы организации возможна ситуация, связанная с разделением существующих ресурсов, как в рамках отделов так и по уровню конфиденциальности. В частности, если есть необходимость вести разработку разной продукции, части или компоненты которой могут пересекаться между собой.

Использование механизма МРД позволяет усилить безопасность конфиденциальной информации, создавая дополнительный шаг, который в свою очередь уменьшает влияние человеческого фактора в вопросах безопасности, за счет использования меток категории.

Для примера матрица доступа к ресурсам ПК СВ (образы и ВМ). Пользователь с уровнем конфиденциальности 2 и категорией доступа 1, сможет видеть ресурсы с такими уровнями допуска, но не получит доступ к ресурсам, созданными другими пользователями с тем же уровнем конфиденциальности, но в другой категории. Тогда как Администратор группы или пользователь с назначенными категориями 1-3 сможет увидеть все ресурсы в рамках данных категорий и уровня конфиденциальности 2.

Таким образом, на уровне сервера виртуализации, можно разграничить ресурсы ПК СВ используя допуски системы, разделив отделы, а также разнести информацию по уровням конфиденциальности, ограничив доступ к информации в зависимости от выполняемых задач. Такое деление, помимо прочего, позволяет минимизировать риск несанкционированного доступа в случае человеческой ошибки при назначении группы Пользователя.

В нижеприведенном примере каждому пользователю определенной FreeIPA-группы назначается одна категория, внутри одной FreeIPA-группы можно разграничить доступ используя иерархический уровень конфиденциальности.

Пользователи принадлежат разным FreeIPA-группам, а также принадлежат разным уровням и категориям конфиденциальности:

- Пользователь 1 состоит в Группе 1 и имеет Уровень 0 и Категорию 0;
- Пользователь 2 состоит в Группе 2 и имеет Уровень 0 и Категорию 1;
- Пользователь 3 состоит в Группе 1 и имеет Уровень 1 и Категорию 0;
- Пользователь 4 состоит в Группе 2 и имеет Уровень 1 и Категорию 1;
- Пользователь 5 состоит в Группе 2 и имеет Уровень 1 и Категории 0 и 1.

Для таких пользователей общее мандатное представление доступа будет выглядеть следующим образом (см. рис. 81).

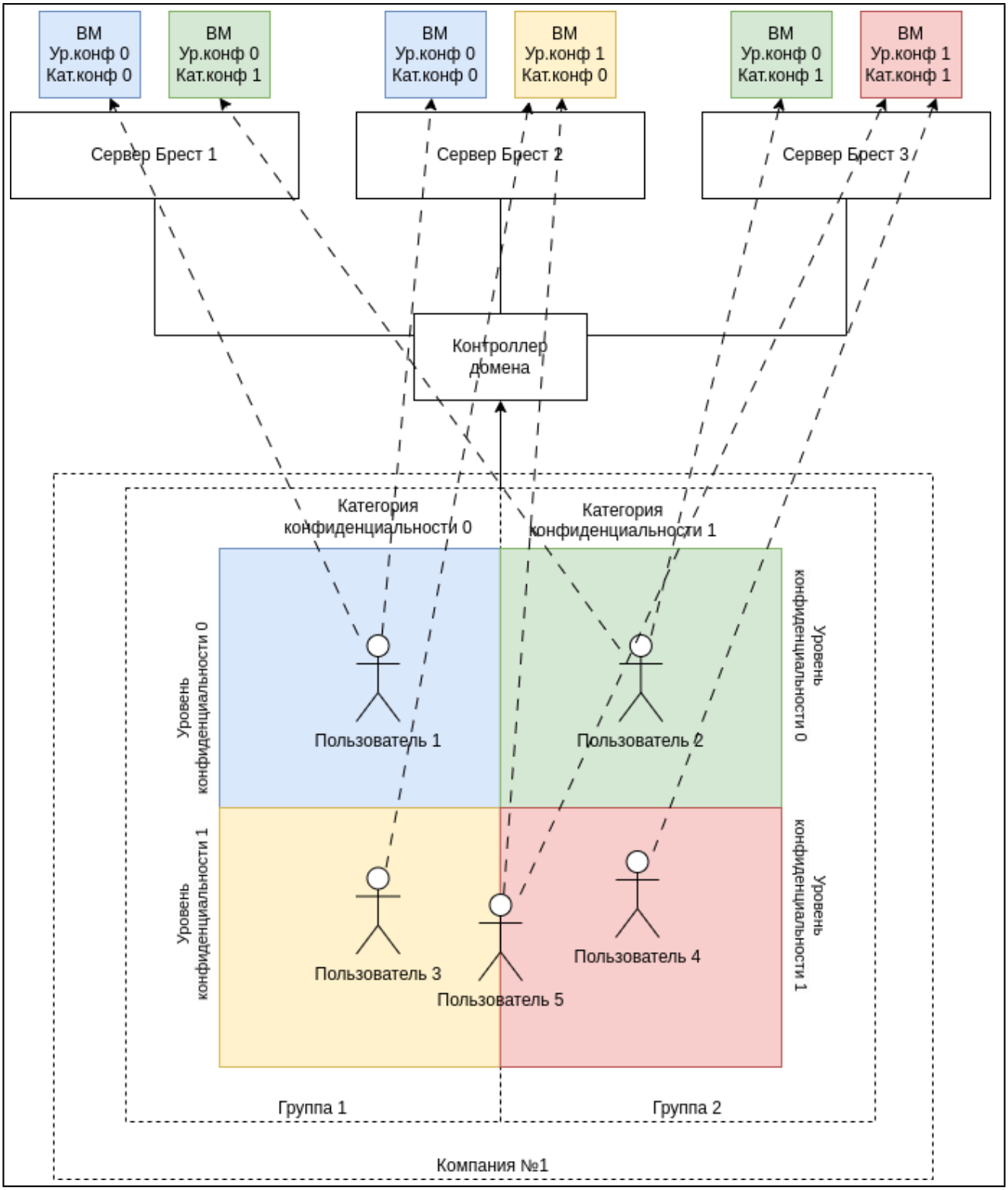

Рис. 81

Где для каждого отдельного пользователя:

- Доступ к ВМ Пользователя 1 (см. рис. 82):

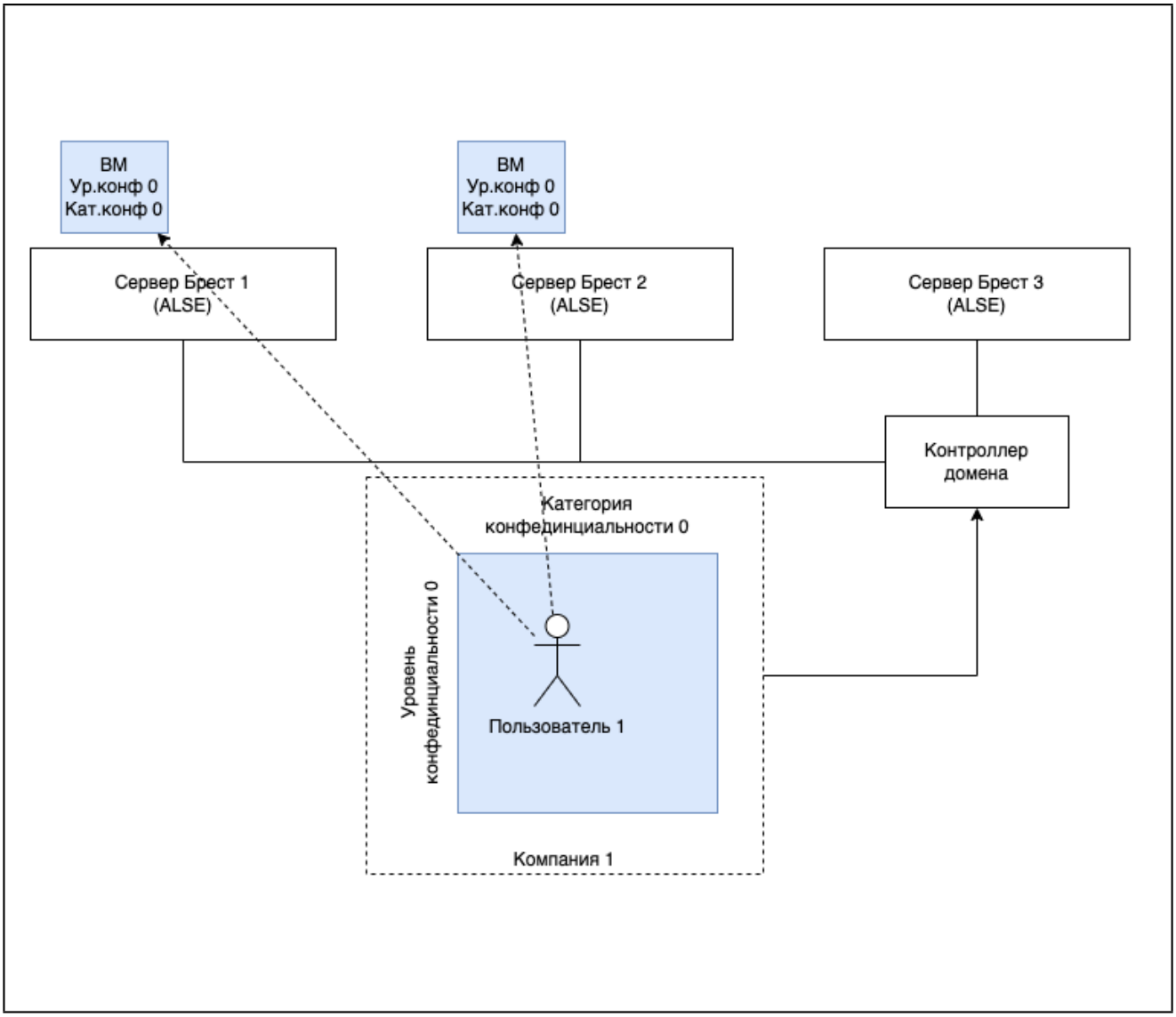

Рис. 82

- Доступ к ВМ Пользователя 2 (см. рис. 83):

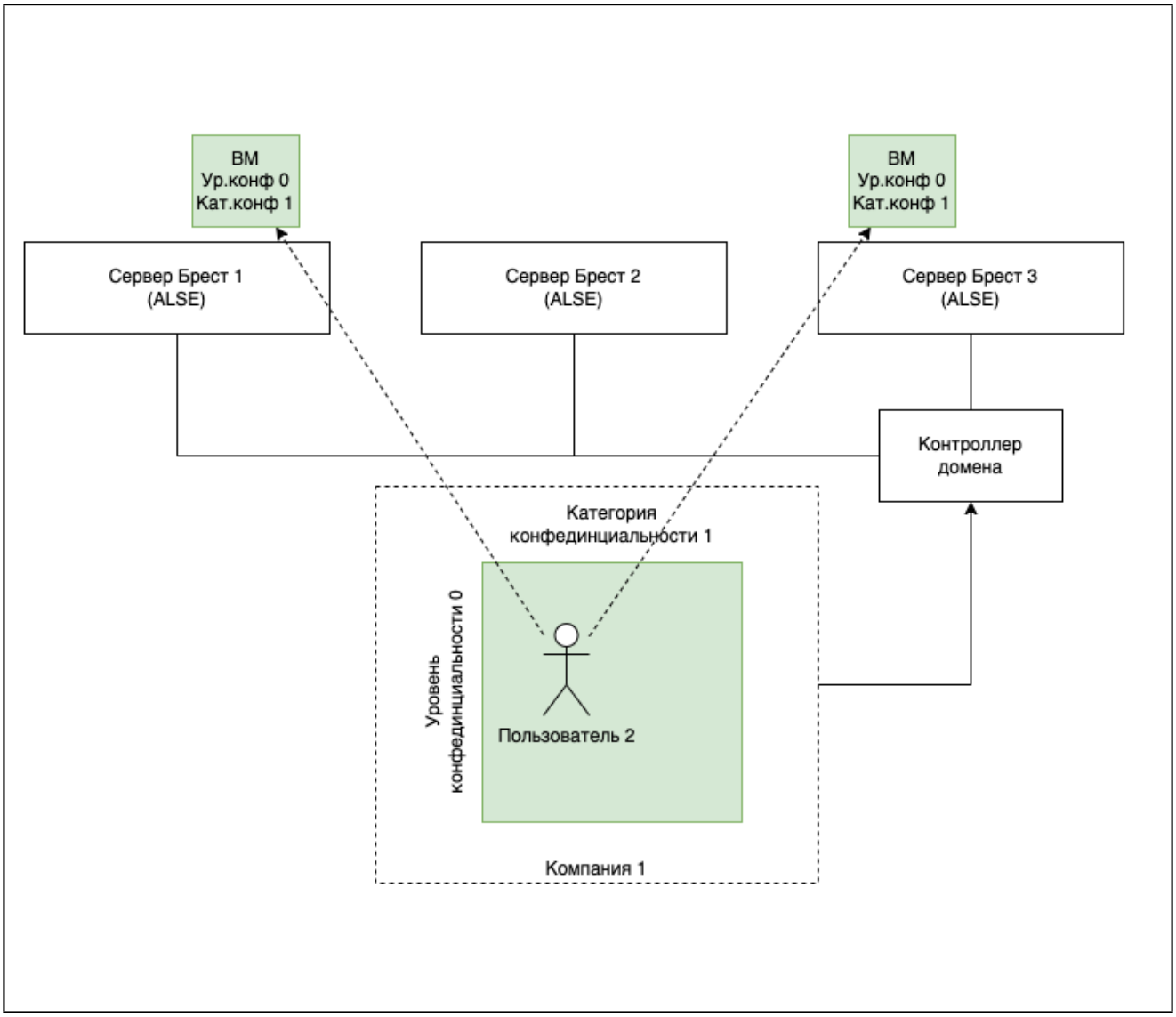

Рис. 83

- Доступ к ВМ Пользователя 3 (см. рис. 84):

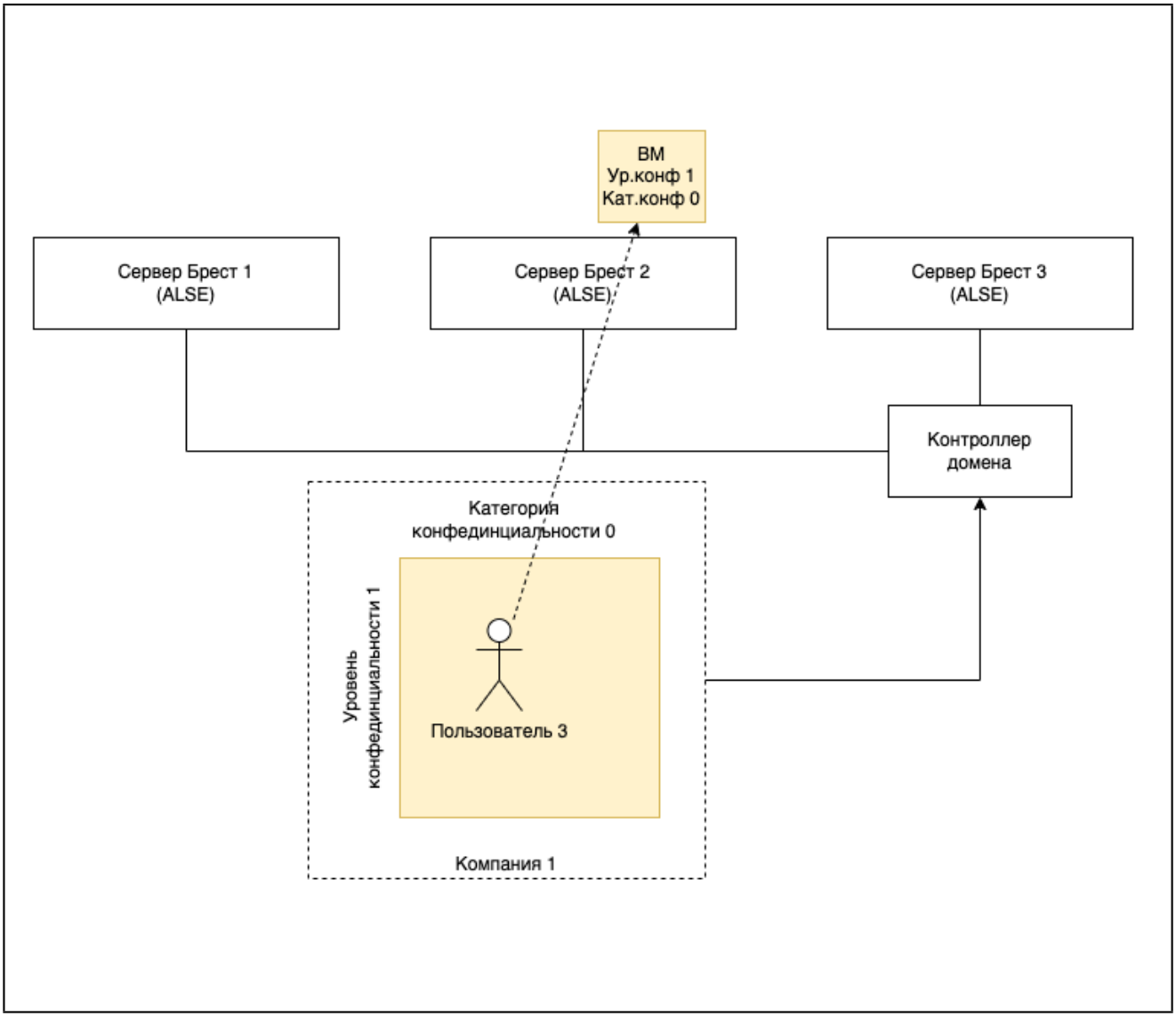

Рис. 84

- Доступ к ВМ Пользователя 4 (см. рис. 85):

