Утвержден

РДЦП.10001-03-УД

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

ПРОГРАММНЫЙ КОМПЛЕКС «СРЕДСТВА ВИРТУАЛИЗАЦИИ «БРЕСТ»

Руководство администратора. Часть 2

РДЦП.10001-03 95 01-2

Листов 139

2023

Литера $О_1$

АННОТАЦИЯ

Настоящий документ является руководством администратора программного изделия «Программный комплекс «Средства виртуализации «Брест» (ПК СВ «Брест») РДЦП.10001-03 (далее по тексту — ПК СВ) в части применения по назначению ПК СВ с учетом особенностей операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.7) (далее по тексту — ОС СН), под управлением которой функционирует ПК СВ.

Документ предназначен для администраторов средства виртуализации (администраторов ПК СВ).

Документ не охватывает порядок установки и развертывания ПК СВ и предназначен для использования совместно с эксплуатационными документами согласно ведомости РДЦП.10001-03 20 01 «Программный комплекс «Средства виртуализации «Брест». Ведомость эксплуатационных документов».

Руководство администратора состоит из двух частей:

- РДЦП.10001-03 95 01-1 «Программный комплекс «Средства виртуализации «Брест». Руководство администратора. Часть 1»;
- РДЦП.10001-03 95 01-2 «Программный комплекс «Средства виртуализации «Брест». Руководство администратора. Часть 2».

В первой части руководства описан порядок развертывания и первичной настройки ПК СВ.

Во второй части руководства представлен порядок администрирования ПК СВ с учетом использования среды виртуализации, обеспечения отказоустойчивости и масштабирования развернутого ПК СВ.

СОДЕРЖАНИЕ

1. ФУНКЦИИ АДМИНИСТРАТОРА ПК СВ

В ПК СВ администратор ПК СВ (пользователь, реализующий роль администраторарасредства виртуализации) выполняет следующие функции:

1) управление учетными записями пользователей ПК СВ, включая создание и удаление учетных записей (см. 5.2);

2) управление правами доступа пользователей ПК СВ к виртуальным машинам(см. 5.5);

3) запуск, остановка, а также удаление экземпляров ВМ (см. 7.1.2 и 7.1.3);

4) управление квотами доступа ВМ к физическому и виртуальному оборудованию(см. 5.7);

5) создание снимков состояния виртуальных машин, включающих файл конфигурации ВМ, образа диска ВМ и образа памяти ВМ, а также отдельное созданиеснимков состояния образа диска ВМ (см. 7.1.13);

6) управление виртуальным оборудованием ПК СВ, включая создание и удалениевиртуального оборудования.

В ПК СВ в качестве виртуального оборудования выступают:

- серверы виртуализации;
- виртуальные сети;
- образы дисков ВМ;
- шаблоны ВМ;
- экземпляры ВМ.

Администратор ПК СВ осуществляет управление следующим виртуальным оборудо-ванием:

- серверами виртуализации (см. 3);
- виртуальными сетями (см. 6).

Управление образами дисков, шаблонами и экземплярами ВМ выполняется администратором ВМ и описано в документе РДЦП.10001-03 93 01.

2. ИНСТРУМЕНТЫ УПРАВЛЕНИЯ ПК СВ

2.1. Инструменты командной строки

Для управления функциональными элементами ПК СВ можно воспользоваться инструментами командной строки, перечисленными в таблице 1.

Таблица 1

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 администратора ПК СВ.

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

`<наименование_инструмента> -h`

2.2. 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 пользователя ПК СВ (например, `brestadmin` — имя администратора ПК СВ, который был создан во время выполнения действий по установке программных компонент ПК СВ);
- в поле «Пароль» ввести пароль пользователя ПК СВ;
- 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 (например, аутентификационные параметры администратора 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. УПРАВЛЕНИЕ СЕРВЕРАМИ ВИРТУАЛИЗАЦИИ И КЛАСТЕРАМИ

Установка и инициализация службы сервера виртуализации производятся в соответствии с документом РДЦП.10001-03 95 01-1 «Программный комплекс «Средства виртуализации «Брест». Руководство администратора. Часть 1».

Управление серверами виртуализации и кластерами осуществляется администратором ПК СВ (администратором средства виртуализации).

Кластеры (Clusters) представляют собой группы серверов виртуализации с общими хранилищами и сетями. Более подробная информация о кластерах приведена в 3.2.

3.1. Серверы виртуализации

3.1.1. Добавление сервера виртуализации

Для использования сервера виртуализации в ПК СВ его необходимо зарегистрировать на сервере управления.

В дискреционном режиме функционирования ПК СВ регистрация сервера виртуализации производится автоматически при инициализации службы сервера виртуализации.

В 3.1.1.1 — 3.1.1.2 описан процесс регистрации сервера виртуализации в сервисном режиме функционирования ПК СВ.

ВНИМАНИЕ! Если в сети ПК СВ не используется служба DNS, то перед регистрацией сервера виртуализации необходимо на сервере управления в файле `/etc/host` указать информацию о добавляемом сервере виртуализации (IP-адрес и сетевое имя).

3.1.1.1. Регистрация сервера виртуализации в интерфейсе командной строки

Для регистрации сервера виртуализации в интерфейсе командной строки необходимо использовать команду:

```
onehost create <сетевое_имя_сервера_виртуализации> \
      --im <информационный_драйвер> --vm <драйвер_виртуализации>
```

Процесс регистрации сервера виртуализации занимает от 20 до 60 секунд.

Пример

Регистрация сервера виртуализации с гипервизором KVM:

```
onehost create node1 --im kvm --vm kvm
```

Пример вывода после выполнения команды:

```
ID: 1
```

3.1.1.2. Регистрация сервера виртуализации в веб-интерфейсе ПК СВ

Для того чтобы зарегистрировать сервер виртуализации в веб-интерфейсе ПК СВ, необходимо:

1) в меню слева выбрать пункт меню «Инфраструктура — Узлы» и на открывшейся странице «Узлы» нажать на кнопку **[+]**;

2) на открывшейся странице `Создать узел` (см. рис. 1):

а) в поле «Тип» указать тип драйвера виртуализации,

б) в поле «Имя хоста» ввести сетевое имя сервера виртуализации,

в) в поле «Логин администратора» ввести имя локального администратора компьютера, выполняющем функцию сервера виртуализации,

г) в поле «Пароль администратора» ввести пароль локального администратора компьютера, выполняющем функцию сервера сервер виртуализации,

д) нажать на кнопку **[Создать]**;

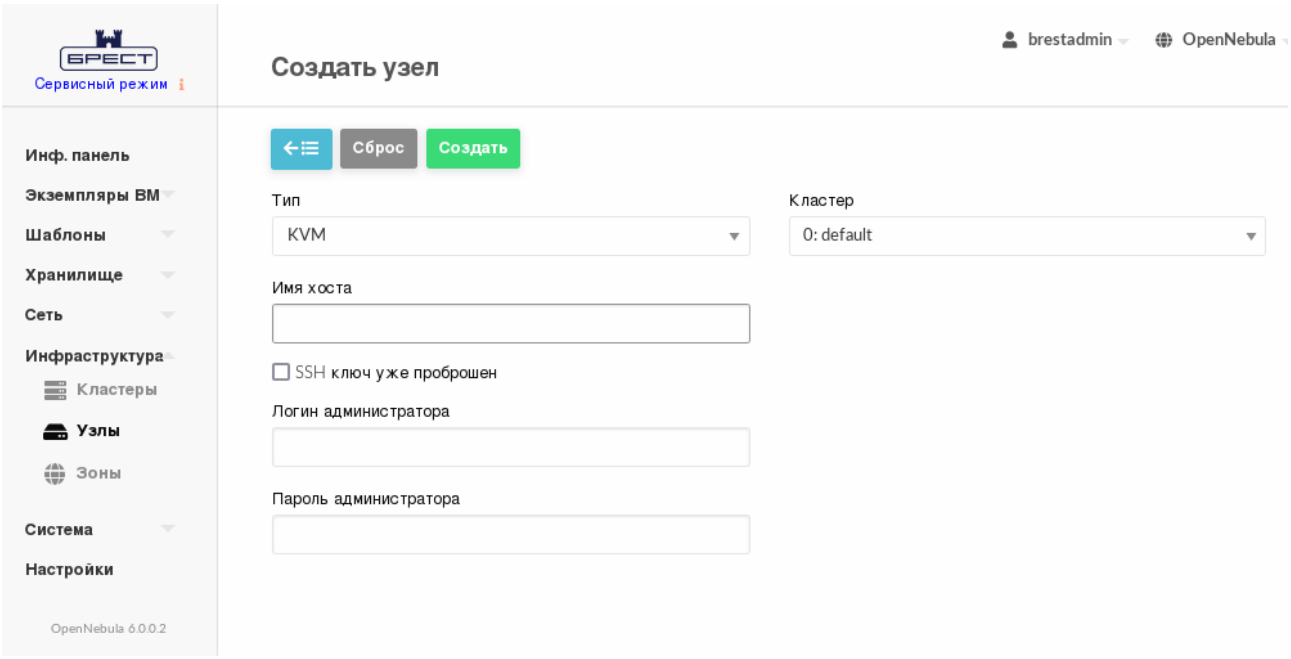

Рис. 1

3) на открывшейся странице «Узлы» появится запись о зарегистрированном сервере виртуализации. Необходимо дождаться пока в столбце `Статус` для этого сервера виртуализации значение `Инициализация` не изменится на `ВКЛ`. Процесс регистрации сервера виртуализации занимает от 20 до 60 секунд. Для обновления отображаемого статуса можно воспользоваться кнопкой **[Обновить]** (см. рис. 2).

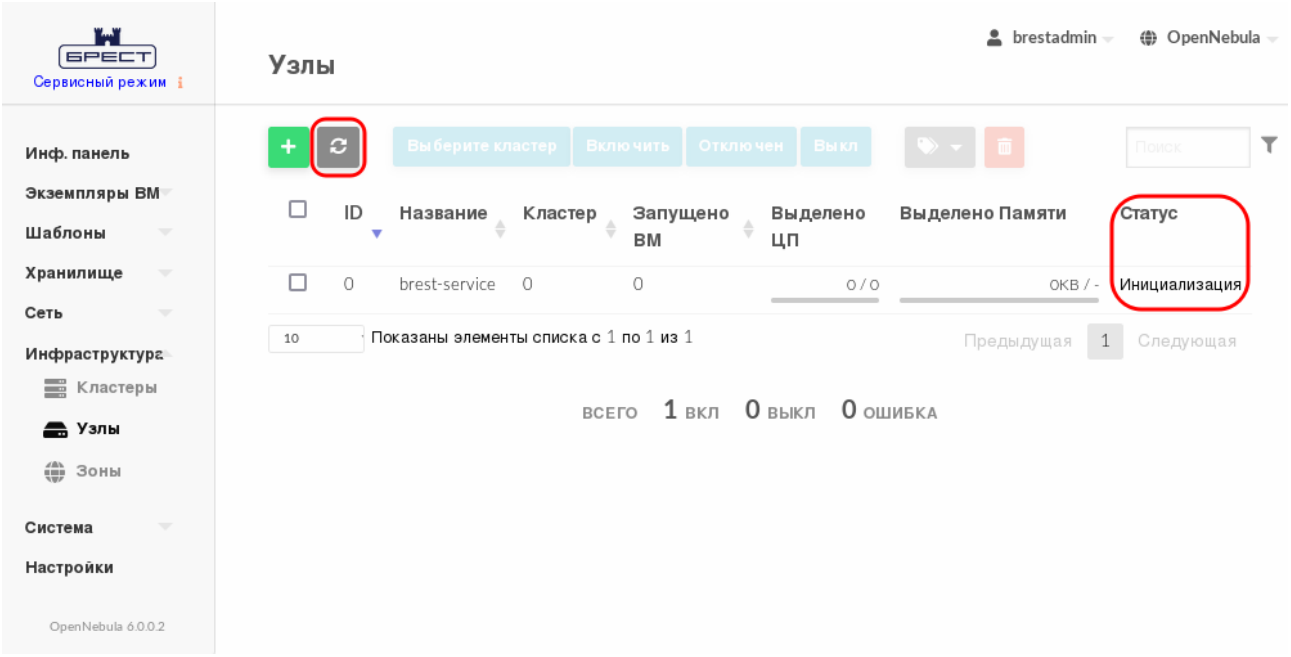

Рис. 2

3.1.2. Отображение информации о сервере виртуализации и просмотр перечня серверов виртуализации

3.1.2.1. В интерфейсе командной строки

Для отображения информации об конкретном сервере виртуализации в интерфейсе командной строки необходимо использовать команду:

```
onehost show <идентификатор_сервера_виртуализации>
```

Информация о сервере виртуализации включает:

- общую информацию с указанием его названия и драйверов, которые используются для взаимодействия с ним;
- информацию о производительности (совместно используемые ресурсы сервера виртуализации) для центрального процессора (ЦП) и оперативной памяти;
- информацию о подключенном хранилище;
- информацию мониторинга (см. 3.1.5).

Пример

Отображение информации о сервере виртуализации с идентификатором 1:

```
onehost show 1
```

Пример вывода после выполнения команды:

```
HOST 1 INFORMATION
ID : 1
NAME : host01
CLUSTER : default
STATE : MONITORED
IM_MAD : kvm
```

```
VM_MAD : kvm
LAST MONITORING TIME : 07/11 17:19:05

HOST SHARES
RUNNING VMS : 0
MEMORY
TOTAL : 3.8G
TOTAL +/- RESERVED : 3.8G
USED (REAL) : 230.8M
USED (ALLOCATED) : 0K
CPU
TOTAL : 400
TOTAL +/- RESERVED : 400
USED (REAL) : 28
USED (ALLOCATED) : 0

MONITORING INFORMATION
ARCH="x86_64"
CLUSTER_ID="0"
CPUSPEED="2304"
HOSTNAME="host01"
HYPERVISOR="kvm"
IM_MAD="kvm"
...
VM_MAD="kvm"
...
```

Для просмотра перечня всех зарегистрированных серверов виртуализации необходимо выполнить команду `onehost list`:

Пример вывода после выполнения команды:

```
ID NAME           CLUSTER  TVM  ALLOCATED_CPU   ALLOCATED_MEM  STAT
1  host01         default    0   0 / 400 (0%)  0K / 3.8G (0%)  on
0  brest-service  default    0   0 / 600 (0%)  0K / 5.8G (0%)  on
```

3.1.2.2. В веб-интерфейсе ПК СВ

Для отображения перечня всех зарегистрированных серверов виртуализации в веб-интерфейсе ПК СВ необходимо в меню слева выбрать пункт меню «Инфраструктура — Узлы». На открывшейся странице «Узлы» будет представлена таблица состояний серверов виртуализации, аналогичная таблице, отображаемой в интерфейсе командной строки после выполнения команды `onehost list`.

Для отображения информации об конкретном сервере виртуализации на странице «Узлы» необходимо выбрать соответствующий сервер виртуализации. После этого откроется

страница с информацией о сервере виртуализации (вкладка «Сведения» — см. рис. 3).

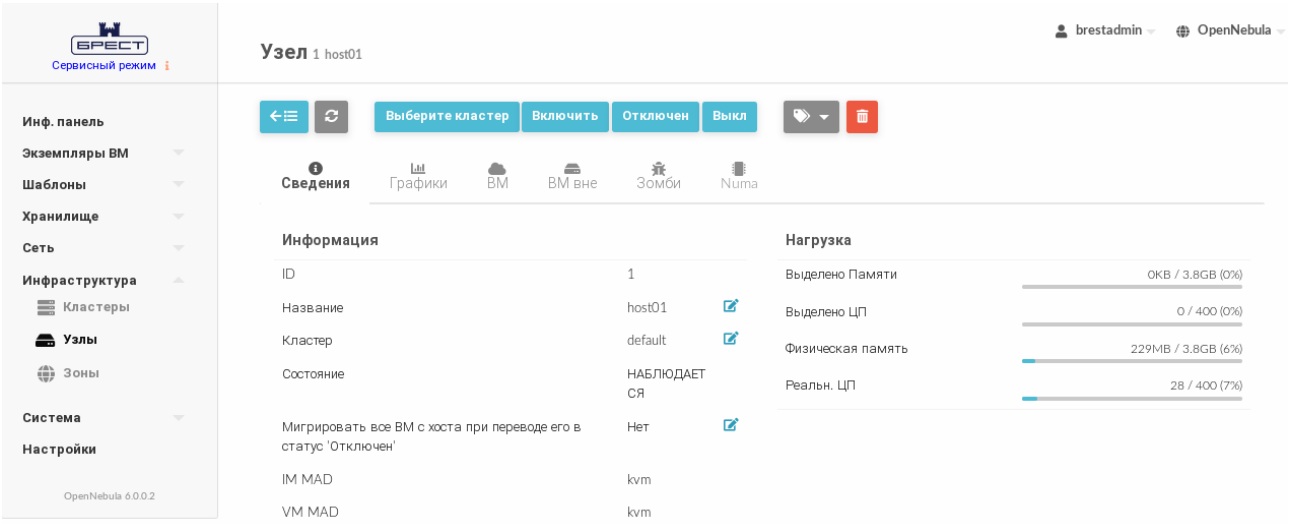

Рис. 3

3.1.3. Жизненный цикл сервера виртуализации

3.1.3.1. Общие сведения

Для управления жизненным циклом сервера виртуализации его можно переключать в различные состояния: включен (on), выключен (dsbl), отключен от сети (off) и др. Состояния описаны в таблице 2:

Таблица 2

Состояние	Контроль	Развертывание ВМ		Значение
		Вручную	Планир.	
Включен (on)	Да	Да	Да	Сервер виртуализации находится в полностью рабочем состоянии
Обновление (update)	Да	Да	Да	Обновление информации о состоянии сервера виртуализации в системе мониторинга
Отключен (dsbl)	Да	Да	Нет	Отключен, например, для проведения техобслуживания
Отключен от сети (off)	Нет	Нет	Нет	Сервер виртуализации полностью отключен от сети
Ошибка (err)	Да	Да	Нет	При обновлении информации о состоянии сервера виртуализации выявлена ошибка. Можно использовать команду `onehost show` Для просмотра описания ошибки
Повторить попытку (retry)	Да	Да	Нет	Обновление информации о сервере виртуализации, который находится в состоянии ошибки

3.1.3.2. Управление сервером виртуализации в интерфейсе командной строки

Инструмент командной строки `onehost` содержит три команды для установки состояния сервера виртуализации:

1) для отключения сервера виртуализации необходимо использовать команду:

```
onehost disable <идентификатор_сервера_виртуализации>
```

2) чтобы снова включить сервер виртуализации, необходимо использовать команду:

```
onehost enable <идентификатор_сервера_виртуализации>
```

3) для полного отключения сервера виртуализации необходимо использовать команду:

```
onehost offline <идентификатор_сервера_виртуализации>
```

Примеры:

1. Перевод сервера виртуализации с идентификатором 1 в состояние «Отключен»

```
onehost disable 1
```

Для просмотра состояния сервера виртуализации можно воспользоваться командой `onehost list`. Пример вывода после выполнения команды:

```
ID NAME           CLUSTER  TVM  ALLOCATED_CPU   ALLOCATED_MEM  STAT
1  host01         default    0   0 / 400 (0%)   0K / 3.8G (0%)  dsbl
0  brest-service  default    0   0 / 600 (0%)   0K / 5.8G (0%)  on
```

2. Включение сервера виртуализации с идентификатором 1

```
onehost enable 1
```

Процесс включения сервера виртуализации занимает от 20 до 60 секунд. Для просмотра состояния сервера виртуализации можно воспользоваться командой `onehost list`. Пример вывода после выполнения команды:

```
ID NAME           CLUSTER  TVM  ALLOCATED_CPU   ALLOCATED_MEM  STAT
1  host01         default    0   0 / 400 (0%)   0K / 3.8G (0%)  on
0  brest-service  default    0   0 / 600 (0%)   0K / 5.8G (0%)  on
```

3. Полное отключение сервера виртуализации с идентификатором 1

```
onehost offline 1
```

Для просмотра состояния сервера виртуализации можно воспользоваться командой `onehost list`. Пример вывода после выполнения команды:

```
ID NAME           CLUSTER  TVM  ALLOCATED_CPU   ALLOCATED_MEM  STAT
1  host01         default    0               -               -  off
0  brest-service  default    0   0 / 600 (0%)   0K / 5.8G (0%)  on
```

Команды `disable` и `offline` не влияют на состояние ВМ, работающих на сервере виртуализации. Для того чтобы выполнить автоматическую миграцию ВМ на другие серверы виртуализации, обладающие достаточным вычислительным ресурсом, необходимо выполнить команду

```
onehost flush <наименование_сервера_виртуализации>
```

В качестве наименования сервера виртуализации можно указать перечень серверов виртуализации (идентификаторов или наименований, разделенных запятыми) или диапазон идентификаторов серверов виртуализации (в качестве разделителя используются две точки — «..»).