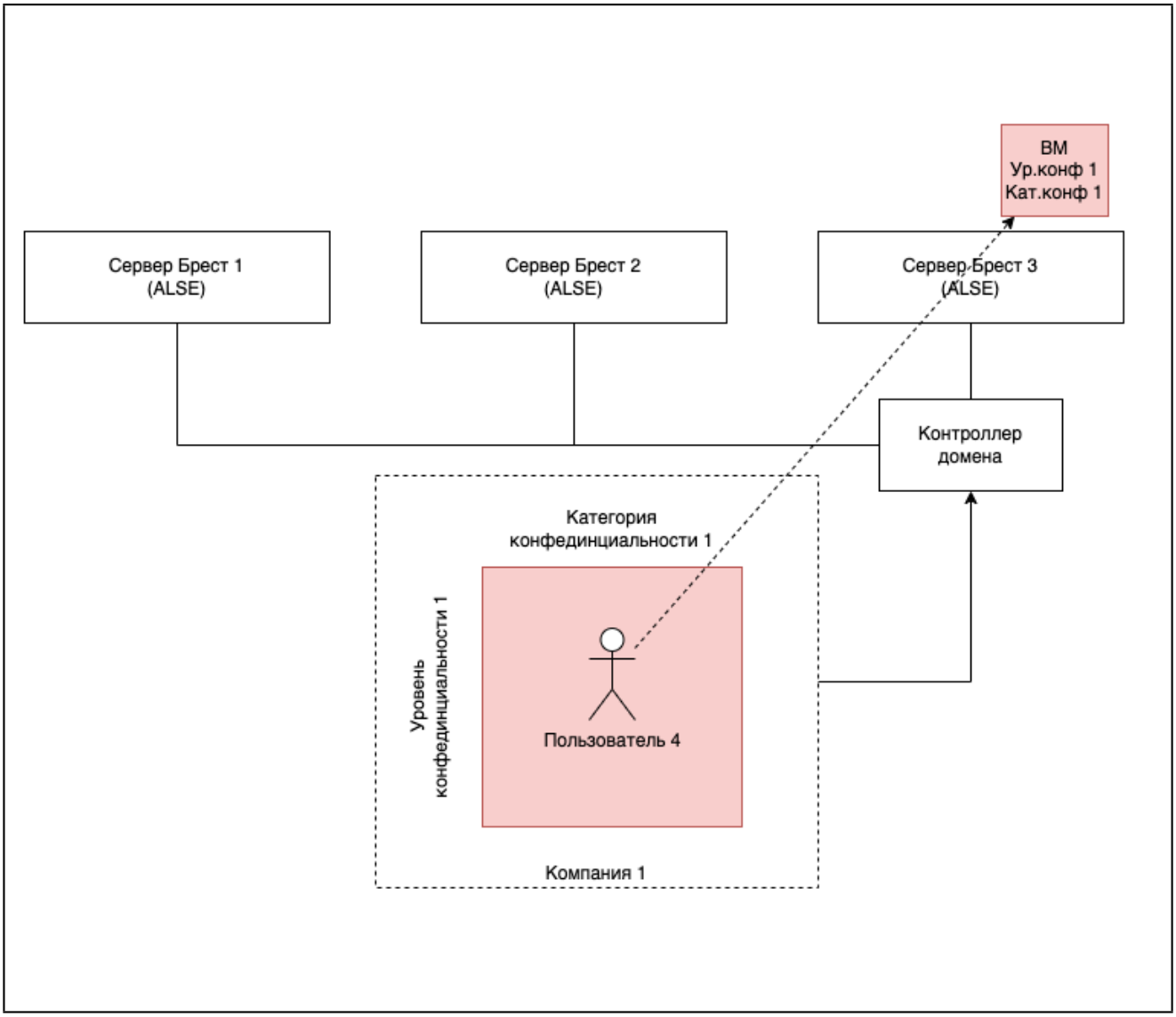

Рис. 85

- Доступ к ВМ Пользователя 5 (см. рис. 86):

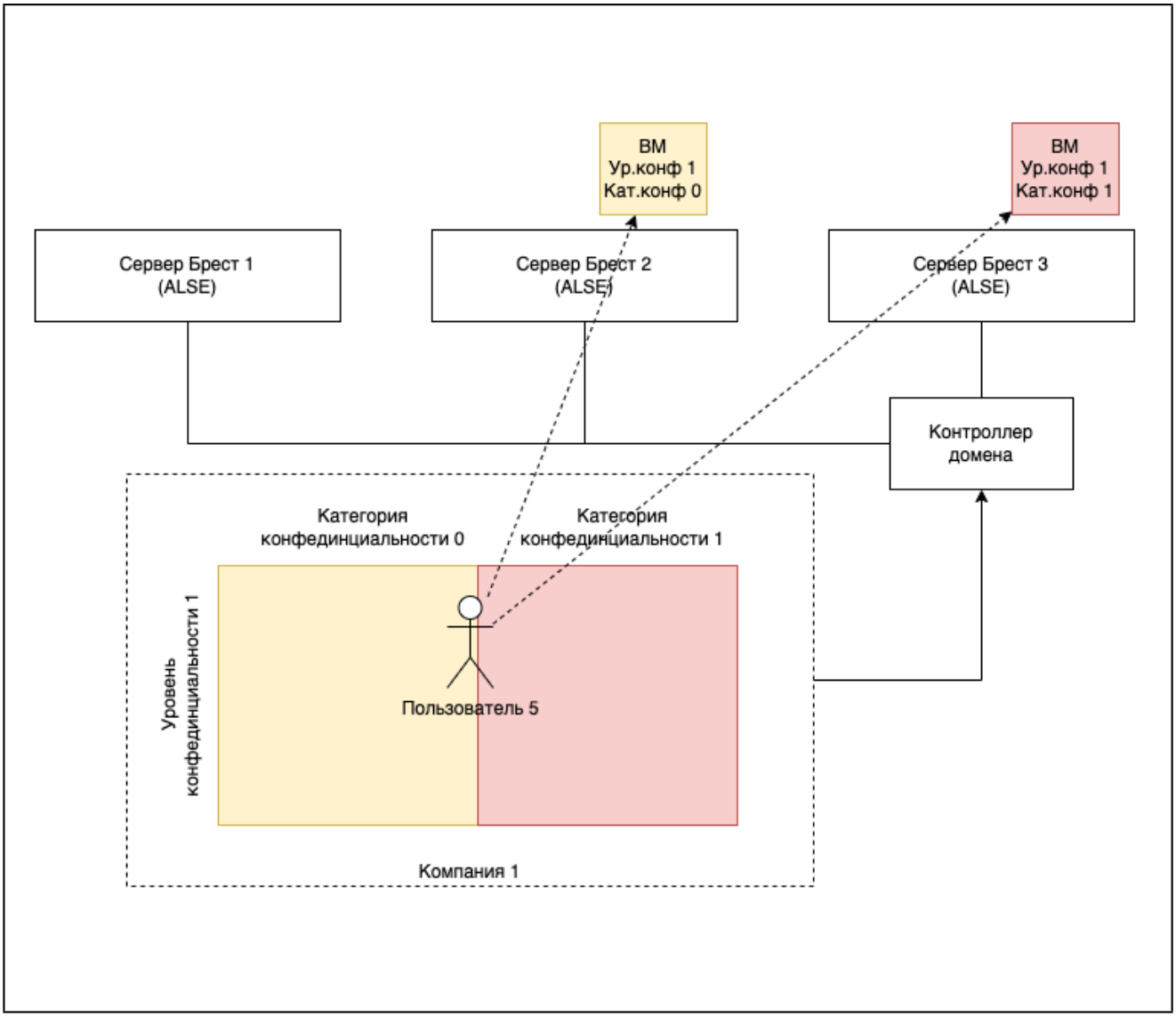

Рис. 86

Для настройки разграничение ВМ для групп в одной компании необходимо:

1) Создать группы пользователей, для этого в веб-интерфейсе ПК СВ в меню слева выбрать пункт «Система — Группы» и нажать кнопку [+]:

- в открывшемся окне во вкладке «Общее» указать название группы (см. рис. 87):

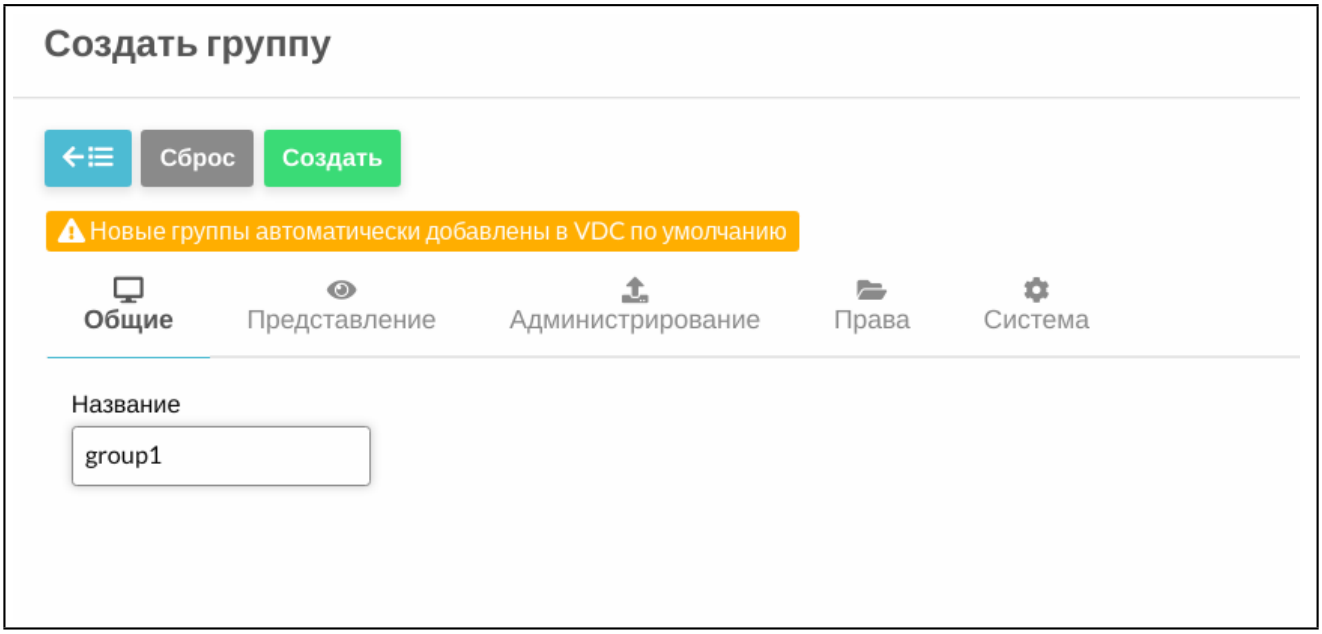

Рис. 87

ВНИМАНИЕ! В названии группы не допускается использовать буквы в верхнем регистре.

- указать необходимые настройки во вкладке «Представление» (см. рис. 108):

Рис. 88

- во вкладке «Права» настроить права доступа (см. рис. 109):

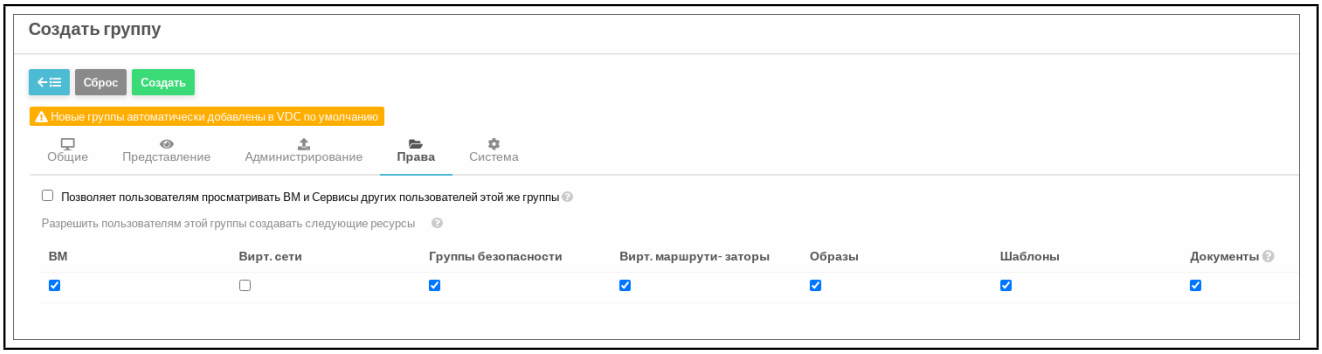

Рис. 89

- нажать кнопку [Создать];

2) Создать пользователей, для этого в веб-интерфейсе ПК СВ в меню слева выбрать пункт «Система — Пользователи» и нажать кнопку [+]:

- в открывшемся окне «Создать пользователя» необходимо указать имя пользователя, пароль, подтверждение пароля и снять флаг «Сменить пароль при первом входе в систему» (см. рис. 110):

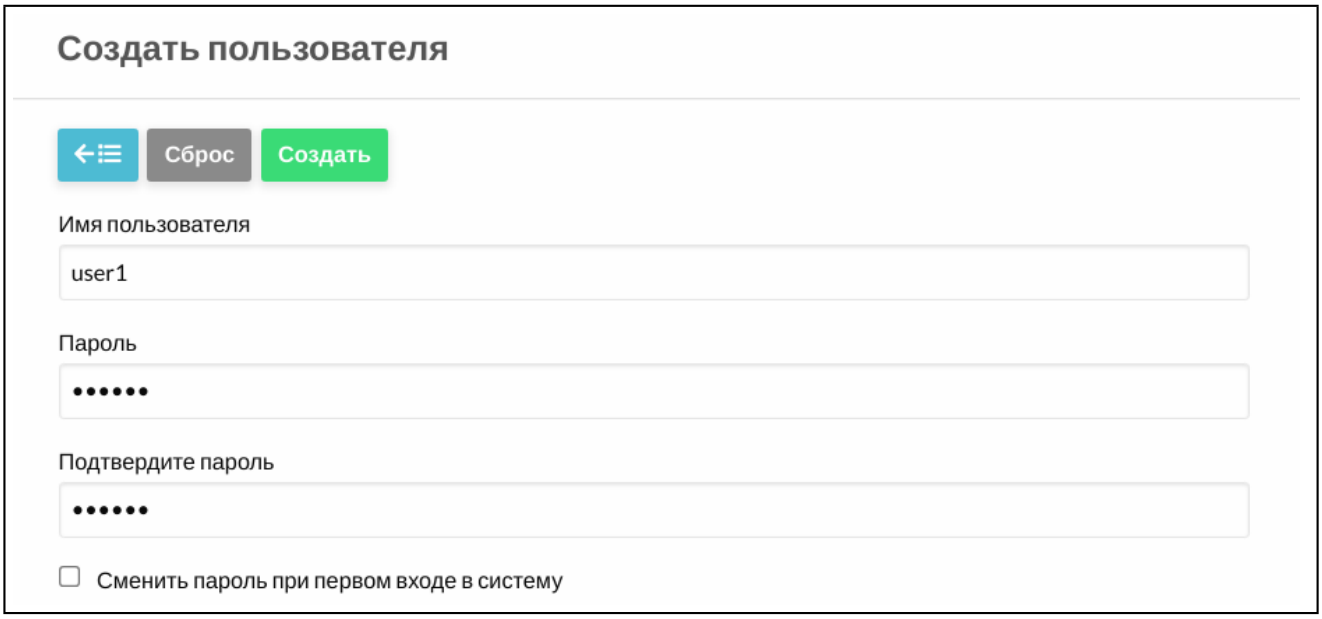

Рис. 90

Примечание. Если оставить флаг Сменить пароль при первом входе в систему, пользователь сможет зайти в систему только после смены пароля через веб-интерфейс Контролера домена.

- в выпадающем списке «Основная группа» выбрать группу, созданную на предыдущем шаге (см. рис. 91):

Рис. 91

- в «Дополнительные группы» указать `brestusers` (см. рис. 92):

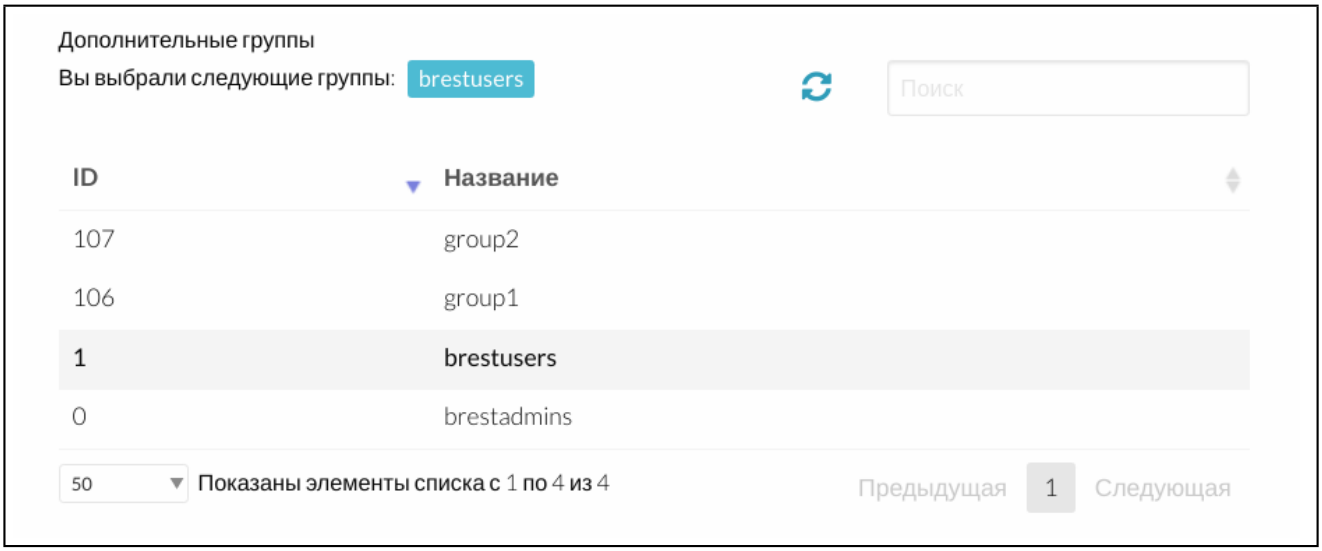

Рис. 92

- нажать кнопку [Создать];

3) Создать Администратора групп, для этого действиями, описанными на предыдущем шаге, создать учетную запись Администратора группы:

- В веб-интерфейсе ПК СВ в меню слева выбрать пункт «Система — Группы», в списке групп выбрать созданную ранее группу;
- во вкладке Пользователи нажать кнопку [Редактировать администраторов] (см. рис. 113):

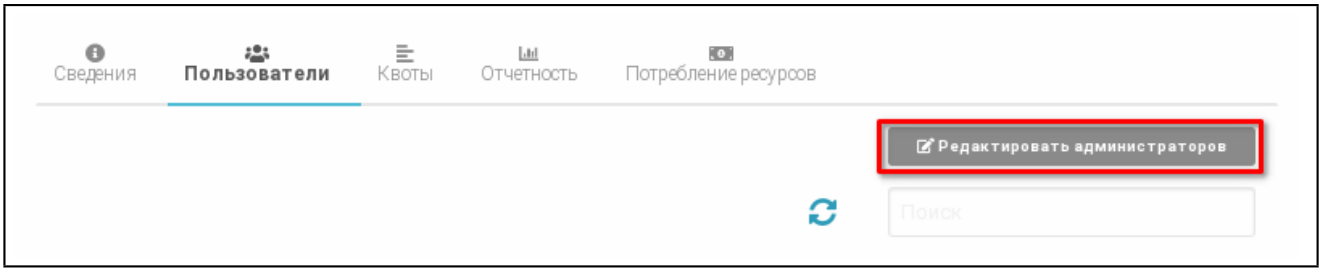

Рис. 93

- в открывшемся списке выбрать необходимого пользователя и нажать кнопку [Применить] (см. рис. 94):

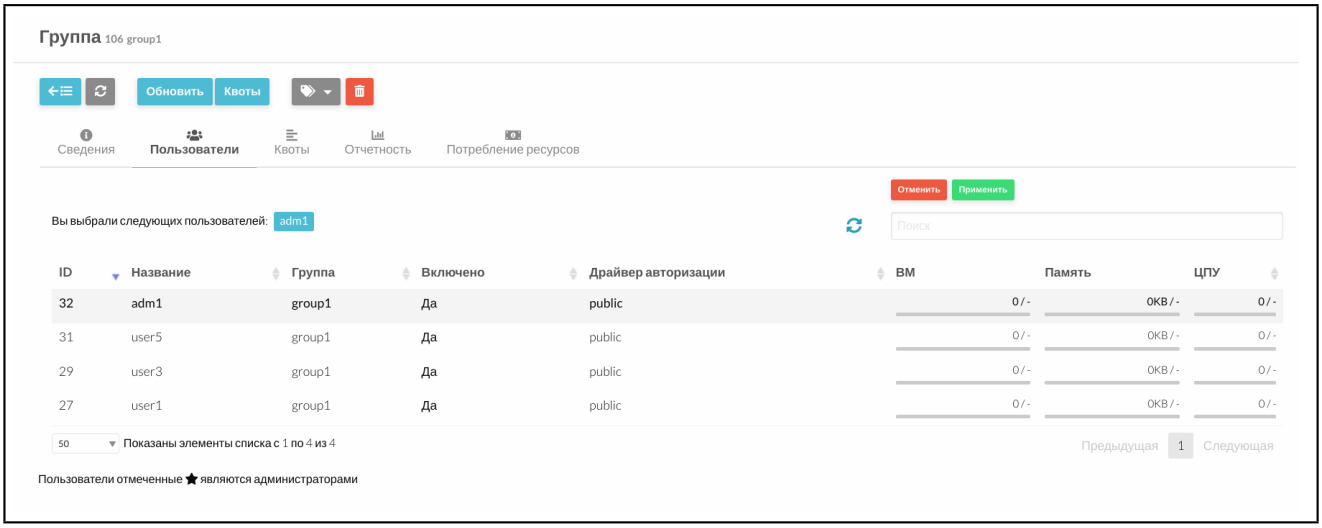

Рис. 94

4) Настроить группы FreeIPA, для этого подключиться к веб-интерфейсу Контролера домена пользователем с административными полномочиями:

- во вкладке «Пользователи» в меню слева выбрать пункт «Активные пользователи» (см. рис. 115):

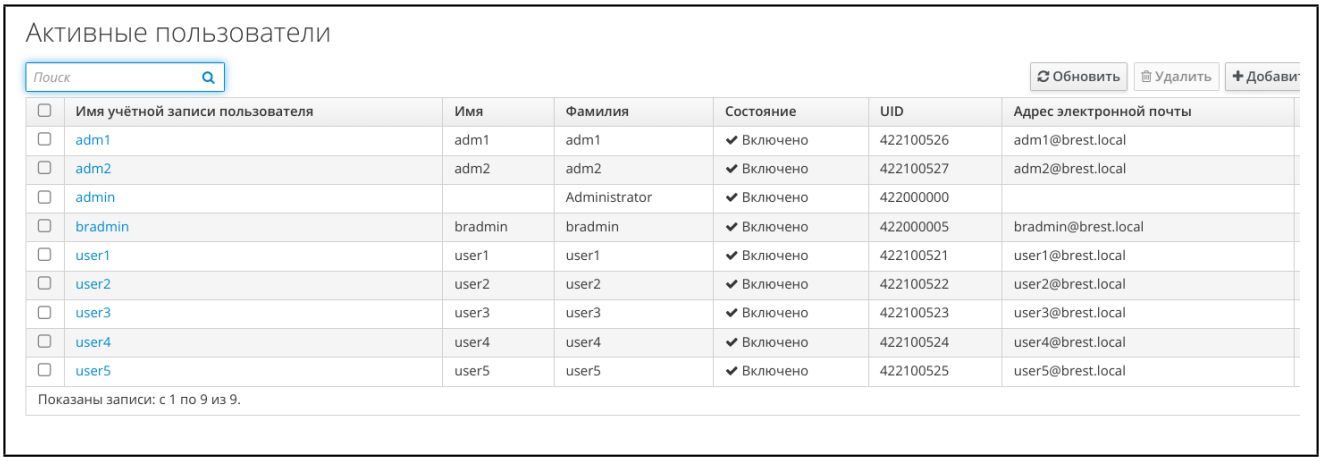

Рис. 95

- нажать на имя нужного пользователя для редактирования;
- в открывшемся окне «Параметры» выбрать требуемые уровни конфиденциальности в выпадающих списках «Минимальный уровень конфиденциальности» и «Максимальный уровень конфиденциальности» (см. рис. 116):

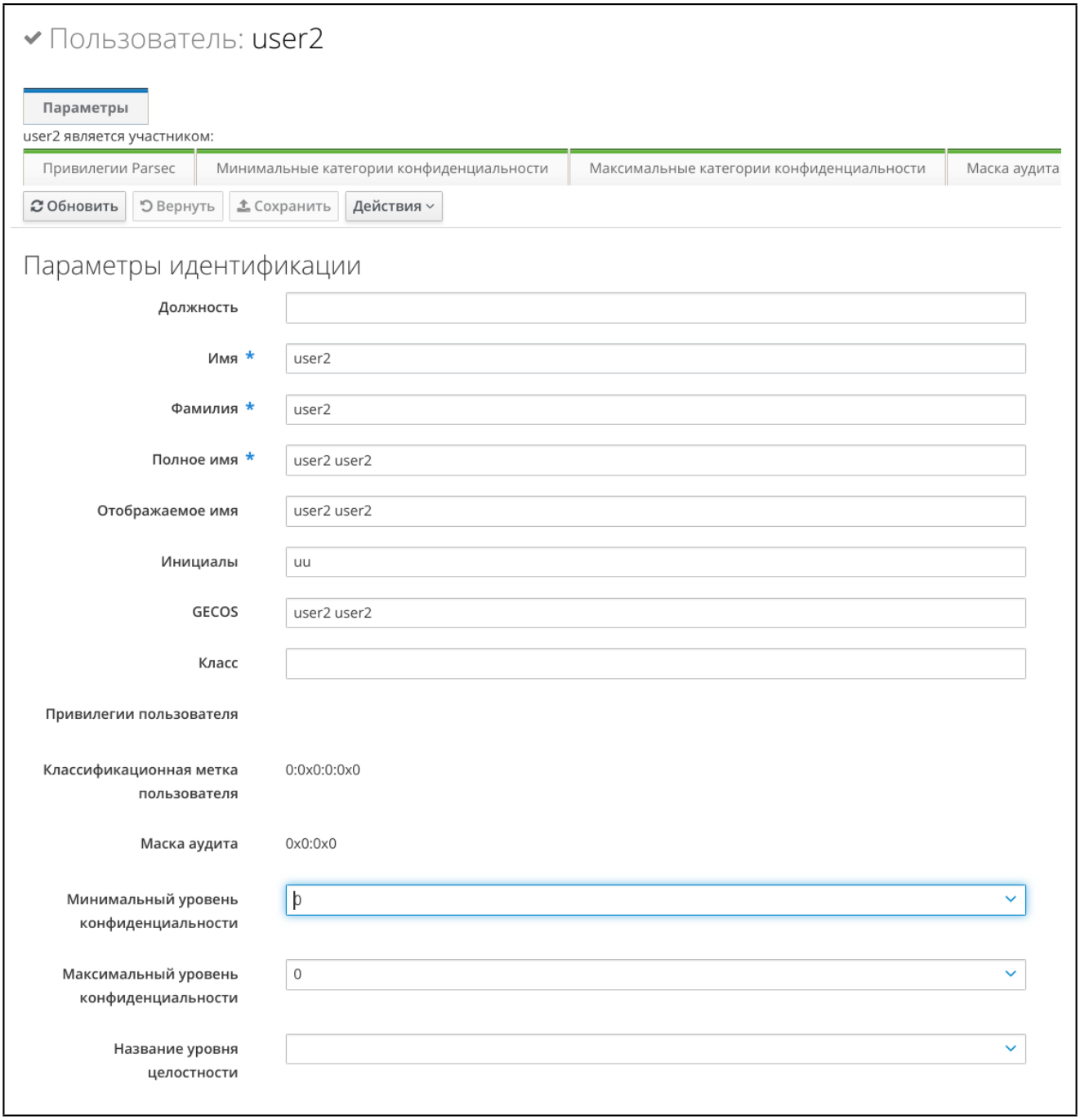

Рис. 96

- нажать кнопку [Сохранить];
- перейти во вкладку «Минимальная категория конфиденциальности» и нажать кнопку [Добавить] (см. рис. 117):

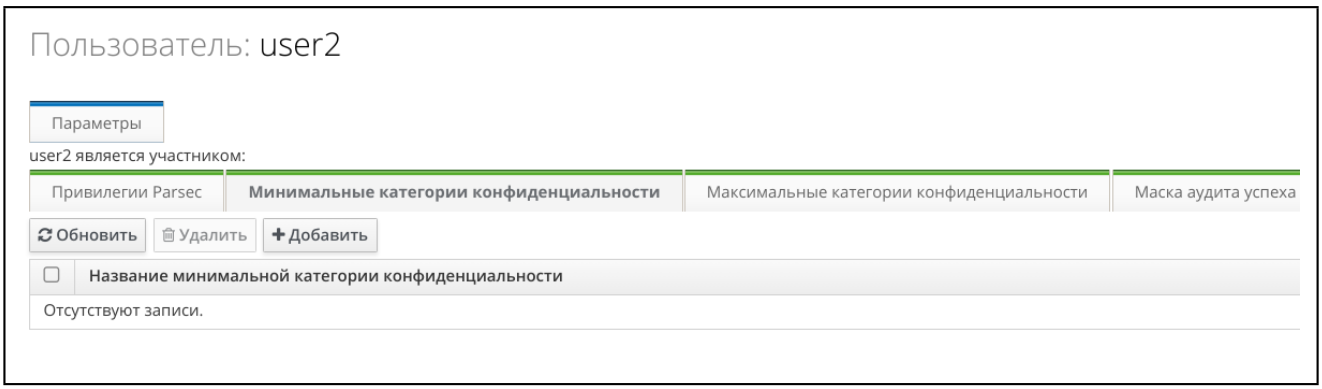

Рис. 97

- в открывшемся окне в списке «Доступно» отметить необходимые категории и перенести их в список «Ожидается» нажав кнопку [>]. Нажать кнопку [Добавить] (см. рис. 118):

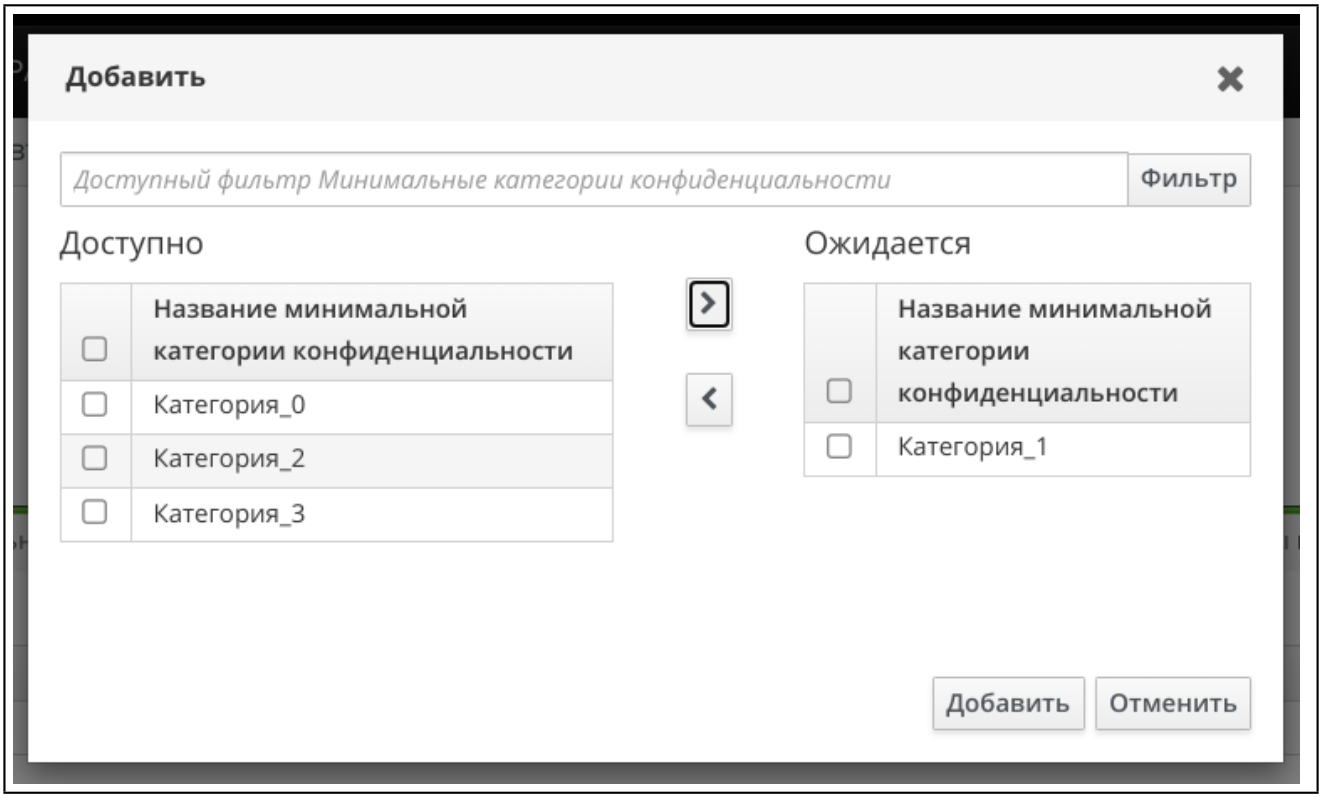

Рис. 98

Примечание. При первом назначении категорий их применение происходит мгновенно. При редактировании уже назначенных категорий изменения применяются с задержкой в полтора часа, из-за обновления информации в кэше службы SSSD фронтальных серверов.

- перейти во вкладку Максимальные категория конфиденциальности и настроить аналогичным образом;

5) Подключиться к веб-интерфейсу ПК СВ, для этого при первом подключении к веб-интерфейсу ПК СВ необходимо настроить браузер, добавив обработку обмена

данными аутентификации из ОС:

Примечание. Для полноценной работы с механизмом МРД, необходимо выполнить вход в систему используя терминал (ПК), заведенный в домен, к которому принадлежит ПК СВ, а также ОС терминала должна поддерживать работу с механизмом МРД. Если пользователю назначено несколько уровней конфиденциальности, то при входе можно будет выбрать необходимый уровень. Сменить уровень конфиденциальности можно только выполнив вход в систему заново, категории конфиденциальности используются автоматически.