3.1.3.3. Управление сервером виртуализации в веб-интерфейсе ПК СВ

Для управления сервером виртуализации в веб-интерфейсе ПК СВ необходимо:

1) в меню слева выбрать пункт меню «Инфраструктура — Узлы»;

2) на открывшейся странице «Узлы» выбрать необходимый сервер виртуализации.

После этого откроется страница с информацией о сервере виртуализации. Для изменения состояния сервера виртуализации можно воспользоваться кнопками (см. рис. 3):

- **[Отключен]** — для перевода сервера виртуализации в состояние «Отключен», например, для проведения техобслуживания;
- **[Включить]** — для включения сервера виртуализации;
- **[Выкл]** — для полного отключения сервера виртуализации.

3.1.4. Удаление сервера виртуализации

3.1.4.1. В интерфейсе командной строки

Для удаления сервера виртуализации в интерфейсе командной строки необходимо использовать команду:

```
onehost delete <сетевое_имя_сервера_виртуализации>
```

или команду:

```
onehost delete <идентификатор_сервера_виртуализации>
```

Пример

Удаление сервера виртуализации `node01`:

```
onehost delete node1
```

3.1.4.2. В веб-интерфейсе ПК СВ

Для удаления сервера виртуализации в веб-интерфейсе ПК СВ необходимо:

1) в меню слева выбрать пункт меню «Инфраструктура — Узлы»;

2) на открывшейся странице «Узлы» выделить необходимый сервер виртуализации и нажать на кнопку **[Удалить]** (см. рис. 4).

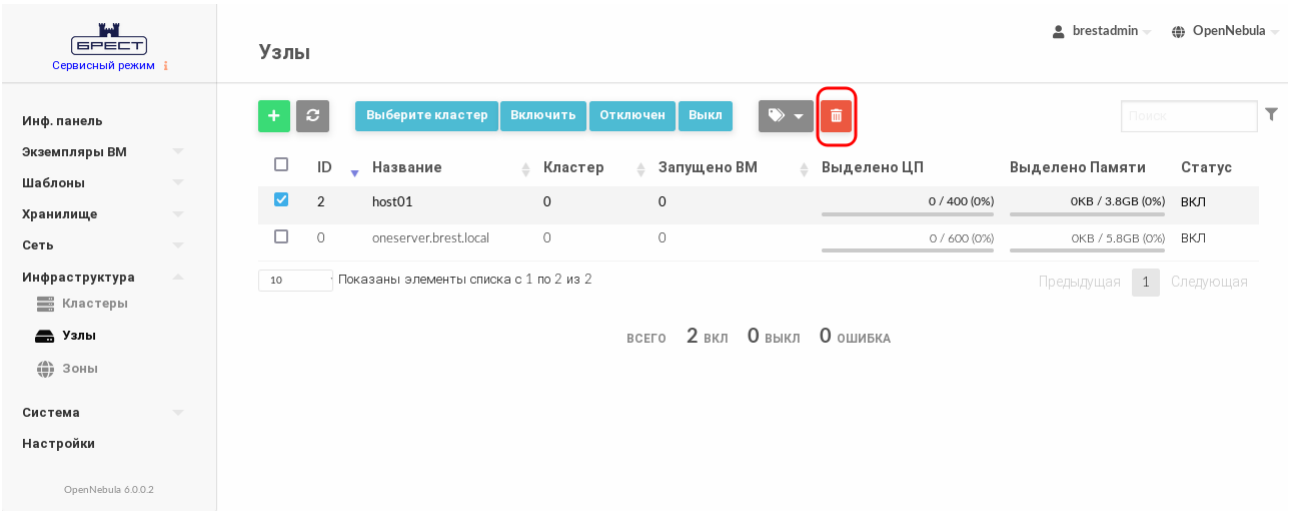

Рис. 4

3) в открывшемся окне нажать на кнопку **[OK]** (см. рис. 5).

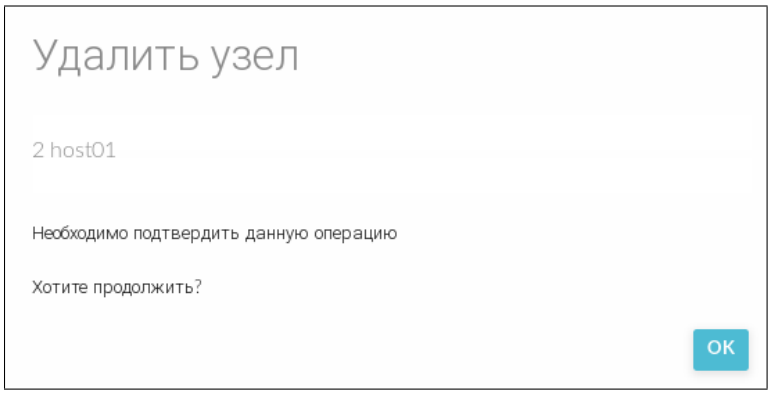

Рис. 5

3.1.5. Мониторинг сервера виртуализации

В ПК СВ используется распределенная система мониторинга. На сервере виртуализации функционирует агент мониторинга, который с заданной периодичностью выполняет тесты и отсылает собранные данные службе `onemonitord` на сервере управления.

Примечание. Функционирование системы мониторинга ПК СВ описано в документе РДЦП.10001-03 95 01-1.

Информация мониторинга, собранная в ходе выполнения тестов, содержит значения параметров, приведенных в таблице 3.

Таблица 3

Параметр	Описание
`HYPERVISOR`	Название гипервизора сервера виртуализации, применяется для выбора серверов виртуализации с определенной технологией
`ARCH`	Архитектура ЦП сервера виртуализации, например, x86_64
`MODELNAME`	Название модели ЦП сервера виртуализации, например, Intel(R) Core(TM) i7-2620M CPU @ 2.70GHz

Продолжение таблицы 3

Параметр	Описание
CPUSPEED	Частота ЦП в МГц
HOSTNAME	Сетевое имя сервера виртуализации (в соответствии с ответом на команду hostname)
VERSION	Версия тестовых программ. Используются для контроля локальных изменений и обновления
MAX_CPU	Количество ЦП, умноженное на 100. Например, значение для машины с 16 ядрами будет составлять 1600. Кроме того, это значение отображается в виде параметра CPU TOTAL в секции HOST SHARE после выполнения команды onehost show (см. 3.1.2.1)
MAX_MEM	Максимальное количество памяти, которое может использоваться для ВМ. Кроме того, это значение отображается в виде параметра MEMORY TOTAL в секции HOST SHARE после выполнения команды onehost show (см. 3.1.2.1)
MAX_DISK	Общий объем пространства хранилища в МБ
USED_CPU	Процент используемой мощности ЦП, умноженной на количество ядер. Кроме того, это значение отображается как CPU USED в секции HOST SHARE после выполнения команды onehost show (см. 3.1.2.1)
USED_MEM	Используемая память, в килобайтах. Кроме того, это значение отображается в виде параметра MEMORY USED (REAL) в секции HOST SHARE после выполнения команды onehost show (см. 3.1.2.1)
USED_DISK	Используемый объем пространства хранилища в МБ
FREE_CPU	Процент неиспользуемой мощности ЦП, умноженной на количество ядер. Например, если в 4-ядерной машине не используются 50% мощности ЦП, значение данного параметра составит 200
FREE_MEM	Память, доступная для ВМ на данный момент, в КБ
FREE_DISK	Объем свободного пространства хранилища в МБ
CPU_USAGE	Общая мощность ЦП, распределенная среди ВМ, запущенных на данном сервере виртуализации в соответствии с запросом, который указан в параметре CPU в каждом шаблоне ВМ. Кроме того, это значение отображается в виде параметра CPU USED (ALLOCATED) в секции HOST SHARE после выполнения команды onehost show (см. 3.1.2.1)
MEM_USAGE	Общая память, распределенная среди ВМ, запущенных на данном сервере виртуализации в соответствии с запросом, который указан в параметре MEMORY в каждом шаблоне ВМ. Кроме того, это значение отображается в виде параметра MEMORY USED (ALLOCATED) в секции HOST SHARE после выполнения команды onehost show (см. 3.1.2.1)
DISK_USAGE	Общий размер образов диска для ВМ, запущенных на сервере виртуализации, рассчитанный с применением параметра SIZE каждого образа с учетом характеристик хранилища
NETRX	Объем входящего сетевого трафика
NETTX	Объем исходящего сетевого трафика
WILD	Перечень ВМ, разделенных запятой, работающих на сервере виртуализации и которые не были запущены службами ПК СВ и не контролируются в данный момент

Окончание таблицы 3

Параметр	Описание
ZOMBIES	Перечень ВМ, разделенных запятой, работающих на сервере виртуализации и которые были запущены службами ПК СВ, но в данный момент им не контролируются

3.1.6. Пользовательские метки сервера виртуализации и стратегии планирования

Кроме значений параметров, получаемых в ходе выполнения тестов системы мониторинга (см. таблицу 3), можно получать значения пользовательских меток сервера виртуализации. Администратор может добавлять пользовательские метки путем создания дополнительного теста для сервера виртуализации, либо обновляя информацию о сервере виртуализации через команду `onehost update`. Например, чтобы пометить сервер виртуализации как «боевой» (production), нужно добавить пользовательскую метку `TYPE` командой:

```
onehost update
...
TYPE="production"
```

В дальнейшем данная метка может использоваться в целях планирования путем добавления следующего раздела в шаблон виртуальной машины (ВМ):

```
SCHED_REQUIREMENTS="TYPE=\"production\""
```

Использование данной метки в шаблоне ограничит развертывание ВМ только серверами виртуализациих с меткой TYPE=production. Для определения требований планирования можно использовать любой признак, указанный при выполнении команды `onehost show`. Более подробная информация о планировании приведена в разделе 4.

Данная функция полезна для разделения последовательности серверов виртуализации или маркировки некоторых специальных особенностей различных серверов виртуализации. Эти значения можно впоследствии использовать для планировки таких же особенностей, как и те, которые были добавлены контролирующими датчиками, в качестве требования для размещения.

3.1.7. Импорт неконтролируемых виртуальных машин

Система мониторинга в ПК СВ сообщает обо всех найденных в гипервизоре виртуальных машинах, в том числе не запущенных посредством ПК СВ (параметр `WILD` — см. 3.1.5). Такие виртуальные машины называются неконтролируемыми и могут быть импортированы для управления через ПК СВ. Это относится ко всем поддерживаемым гипервизорам, в том числе гибридным.

После импорта виртуальной машины ее состояние, включая создание снимков

(snapshots), можно контролировать через службы ПК СВ. Однако некоторые операции не могут быть выполнены на импортированной виртуальной машине, в том числе: отключение питания, отмена развертывания, перемещение, удаление или восстановление.

3.1.7.1. Импорт неконтролируемых ВМ в интерфейсе командной строки

Для обнаружения неконтролируемых виртуальных машин используется команда:

```
onehost show <идентификатор_сервера_виртуализации>
```

Пример

Пример вывода после выполнения команды `onehost show 3`:

```
HOST 3 INFORMATION
ID                    : 3
NAME                  : host03
CLUSTER               : default
STATE                 : MONITORED
[...]
WILD VIRTUAL MACHINES
NAME            IMPORT_ID                               CPU     MEMORY
Ubuntu14.04VM   4223f951-243a-b31a-018f-390a02ff5c96    1       2048
CentOS7         422375e7-7fc7-4ed1-e0f0-fb778fe6e6e0    1       2048
```

Для импорта неконтролируемых виртуальных машин используется команда:

```
onehost importvm <идентификатор_сервера_виртуализации> <наименование_ВМ>
```

3.1.7.2. Импорт неконтролируемых ВМ в веб-интерфейсе ПК СВ

Для отображения неконтролируемых виртуальных машин в веб-интерфейсе ПК СВ необходимо:

1) в меню слева выбрать пункт меню «Инфраструктура — Узлы»;
2) на открывшейся странице «Узлы» выбрать необходимый сервер виртуализации;
3) на открывшейся странице сервера виртуализации открыть вкладку «ВМ вне» (см. рис. 6).

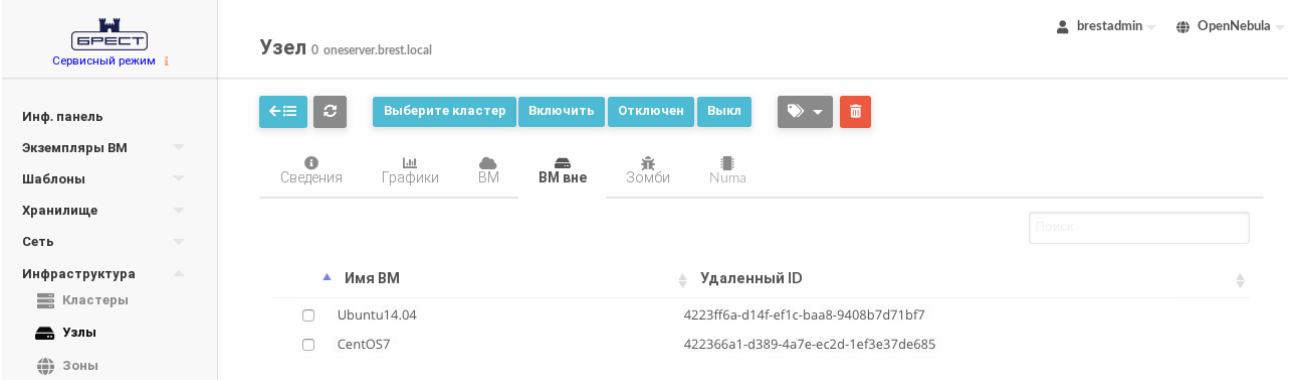

Рис. 6

3.2. Кластеры

Кластер представляет собой группу серверов виртуализации. В зависимости от настроек кластеры могут иметь общие хранилища и сети.

3.2.1. Управление кластером

3.2.1.1. В интерфейсе командной строки

Управление кластерами в интерфейсе командной строки осуществляется с помощью команды `onecluster`:

1) для создания нового кластера используется команда:

```
onecluster create <наименование_кластера>
```

2) чтобы просмотреть перечень кластеров, необходимо использовать команду:

```
onecluster list
```

3) для отображения информации о конкретном кластере необходимо использовать команду:

```
onecluster show <наименование_кластера>
```

Примеры:

1. Создание кластера с наименованием «production»:

```
onecluster create production
```

Пример вывода после выполнения команды:

```
ID: 100
```

2. Просмотр перечня кластеров:

```
onecluster list
```

Пример вывода после выполнения команды:

```
ID   NAME         HOSTS  VNETS   DATASTORES
100  production       0      0            0
0    default          1      1            3
```

3. Просмотр информации о кластере с наименованием «production»:

```
onecluster show production
```

Пример вывода после выполнения команды:

```
CLUSTER 100 INFORMATION
ID                : 100
NAME              : production

CLUSTER RESOURCES

CLUSTER TEMPLATE
RESERVED_CPU=""
RESERVED_MEM=""
```

```
HOSTS
VNETS
DATASTORES
```

3.2.1.2. В веб-интерфейсе ПК СВ

Для отображения перечня всех кластеров в веб-интерфейсе ПК СВ необходимо в меню слева выбрать пункт меню «Инфраструктура — Кластеры». На открывшейся странице «Кластеры» будет представлена таблица кластеров, аналогичная таблице, отображаемой в интерфейсе командной строки после выполнения команды `onecluster list`.

Для отображения информации об конкретном кластере на странице «Кластеры» необходимо выбрать соответствующий кластер. После этого откроется страница с информацией о кластере (см. рис. 7).

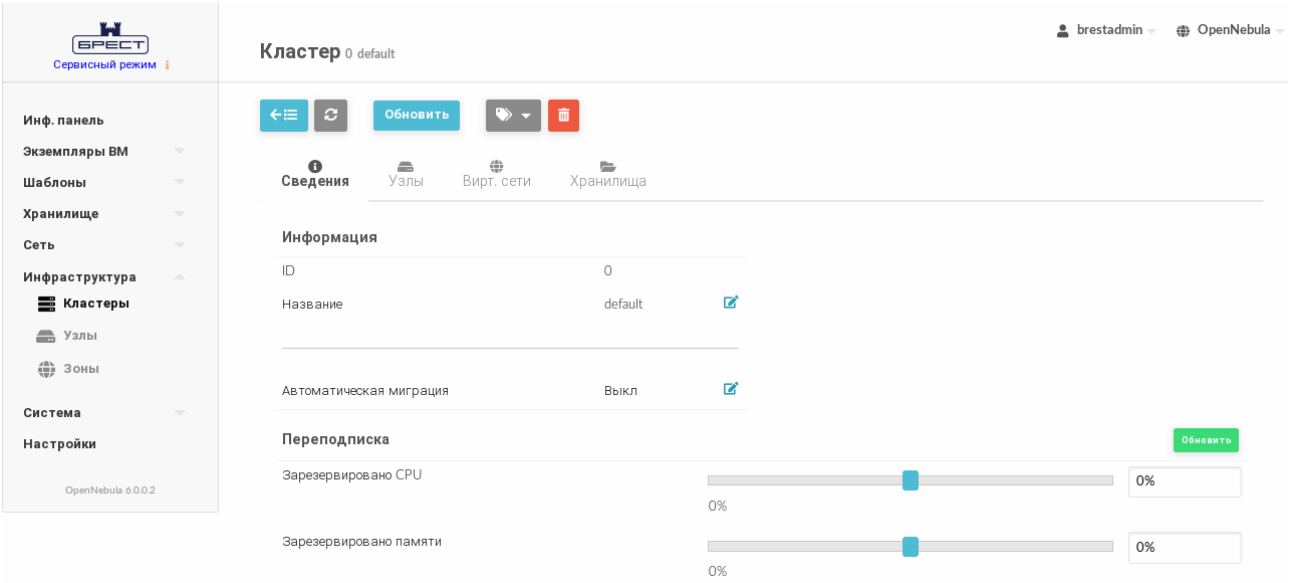

Рис. 7

3.2.2. Добавление серверов виртуализации к кластеру

3.2.2.1. В интерфейсе командной строки

Серверы виртуализации можно регистрировать непосредственно в кластере с помощью команды `onehost create` (см. 3.1.1.1), указав в команде аргумент `--cluster <идентификатор/наименование_кластера>`.

Чтобы добавить сервер виртуализации в кластер необходимо выполнить команду:

```
onecluster addhost  <идентификатор/наименование_кластера> \
    <идентификатор/наименование_сервера_виртуализации>
```

Одновременно сервер виртуализации может находиться только в одном кластере.

Для исключения сервера виртуализации из кластера используется команда:

```
onecluster delhost  <идентификатор/наименование_кластера> \
```

<идентификатор/наименование_сервера_виртуализации>

Так как сервер виртуализации должен принадлежать какому-либо кластеру, то после исключения из определенного кластера он будет перемещен в кластер по умолчанию (с наименованием «default»).

Примеры:

1. Добавление сервера виртуализации с наименованием «host01» в кластер с наименованием «production»:

```
onecluster addhost production host01
```

Для просмотра информации о принадлежности сервера виртуализации кластеру можно воспользоваться командой `onehost list`. Пример вывода после выполнения команды:

```
ID NAME            CLUSTER    TVM  ALLOCATED_CPU   ALLOCATED_MEM  STAT
1  host01          production 0    0 / 400 (0%)    0K / 3.8G (0%) dsbl
0  brest-service   default    0    0 / 600 (0%)    0K / 5.8G (0%) on
```

2. Просмотр информации о кластере с наименованием «production» после добавления сервера виртуализации:

```
onecluster show production
```

Пример вывода после выполнения команды:

```
CLUSTER 100 INFORMATION
ID                  : 100
NAME                : production

CLUSTER RESOURCES
TOTAL CPUs: 4
OCCUPIED CPUs: 0
AVAILABLE CPUs: 4

TOTAL RAM: 3
OCCUPIED RAM: 0
AVAILABLE RAM: 3

CLUSTER TEMPLATE
RESERVED_CPU=""
RESERVED_MEM=""

HOSTS
1
VNETS
```

```
DATASTORES
```

3.2.2.2. В веб-интерфейсе ПК СВ

Чтобы в веб-интерфейсе ПК СВ добавить сервер виртуализации в кластер, необходимо:

1) в меню слева выбрать пункт меню «Инфраструктура — Узлы»;
2) на открывшейся странице «Узлы» выделить необходимый сервер виртуализации и нажать на кнопку **[Выберите кластер]**;
3) в открывшемся окне выбрать необходимый кластер и нажать на кнопку **[OK]** (см. рис. 8).

Рис. 8

3.2.3. Добавление ресурсов к кластеру

В кластере можно зарегистрировать хранилища и сети. В этом случае если в шаблоне ВМ определены идентификаторы этих хранилищ и/или сетей, то ВМ может быть запущена на любом сервере виртуализации кластера. Хранилища и сети можно регистрировать одновременно в нескольких кластерах.

Для добавления/удаления сети используется команда:

```
onecluster addvnet / delvnet  <идентификатор/наименование_кластера> \
   <идентификатор/наименование_сети>
```

Для добавления/удаления хранилища используется команда:

```
onecluster adddatastore / deldatastore  <идентификатор/наименование_кластера> \
   <идентификатор/наименование_сервера_виртуализации>
```

Примеры:

1. Добавление в кластер с наименованием «production» сети и хранилища образов:

```
onecluster addvnet production priv-ovswitch
onecluster adddatastore production iscsi
```

2. Просмотр информации о кластере с наименованием «production» после добавления сети и хранилища образов:

```
onecluster show production
```

Пример вывода после выполнения команды:

```
CLUSTER 100 INFORMATION
ID                : 100
NAME              : production

CLUSTER RESOURCES
TOTAL CPUs: 4
OCCUPIED CPUs: 0
AVAILABLE CPUs: 4

TOTAL RAM: 3
OCCUPIED RAM: 0
AVAILABLE RAM: 3

CLUSTER TEMPLATE
RESERVED_CPU=""
RESERVED_MEM=""

HOSTS

VNETS
1
DATASTORES
100
```

3.2.4. Планирование и кластеры

3.2.4.1. Автоматические требования

Когда ВМ использует ресурсы (образы или виртуальные сети) из кластера, ПК СВ добавляет следующее требование к шаблону:

```
AUTOMATIC_REQUIREMENTS="CLUSTER_ID = 100"
```

Поэтому при попытке использовать ресурсы, не принадлежащие одному и тому же кластеру, создание ВМ завершится неудачей с выводом на экран сообщения, аналогичного следующему:

```
onetemplate instantiate 0
[TemplateInstantiate] Error allocating a new virtual machine. Incompatible /
   cluster IDs.
DISK [0]: IMAGE [0] from DATASTORE [1] requires CLUSTER [101]
```

```
NIC [0]: NETWORK [1] requires CLUSTER [100]
```

3.2.4.2. Требования и ранг

Параметры размещения SCHED_REQUIREMENTS и SCHED_RANK, используемые в планировщике (см. раздел 4) могут использовать параметры из шаблона кластера.

Пример

Просмотр информации о сервера виртуализациих, пример вывода после выполнения команды onehost list:

```
ID  NAME    CLUSTER         ALLOCATED CPU   ALLOCATED MEM  STAT
1   host01  cluster_a 0 0 / 200 (0%) 0K   / 3.6G (0%)      on
2   host02  cluster_a 0 0 / 200 (0%) 0K   / 3.6G (0%)      on
3   host03  cluster_b 0 0 / 200 (0%) 0K   / 3.6G (0%)      on
```

Просмотр информации о кластере, пример вывода после выполнения команды onecluster show cluster_a:

```
...
CLUSTER TEMPLATE QOS="GOLD"
...
```

Просмотр информации о сервере виртуализации, пример вывода после выполнения команды onecluster show cluster_b:

```
...
CLUSTER TEMPLATE QOS="SILVER"
...
```

Для приведенного выше примера можно использовать следующие выражения:

```
SCHED_REQUIREMENTS="QOS=GOLD"
SCHED_REQUIREMENTS="QOS!=GOLD&HYPERVISOR=kvm"
```

4. ПЛАНИРОВЩИК

Планировщик отвечает за распределение виртуальных машин, ожидающих запуска, между зарегистрированными серверами виртуализации. Кроме того, планировщик используется для эффективного распределения дисков виртуальных машин между несколькими системными хранилищами, а также для распределения сетевых интерфейсов ВМ между доступными виртуальными сетями.

В ПК СВ планировщик реализован в виде службы `opennebula-scheduler`, которая разворачивается автоматически при установке и инициализации службы сервера управления.

Действия по настройке планировщика осуществляются администратором ПК СВ.

4.1. Настройка планировщика

4.1.1. Общие параметры планировщика

Действия планировщика настраиваются с целью адаптации под определенную инфраструктуру. Значения параметров планировщика определяются в конфигурационном файле `/etc/one/sched.conf`. Для настройки действий планировщика используются параметры, приведенные в таблице 4.:

Таблица 4

Параметр	Описание
`ONE_XMLRPC`	Адрес для подключения к API службы управления ПК СВ по протоколу XML-RPC (по умолчанию `http://localhost:2633/RPC2`)
`MESSAGE_SIZE`	Размер буфера в байтах для откликов XML-RPC (по умолчанию 1073741824)
`TIMEOUT`	Время ожидания в секундах для откликов XML-RPC (по умолчанию 60)
`SCHED_INTERVAL`	Интервал между итерациями действий планирования в секундах (по умолчанию 15)
`MAX_VM`	Максимальное количество виртуальных машин, задействованных в каждом действии планирования (по умолчанию 5000). Для планирования всех ожидающих ВМ использовать значение «0»
`MAX_DISPATCH`	Максимальное количество виртуальных машин, фактически отправленных на сервер виртуализации в каждом действии планирования (по умолчанию 30)
`MAX_HOST`	Максимальное количество виртуальных машин, отправленных на определенный сервер виртуализации в каждом действии планирования (по умолчанию 1)
`LIVE_RESCHEDS`	Режим миграции, может принимать следующие значения: «1» — перемещение работающих ВМ (установлено по умолчанию); «0» — перемещение выключенных ВМ

Окончание таблицы 4

Параметр	Описание
COLD_MIGRATE_MODE	Режим выключения ВМ перед перемещением, может принимать следующие значения: «0» — режим save, выключение с сохранением состояния ВМ (установлено по умолчанию); «1» — режим poweroff, корректное выключение ВМ без сохранения состояния; «2» — режим poweroff-hard, принудительное выключение ВМ без сохранения состояния
DEFAULT_SCHED	Блок параметров стратегии размещения (подробнее — см. 4.1.2)
DEFAULT_DS_SCHED	Блок параметров стратегии хранения (подробнее — см. 4.1.3)
DEFAULT_NIC_SCHED	Блок параметров стратегии использования сетей (подробнее — см. 4.1.4)
LOG	Блок параметров для настройки регистрации событий планировщика. Содержит следующие параметры: 1) SYSTEM — тип системы регистрации, возможные значения: - file — регистрация в файл /var/log/one/sched.log (установлено по умолчанию), - syslog — регистрация в системный журнал, - std — регистрация в стандартный поток ошибок; 2) DEBUG_LEVEL — уровень протоколирования, возможные значения: - «0» — регистрировать сообщения об ошибках, - «1» — регистрировать предупреждения, - «2» — регистрировать информационные сообщения, - «3» — регистрировать общие отладочные сообщения (установлено по умолчанию), - «4» — регистрировать отладочные сообщения, включая дату и время каждой итерации перемещения, - «5» — регистрировать подробные отладочные сообщения

Оптимальные значения параметров планировщика зависят от объема системы хранения, вычислительной мощности и количества физических серверов виртуализации. Значения параметров можно получить путем выяснения максимального количества виртуальных машин, которые могут быть запущены без возникновения ошибок в имеющейся конфигурации ПК СВ.

После внесения изменений в конфигурационный файл необходимо перезагрузить службу планировщика командой:

```
sudo systemctl restart opennebula-scheduler
```

Конфигурацию стратегий планирования можно настроить в двух местах:

- для каждой ВМ в соответствии с определением параметров SCHED_RANK и SCHED_DS_RANK в шаблоне ВМ;

- для всех виртуальных машин в целом — в файле /etc/one/sched.conf (требуется перезапуск службы opennebula-scheduler).

4.1.2. Настройка стратегии размещения

Стратегия размещения применяется для эффективного распределения виртуальных машин между серверами виртуализации.

4.1.2.1. Параметры стратегии размещения

Для настройки стратегии размещения в конфигурационном файле `/etc/one/sched.conf` используется блок `DEFAULT_SCHED`, в котором определены значения следующих параметров:

- `RANK` — арифметическое выражение для ранжирования подходящих серверов виртуализации в зависимости от их производительности (используется при настройке пользовательской стратегии размещения);
- `POLICY` — номер используемой стратегии размещения (см. таблицу 5).

Таблица 5

Стратегия	Описание
0	Предустановленная стратегия вида «Уплотнение»: свести к минимуму количество используемых серверов виртуализации за счет уплотнения ВМ на сервере виртуализации
1	Предустановленная стратегия вида «Распределение»: свести к максимуму количество доступных для ВМ ресурсов путем распределения ВМ на серверах виртуализации (установлено по умолчанию)
2	Предустановленная стратегия вида «С учетом нагрузки»: свести к максимуму количество доступных для ВМ ресурсов путем размещения ВМ на сервере виртуализации с меньшей нагрузкой
3	Пользовательская стратегия: для размещения ВМ выбирается сервер виртуализации в соответствии с правилом, заданным в параметре `RANK`
4	Предустановленная стратегия вида «Фиксированная»: серверы виртуализации будут ранжироваться в соответствии со значением параметра `PRIORITY` (приоритет), заданном в шаблоне сервера виртуализации или кластера

4.1.2.2. Особенности ранжирования серверов виртуализации

При развертывании ВМ для каждого сервера виртуализации вычисляется значение ранга. Таким образом обеспечивается выбор наилучшего сервера виртуализации для запуска ВМ.

Ранг сервера виртуализации вычисляется в соответствии с арифметическим выражением, заданным в параметре `RANK`. В качестве операндов такого выражения выступают числовые константы и параметры серверов виртуализации, значения которых собираются информационными драйверами системы мониторинга или задаются вручную в шаблоне сервера виртуализации. Для вычисления значения ранга допускается использовать следующие арифметические операции:

- «+» — сложение;

- «-» — вычитание;
- «*» — умножение;
- «/» — деление.

При вычислении ранга используется арифметика с плавающей запятой, однако результат округляется до целого числа.

Арифметическое выражение может состоять только из одного параметра.

Пример

Высший ранг имеет сервер виртуализации с наибольшим количеством работающих ВМ: `RANK=RUNNING_VMS`

Кроме того, в качестве значения ранга могут выступать отрицательные числа.

Пример

Высший ранг имеет сервер виртуализации с наименьшим количеством работающих ВМ: `RANK="- RUNNING_VMS"`

4.1.2.3. Предустановленные стратегии размещения

Стратегия вида «Уплотнение»:

- цель: свести к минимуму количество используемых серверов виртуализации;
- эвристическая процедура: плотно разместить ВМ на серверах виртуализации;
- реализация: сначала использовать сервер виртуализации с наибольшим количеством работающих ВМ.

Этой стратегии соответствует следующее арифметическое выражение для ранжирования серверов виртуализации:

```
RANK=RUNNING_VMS
```

Стратегия вида «Распределение»:

- цель: свести к максимуму ресурсы, доступные для ВМ на сервере виртуализации;
- эвристическая процедура: равномерно распределить ВМ на серверах виртуализации;
- реализация: сначала использовать сервер виртуализации с меньшим количеством работающих ВМ.

Этой стратегии соответствует следующее арифметическое выражение для ранжирования серверов виртуализации:

```
RANK="- RUNNING_VMS"
```

Стратегия вида «С учетом нагрузки»:

- цель: свести к максимуму ресурсы, доступные для ВМ на сервере виртуализации;
- эвристическая процедура: использовать серверы виртуализации с меньшей нагрузкой;

- реализация: сначала использовать сервер виртуализации с наибольшим количеством свободных ЦП.

Этой стратегии соответствует следующее арифметическое выражение для ранжирования серверов виртуализации:

```
RANK=FREE_CPU
```

Стратегия вида «Фиксированная»:

- цель: сортировать серверы виртуализации вручную;
- эвристическая процедура: учитывать значение параметра `PRIORITY` (приоритет), заданный в шаблоне сервера виртуализации или кластера;
- реализация: сначала использовать сервер виртуализации с более высоким приоритетом.

Этой стратегии соответствует следующее арифметическое выражение для ранжирования серверов виртуализации:

```
RANK=PRIORITY
```

4.1.2.4. Перепланирование размещения виртуальных машин

ВМ может быть перепланирована без выключения. При выполнении команды `onevm resched` для ВМ устанавливается метка перепланирования. При следующей итерации действий планировщика ВМ будет представлена на перепланирование, если выполняются следующие условия:

- существует подходящий сервер виртуализации для ВМ;
- ВМ еще не запущена на нем.

4.1.2.5. Ограничение ресурсов, предоставляемых сервером виртуализации

Перед назначением ВМ на сервер виртуализации проверяется его доступная вычислительная мощность, чтобы убедиться, что имеющихся ресурсов сервера виртуализации достаточно для развертывания ВМ. Данные о вычислительной мощности передаются агентами мониторинга (см. 3.1.5). Данный алгоритм можно изменить, зарезервировав определенное количество вычислительной мощности (MEMORY и CPU). Для резервирования доступны следующие методы:

- резервирование на уровне кластера при обновлении шаблона кластера (например, с помощью команды `onecluster update`). Все серверы виртуализации кластера зарезервируют одинаковое количество вычислительной мощности;
- резервирование на уровне сервера виртуализации путем обновления шаблона сервера виртуализации (например, с помощью команды `onehost update`). При этом будут заменены значения параметров, которые были указаны на уровне кластера.

В частности, возможно резервирование следующих параметров вычислительной мощности:

- `RESERVED_CPU` в процентах. Будет вычитаться из `TOTAL CPU`;

- RESERVED_MEM в КБ. Будет вычитаться из TOTAL MEM.

Примечание. Данные значения могут быть отрицательными. В этом случае фактически требуется увеличить общую вычислительную мощность, тем самым перегружая сервер виртуализации.

4.1.3. Настройка стратегии хранения

Стратегия хранения применяется для эффективного распределения дисков виртуальных машин между различными системными хранилищами.

ВНИМАНИЕ! Любой сервер виртуализации, принадлежащий определенному кластеру, должен иметь доступ к любому системному хранилищу или хранилищу образа, определенному для данного кластера.

Примечание. Полномочия администратора позволяют развернуть ВМ в определенном системном хранилище, используя команду onevm deploy.

4.1.3.1. Параметры стратегии хранения

Для настройки стратегии размещения в конфигурационном файле /etc/one/sched.conf используется блок DEFAULT_DS_SCHED, в котором определены значения следующих параметров:

- RANK — арифметическое выражение для ранжирования подходящих хранилищ в зависимости от их параметров (используется при настройке пользовательской стратегии хранения);
- POLICY — номер используемой стратегии хранения (см. таблицу 6).

Таблица 6

Стратегия	Описание
0	Предустановленная стратегия вида «Уплотнение»: попытаться свести к минимуму количество используемых системных хранилищ;
1	Предустановленная стратегия вида «Распределение»: оптимизация операций ввода-вывода путем равномерного распределения дисков виртуальных машин между системными хранилищами (установлено по умолчанию)
2	Пользовательская стратегия: для размещения диска ВМ выбирается системное хранилище в соответствии с правилом, заданным в параметре RANK
4	Предустановленная стратегия вида «Фиксированная»: системные хранилища будут ранжироваться в соответствии со значением параметра PRIORITY (приоритет), заданном в шаблоне системного хранилища

4.1.3.2. Особенности ранжирования системных хранилищ

При размещении диска ВМ для каждого системного хранилища вычисляется значение ранга. Таким образом обеспечивается выбор наилучшего системного хранилища для размещении диска ВМ.

Ранг системного хранилища вычисляется в соответствии с арифметическим выра-

жением, заданным в параметре RANK. В качестве операндов такого выражения выступают числовые константы и параметры системных хранилищ, значения которых собираются информационными драйверами системы мониторинга или задаются вручную в шаблоне системного хранилища. Для вычисления значения ранга допускается использовать следующие арифметические операции:

- «+» — сложение;
- «-» — вычитание;
- «*» — умножение;
- «/» — деление.

При вычислении ранга используется арифметика с плавающей запятой, однако результат округляется до целого числа.

Арифметическое выражение может состоять только из одного параметра.

Пример

Высший ранг имеет системное хранилище с наибольшим количеством свободного места: RANK=FREE_MB

Кроме того, в качестве значения ранга могут выступать отрицательные числа.

Пример

Высший ранг имеет системное хранилище с наименьшим количеством свободного места: RANK="- FREE_MB"

4.1.3.3. Предустановленные стратегии размещения

Стратегия вида «Уплотнение»:

- цель: свести к минимуму количество используемых системных хранилищ;
- эвристическая процедура: плотно разместить ВМ в системных хранилищах;
- реализация: сначала использовать системное хранилище с наименьшим количеством свободного места.

Этой стратегии соответствует следующее арифметическое выражение для ранжирования системных хранилищ:

```
RANK="- FREE_MB"
```

Стратегия вида «Распределение»:

- цель: оптимизация операций ввода-вывода для системы хранения;
- эвристическая процедура: равномерно распределить ВМ между системными хранилищами;
- реализация: сначала использовать системное хранилище с наибольшим количеством свободного места.