- запустить браузер Mozilla Firefox,в адресную строку ввести `about:config` и нажать клавишу <Enter>;
- на открывшейся странице с предупреждением нажать на кнопку [Принять риск и продолжить] (см. рис. 119):

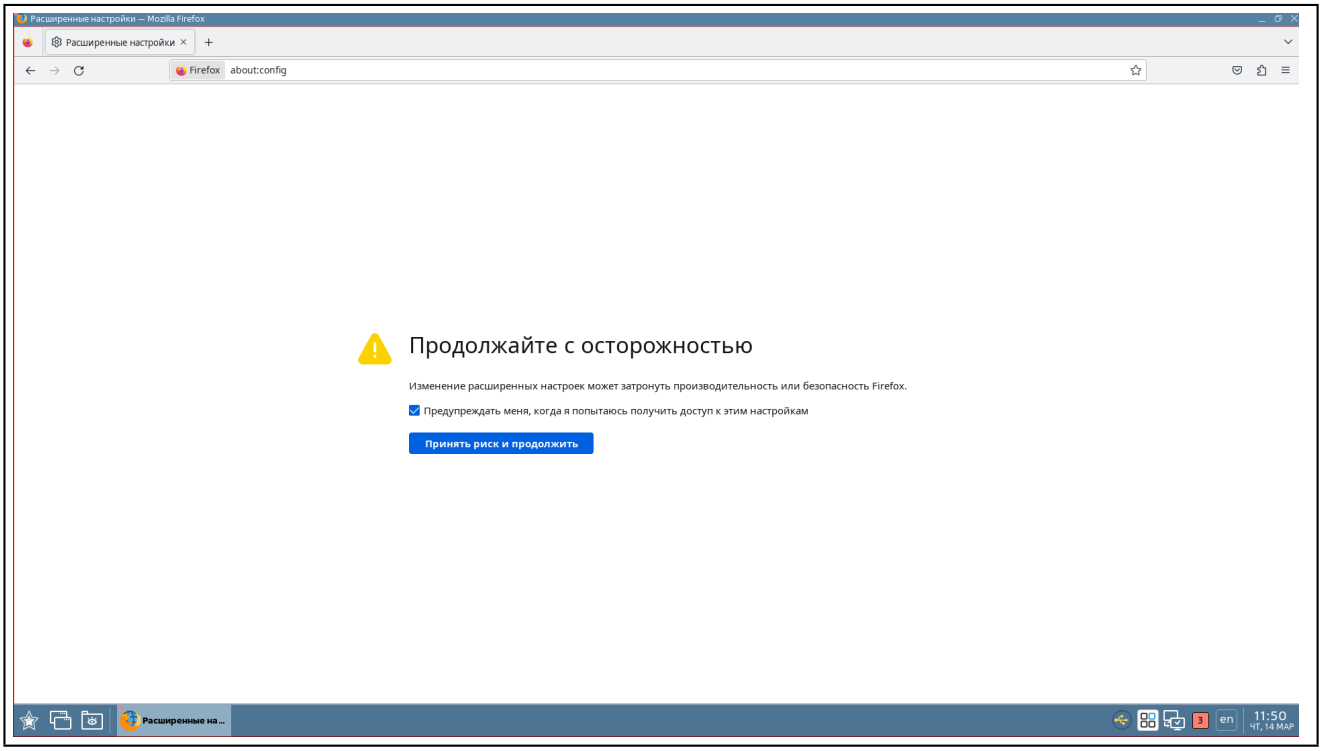

Рис. 99

- на открывшейся странице «Расширенные настройки» в поле поиска ввести слово `uris`;
- для параметров `network.negotiate-auth.trusted-uris` и `network.negotiate-auth.delegation-uris` установить значение `https://` (см. рис. 120):

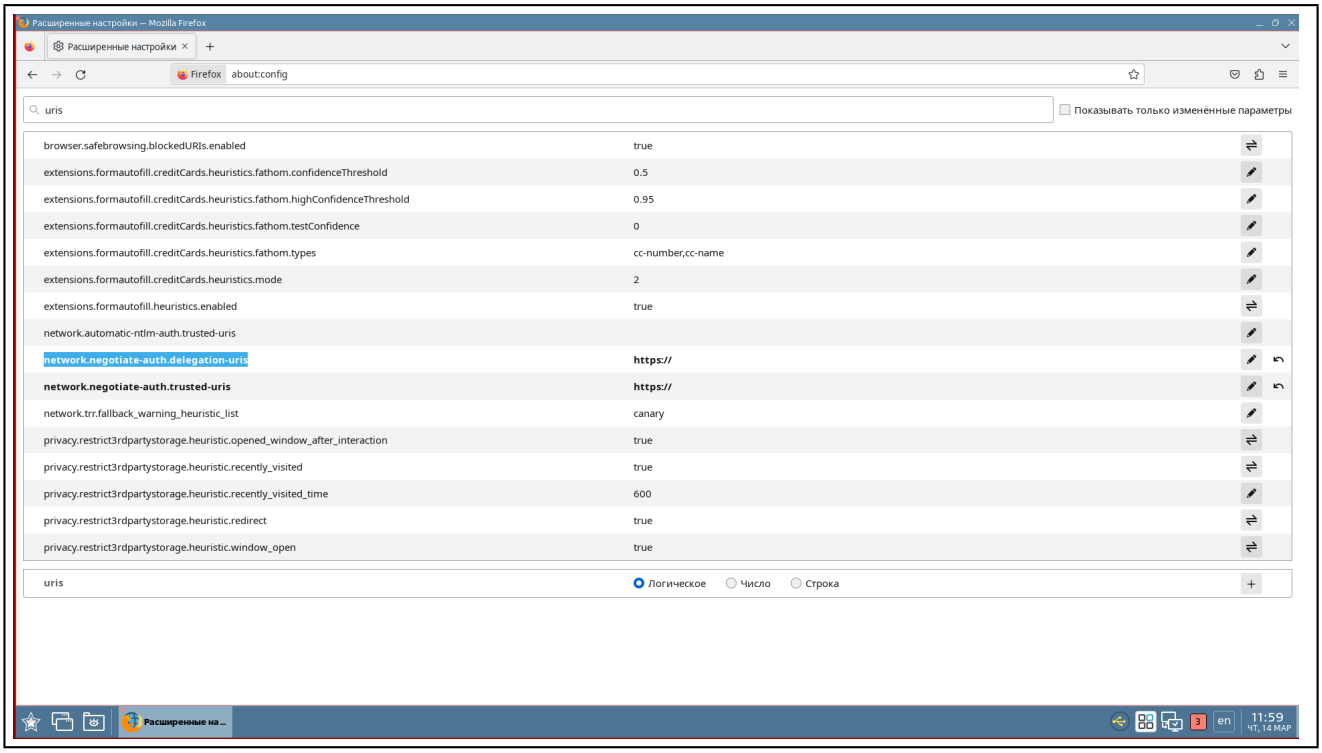

Рис. 100

В дальнейшем работа с ПК СВ не отличается от обычной.

Примечание. Настроить или скорректировать необходимые доступы к ВМ может сам пользователь на странице ВМ во вкладке Безопасность. При использовании Динамической модели Parsec, ВМ получает максимально возможную метку категории и уровень конфиденциальности, согласно доступам, создающего ВМ, пользователя. Для корректировки используемой метки необходимо выбрать Статическую модель и указать желаемую метку.

3.12.2. Мандатное разграничение ВМ между разными компаниями

Еще одним вариантом применения МРД для разграничения доступа к ресурсам является его использование в группе-компаний, имеющей единую систему виртуализации для консолидации и оптимизации использования аппаратного обеспечения. Пользователи разных компаний не будут иметь доступ к ресурсам других организаций холдинга за счет использования механизма допусков ПК СВ, но, при необходимости, можно будет открыть доступ, скорректировав эту настройку для необходимого ресурса. Тогда как уровни конфиденциальности помогут разграничить доступ к ресурсам внутри компании. Также использование механизма МРД позволит минимизировать риск компрометирования важной информации в случае ошибочного добавления пользователя к группе, за счет назначения группе свою метку категории конфиденциальности.

В нижеприведенном примере каждому пользователю определенной компании назначается одна категория, внутри одной FreeIPA-группы можно разграничить доступ используя иерархический уровень конфиденциальности.

При такой схеме организации работы, механизм ACL будет использован для разделения компаний, в то время как механизм меток МРД для разделения внутри компании:

- Пользователь 1 состоит в Компании 1 и имеет Уровень 0 и Категорию 0;
- Пользователь 2 состоит в Компании 2 и имеет Уровень 0 и Категорию 1;
- Пользователь 3 состоит в Компании 1 и имеет Уровень 1 и Категорию 0;
- Пользователь 4 состоит в Компании 2 и имеет Уровень 1 и Категорию 1;
- Пользователь 5 состоит в Компании 2 и имеет Уровни 0 и 1, Категорию 1.

Для таких пользователей общее мандатное представление доступа будет выглядеть следующим образом (см. рис. 101).

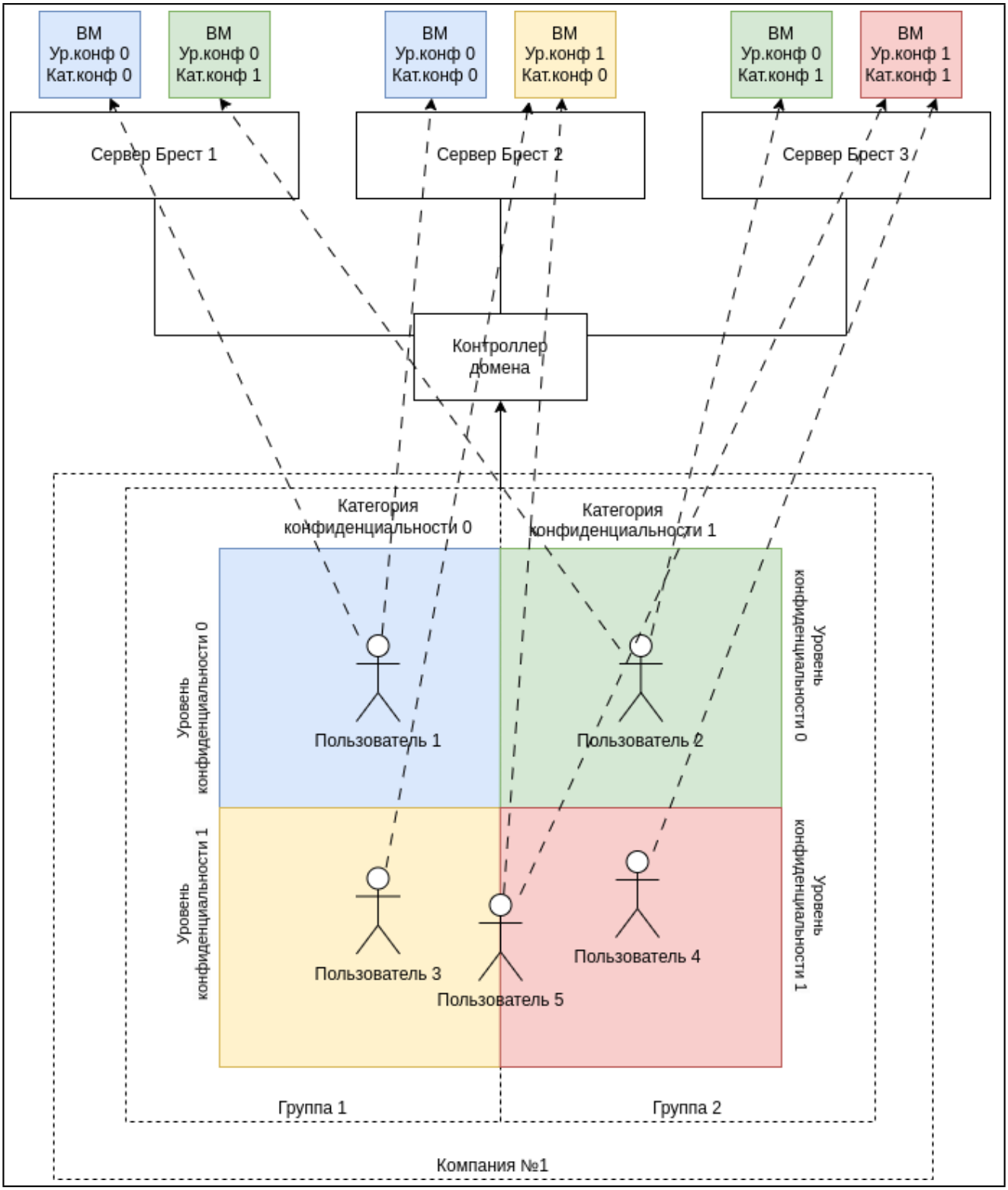

Рис. 101

Где для каждого отдельного пользователя:

- Доступ к ВМ Пользователя 1 (см. рис. 102):

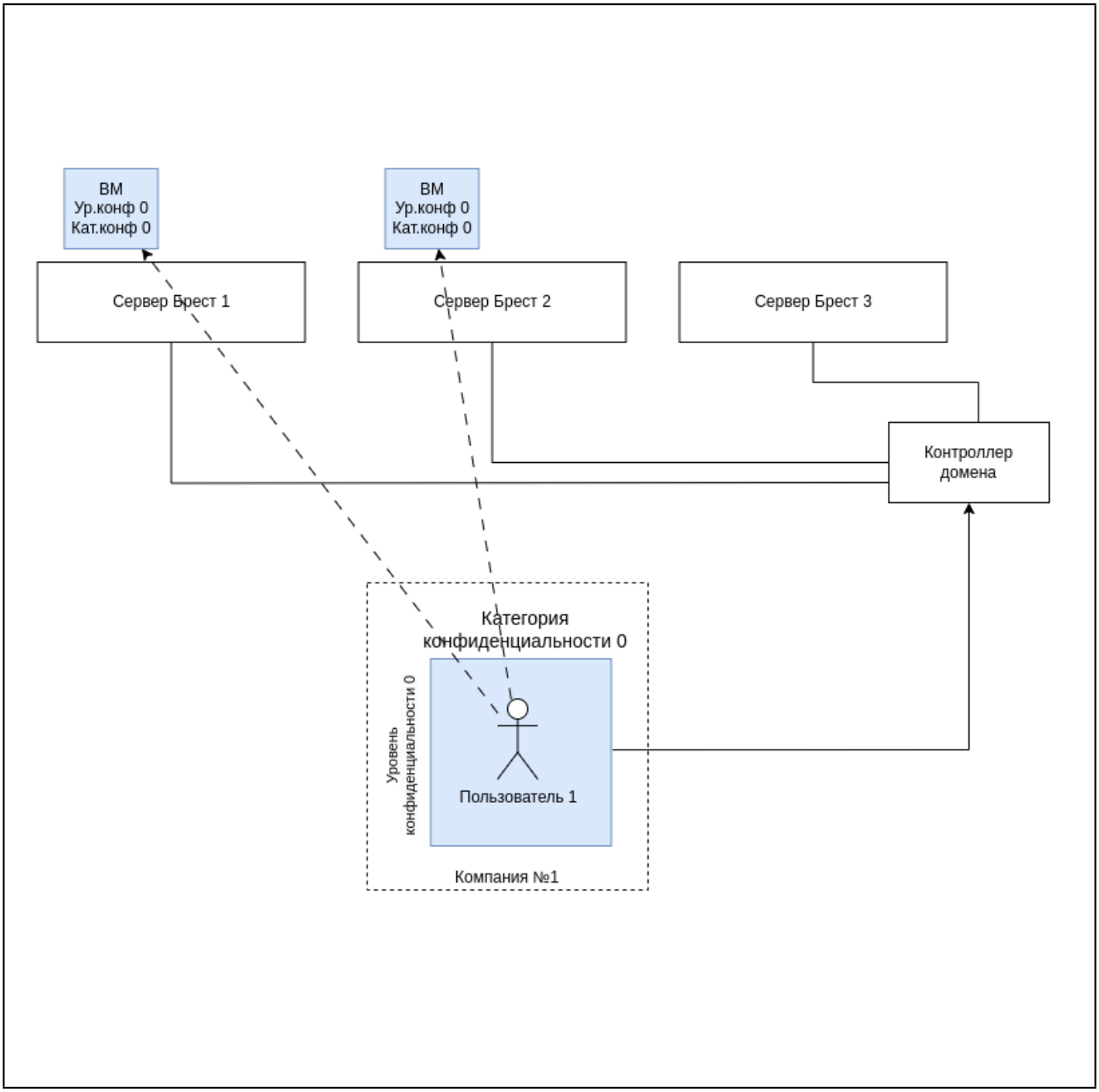

Рис. 102

- Доступ к ВМ Пользователя 2 (см. рис. 103):

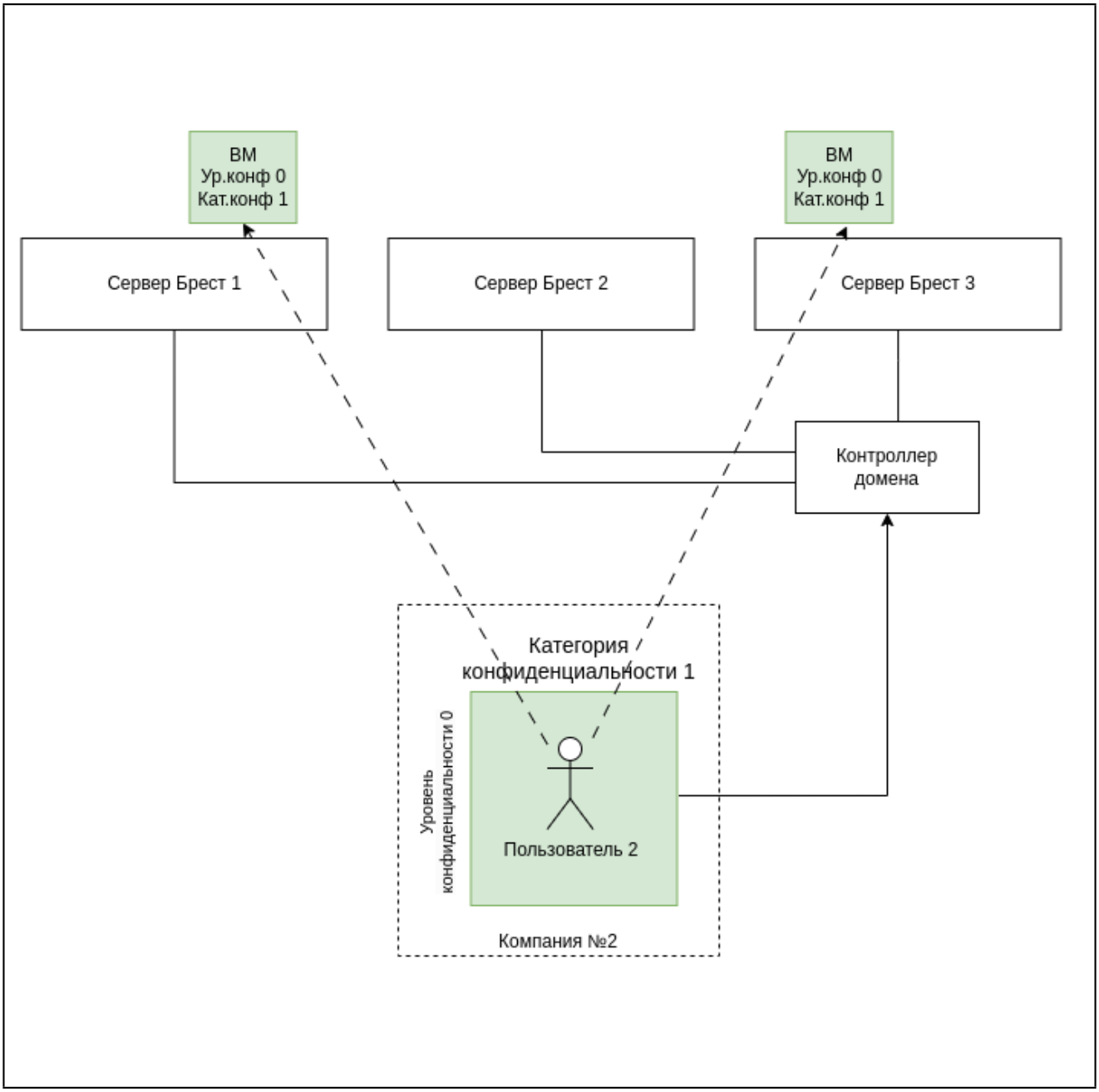

Рис. 103

- Доступ к ВМ Пользователя 3 (см. рис. 104):