Этой стратегии соответствует следующее арифметическое выражение для ранжирования

системных хранилищ:

```
RANK=FREE_MB
```

Стратегия вида «Фиксированная»:

- цель: сортировать хранилища данных вручную;
- эвристическая процедура: учитывать значение параметра PRIORITY (приоритет), заданный в шаблоне системного хранилища;
- реализация: сначала использовать системное хранилище с более высоким приоритетом (PRIORITY).

Этой стратегии соответствует следующее арифметическое выражение для ранжирования системных хранилищ:

```
RANK=PRIORITY
```

4.1.3.4. Перемещение диска ВМ

После размещения образа диска ВМ в системном хранилище администратор может перенести его в другое системное хранилище. Для этого нужно сначала выключить ВМ, затем выполнить команду `onevm migrate`. Новое системное хранилище должно иметь такой же драйвер (параметр `TM_MAD`), что и исходное системное хранилище.

4.1.3.5. Отключение хранилища

Системные хранилища можно отключить, чтобы запретить планировщику развертывать на них новые виртуальные машины. Хранилища в отключенном (disabled) состоянии контролируются планировщиком в штатном режиме, а существующие виртуальные машины продолжают работать.

Пример

Отключение системного хранилища:

```
onedatastore disable system -v
```

Пример вывода после выполнения команды:

```
DATASTORE 0: disabled
```

Просмотр информации о системном хранилище. Пример вывода после выполнения команды `onedatastore show system`:

```
DATASTORE 0 INFORMATION
ID:0
:system
...
:DISABLED
```

4.1.4. Настройка стратегии использования сетей

Данная стратегия применяется для эффективного распределения сетевых интерфейсов ВМ между доступными виртуальными сетями.

4.1.4.1. Параметры стратегии использования сетей

Для настройки стратегии использования сетей в конфигурационном файле `/etc/one/sched.conf` используется блок `DEFAULT_NIC_SCHED`, в котором определены значения следующих параметров:

- `RANK` — логическое (булево) выражение для фильтрации доступных виртуальных сетей (используется при настройке пользовательской стратегии размещения);
- `POLICY` — номер используемой стратегии размещения (см. таблицу 7).

Таблица 7

Стратегия	Описание
0	Предустановленная стратегия вида «Уплотнение»: оптимизация использования адресных пространств путем выбора виртуальной сети с меньшим количеством свободных (арендованных) адресов. Производится ранжирование виртуальных сетей по возрастанию значения параметра `USED_LEASES`
1	Предустановленная стратегия вида «Распределение»: оптимизация использования адресных пространств путем распределения сетевых интерфейсов (арендованных адресов) между доступными виртуальными сетями. Производится ранжирование виртуальных сетей по убыванию значения параметра `USED_LEASES` (установлено по умолчанию)
2	Пользовательская стратегия: виртуальные сети фильтруются в соответствии с правилом, заданным в параметре `RANK`. Затем применяется стратегия вида «Распределение»
3	Предустановленная стратегия вида «Фиксированная»: виртуальные сети будут ранжироваться в соответствии со значением параметра `PRIORITY` (приоритет), заданном в шаблоне виртуальной сети

4.1.4.2. Особенности фильтрации виртуальных сетей

Фильтрации виртуальных сетей осуществляется в соответствии с логическим выражением, заданным в параметре `RANK`. В качестве операндов такого выражения выступают числовые константы и параметры виртуальных сетей, значения которых собираются информационными драйверами системы мониторинга или задаются вручную в шаблоне виртуальной сети. Для фильтрации виртуальных сетей допускается использовать следующие логические операции:

- логические операции с числами:
  - « = » — равно,
  - « != » — не равно,
  - « > » — больше,
  - « < » — меньше,
  - « @> » — содержит (например, массив содержит определенное число);
- логические операции со строками:
  - « = » — строки идентичны,

- « != » — строки не идентичны,
- « @> » — строка содержит.

Логические выражения можно объединять в скобки. Кроме того над выражениями можно выполнять следующие логические операции:

- « & » — конъюнкция (логическое умножение, операция «И»);
- « | » — дизъюнкция (логическое сложение, операция «ИЛИ»);
- « ! » — инверсия (логическое отрицание, операция «НЕ»).

4.2. Алгоритм работы планировщика

В состав планировщика входит программный модуль установления соответствия (mm_sched), реализующий стратегию планирования ранга (Rank Scheduling Policy). Данная стратегия нацелена на определение приоритета ресурсов, подходящих для ВМ.

Алгоритм установления соответствия работает следующим образом:

1) виртуальные машины, для размещения диска которых требуется больше дискового пространства, чем доступно на данный момент, отфильтровываются и остаются в состоянии ожидания (pending);

2) серверы виртуализации, которые не соответствуют требованиям (задаются параметром `SCHED_REQUIREMENTS` в шаблоне ВМ) или не имеют достаточной вычислительной мощности (свободных ЦП и оперативной памяти) для запуска ВМ, отфильтровываются;

3) системные хранилища, которые не соответствуют требованиям (задаются параметром `SCHED_DS_REQUIREMENTS` в шаблоне ВМ) или не имеют достаточного дискового ресурса, отфильтровываются;

4) виртуальные сети, которые не соответствуют требованиям (задаются параметром `SCHED_REQUIREMENTS` в блоке параметров `NIC` шаблона ВМ) или не имеют достаточного количества свободных (арендованных) адресов, отфильтровываются;

5) производится финальная фильтрация и ранжирование серверов виртуализации, системных хранилищ и виртуальных сетей в соответствии со значениями параметров, указанных в следующих источниках (по убыванию приоритета):

- в шаблоне ВМ (используются параметры `SCHED_RANK` и `SCHED_DS_RANK`);
- для всех виртуальных машин в целом — в файле `/etc/one/sched.conf` (используются блоки параметров `DEFAULT_SCHED`, `DEFAULT_DS_SCHED` и `DEFAULT_NIC_SCHED`).

6) при развертывании ВМ в первую очередь используются ресурсы с более высоким рангом.

5. ПОЛЬЗОВАТЕЛИ И ГРУППЫ

5.1. Идентификация и аутентификация пользователей

Сведения о порядке идентификации и аутентификации пользователей и управлении доступом приведены в документе РУСБ.10015-01 97 01.

Идентификация и аутентификация пользователей осуществляется с использованием функций ОС СН.

В сервисном режиме функционирования ПК СВ процедуры идентификации и аутентификации пользователе 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`). Порядок настройки механизма PAM представлен в документе РУСБ.10015-01 97 01-1.

В дискреционном режиме функционирования ПК СВ процедуры идентификации и аутентификации пользователей реализованы посредством службы FreeIPA из состава ОС СН. При этом аутентификация пользователей осуществляется централизованно по протоколу Kerberos. В качестве источника данных для идентификации и аутентификации пользователей применяются службы каталогов LDAP. В этом случае необходимо, чтобы все компьютеры, на которых развернуты программные компоненты ПК СВ, входили в один домен. Порядок настройки службы FreeIPA, в том числе процедур идентификации и аутентификации пользователей, описан в документе РДЦП.10001-03 95 01-1.

5.2. Управление пользователями

Создание и управление учетными записями пользователей (управление пользователями), назначение прав доступа к виртуальным машинам осуществляются администратором ПК СВ.

При развертывании службы сервера управления автоматически создаются следующие группы:

- `brestadmins` — группа администраторов ПК СВ. При этом в этой группе автоматически создаются следующие системные пользователи;
- `oneadmin` — используется для взаимодействия всех программных компонентов ПК СВ;
- `serveradmin` — используется службой веб-интерфейса ПК СВ для взаимодействия с другими программными компонентами ПК СВ;
- `brestusers` — группа пользователей ПК СВ.

ВНИМАНИЕ! Использование системных пользователей oneadmin и serveradmin для интерактивного входа в ОС СН и подключения к веб-интерфейсу ПК СВ заблокировано.

Кроме того, при инициализации службы сервера управления в ПК СВ создается первый пользователь группы администраторов ПК СВ:

- в сервисном режиме функционирования ПК СВ — пользователь `brestadmin`;
- в дискреционном режиме функционирования ПК СВ — доменный пользователь, имя которого указывается вручную при инициализации службы сервера управления.

ПК СВ Брест позволяет разделять виртуальные ресурсы на логические сущности (тенанты). Разделение осуществляется путем создания групп пользователей. Роли определяются внутри каждой группы.

Назначение ролей и полномочий необходимо выполнять в ОС СН под учетной записью администратора с высоким уровнем целостности.

Для реализации роли администратора средства виртуализации необходимо включить пользователя в следующие группы: `brestadmins`, `brestusers`, `libvirt-admins` и `admins` (см. 5.6).

5.2.1. Управление пользователями в интерфейсе командной строки

Для управления пользователями используется инструмент командной строки `oneuser`.

ВНИМАНИЕ! В дискреционном режиме функционирования ПК СВ добавление пользователей необходимо выполнять только в веб-интерфейсе ПК СВ.

В сервисном режиме функционирования ПК СВ для создания нового пользователя используется команда:

```
oneuser create <имя_пользователя> <пароль>
```

ВНИМАНИЕ! В ПК СВ зарезервированы и не могут быть использованы следующие имена пользователей:

- `admin`;
- `brestadmin`;
- `oneadmin`;
- `serveradmin`;

Кроме того, в имени пользователя не допускается использование:

- служебных символов;
- букв в верхнем регистре;
- цифрового знака в начале имени пользователя.

Пароль может быть указан в явном виде или прочитан из файла. Более подробные сведения можно получить, выполнив команду:

```
oneuser create -h
```

По умолчанию будет создан пользователь, принадлежащий группе `brestusers`. Чтобы при создании пользователя указать другую группу, необходимо выполнить команду:

```
oneuser create <имя_пользователя> <пароль> \
   --group <идентификатор/наименование_группы>
```

Чтобы изменить основную группу пользователя (в том числе перенос пользователя в группу `brestadmins`) необходимо выполнить команду:

```
oneuser chgrp <имя_пользователя> <идентификатор/наименование_группы>
```

В качестве имени пользователя можно указать перечень пользователей (идентификаторов или имен, разделенных запятыми) или диапазон идентификаторов пользователей (в качестве разделителя используются две точки — «..»).

Чтобы просмотреть перечень пользователей необходимо выполнить команду:

```
oneuser list
```

Для временной блокировки/разблокировки пользователя необходимо выполнить команду:

```
oneuser disable / enable <идентификатор/имя_пользователя>
```

В качестве имени пользователя можно указать перечень пользователей (идентификаторов или имен, разделенных запятыми) или диапазон идентификаторов пользователей (в качестве разделителя используются две точки — «..»).

Чтобы удалить пользователя необходимо выполнить команду:

```
oneuser delete <идентификатор/имя_пользователя>
```

В качестве имени пользователя можно указать перечень пользователей (идентификаторов или имен, разделенных запятыми) или диапазон идентификаторов пользователей (в качестве разделителя используются две точки — «..»).

ВНИМАНИЕ! В дискреционном режиме функционирования ПК СВ при удалении пользователя его доменная учетная запись сохраняется. Ее необходимо вручную удалить в веб-интерфейсе контролера домена.

Примеры:

1. Создание пользователя с именем «newuser»:

```
oneuser create newuser <ПАРОЛЬ>
```

Пример вывода после выполнения команды:

```
ID: 6
```

2. Просмотр перечня пользователей:

```
oneuser list
```

Пример вывода после выполнения команды:

```
ID NAME       ENAB  GROUP     AUTH        VMS       MEMORY    CPU
6 newuser      yes  brestuse  core        0 / -     0M /      0.0 / -
5 domainuser   yes  brestadm  public      0 / -     0M /      0.0 / -
4 otheradmin   yes  brestadm  core        0 / -     0M /      0.0 / -
3 testuser     yes  brestuse  public      0 / -     0M /      0.0 / -
```

```
2 brest-admin yes  brestadm  public      2 / -     4G /      0.5 / -
1 serveradmin yes  brestadm  server_c    0 / -     0M /      0.0 / -
0 oneadmin    yes  brestadm  core            -         -           -
```

3. Временная блокировка пользователей с идентификаторами от 4 до 6:

```
oneuser disable 4..6
```

4. Удаление пользователя с идентификатором 3:

```
oneuser delete 3
```

5. Просмотр перечня пользователей:

```
oneuser list
```

Пример вывода после выполнения команды:

```
ID NAME        ENAB GROUP     AUTH        VMS       MEMORY    CPU
6 newuser      no   brestuse  core        0 / -     0M /      0.0 / -
5 domainuser   no   brestadm  public      0 / -     0M /      0.0 / -
4 otheradmin   no   brestadm  core        0 / -     0M /      0.0 / -
2 brest-admin  yes  brestadm  public      2 / -     4G /      0.5 / -
1 serveradmin  yes  brestadm  server_c    0 / -     0M /      0.0 / -
0 oneadmin     yes  brestadm  core            -         -           -
```

5.2.2. Управление пользователями в веб-интерфейсе ПК СВ

Для отображения перечня всех пользователей в веб-интерфейсе ПК СВ необходимо в меню слева выбрать пункт «Система — Пользователи». На открывшейся странице «Пользователи» будет представлена таблица пользователей, аналогичная таблице, отображаемой в интерфейсе командной строки после выполнения команды `oneuser list` (см. рис. 9).

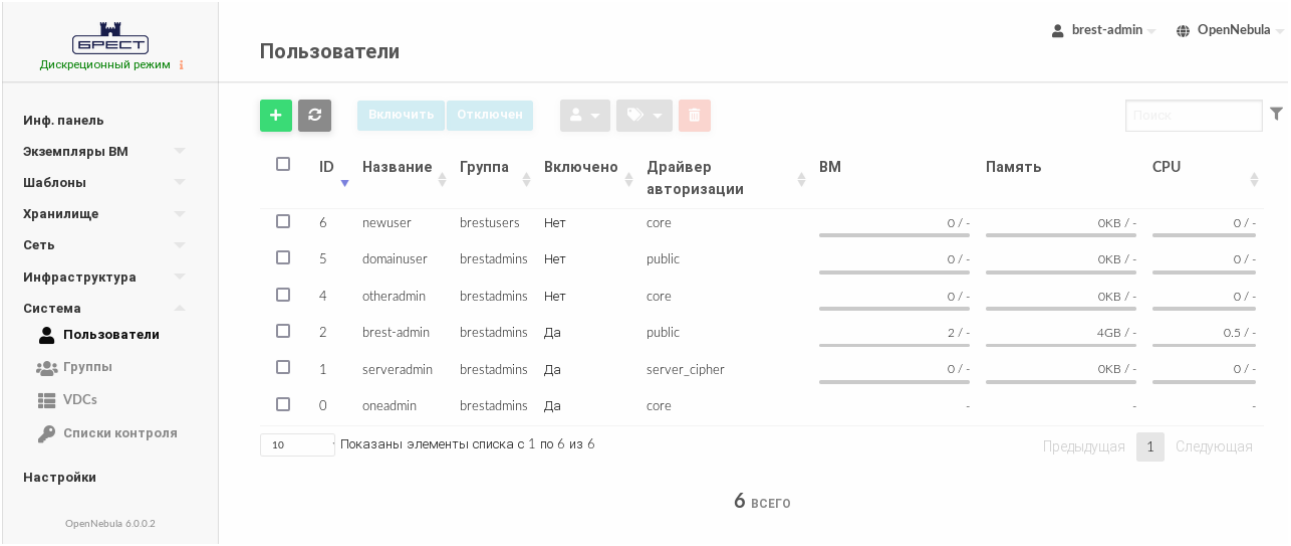

Рис. 9

Для добавления пользователя в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

1) в меню слева выбрать пункт «Система — Пользователи» и на открывшейся странице «Пользователи» нажать на кнопку **[+]**;

2) на открывшейся странице «Создать пользователя» (см. рис. 10) необходимо задать имя и пароль пользователя, а также, при необходимости, указать группу (по умолчанию новый пользователь будет принадлежать группе `brestusers`);

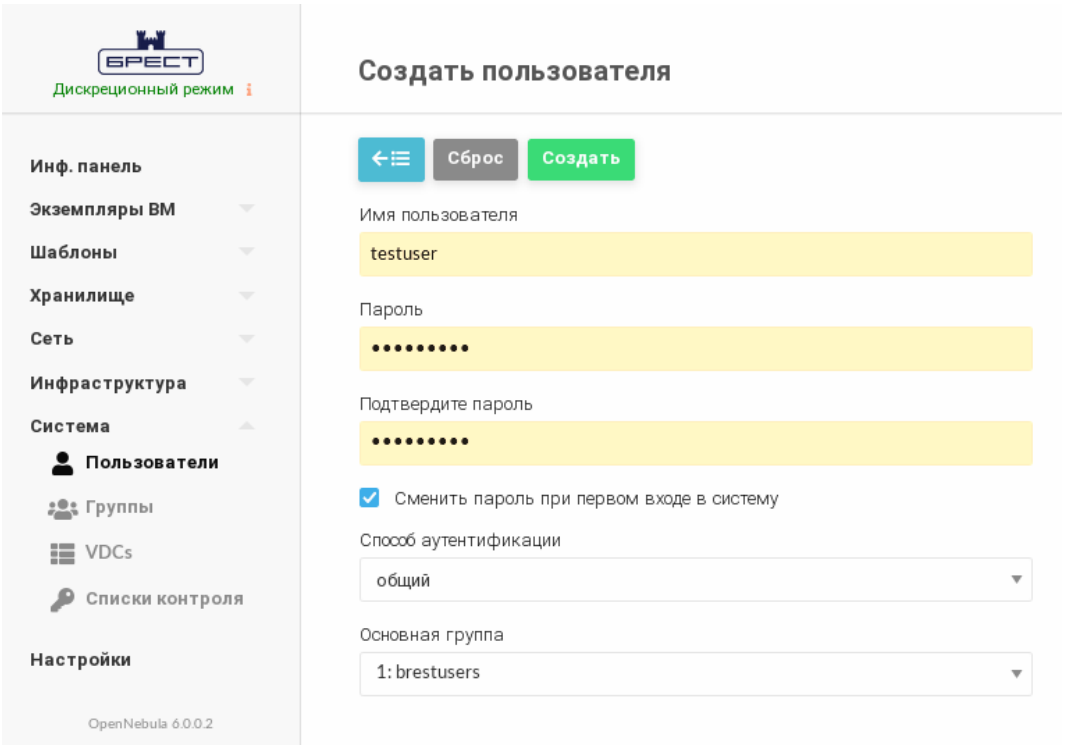

Рис. 10

ВНИМАНИЕ! В ПК СВ зарезервированы и не могут быть использованы следующие имена пользователей:

- admin;
- brestadmin;
- oneadmin;
- serveradmin;

Кроме того, в имени пользователя не допускается использование:

- служебных символов;
- букв в верхнем регистре;
- цифрового знака в начале имени пользователя.

ВНИМАНИЕ! Пароль пользователя должен удовлетворять следующим требованиям сложности:

- пароль пользователя должен содержать не менее 8 символов при алфавите пароля не менее 70 символов;
- максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки — 4.

3) на странице «Создать пользователя» нажать на кнопку **[Создать]**;

После этого на открывшейся странице «Пользователи» появится запись о созданном пользователе.

Примечание. В дискреционном режиме функционирования ПК СВ для нового пользователя будет создана доменная учетная запись (см. рис. 11).

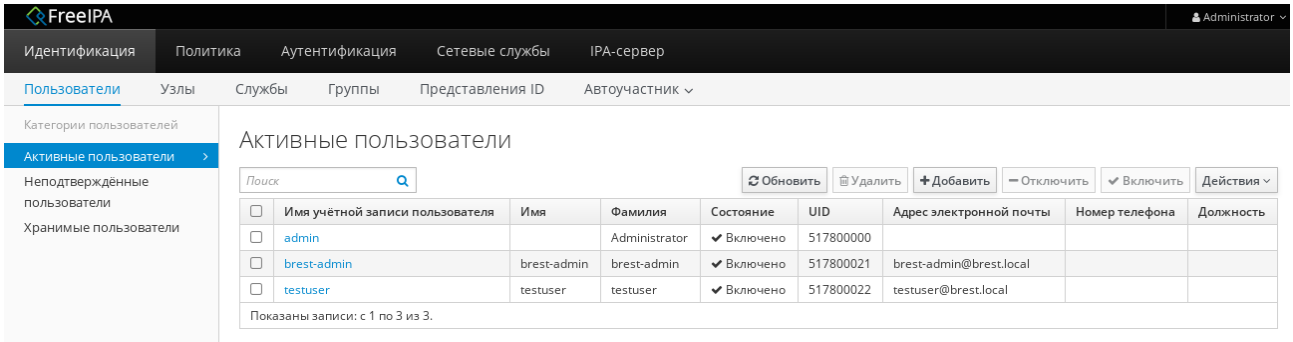

Рис. 11

ВНИМАНИЕ! Если установлен флаг «Сменить пароль при первом входе в систему», созданный пользователь не сможет авторизоваться через веб-интерфейс. Необходимо предварительно изменить пароль этого пользователя.

Первичная смена пароля может быть осуществлена:

- при аутентификации пользователя в ОС сервера управления (как в графическом, так и консольном режиме);
- при аутентификации пользователя через веб-интерфейс контроллера домена

(только в дискреционном режиме функционирования ПК СВ).

В ПК СВ не реализована смена пароля пользователя в следующих случаях:

- при подключении по SSH;
- при управлении учетной записью пользователя в веб-интерфейсе ПК СВ.

Для просмотра информации о конкретном пользователе на странице «Пользователи» необходимо выбрать соответствующую строку. После этого откроется страница пользователя (вкладка «Сведения» — см. рис. 12).

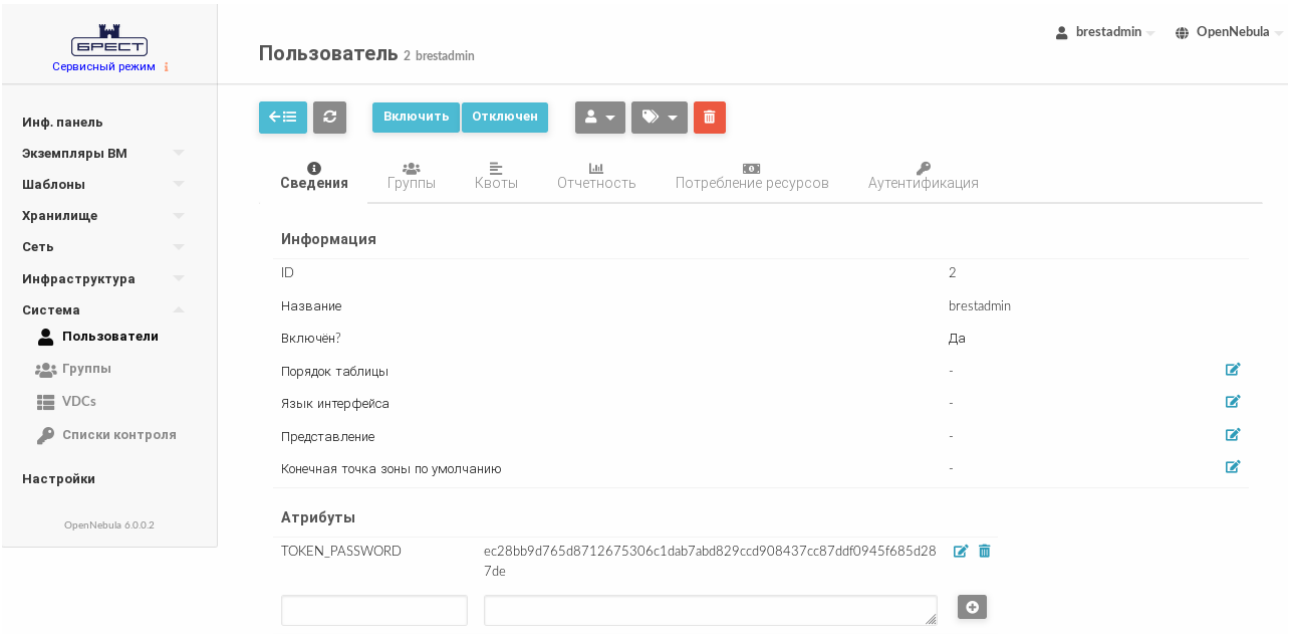

Рис. 12

Для управления учетной записью пользователя в веб-интерфейсе ПК СВ используются следующие элементы интерфейса (см. рис. 13):

1) кнопка **[Отключен]** — для временной блокировки пользователя;
2) кнопка **[Включить]** — для разблокировки пользователя;
3) при нажатии на кнопку **[Группы]** откроется пункт меню «Изменить основную группу»;
4) кнопка **[Удалить]** — для удаления учетной записи пользователя.

Рис. 13

ВНИМАНИЕ! В дискреционном режиме функционирования ПК СВ при удалении пользователя его доменная учетная запись сохраняется. Ее необходимо вручную удалить в веб-интерфейсе контролера домена.

5.3. Управление группами

5.3.1. Общие сведения

Группы в ПК СВ позволяют изолировать пользователей и ресурсы. При этом пользователь может видеть и получить доступ к ресурсам других пользователей группы.

В группах изоляция осуществляется за счет разграничения прав доступа пользователей. Однако, в ПК СВ возможно разделить физические вычислительные ресурсы между группами, используя виртуальные дата-центры (VDC) — см. 5.4.

При добавлении группы можно создать администратора группы — пользователя, обладающего такими же правами что и другие пользователи, но дополнительно он может управлять пользователями в рамках группы.

По умолчанию при создании пользователя он будет включен в группу пользователей ПК СВ (`brestusers`). Создаваемые пользователем ресурсы (образы, ВМ и др.) будут принадлежать этой основной группе. При этом пользователь может входить в несколько групп. Все другие группы называются дополнительными. Пользователю доступны для просмотра ресурсы дополнительных групп.

ВНИМАНИЕ! Группа `brestadmins` не может быть установлена в качестве дополнительной.

Примечание. Пользователя можно включить только в группу пользователей ПК СВ. Группы пользователей, зарегистрированные в ОС СН не доступны.

Включать пользователя в дополнительные группы может только администратор ПК СВ. Однако, пользователи могут менять свою основную группу на любую из дополнительных групп без вмешательства администратора ПК СВ.

Для реализации роли администратора ВМ необходимо включить пользователя в группу `brestusers`.

Для реализации роли разработчика ВМ необходимо выполнить следующие действия:

1) для группы, в которую входит пользователь, предоставить полномочия USE в отношении следующих ресурсов виртуализации: хранилища и виртуальные сети. Для этого создать соответствующее правило ACL командой:

```
{oneacl create "@<идентификатор_группы> NET + DATASTORE /* USE"}
```

2) пользователю предоставить полномочия CREATE и MANAGE в отношении шаблонов ВМ. Для этого создать соответствующее правило ACL командой:

```
oneacl create "#<идентификатор_пользователя> TEMPLATE/* CREATE+MANAGE"
```

Если пользователь совмещает роли разработчика ВМ и администратора ВМ, то необходимо выполнить следующие действия:

1) пользователю предоставить полномочия MANAGE в отношении серверов виртуализации. Для этого создать соответствующее правило ACL командой:

```
oneacl create "#<идентификатор_пользователя> HOST /* MANAGE"
```

2) пользователю предоставить полномочия CREATE в отношении остальных ресурсов виртуализации. Для этого создать соответствующее правило ACL командой:

```
oneacl create "#<идентификатор_пользователя> \
VM+IMAGE+TEMPLATE+DOCUMENT+SECGROUP+VROUTER+VMGROUP /* CREATE"
```

5.3.2. Управление группами в интерфейсе командной строки

Для управления группами используется инструмент командной строки `onegroup`. Чтобы создать группу, необходимо выполнить команду:

```
onegroup create <наименование_группы>
```

Примечание. При создании новой группы создается и новое правило ACL, чтобы установить стандартный алгоритм, позволяющий пользователям создавать ресурсы. Подробная информация о правилах ACL приведена в 5.6.

Чтобы при создании группы автоматически создать администратора группы, необходимо выполнить команду:

```
onegroup create <наименование_группы> \
   --admin_user <имя_администратора_группы> --admin_password <пароль>
```

Чтобы пользователю группы присвоить / отозвать права администратора группы, необходимо выполнить команду:

```
onegroup addadmin / deladmin <наименование_группы> \
   <идентификатор_пользователя>
```

В качестве наименование группы можно указать перечень групп (идентификаторов или наименований, разделенных запятыми) или диапазон идентификаторов групп (в качестве разделителя используются две точки — «..»).

Чтобы при создании группы определить к каким ресурсам пользователей группы будут иметь доступ другие пользователи этой группы, необходимо при выполнении команды `onegroup create` дополнительно указать аргумент `- - resources` и перечислить общие ресурсы, разделяя их знаком «+».

```
onegroup create <наименование_группы> \
--admin_user <имя_администратора_группы> --admin_password <пароль>
```

Примеры:

1. Создание группы с наименованием «new group»:

```
onegroup create "new group"
```

Пример вывода после выполнения команды:

```
ID: 100
```

2. Создание группы с одновременным созданием администратора группы:

```
onegroup create --name groupA \
   --admin_user admin_userA --admin_password <ПАРОЛЬ>
```

Пример вывода после выполнения команды:

```
ID: 101
```

3. Просмотр перечня групп:

```
onegroup list
```

Пример вывода после выполнения команды:

```
ID  NAME          USERS   VMS     MEMORY   CPU
101 groupA        1     0 / -   0M / -   0.0 / -
100 new group     0     0 / -   0M / -   0.0 / -
1   brestusers    0     0 / -   0M / -   0.0 / -
0   brestadmins   3         -       -        -
```

4. Создание группы с указанием следующих ресурсов: ВМ, образы и шаблоны в качестве общих:

```
onegroup create --name another-group --resources VM+IMAGE+TEMPLATE
```

Пример вывода после выполнения команды:

```
ID: 102
```

Чтобы изменить основную группу пользователя (в том числе в качестве основной указать группу `brestadmins`), необходимо выполнить команду:

```
oneuser chgrp <имя_пользователя> <идентификатор/наименование_группы>
```

Пользователь всегда должен принадлежать основной группе. Для исключения пользователя из, например, группы администраторов, необходимо переместить его в стандартную группу `brestusers`.

Чтобы включить пользователя в дополнительную группу или исключить его из дополнительной группы, необходимо выполнить команду:

```
oneuser addgroup /  delgroup <имя_пользователя> \
   <идентификатор/наименование_группы>
```

В качестве имени пользователя можно указать перечень пользователей (идентификаторов или имен, разделенных запятыми) или диапазон идентификаторов пользователей (в качестве разделителя используются две точки — «..»).

5.3.3. Управление группами в веб-интерфейсе ПК СВ

Для отображения перечня всех групп в веб-интерфейсе ПК СВ необходимо в меню слева выбрать пункт «Система — Группы». На открывшейся странице «Группы» будет представлена таблица групп, аналогичная таблице, отображаемой в интерфейсе командной строки после выполнения команды `onegroup list` (см. рис. 14).

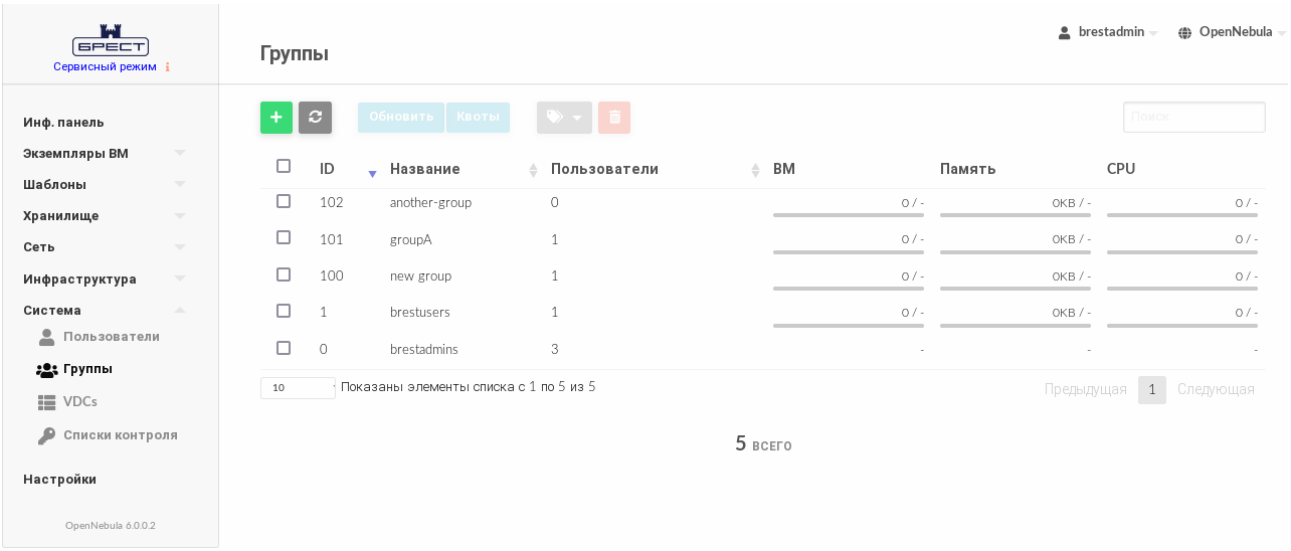

Рис. 14

Для добавления группы в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

1) в меню слева выбрать пункт «Система — Группы» и на открывшейся странице «Группы» нажать на кнопку **[+]**;

2) на открывшейся странице «Создать группу»:

а) во вкладке «Общие» задать наименование группы,

б) если необходимо создать администратора группы, во вкладке «Администрирование» установить флаг «Создать пользователя с административными правами», задать имя и пароль пользователя,

в) во вкладке «Права» указать общие ресурсы, установив соответствующие флаги;

3) на странице «Создать группу» нажать на кнопку **[Создать]**;

После этого на открывшейся странице «Группы» появится запись о созданной группе.

Для просмотра информации о конкретной группе на странице «Группы» необходимо выбрать соответствующую строку. После этого откроется страница «Группа» (вкладка «Сведения» — см. рис. 15).

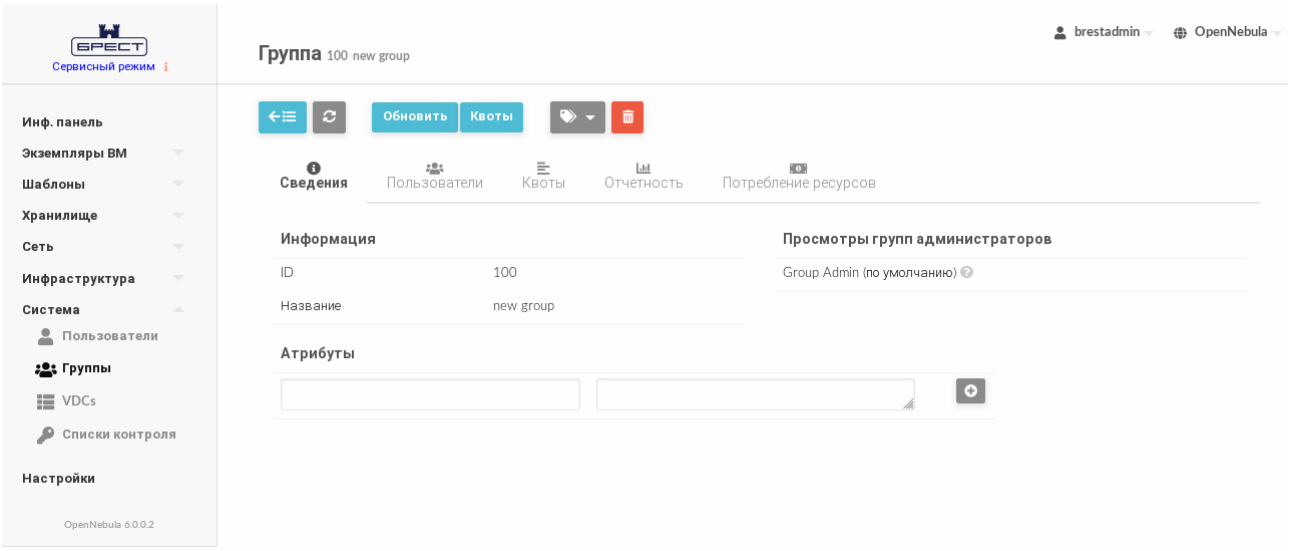

Рис. 15

Чтобы изменить основную группу пользователя или скорректировать перечень дополнительных групп в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

1) в меню слева выбрать пункт «Система — Пользователи» и на открывшейся странице «Пользователи» выбрать необходимого пользователя;

2) на открывшейся странице «Пользователь» открыть вкладку «Группы» и нажать на кнопку **[Изменить]** (см. рис. 16);

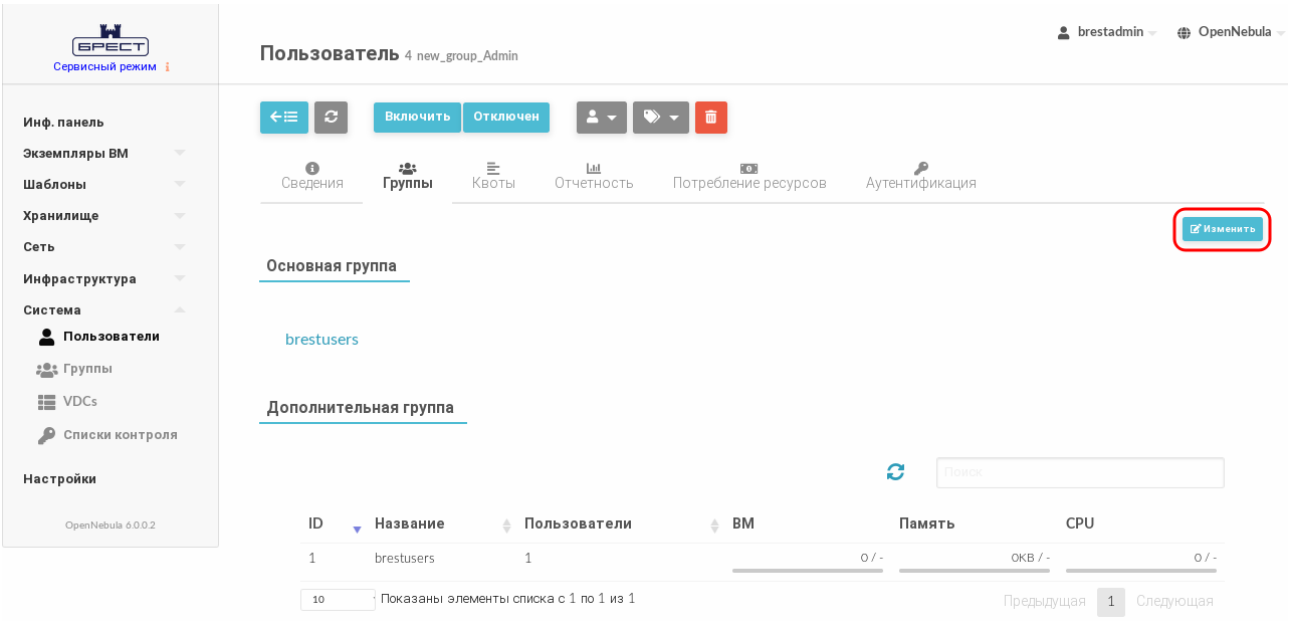

Рис. 16

3) на странице «Пользователь» во вкладке «Группы»:

а) в секции «Основная группа» в выпадающем списке выбрать одну из групп;

б) в секции «Дополнительная группа» в таблице выбрать необходимые группы (если необходимо исключить пользователя из группы — снять выделение);

в) нажать на кнопку **[Применить изменения]** (см. рис. 17).