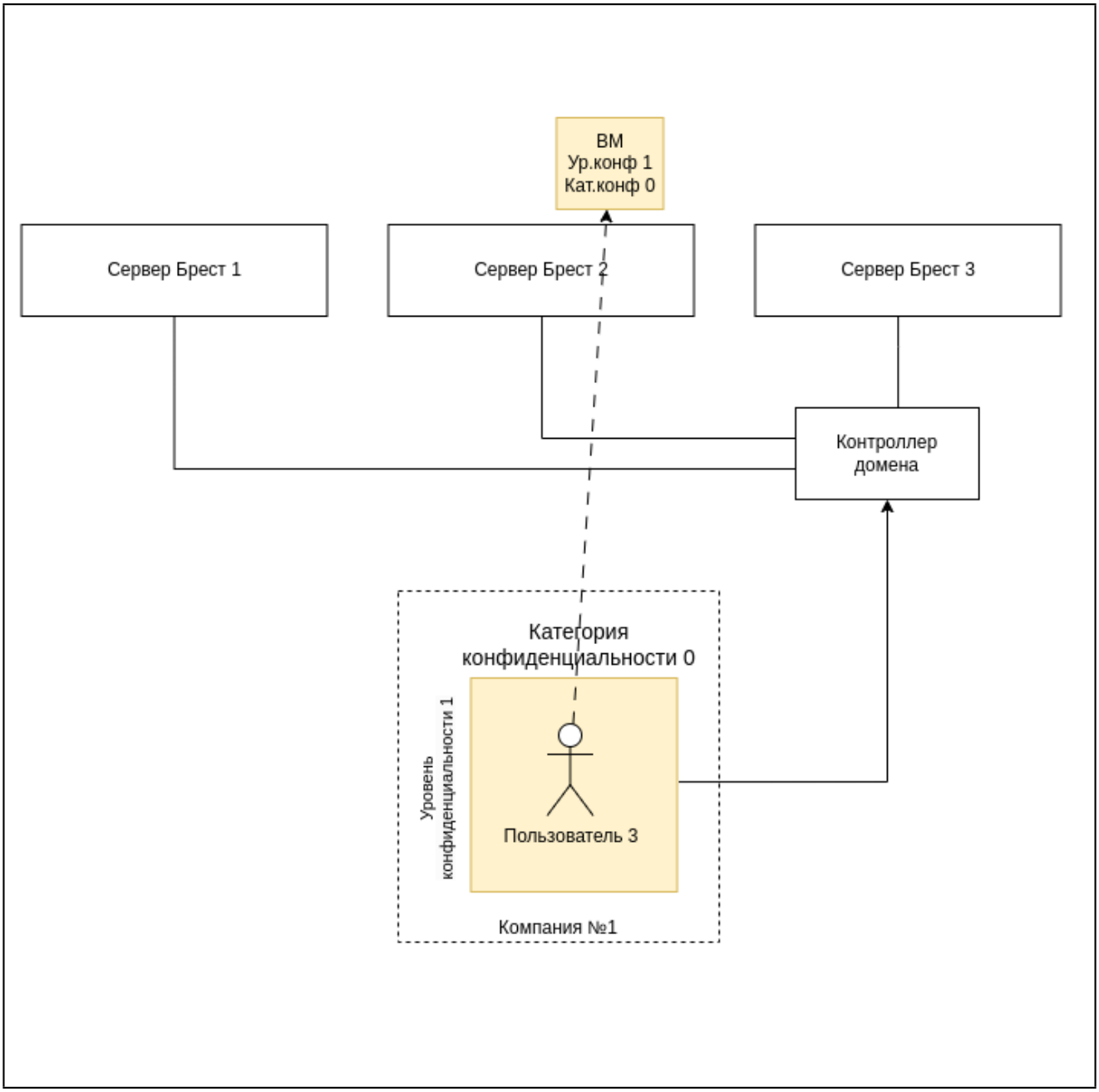

Рис. 104

- Доступ к ВМ Пользователя 4 (см. рис. 105):

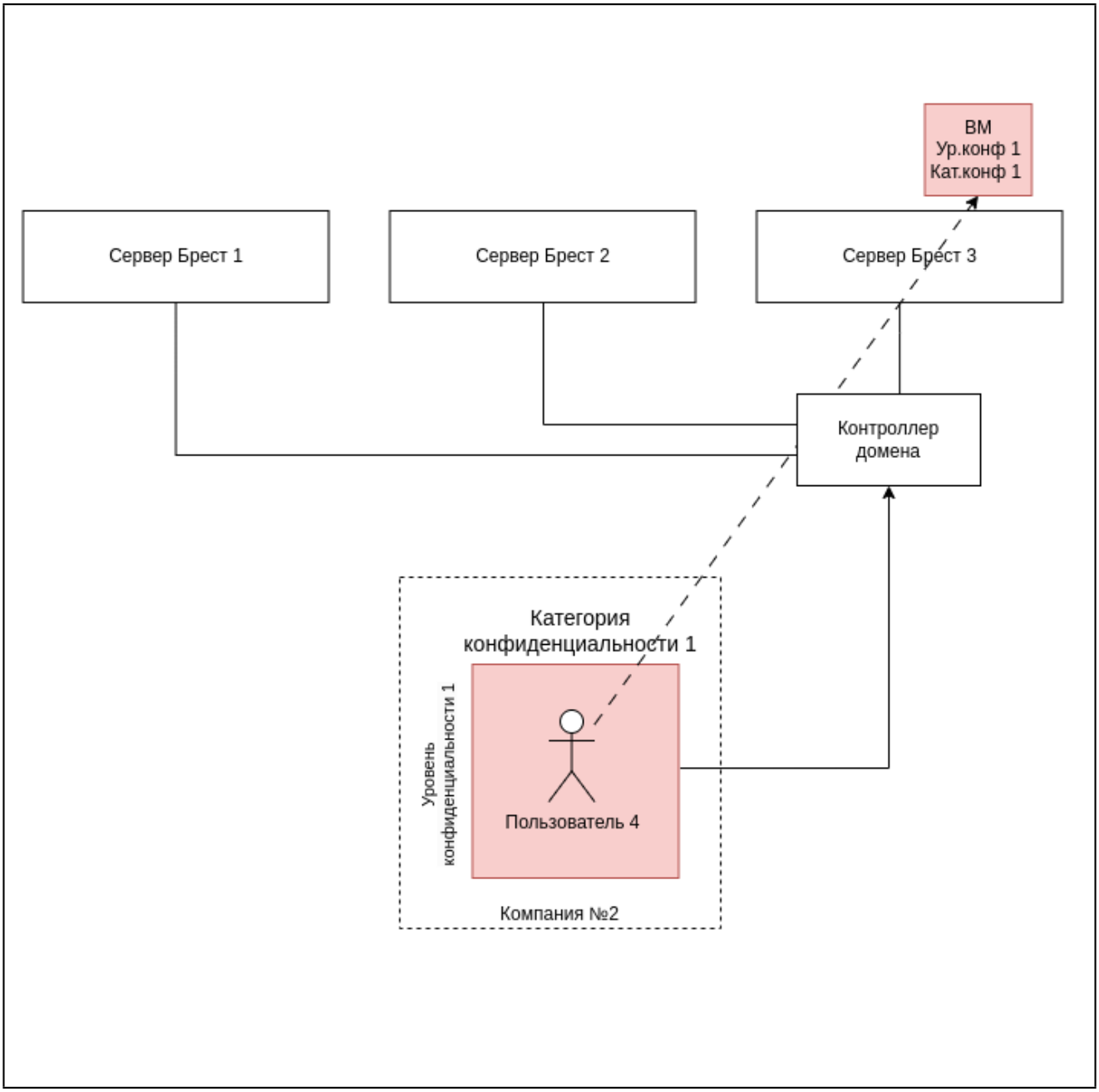

Рис. 105

- Доступ к ВМ Пользователя 5 (см. рис. 106):

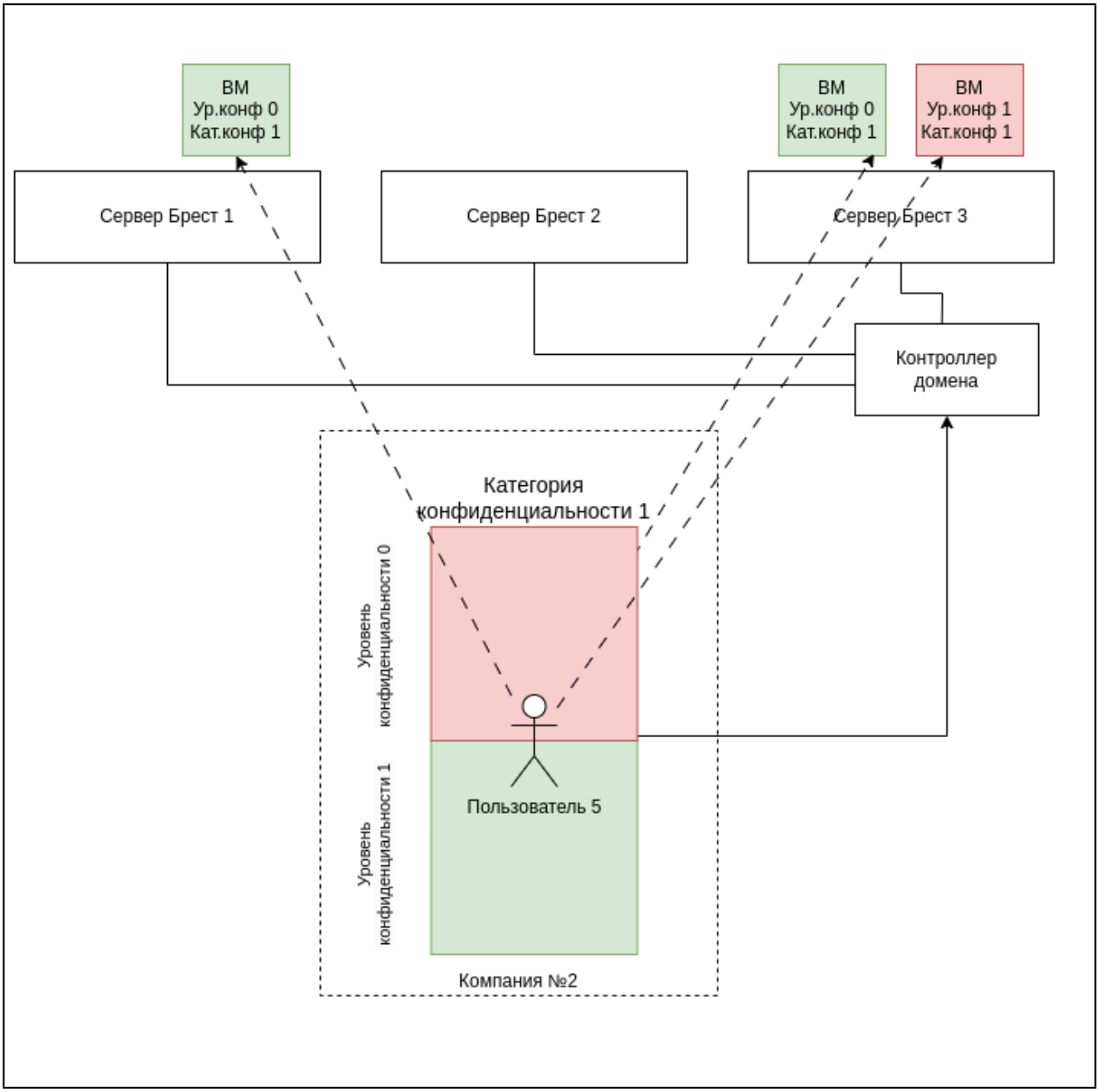

Рис. 106

Для настройки разграничение ВМ для групп в разных компаниях необходимо:

1) Создать группы пользователей, для этого в веб-интерфейсе ПК СВ в меню слева выбрать пункт «Система — Группы» и нажать кнопку [+]:

- в открывшемся окне во вкладке «Общее» указать название группы (см. рис. 107):

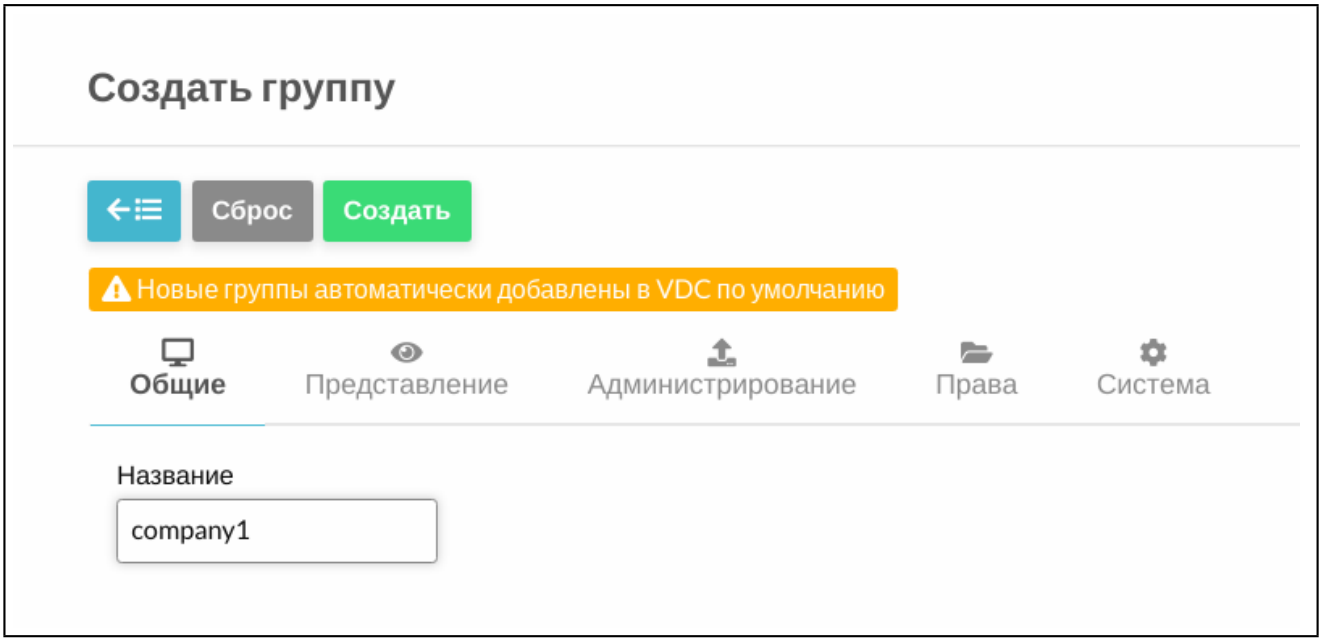

Рис. 107

ВНИМАНИЕ! В названии группы не допускается использовать буквы в верхнем регистре.