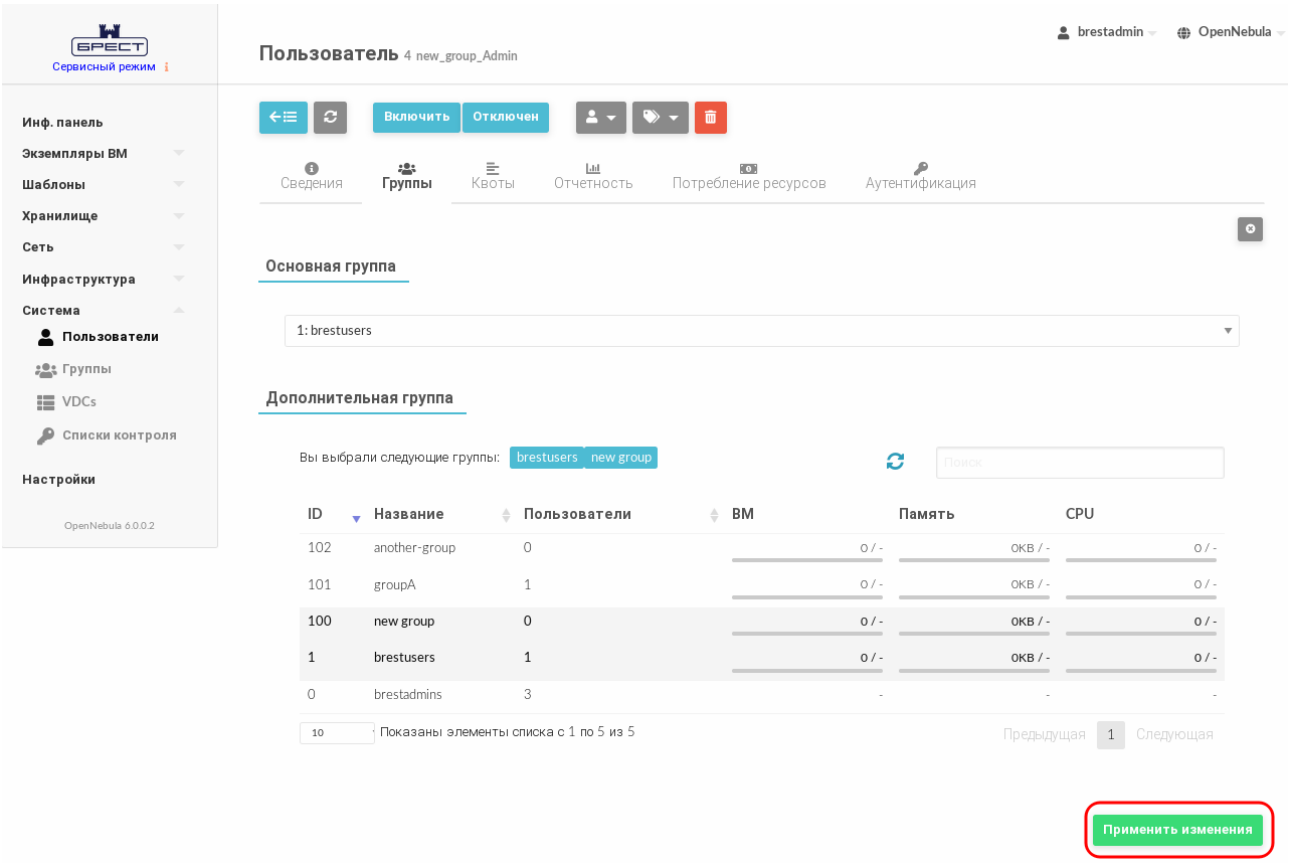

Рис. 17

5.4. Управление VDC

5.4.1. Общие сведения

Использование VDC (виртуального дата-центра) позволяет закрепить пул физических вычислительных ресурсов за одной или несколькими группами пользователей. Данный пул включает вычислительные ресурсы из одного или нескольких кластеров, которые могут принадлежать различным зонам или общедоступным внешним облачным сервисам для гибридных конфигураций.

При инициализации сервера управления в ПК СВ создается стандартный VDC (с наименованием `default`), который позволяет пользователям всех групп использовать все физические вычислительные ресурсы.

Любая новая группа пользователей автоматически добавляется к стандартному VDC. Из стандартного VDC можно частично или полностью исключить физические вычислительные ресурсы, но непосредственно сам стандартный VDC удалить нельзя.

Примечание. Перед добавлением группы пользователей к другому VDC предварительно необходимо удалить ее из стандартного VDC, поскольку он позволяет использовать физические ресурсы с меткой ALL (полный доступ ко всем ресурсам).

5.4.2. Управление VDC в интерфейсе командной строки

Для управления виртуальными дата-центрами используется инструмент командной строки `onevdc`.

Для того чтобы создать VDC, необходимо выполнить команду:

```
onevdc create <наименование_vdc>
```

Для добавления группы пользователей в VDC используется следующая команда:

```
onevdc addgroup <наименование_vdc> <идентификатор/наименование_группы>
```

Примечание. В представленной выше команде и далее по тексту в качестве наименования VDC можно указать перечень VDC (идентификаторов или наименований, разделенных запятыми) или диапазон идентификаторов VDC (в качестве разделителя используются две точки — «..»).

Для исключения группы из VDC используется следующая команда:

```
onevdc delgroup <наименование_vdc> <идентификатор/наименование_группы>
```

Примеры:

1. Создание VDC с наименованием «high-performance»:

```
onevdc create high-performance
```

Пример вывода после выполнения команды:

```
ID: 100
```

2. Просмотр перечня VDC:

```
onevdc list
```

Пример вывода после выполнения команды:

```
ID  NAME                GROUPS    CLUSTERS    HOSTS    VNETS    DATASTORES
100 high-performance    0         0           0        0        0
0   default             3         ALL         0        0        0
```

3. Создание VDC с наименованием «test»:

```
onevdc create test
```

Пример вывода после выполнения команды:

```
ID: 101
```

4. Добавление группы с идентификатором 102 в VDC, идентификаторы которых имеют значения с 100 по 101:

```
onevdc addgroup 100..101 102
```

5. Просмотр перечня VDC после добавления группы:

```
onevdc list
```

Пример вывода после выполнения команды:

```
ID  NAME                GROUPS    CLUSTERS    HOSTS    VNETS    DATASTORES
101 test                1         0           0        0        0
100 high-performance    1         0           0        0        0
```

```
0   default             3        ALL        0       0       0
```

6. Исключение из VDC с наименованием «test» группы с наименованием «another-group»:

```
onevdc delgroup test another-group
```

7. Просмотр перечня VDC после исключения группы:

```
onevdc list
```

Пример вывода после выполнения команды:

```
ID  NAME                GROUPS   CLUSTERS   HOSTS   VNETS   DATASTORES
101 test                0        0          0       0       0
100 high-performance    1        0          0       0       0
0   default             3        ALL        0       0       0
```

В VDC можно добавлять физические ресурсы (серверы виртуализации, сети и хранилища). При добавлении ресурсов VDC создает правила ACL для внутренних целей, которые позволяют группам пользователей в составе VDC использовать этот пул ресурсов.

Однако, обычно в VDC добавляют кластер серверов виртуализации. Для этого используется следующая команда:

```
onevdc addcluster <наименование_vdc> \
   <идентификатор_зоны> <идентификатор_кластера>
```

Для добавления отдельных серверов виртуализации, сетей и хранилищ применяются следующие команды:

- добавление сервера виртуализации:

```
onevdc addhost <наименование_vdc> \
    <идентификатор_зоны> <идентификатор_сервера_виртуализации>
```

- добавление виртуальной сети:

```
onevdc addvnet <наименование_vdc> \
    <идентификатор_зоны> <идентификатор_сети>
```

- добавление хранилища:

```
onevdc adddatastore <наименование_vdc> \
    <идентификатор_зоны> <идентификатор_хранилища>
```

Специальный идентификатор ALL можно использовать, чтобы добавить все кластеры (серверы виртуализации, сети, хранилища) из определенной зоны.

Пример

Добавление всех хранилищ зоны с идентификатором 0 в VDC с наименованием «test»:

```
onevdc adddatastore test 0 ALL
```

Просмотр перечня VDC после добавления хранилищ:

```
onevdc list
```

Пример вывода после выполнения команды:

```
ID  NAME             GROUPS  CLUSTERS  HOSTS  VNETS  DATASTORES
101 test             0       0         0      0      ALL
100 high-performance 1       0         0      0      0
0   default          3       ALL       0      0      0
```

Чтобы исключить физические вычислительные ресурсы из VDC, необходимо совместно с инструментом командной строки `onevdc` использовать команды `delcluster`, `delhost`, `delvnet`, `deldatastore`.

5.4.3. Управление VDC в веб-интерфейсе ПК СВ

Для отображения перечня всех VDC в веб-интерфейсе ПК СВ необходимо в меню слева выбрать пункт «Система — VDCs». На открывшейся странице «Виртуальные Дата Центры» будет представлена таблица VDC, аналогичная таблице, отображаемой в интерфейсе командной строки после выполнения команды `onevdc list` (см. рис. 18).

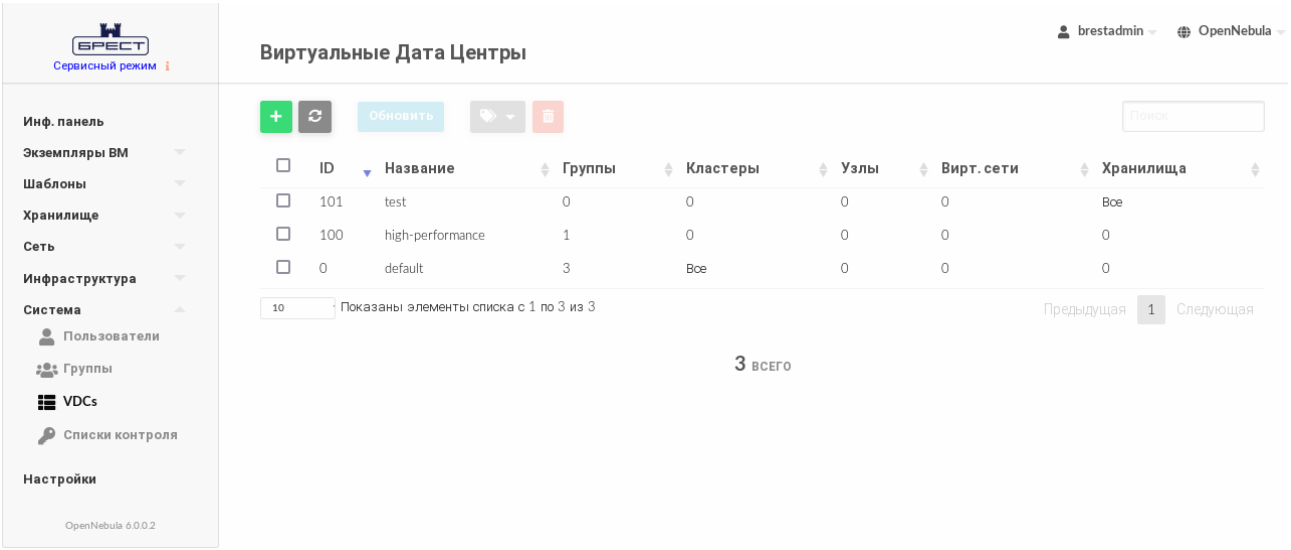

Рис. 18

Для добавления VDC в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

1) в меню слева выбрать пункт «Система — VDCs» и на открывшейся странице «Виртуальные Дата Центры» нажать на кнопку **[+]**;
2) на открывшейся странице **Создать Виртуальный Дата-Центр**:
   а) во вкладке «Общие» задать наименование VDC,
   б) во вкладке «Группы» выбрать необходимые группы пользователей для включения в создаваемый VDC,
   в) во вкладке «Ресурсы» указать физические вычислительные ресурсы, которые необходимо зарегистрировать в создаваемом VDC;

ВНИМАНИЕ! Для того чтобы указать узел, сеть или хранилище из состава

определенного кластера, предварительно необходимо выделить этот кластер во вкладке «Ресурсы» в секции «Кластеры» (см. рис. 19)

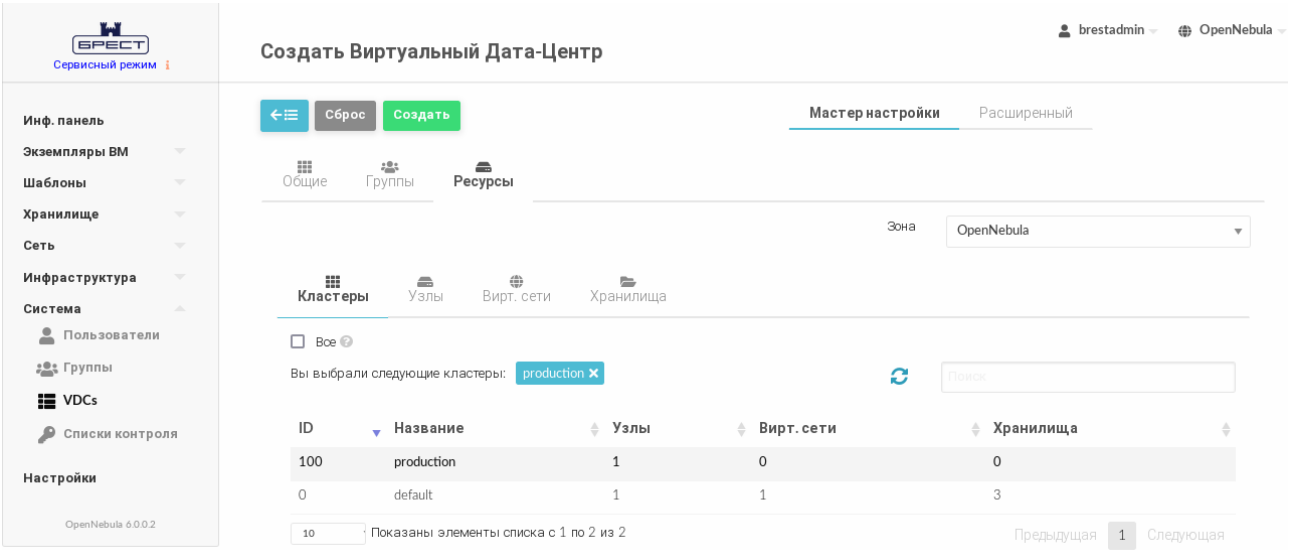

Рис. 19

3) на странице **Создать Виртуальный Дата-Центр** нажать на кнопку **[Создать]**;

После этого на открывшейся странице «Виртуальные Дата Центры» появится запись о созданном VDC.

Для просмотра информации о конкретном VDC на странице «Виртуальные Дата Центры» необходимо выбрать соответствующую строку. После этого откроется страница «Виртуальный Дата Центр» (вкладка «Сведения» — см. рис. 20).

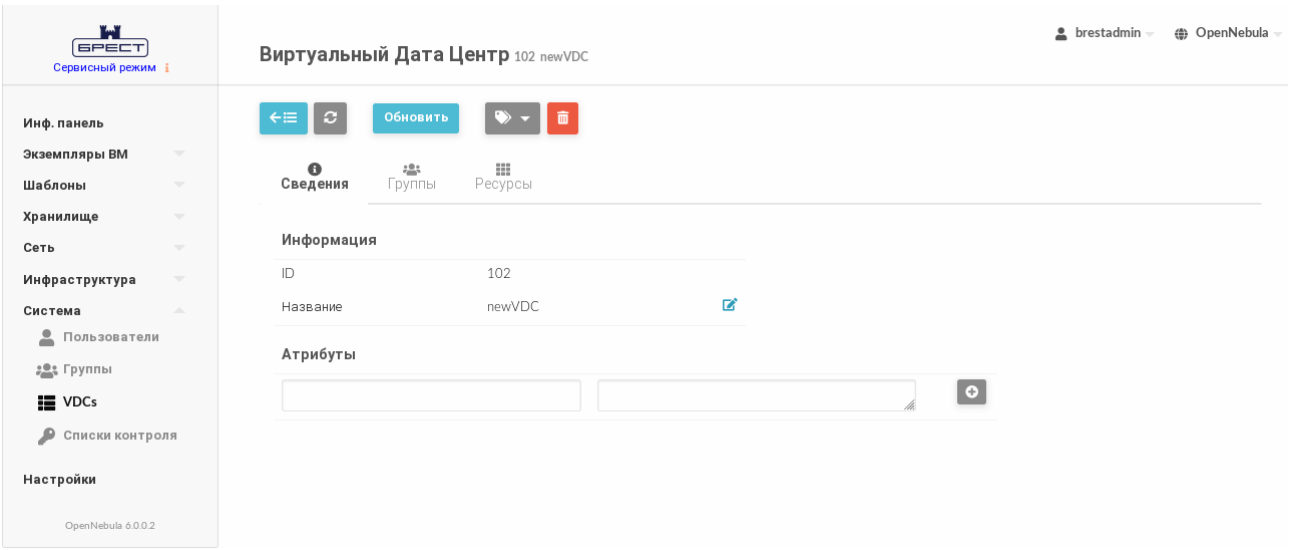

Рис. 20

Чтобы изменить наименование, состав групп или скорректировать перечень физических вычислительных ресурсов, зарегистрированных в VDC, в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

1) в меню слева выбрать пункт «Система — VDCs» и на открывшейся странице «Виртуальные Дата Центры» выбрать необходимый VDC;

2) на открывшейся странице «Виртуальный Дата Центр» нажать на кнопку **[Обновить]**;

3) на странице «Виртуальный Дата Центр»:

а) во вкладке «Общие» изменить наименование VDC,

б) во вкладке «Группы» выделить необходимые группы пользователей для включения в VDC (если необходимо исключить группу — снять выделение),

в) во вкладке «Ресурсы» указать физические вычислительные ресурсы, которые необходимо зарегистрировать в VDC (если необходимо исключить ресурс — снять выделение);

ВНИМАНИЕ! Для того чтобы указать сервер виртуализации, сеть или хранилище из состава определенного кластера, предварительно необходимо выделить этот кластер во вкладке «Ресурсы» в секции «Кластеры» (см. рис. 19)

4) на странице «Виртуальный Дата Центр» нажать на кнопку **[Обновить]**.