- указать необходимые настройки во вкладке «Представление» (см. рис. 108):

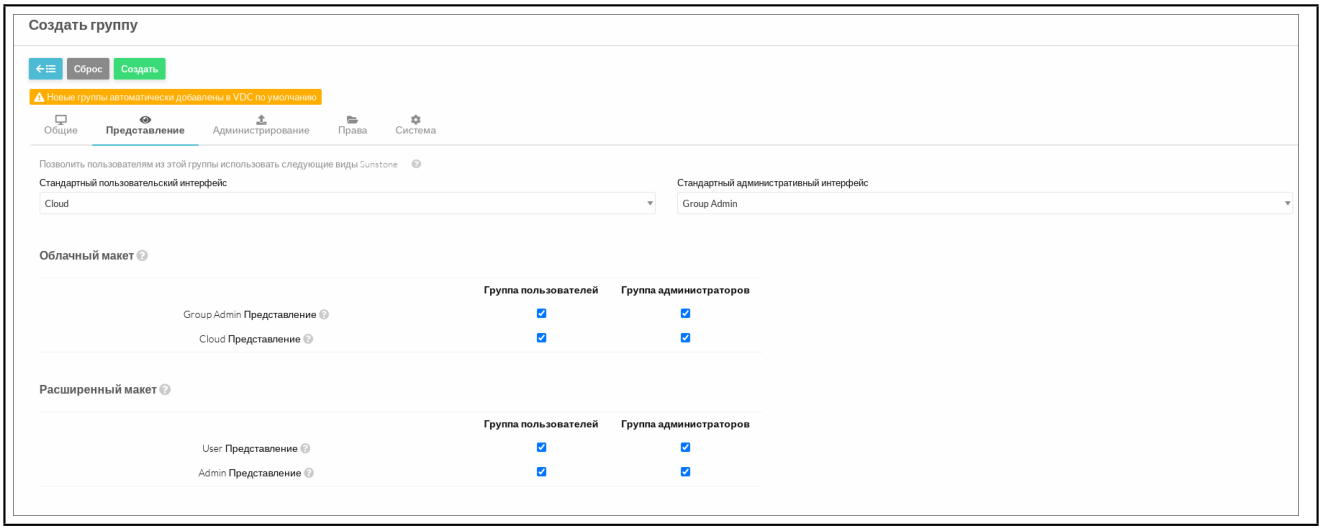

Рис. 108

- во вкладке «Права» настроить права доступа (см. рис. 109):

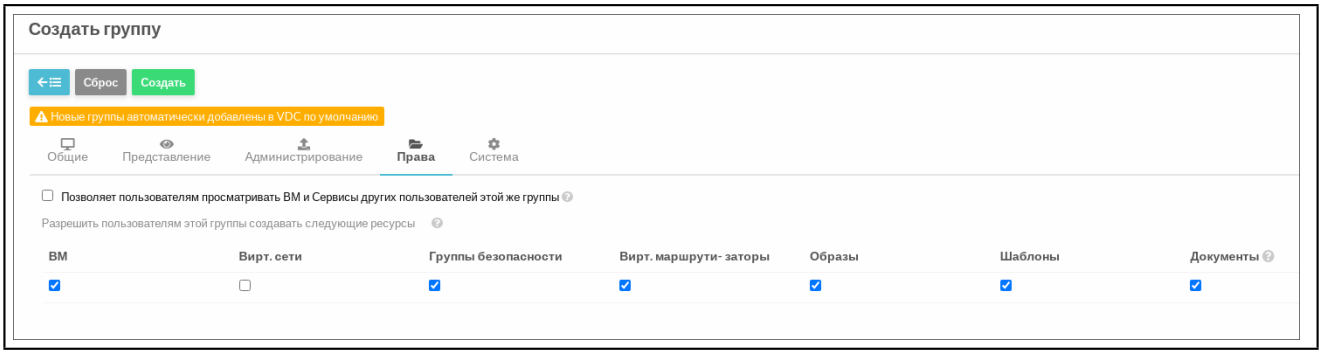

Рис. 109

- нажать кнопку [Создать];

2) Создать пользователей, для этого в веб-интерфейсе ПК СВ в меню слева выбрать пункт «Система — Пользователи» и нажать кнопку [+]:

- в открывшемся окне «Создать пользователя» необходимо указать имя пользователя, пароль, подтверждение пароля и снять флаг «Сменить пароль при первом входе в систему» (см. рис. 110):

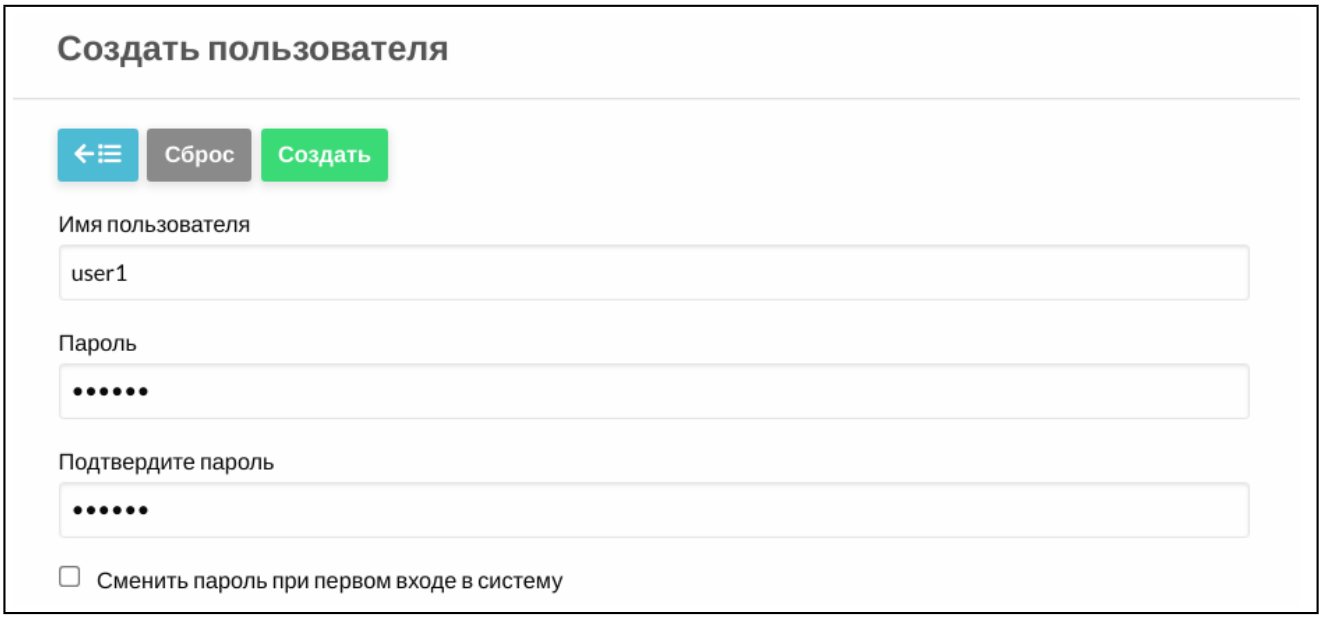

Рис. 110

Примечание. Если оставить флаг Сменить пароль при первом входе в систему, пользователь сможет зайти в систему только после смены пароля через веб-интерфейс Контролера домена.

- в выпадающем списке «Основная группа» выбрать группу, созданную на предыдущем шаге (см. рис. 111):

Рис. 111

- в «Дополнительные группы» указать `brestusers` (см. рис. 112):

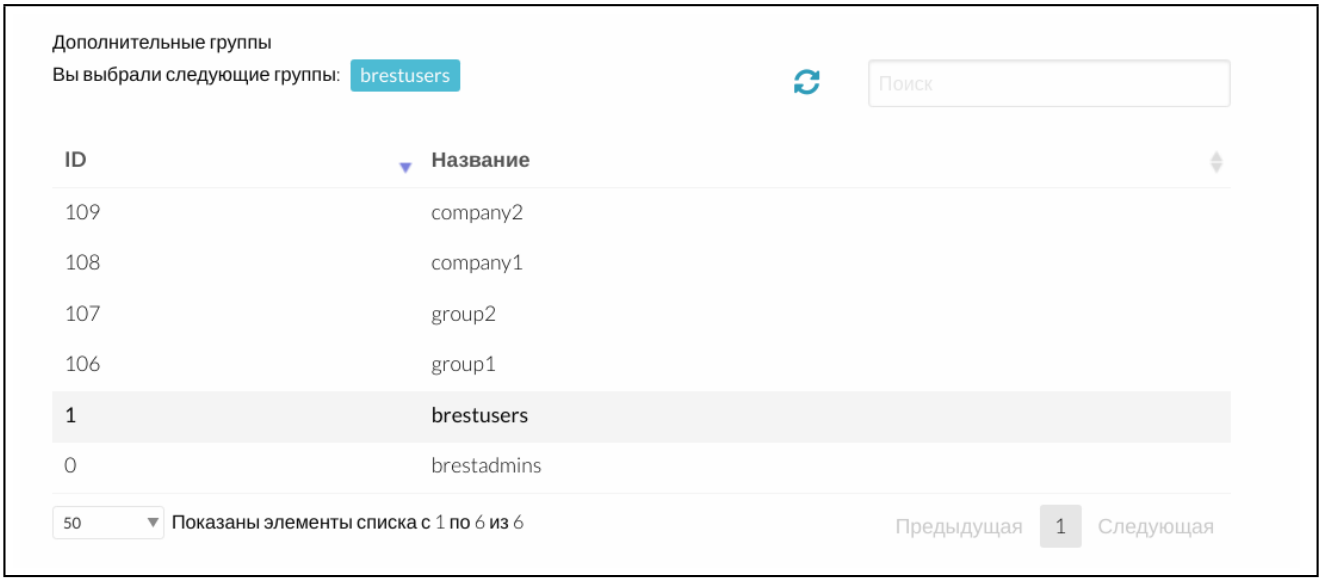

Рис. 112

- нажать кнопку [Создать];

3) Создать Администратора групп, для этого действиями, описанными на предыдущем шаге, создать учетную запись Администратора группы:

- В веб-интерфейсе ПК СВ в меню слева выбрать пункт «Система — Группы», в списке групп выбрать созданную ранее группу;
- во вкладке Пользователи нажать кнопку [Редактировать администраторов] (см. рис. 113):

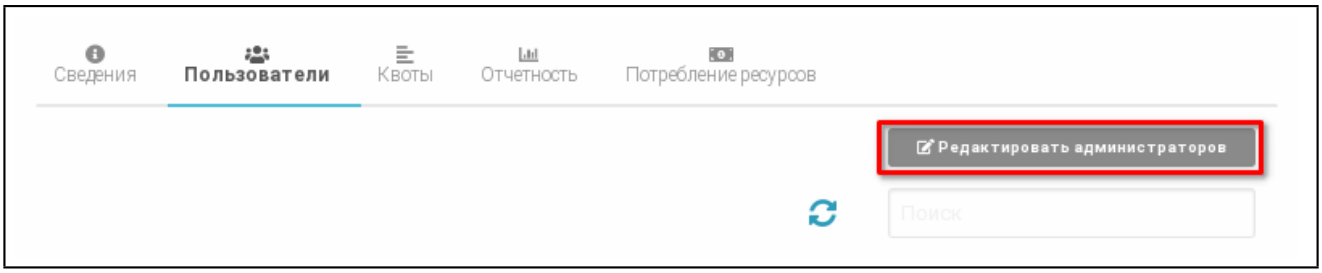

Рис. 113

- в открывшемся списке выбрать необходимого пользователя и нажать кнопку [Применить] (см. рис. 114):

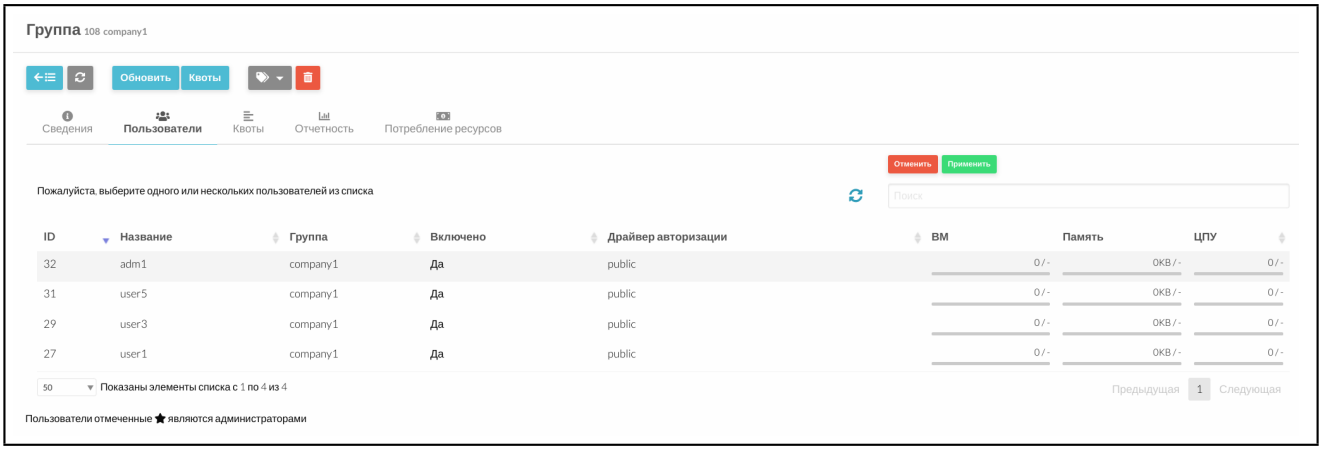

Рис. 114

4) Настроить группы FreeIPA, для этого подключиться к веб-интерфейсу Контролера домена пользователем с административными полномочиями:

- во вкладке «Пользователи» в меню слева выбрать пункт «Активные пользователи» (см. рис. 115):

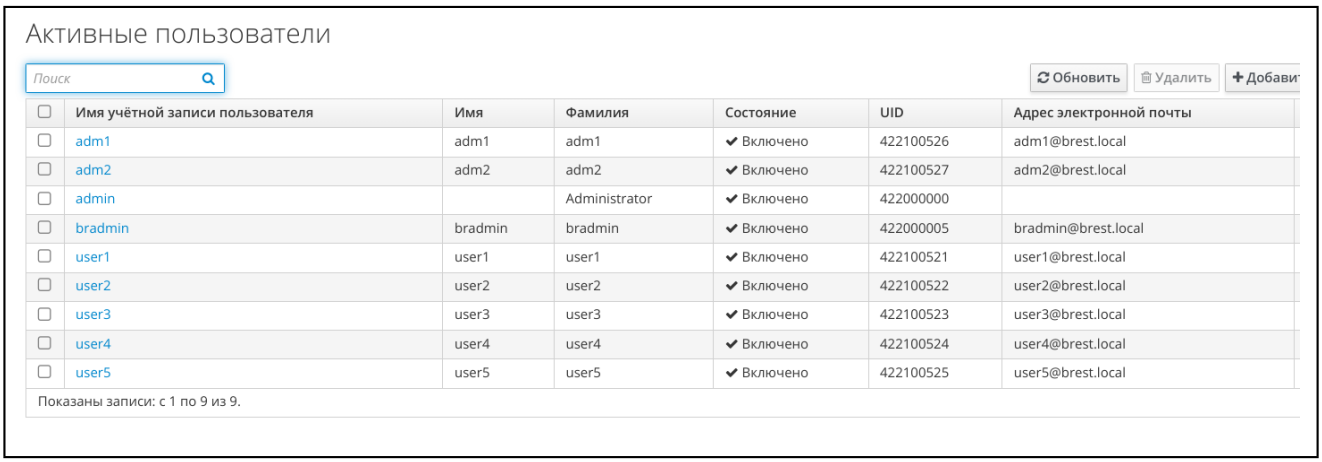

Рис. 115

- нажать на имя нужного пользователя для редактирования;
- в открывшемся окне «Параметры» выбрать требуемые уровни конфиденциальности в выпадающих списках «Минимальный уровень конфиденциальности» и «Максимальный уровень конфиденциальности» (см. рис. 116):

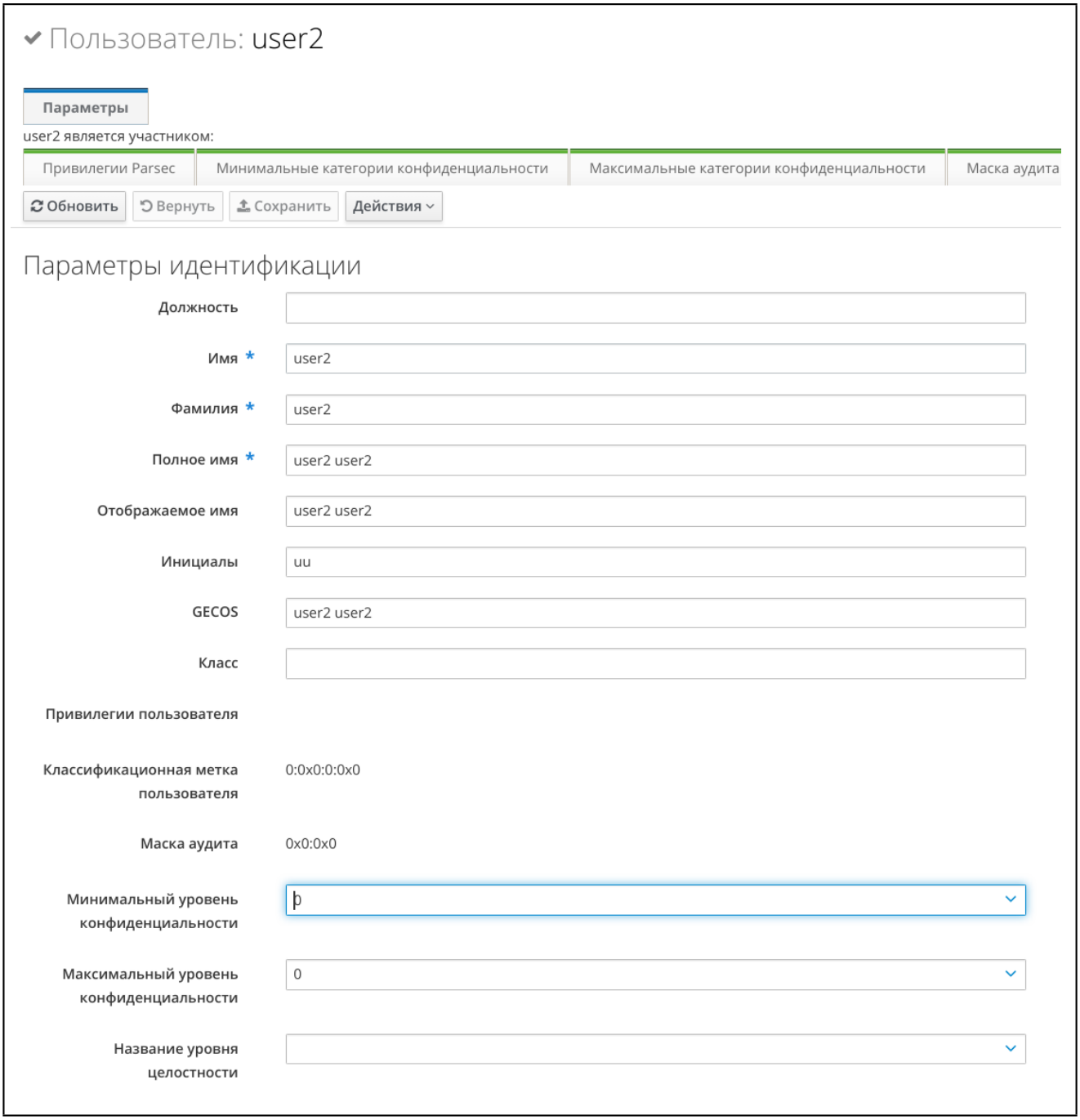

Рис. 116

- нажать кнопку [Сохранить];
- перейти во вкладку «Минимальная категория конфиденциальности» и нажать кнопку [Добавить] (см. рис. 117):

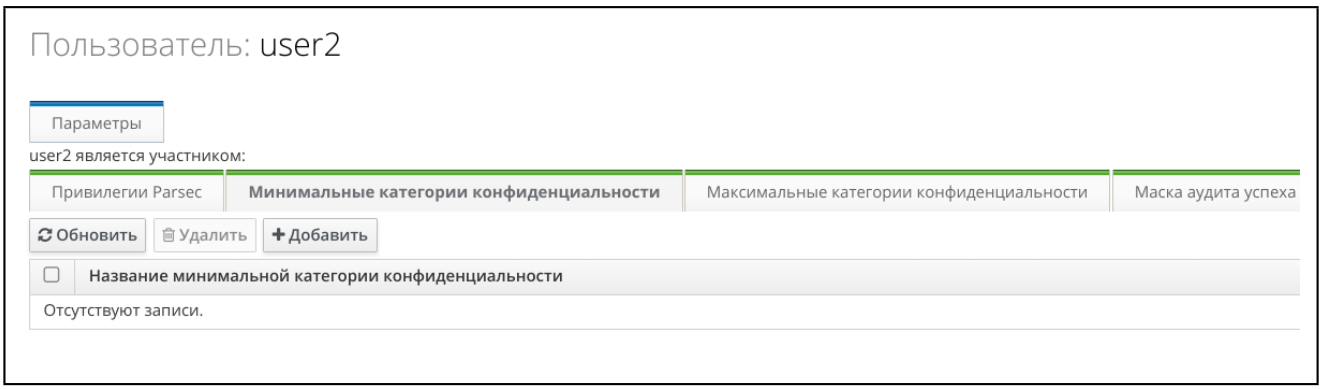

Рис. 117

- в открывшемся окне в списке «Доступно» отметить необходимые категории и перенести их в список «Ожидается» нажав кнопку [>]. Нажать кнопку [Добавить] (см. рис. 118):

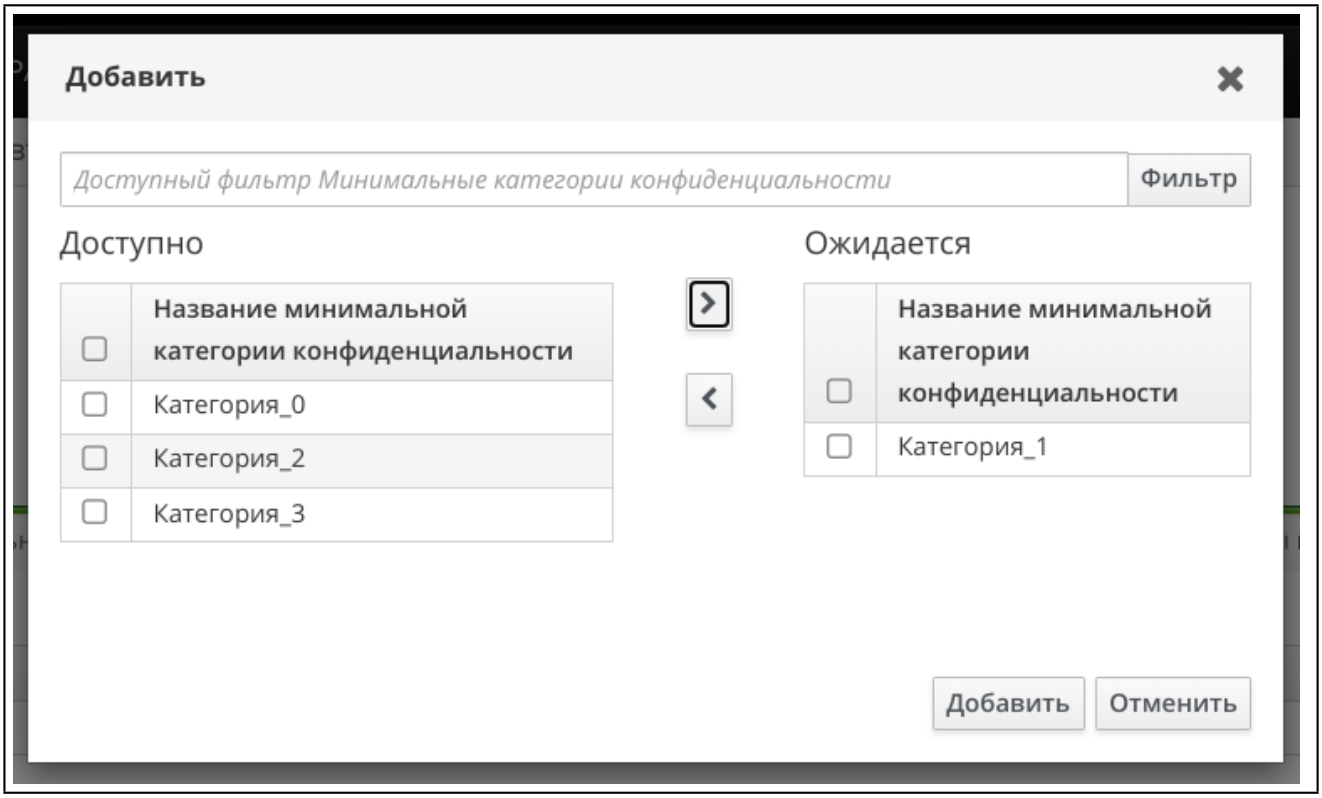

Рис. 118

Примечание. При первом назначении категорий их применение происходит мгновенно. При редактировании уже назначенных категорий изменения применяются с задержкой в полтора часа, из-за обновления информации в кэше службы SSSD фронтальных серверов.

- перейти во вкладку «Максимальные категория конфиденциальности» и настроить аналогичным образом;

5) Подключиться к веб-интерфейсу ПК СВ, для этого при первом подключении к веб-интерфейсу ПК СВ необходимо настроить браузер, добавив обработку обмена

данными аутентификации из ОС:

Примечание. Для полноценной работы с механизмом МРД, необходимо выполнить вход в систему используя терминал (ПК), заведенный в домен, к которому принадлежит ПК СВ, а также ОС терминала должна поддерживать работу с механизмом МРД. Если пользователю назначено несколько уровней конфиденциальности, то при входе можно будет выбрать необходимый уровень. Сменить уровень конфиденциальности можно только выполнив вход в систему заново, категории конфиденциальности используются автоматически.

- запустить браузер Mozilla Firefox,в адресную строку ввести `about:config` и нажать клавишу <Enter>;
- на открывшейся странице с предупреждением нажать на кнопку [Принять риск и продолжить] (см. рис. 119):

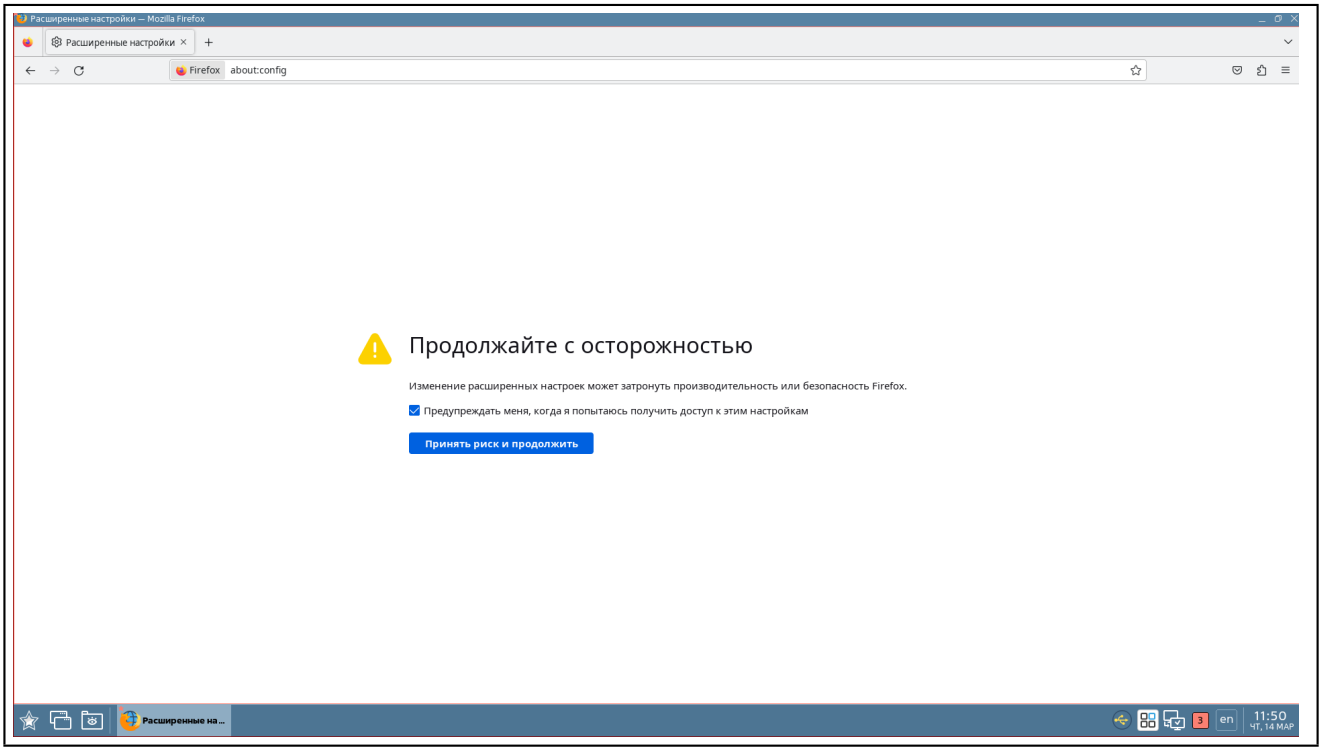

Рис. 119

- на открывшейся странице «Расширенные настройки» в поле поиска ввести слово `uris`;
- для параметров `network.negotiate-auth.trusted-uris` и `network.negotiate-auth.delegation-uris` установить значение `https://` (см. рис. 120):

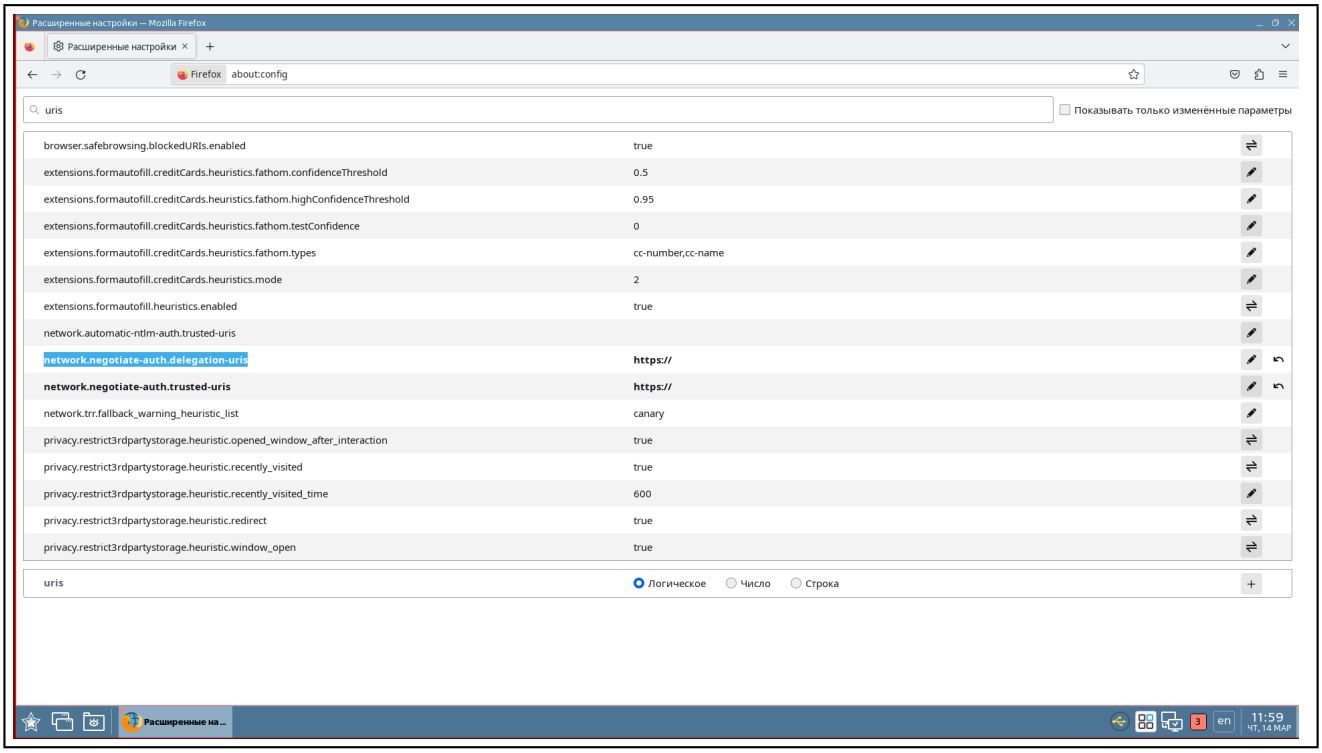

Рис. 120

В дальнейшем работа с ПК СВ не отличается от обычной.

Примечание. Настроить или скорректировать необходимые доступы к ВМ может сам пользователь на странице ВМ во вкладке Безопасность. При использовании Динамической модели Parsec, ВМ получает максимально возможную метку категории и уровень конфиденциальности, согласно доступам, создающего ВМ, пользователя. Для корректировки используемой метки необходимо выбрать Статическую модель и указать желаемую метку.

3.13. Отказоустойчивость виртуальной машины

В ПК СВ интегрирован механизм (модуль) обеспечения отказоустойчивости ВМ с сохранением мандатных и дискреционных атрибутов безопасности.

Для работы модуля необходимо соблюдение следующих условий:

- наличие в кластере минимум двух рабочих серверов виртуализации;
- общее хранилище дисков ВМ, доступное на каждом из серверов виртуализации;
- поддержка со стороны серверов виртуализации технологии IPMI (Intelligent Platform Management Interface). Данные для авторизации по IPMI должны быть указаны в настройках каждого сервера виртуализации;
- для ВМ должен быть установлен признак отказоустойчивости (Высокая доступность) — см. рис. 121.

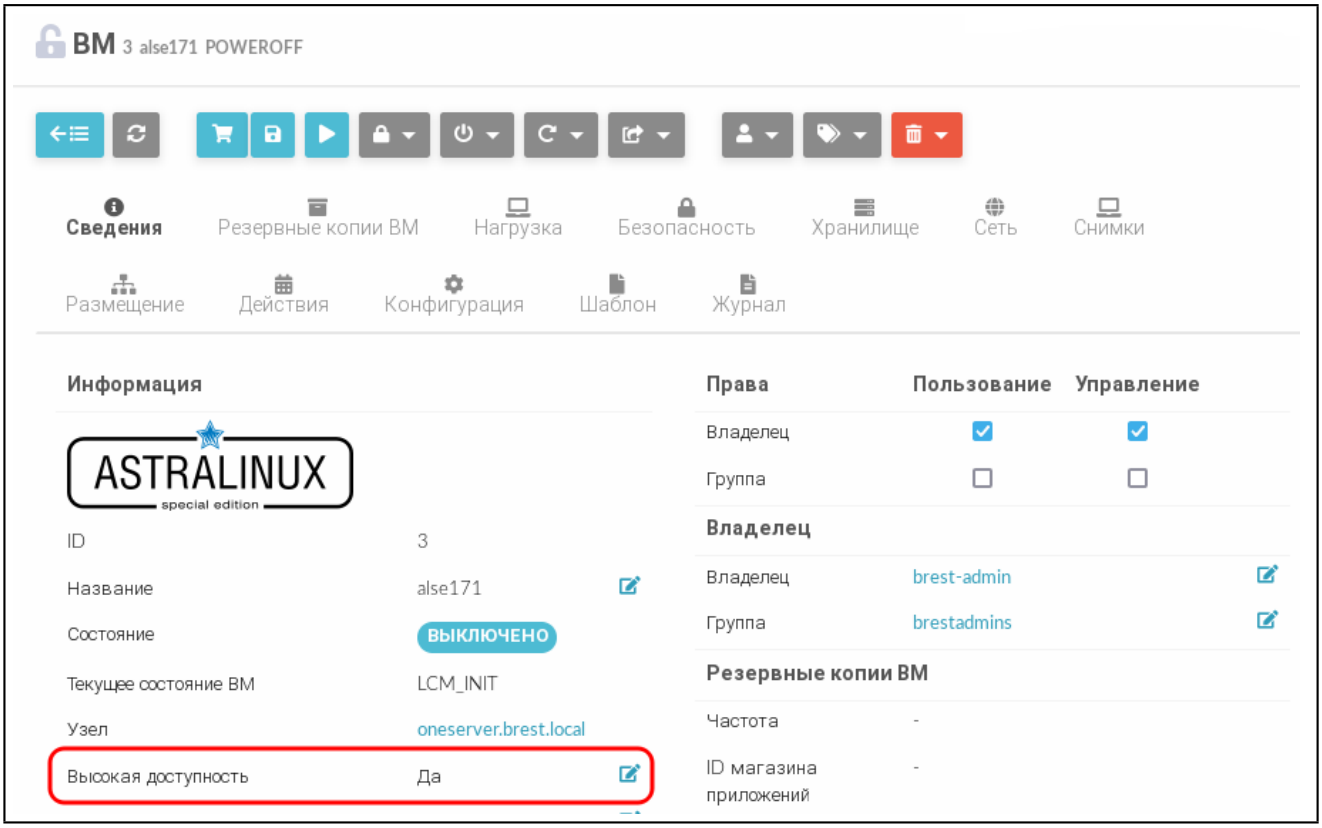

Рис. 121

В процессе работы модуля:

- ПК СВ получает сигнал о неисправности сервера виртуализации;
- считывается список ВМ с установленным признаком отказоустойчивости (высокая доступность), запущенных на неисправном сервере виртуализации;
- считываются установленные атрибуты безопасности ВМ (мандатная метка и имя пользователя, запустившего виртуальную машину) и производится перезапуск этой ВМ на рабочем сервере виртуализации.