5.5. Управление полномочиями

5.5.1. Общие сведения

У большинства ресурсов ПК СВ имеются соответствующие разрешения для его владельца (`owner`), пользователей группы (`group`) и других пользователей (`others`). Для каждой из этих категорий можно назначить три типа полномочий: USE (применение), MANAGE (управление) и ADMIN (администрирование). Эти полномочия соответствуют следующим операциям:

- USE — операции, которые не изменяют ресурс, такие как просмотр или использование в ВМ (например, использование непостоянного образа или виртуальной сети). В основном полномочия типа USE применяются для разделения ресурсов с другими пользователями данной группы или с остальными пользователями;
- MANAGE — операции, которые изменяют ресурс, например, остановка виртуальной машины, изменение типа образа (постоянный/непостоянный) или корректировка IP-адреса, закрепленного за ВМ. В основном полномочия типа MANAGE предоставляются пользователям, которые будут управлять ресурсами;
- ADMIN — специальные операции, предназначенные для администрирования, например, обновление данных сервера виртуализации или удаление группы пользователей. В основном полномочия типа ADMIN предоставляются пользователям, которые выполняют функции администратора ПК СВ.

Указанные выше полномочия могут быть применены в отношении следующих ресур-

сов:

- шаблоны;
- виртуальные машины;
- образы;
- сети.

5.5.2. Управление полномочиями в интерфейсе командной строки

5.5.2.1. Просмотр и изменение установленных полномочий для ресурса

Для просмотра установленных полномочий используется команда `show` с указанием идентификатора ресурса.

Пример

Просмотр установленных полномочий шаблона с идентификатором 0

```
onetemplate show 0
```

Пример вывода после выполнения команды:

```
TEMPLATE 0 INFORMATION
ID              : 0
NAME            : alse-171
USER            : simpleuser
GROUP           : another-group
LOCK            : None
REGISTER TIME   : 07/14 09:41:49

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

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

5.5.2.2. Изменение установленных полномочий для ресурса

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

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

В качестве числового кода полномочий используется трехзначное восьмеричное

число, где каждый знак из трех соответствует определенной категории пользователей:

1) владелец (`owner`);
2) пользователи группы (`group`);
3) остальные пользователи (`others`).

Каждое восьмеричное число знака определяет полномочия для соответствующей категории пользователей. Полномочия выражаются следующими значениями:

- бит USE общее значение увеличивает на 4 (100 в двоичной системе);
- бит MANAGE общее значение увеличивает на 2 (010 в двоичной системе);
- бит ADMIN общее значение увеличивает на 1 (001 в двоичной системе).

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
```

5.5.2.3. Установка полномочий по умолчанию

Настройка полномочий, устанавливаемых по умолчанию в отношении вновь созданных ресурсов, может выполняться следующим образом:

- в целом для ПК СВ, используя параметр `DEFAULT_UMASK` в конфигурационном файле `/etc/one/oned.conf`;
- отдельно для каждого пользователя, используя команду `oneuser umask`.

В этом случае для установки полномочий используется трехзначная восьмеричная маска (по аналогии с командой `umask` в ОС СН) — каждый установленный бит отменяет соответствующие полномочия для `owner`, `group` и `other`.

В таблице 8 приведены примеры соответствия маски, используемой совместно с командой `umask` и числового кода полномочий, используемого совместно с командой `chmod`.

Таблица 8

маска `umask`	числовой код `chmod`	Полномочия
177	600	`um-  ---  ---`
137	640	`um-  u--  ---`
113	664	`um-  um-  u--`

5.5.3. Управление полномочиями в веб-интерфейсе ПК СВ

5.5.3.1. Просмотр и изменение установленных полномочий

Для просмотра полномочий, установленных для ресурса, необходимо перейти на страницу этого ресурса (вкладка «Сведения»).

Пример

Просмотр установленных полномочий шаблона с идентификатором 0 (см. рис. 21).

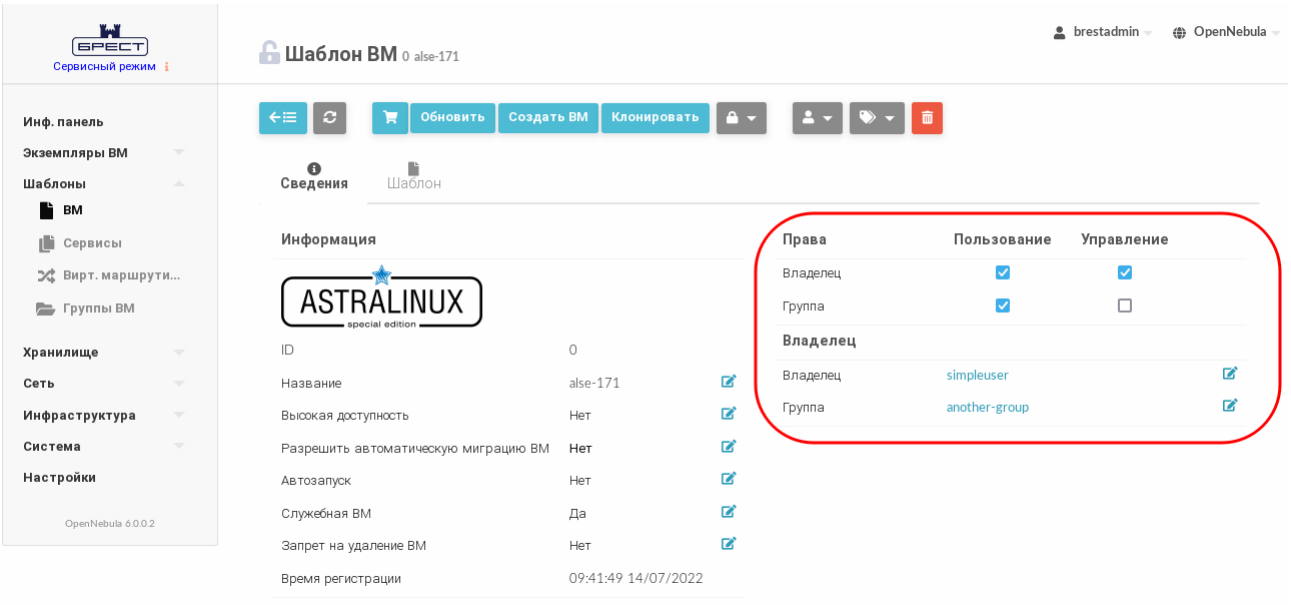

Рис. 21

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

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

5.5.3.2. Установка полномочий, присваиваемых по умолчанию пользователю

Настройка полномочий, присваиваемых по умолчанию пользователю в отношении вновь созданных ресурсов, в веб-интерфейсе ПК СВ выполняется следующим образом:

1) в меню слева выбрать пункт «Система — Пользователи»;

2) на открывшейся странице «Пользователи» выбрать необходимого пользователя;

3) на открывшейся странице пользователя во вкладке «Сведения» в секции «Атрибуты» (см. рис. 22) выполнить следующие действия:

а) в левом поле ввести наименование атрибута: «umask»,

б) в правом поле указать трехзначную восьмеричную маску (см. 5.5.2.3),

в) нажать на кнопку **[+]**.

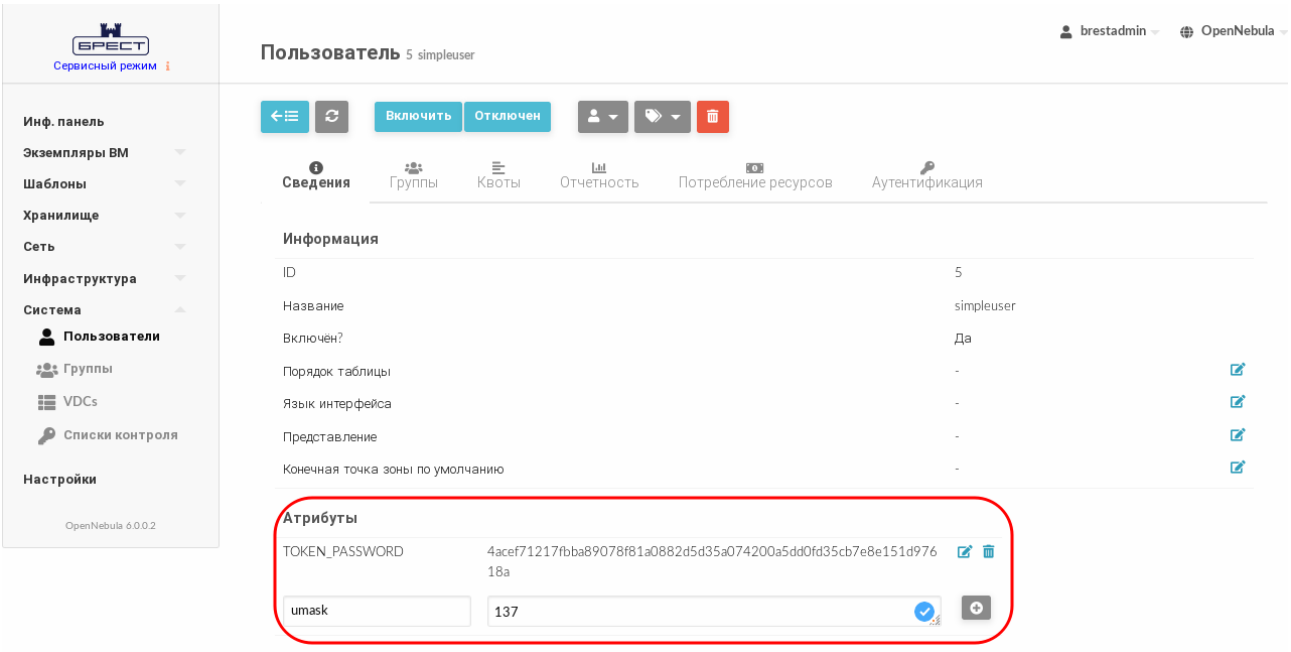

Рис. 22

5.6. Управление правилами ACL

5.6.1. Общие сведения

Разрешительная система ACL позволяет выполнять тонкую настройку операций, доступных для любого пользователя или группы пользователей. При каждой операции формируется запрос авторизации, который проверяется на соответствие зарегистрированному набору правил ACL. После проверки служба сервера управления может предоставить доступ или отклонить запрос.

Использование правил ACL позволяет администраторам ПК СВ адаптировать роли пользователей под нужды инфраструктуры. Например, при помощи правил ACL ограничиваются права разработчика и пользователей виртуальных машин. Или можно предоставить определенному пользователю полномочия только для управления виртуальными сетями некоторых существующих групп.

5.6.2. Структура правил ACL

Правило ACL в общем виде состоит из четырех компонентов, разделенных пробелом:

1) компонент User (пользователь) — идентификатор субъекта;
2) компонент Resources (ресурсы), состоит из следующих полей:
   - перечень типов ресурсов, разделенных знаком «+»,
   - знак «/»,
   - идентификатор объекта;
3) компонент Rights (права) — перечень типов полномочий, разделенных знаком «+» (типы полномочий описаны в 5.5.1);
4) компонент Zone (зона) — идентификатор зоны или перечень идентификаторов зон, в которых действует правило. Этот компонент не обязателен, его можно не указывать, если конфигурация ПК СВ не настроена для работы в федерации.

В правиле ACL идентификатор субъекта может принимать следующие значения:
1) #<идентификатор_пользователя> — для отдельного пользователя;
2) @<идентификатор_группы> — для группы пользователей;
3) * — для всех пользователей.

В правиле ACL идентификатор объекта может принимать следующие значения:
1) %<идентификатор_кластера> — для отдельного кластера;
2) #<идентификатор_ресурса> — для отдельного ресурса;
3) @<идентификатор_группы> — для группы которой принадлежит ресурс;
4) * — для всех ресурсов.

Примеры:

1. Правило предоставляет пользователю с идентификатором 5 право выполнять операции типа USE и MANAGE в отношении всех образов и шаблонов, принадлежащих группе с идентификатором 103:

```
#5 IMAGE+TEMPLATE/@103 USE+MANAGE #0
```

2. Правило позволяет всем пользователям группы с идентификатором 105 создавать новые ресурсы:

```
@105 VM+NET+IMAGE+TEMPLATE/* CREATE
```

3. Правило позволяет всем пользователям группы с идентификатором 106 применять виртуальную сеть с идентификатором 47. Это означает, что они могут разворачивать ВМ, в которых используется данная сеть:

```
@106 NET/#47 USE
```

4. Правило дает полномочия пользователям группы с идентификатором 106 выполнять развертывание ВМ на сервера виртуализациих, закрепленных за кластером с идентификатором 100:

```
@106 HOST/%100 MANAGE
```

Примечание. Следует обратить внимание на отличие «* NET/#47 USE» от

«* NET/@47 USE». В первом случае все пользователи могут использовать сеть с идентификатором 47, а во втором все пользователи могут использовать сети, которые принадлежат группе с идентификатором 47.

ВНИМАНИЕ! В ПК СВ существует неявное правило ACL: пользователь oneadmin и пользователи группы brestadmins имеют право выполнять любую операцию.

Важный момент при работе с набором правил ACL заключается в том, что каждое правило добавляет новые полномочия, и они не могут ограничивать уже существующие. Таким образом если хотя бы одно из правил предоставляет полномочия, выполнение операции разрешается. Следовательно, необходимо учитывать правила, которые применяются в отношении пользователя и его группы.

Пример

Если пользователь с идентификатором 7 состоит в группе с идентификатором 108 и существует правило:

```
@108 IMAGE/#45 USE+MANAGE
```

(разрешить всем пользователям группы с идентификатором 108 использовать и управлять образом с идентификатором 45), то правило:

```
#7 IMAGE/#45 USE
```

(разрешить только пользователю с идентификатором 7 только использовать (но не управлять) образ с идентификатором 45) не имеет смысла.

5.6.3. Управление правилами ACL в интерфейсе командной строки

Для управления правилами ACL используется инструмент командной строки oneacl.

Для просмотра действующих правил, необходимо выполнить команду:

```
oneacl list
```

Пример вывода после выполнения команды:

```
ID     USER   RES_VHNIUTGDCOZSvRMAPt   RID   OPE_UMAC   ZONE
0       @1    V--I-T---O-S----P-       *     ---c        *
1        *    ----------Z-------       *     u---        *
2        *    --------------MA--       *     u---        *
3       @1    -H----------------       *     -m--       #0
4       @1    --N---------------       *     u---       #0
5       @1    -------D----------       *     u---       #0
...
```

В представленной выше таблице содержится следующая информация:

- в столбце ID указан идентификатор каждого правила;
- в столбце USER указан идентификатор субъекта;
- в столбце Resources перечислены условные сокращения существующих типов

ресурсов. В каждом правиле указываются следующие условные сокращения типов ресурсов, к которым оно применяется:

- V — VM
- H — HOST
- N — NET
- I — IMAGE
- U — USER
- T — TEMPLATE
- G — GROUP
- D — DATASTORE
- C — CLUSTER
- O — DOCUMENT
- Z — ZONE
- S — SECURITY GROUP
- v — VDC
- R — VROUTER
- M — MARKETPLACE
- A — MARKETPLACEAPP
- P — VMGROUP
- t — VNTEMPLATE

- в столбце RID указан идентификатор объекта;
- в столбце Operations перечислены сокращения допустимых операций:
  - U — USE
  - M — MANAGE
  - A — ADMIN
  - C — CREATE
- в столбце Zone указаны зоны, в которых действует правило. Это может быть идентификатор отдельной зоны или всех зон.

Правила с идентификаторами 0 - 5 автоматически создаются при инициализации программных компонентов ПК СВ.

Для того чтобы создать правило ACL, необходимо выполнить команду:

```
oneacl create "<текст_правила>"
```

Для удаления правила ACL, необходимо выполнить команду:

```
oneacl delete <идентификатор_правила>
```

Примечание. В качестве идентификатора правила ACL можно указать перечень идентификаторов, разделенных запятыми или диапазон идентификаторов (в качестве

разделителя используются две точки — «..»).

5.6.4. Управление правилами ACL в веб-интерфейсе ПК СВ

Для отображения перечня всех правил ACL в веб-интерфейсе ПК СВ необходимо в меню слева выбрать пункт «Система — Списки контроля». На открывшейся странице «Списки Контроля Доступа» будет представлена таблица правил, аналогичная таблице, отображаемой в интерфейсе командной строки после выполнения команды `oneacl list` (см. рис. 23).

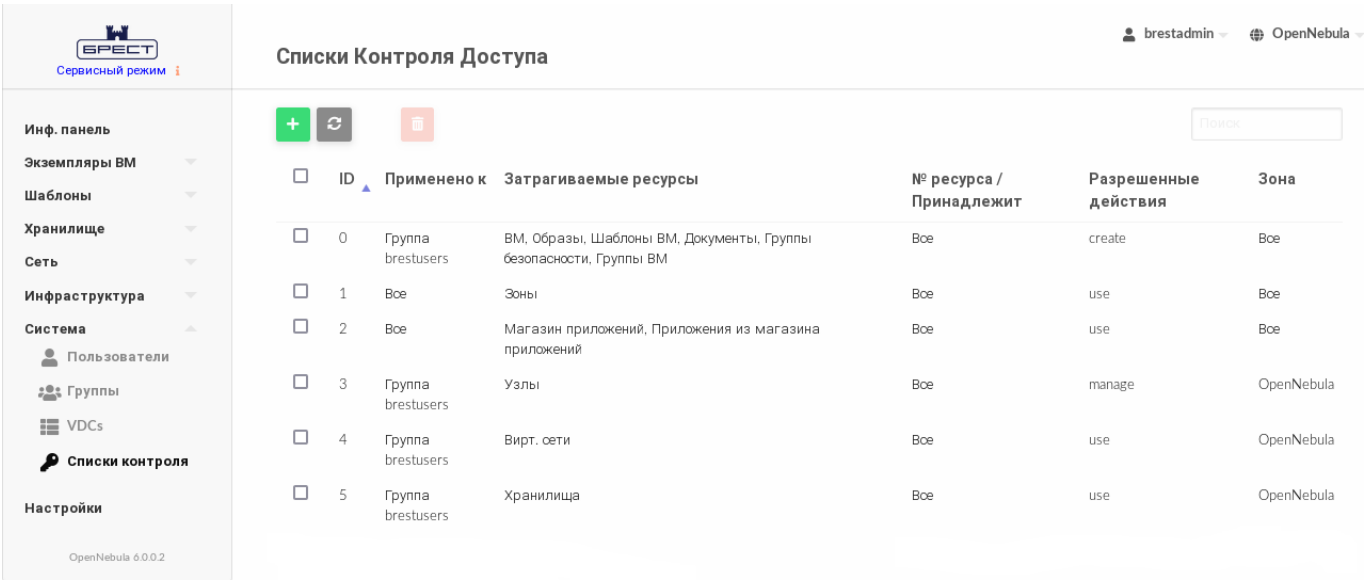

Рис. 23

Для добавления нового правила ACL в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

1) в меню слева выбрать пункт «Система — Списки контроля» и на открывшейся странице «Списки Контроля Доступа» нажать на кнопку **[+]**;
2) на открывшейся странице «Создать правило контроля» (см. рис. 24):
   а) в секции «Область применения» указать субъекта правила,
   б) в секции «Затрагиваемые ресурсы» выбрать необходимые типы ресурсов,
   в) в секции «Подмножество ресурсов» указать идентификатор объекта;
   г) в секции «Разрешенные действия» задать перечень полномочий,