3.14. Автостарт виртуальных машин

Механизм автостарта ВМ позволяет автоматически запустить ВМ, настроенные на автостарт, на серверах виртуализации при восстановлении после аварийного отключения.

Для включения автостарта на ВМ следует в веб-интерфейсе ПК СВ на странице данной ВМ во вкладке «Сведения» в выпадающем списке «Автозапуск» выбрать значение «Да».

Автостарт происходит следующим образом:

1) при восстановлении работы ПК СВ сервер управления запускается в первую очередь;

2) сервер управления проверяет состояние серверов виртуализации, ожидая их запуска;

3) сервер управления проверяет на запущенных серверах виртуализации наличие

ВМ, для которых настроен автостарт;

4) если такие ВМ присутствуют, сервер управления автоматически запускает их.

ВНИМАНИЕ! Если в ПК СВ для обеспечения отказоустойчивости сервера управления применяется технология Raft, то для корректной работы автостарта необходимо в файл `/lib/systemd/system/libvirtd.service`, находящийся на сервере управления, добавить строку:

```
After=opennebula.service
```

Примечание. Алгоритм Raft описан в документе РДЦП.10001-02 95 01-1.

3.15. Миграции дисков ВМ между хранилищами

Миграции дисков ВМ может быть осуществлена только между одинаковыми типами хранилищ (например, из LVM_LVM в LVM_LVM) и только в рамках одного сервера виртуализации.

Для онлайн миграции дисков ВМ (без выключения ВМ) в веб-интерфейсе ПК СВ необходимо:

1) на странице ВМ нажать кнопку управления размещением и в открывшемся меню выбрать пункт «Перенести ВМ» (см. рис. 122);

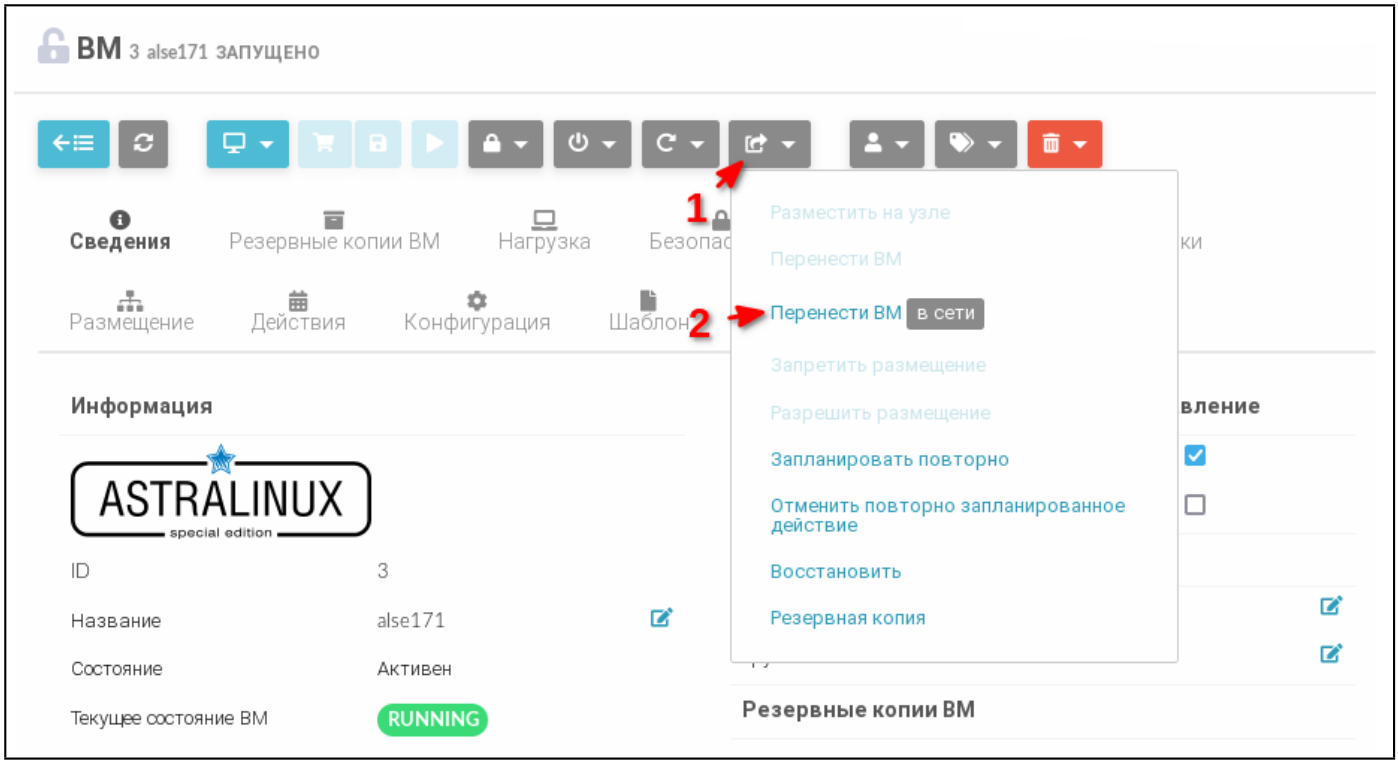

Рис. 122

2) в открывшемся окне «Мигрировать виртуальную машину»:

а) в секции «Выберите Узел» выбрать тот же узел, на котором запущена ВМ (см. рис. 123);

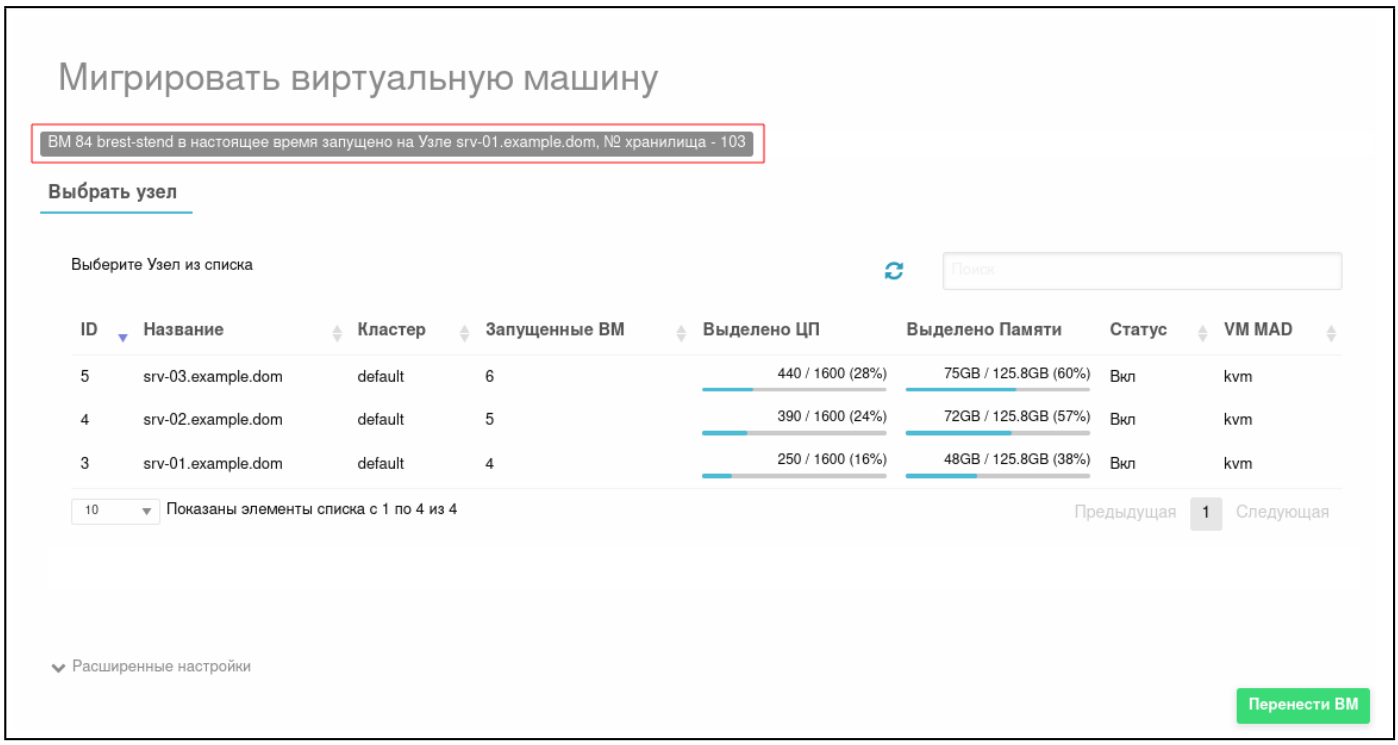

Рис. 123

б) в открывшейся секции «Выберите хранилище» выбрать хранилище такого же типа, как хранилище, в котором на текущий момент хранится диск ВМ (см. рис. 124),

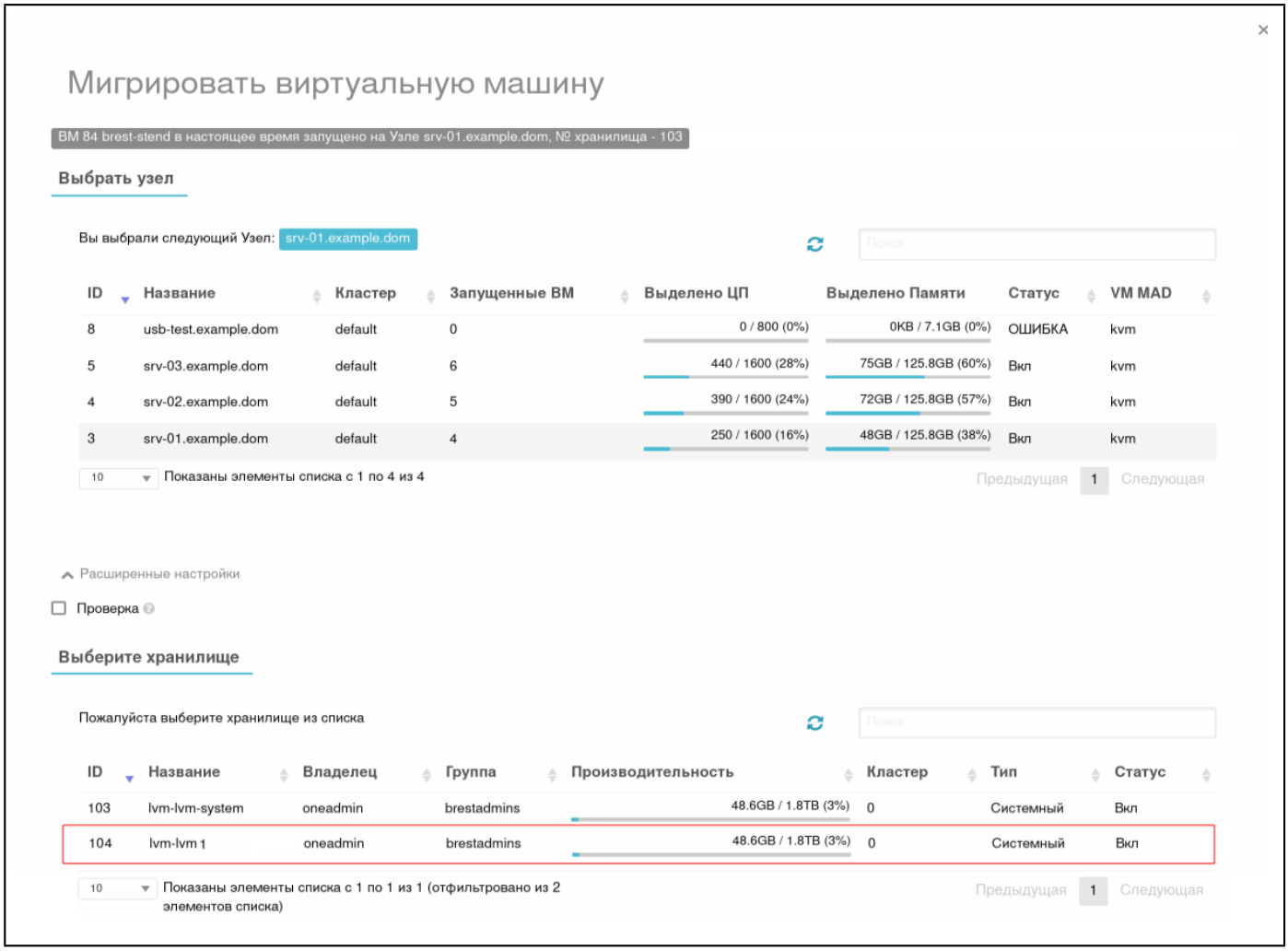

Рис. 124

в) нажать кнопку **[Перенести ВМ]**.

4. СООБЩЕНИЯ ОПЕРАТОРУ

4.1. Типы сообщений

В ходе выполнения программы предусмотрен вывод сообщений двух типов: сообщение об ошибке и информационное сообщение.

Сообщение об ошибке отображается в следующих случаях:

- если при вводе данных были допущены ошибки, введено недопустимое значение или не заполнены поля, обязательные для заполнения;
- при сбоях в работе служб ПК СВ и ОС СН;
- при выполнении действий, недопустимых в соответствии с настроенной ролевой политикой.

Каждое такое сообщение содержит описание ошибки. Пример сообщения об ошибке представлен на рис.125.

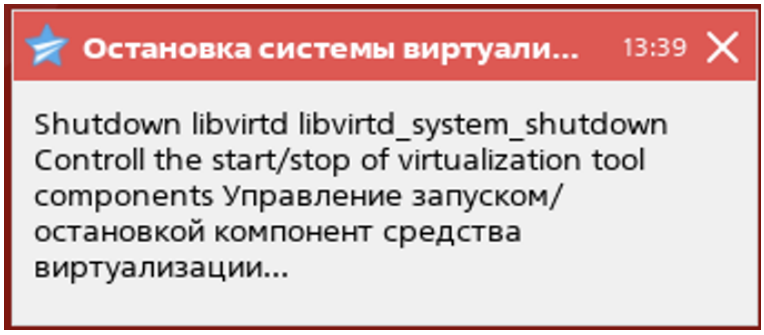

Рис. 125

После выполнения пользователем определенных действий в ПК СВ (переход к разделу программы, сохранение данных) отображаются информационные сообщения. Такие сообщения не требуют каких-либо действий пользователя и скрываются автоматически. Пример информационного сообщения представлен на рис.126.

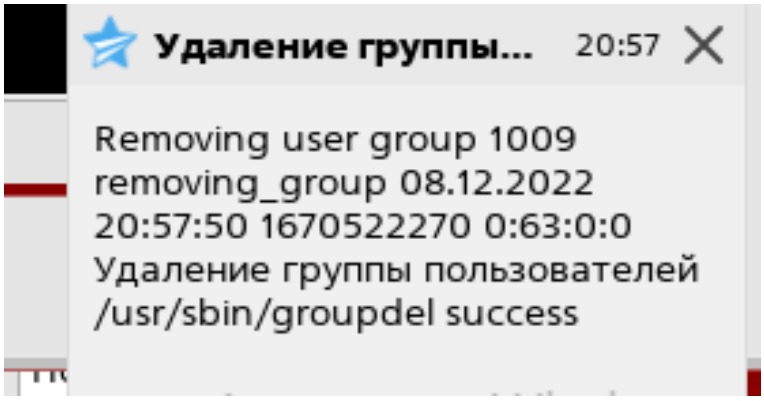

Рис. 126

4.2. Действия пользователя

При возникновении сообщений об ошибке пользователю следует выполнить действия, описанные в таблице 8.

Таблица 8

Тип сообщения об ошибке	Действия пользователя
Ошибка ввода данных	Откорректировать введенные значения или заполнить поля, обязательные для заполнения
Сбой в работе служб ПК СВ	Обратиться к администратору ПК СВ
Сбой в работе служб ОС СН	Обратиться к администратору ОС СН

ПЕРЕЧЕНЬ ТЕРМИНОВ

Администратор ВМ — пользователь, которому предоставляются права для выполнения действий по управлению экземпляром ВМ.

Администратор ОС СН — пользователь ОС СН, входящий в группу `astra-admin`, которому предоставляются права для выполнения действий по настройке ОС, требующих привилегий суперпользователя `root`.

Администратор ПК СВ — пользователь, реализующий роль администратора средства виртуализации.

Разработчик ВМ — пользователь, которому предоставляются права для выполнения действий по созданию изменению конфигурации (шаблонов) виртуальных машин.

Примечание. Описание ролей пользователей представлено в документе РДЦП.10001-02 97 01 «Программный комплекс «Средства виртуализации «Брест». Руководство по КСЗ».

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

БД — база данных

ВМ — виртуальная машина

ЕПП — единое пространство пользователей

ОС — операционная система

ОС СН — операционная система специального назначения «Astra Linux Special Edition»

ПК СВ — программный комплекс «Средства виртуализации «Брест»

ПО — программное обеспечение

СЗИ — средства защиты информации

ФС — файловая система

ЦОХД — центр обработки и хранения данных

ЦП — центральный процессор

ACL — Access Control List (список контроля доступа)

AR — Address Ranges (диапазон IP-адресов)

VDC — Virtual Data Center (виртуальный дата-центр)

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					