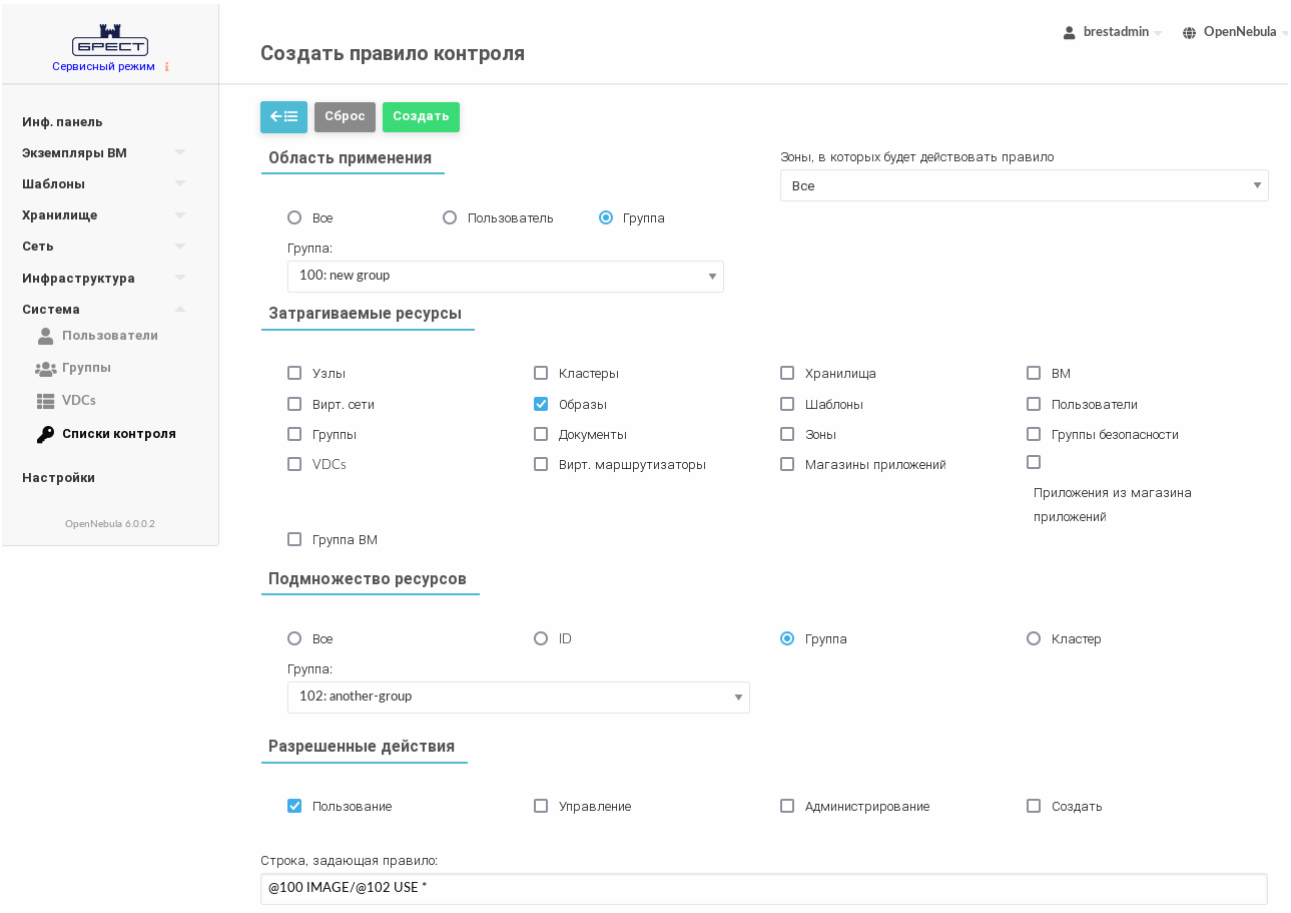

Рис. 24

3) на странице «Создать правило контроля» в поле `Строка, задающая правило` проверить корректность сформированного правила и нажать на кнопку **[Создать]**;

После этого на открывшейся странице «Списки Контроля Доступа» появится запись о созданном правиле ACL.

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

1) в меню слева выбрать пункт «Система — Списки контроля»;

2) на открывшейся странице «Списки Контроля Доступа» выбрать правила, которые необходимо удалить и нажать на кнопку **[Удалить]**;

3) в открывшемся окне «Удалить» нажать на кнопку **[OK]**.

5.7. Управление квотами

5.7.1. Общие сведения

Система квот отслеживает потребление физических вычислительных ресурсов пользователями и группами и позволяет администратору ПК СВ устанавливать ограничения на применение данных ресурсов и квоты доступа виртуальных машин к физическому и виртуальному оборудованию. Квоты можно установить для:

- пользователей, чтобы ограничить использование для определенного пользователя;

- групп, чтобы ограничить общее использование для всех пользователей в определенной группе. Актуально, в частности, для зон и виртуальных дата-центров ПК СВ.

Система квот позволяет отслеживать и ограничивать использование следующих физических вычислительных ресурсов:

- занимаемый объем хранилища, чтобы контролировать дисковый ресурс, выделяемой каждому пользователю/группе в каждом хранилище;
- вычислительную мощность, чтобы ограничивать оперативную память, работу центрального процессора или количества экземпляров ВМ;
- сеть, чтобы ограничивать количество IP-адресов, доступных пользователю/группе в определенной сети. Актуально для сетей с внешними IP-адресами, которые, как правило, ограничены;
- образы, чтобы ограничить число экземпляров ВМ определенного пользователя/группы, использующих определенный образ. Кроме того, данной квотой можно воспользоваться, когда образ содержит расходуемые ресурсы, например, лицензии ПО).

Чтобы управлять квотами пользователя, необходимы полномочия типа MANAGE. Для настройки квот группы необходимы полномочия типа ADMIN. Таким образом, по умолчанию только `oneadmin` может настраивать квоты для группы. Но если определен администратор группы, то он сможет настраивать отдельные квоты для пользователей в данной группе, распределяя ресурсы в соответствии с необходимостью. Данный алгоритм можно изменить путем настройки соответствующих правил ACL.

5.7.2. Управление квотами в интерфейсе командной строки

5.7.2.1. Просмотр установленных квот

Для просмотра квот, установленных для пользователя, используется команда:

```
oneuser show <идентификатор/имя_пользователя>
```

Для просмотра квот, установленных для группы пользователей, используется команда:

```
onegroup show <идентификатор/наименование_группы>
```

Пример

Просмотр квот, установленных для пользователя с идентификатором 5:

```
oneuser show 5
```

Пример вывода после выполнения команды:

```
USER 5 INFORMATION
ID              : 5
NAME            : simpleuser
```

```
GROUP           : another-group
SECONDARY GROUPS: 1,102
PASSWORD        : simpleuser
AUTH_DRIVER     : public
ENABLED         : Yes
...
VMS USAGE & QUOTAS
VMS    MEMORY    CPU       SYSTEM_DISK_SIZE
0/-    0M/-      0.00/-    0M/-

VMS USAGE & QUOTAS - RUNNING
RUNNING VMS    RUNNING MEMORY    RUNNING CPU
0/-            0M/-              0.00/-

DATASTORE USAGE & QUOTAS

NETWORK USAGE & QUOTAS

IMAGE USAGE & QUOTAS
```

В представленном примере в отношении пользователя квоты не установлены.

5.7.2.2. Установка квот

Для установки квоты пользователя используется команда:

```
oneuser quota <идентификатор/имя_пользователя> [<файл-шаблон>]
```

где <файл-шаблон> — файл шаблона для установки квоты. Если файл шаблона не указан, то после ввода команды откроется текстовый редактор Vim для формирования временного шаблона. После сохранения внесенных данных и закрытия редактора, подготовленный шаблон будет применен для установки квоты пользователя, а временный файл шаблона будет удален.

Для установки квоты группы пользователей используется команда:

```
onegroup quota <идентификатор/наименование_группы> [<файл-шаблон>]
```

В файле шаблона квоты могут быть заданы в текстовом виде или в формате XML. В таблице 9 приведено описание параметров, необходимых для настройки каждой квоты:

Таблица 9

Параметр	Описание
Квоты на хранилища. Блок параметров DATASTORE	
ID	Идентификатор хранилища, для которого устанавливается квота

Окончание таблицы 9

Параметр	Описание
SIZE	Максимальный объем (в МБ), который допускается занимать в хранилище
IMAGE	Максимальное количество образов, которые могут быть созданы в хранилище
Квоты на вычислительную мощность. Блок параметров VM	
VMS	Максимальное количество ВМ, которые могут быть созданы
MEMORY	Максимальный объем оперативной памяти (в МБ), который могут запросить ВМ пользователя/группы
CPU	Максимальная производительность ЦП, которую могут запросить ВМ пользователя/группы
RUNNING VMS	Максимальное количество ВМ, которое может запустить пользователь/-группа
RUNNING MEMORY	Максимальный объем оперативной памяти (в МБ), выделяемый для запущенных ВМ пользователя/группы
RUNNING CPU	Максимальная производительность ЦП, выделяемая для запущенных ВМ пользователя/группы
SYSTEM_DISK_SIZE	Максимальный размер (в МБ) системных дисков, который могут запросить ВМ пользователя/группы
Квоты на сеть. Блок параметров NETWORK	
ID	Идентификатор сети, для которой устанавливается квота
LEASES	Максимальное количество IP-адресов, которые можно арендовать у сети
Квоты на образы. Блок параметров IMAGE	
ID	Идентификатор образа, для которого устанавливается квота
RVMS	Максимальное количество ВМ, которые могут одновременно использовать данный образ

Примечание. Следует учитывать, что квоты на вычислительную мощность с префиксом «RUNNING» распространяются также на ВМ, которые находятся в состоянии «ACTIVE», «HOLD», «PENDING» и «CLONING».

Существует два специальных ограничения для каждой квоты:

- «-1» — использование квоты по умолчанию (default quota);
- «-2» — ограничений не установлено (unlimited).

Примеры:

1. Содержание файла шаблона quota.txt:

```
DATASTORE=[
   ID="1",
   IMAGES="-2",
   SIZE="20480"
```

```
]
VM=[
   CPU="5",
   MEMORY="2048",
   VMS="4",
   SYSTEM_DISK_SIZE="-1"
]
NETWORK=[
   ID="1",
   LEASES="4"
]
IMAGE=[
   ID="1",
   RVMS="3"
]
IMAGE=[
   ID="2",
   RVMS="-2"
]
```

В представленном примере:

- максимальный занимаемый объем данных в хранилище с идентификатором `1` составляет 20 ГБ (для неограниченного количества образов);
- количество используемых виртуальных машин — до четырех, при максимальном объеме оперативной памяти до 2 ГБ и пяти ЦП;
- количество предоставляемых IP-адресов — от одного до четырех;
- образ с идентификатором `1` может одновременно использоваться только тремя виртуальными машинами. Использование образа с идентификатором `2` не ограничено.

2. Установка квот для пользователя с идентификатором 5 с использованием файла шаблона `quota.txt`:

```
oneuser quota 5 quota.txt
```

3. Просмотр квот, установленных для пользователя с идентификатором 5:

```
oneuser show 5
```

Пример вывода после выполнения команды:

```
USER 5 INFORMATION
ID              : 5
NAME            : simpleuser
GROUP           : another-group
```

```
SECONDARY GROUPS: 1,102
PASSWORD        : simpleuser
AUTH_DRIVER     : public
ENABLED         : Yes
...
VMS USAGE & QUOTAS
VMS    MEMORY    CPU          SYSTEM_DISK_SIZE
0/4    0M/2G     0.00/5.00    0M/-

VMS USAGE & QUOTAS - RUNNING
RUNNING VMS    RUNNING MEMORY    RUNNING CPU
0/-            0M/-              0.00/-

DATASTORE USAGE & QUOTAS
ID    IMAGES    SIZE
1     0/-       0M/20G

NETWORK USAGE & QUOTAS
ID    LEASES
1     0/4

IMAGE USAGE & QUOTAS
ID    RUNNING VMS
1     0/3
2     0/-
```

Примечание. При использовании сети, образа, хранилищ или ВМ для пользователя создается соответствующий счетчик квоты с неограниченным значением. Это позволяет отслеживать потребление ресурсов со стороны каждого пользователя/группы, даже если квоты не применяются.

5.7.2.3. Изменение установленных квот

Для изменения квоты пользователя/группы используется команда:

```
oneuser / onegroup quota <идентификатор/имя_пользователя>
```

В этом случае файл шаблона для установки квоты не указывается. После ввода команды откроется текстовый редактор `Vim` в котором отобразятся установленные квоты пользователя/группы (для работы редактора используется временный файл шаблона). После сохранения измененных значений параметров и закрытия редактора, измененный шаблон

будет применен для установки квоты пользователя, а временный файл шаблона будет удален.

ВНИМАНИЕ! Параметры с наименованием *_USED, например, CPU_USED, MEMORY_USED, LEASES_USED, предоставляются для справки и не должны изменяться.

Примечание. Можно добавлять необходимые квоты на ресурсы, даже если они не были инициализированы автоматически.

Пример

Изменение квот, установленных для пользователя с идентификатором 5:

```
oneuser quota 5
```

Пример содержания временного файла шаблона, открытого в редакторе Vim:

```
DATASTORE=[
ID="1",
IMAGES="-2",
IMAGES_USED="0",
SIZE="20480",
SIZE_USED="0" ]
VM=[
CPU="5",
CPU_USED="0",
MEMORY="2048",
MEMORY_USED="0",
RUNNING_CPU="-1",
RUNNING_CPU_USED="0",
RUNNING_MEMORY="-1",
RUNNING_MEMORY_USED="0",
RUNNING_VMS="-1",
RUNNING_VMS_USED="0",
SYSTEM_DISK_SIZE="-1",
SYSTEM_DISK_SIZE_USED="0",
VMS="4",
VMS_USED="0" ]
NETWORK=[
ID="1",
LEASES="4",
LEASES_USED="0" ]
IMAGE=[
ID="1",
RVMS="3",
```

```
RVMS_USED="0" ]
IMAGE=[
ID="2",
RVMS="-2",
RVMS_USED="0" ]
```

5.7.2.4. Установка квот для нескольких пользователей/групп

Чтобы установить одинаковые квоты для нескольких пользователей, используется команда:

```
oneuser batchquota <список_пользователей> [<файл-шаблон>]
```

Чтобы установить одинаковые квоты для нескольких групп пользователей, используется команда:

```
onegroup batchquota <список_групп> [<файл-шаблон>]
```

где <файл-шаблон> — файл шаблона для установки квоты. Если файл шаблона не указан, то после ввода команды откроется текстовый редактор Vim для формирования временного шаблона. После сохранения внесенных данных и закрытия редактора, подготовленный шаблон будет применен для установки квоты пользователей/групп, а временный файл шаблона будет удален.

Примечание. В качестве списка пользователей/групп указывается перечень идентификаторов или наименований, разделенных запятыми, или диапазон идентификаторов (в качестве разделителя используются две точки — «..»).

5.7.2.5. Установка квот по умолчанию

Чтобы установить одинаковые квоты для всех пользователей, используется команда:

```
oneuser defaultquota [<файл-шаблон>]
```

Чтобы установить одинаковые квоты для всех групп пользователей, используется команда:

```
onegroup defaultquota [<файл-шаблон>]
```

где <файл-шаблон> — файл шаблона для установки квоты. Если файл шаблона не указан, то после ввода команды откроется текстовый редактор Vim для формирования временного шаблона. После сохранения внесенных данных и закрытия редактора, подготовленный шаблон будет применен для установки квоты пользователей/групп, а временный файл шаблона будет удален.

5.7.3. Управление квотами в веб-интерфейсе ПК СВ

Чтобы просмотреть квоты, установленные для пользователя, в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

1) в меню слева выбрать пункт «Система — Пользователи»;
2) на открывшейся странице «Пользователи» выбрать необходимого пользователя;

3) на открывшейся странице пользователя открыть вкладку «Квоты» (см. рис. 25):

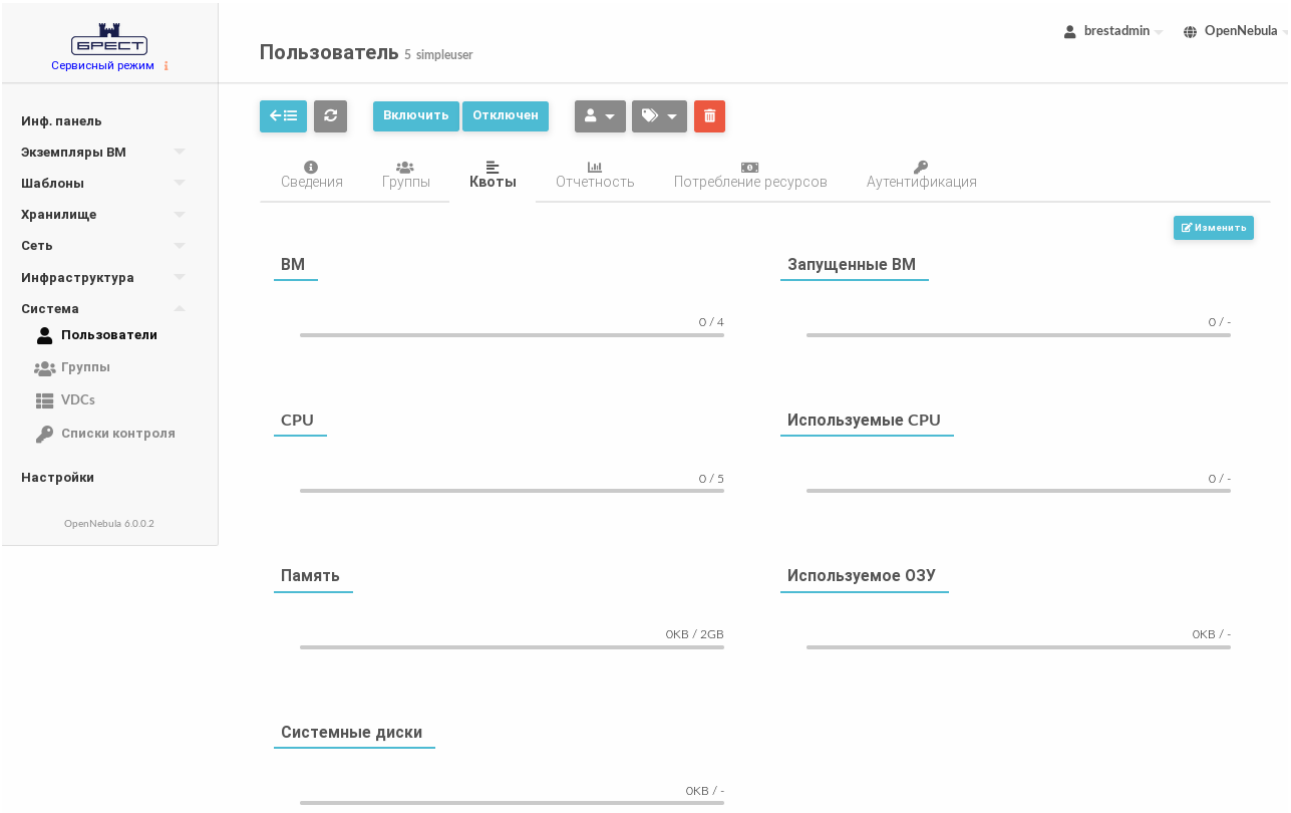

Рис. 25

Для изменения квот, установленных для пользователя, в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

1) в меню слева выбрать пункт «Система — Пользователи»;

2) на открывшейся странице «Пользователи» выбрать необходимого пользователя;

3) на открывшейся странице пользователя открыть вкладку «Квоты» и нажать на кнопку **[Изменить]**;

4) на открывшейся странице установить необходимые значения квот и нажать на кнопку **[Применить]**. Для отмены внесенных изменений нажать на кнопку **[Отменить]** (см. рис. 26):

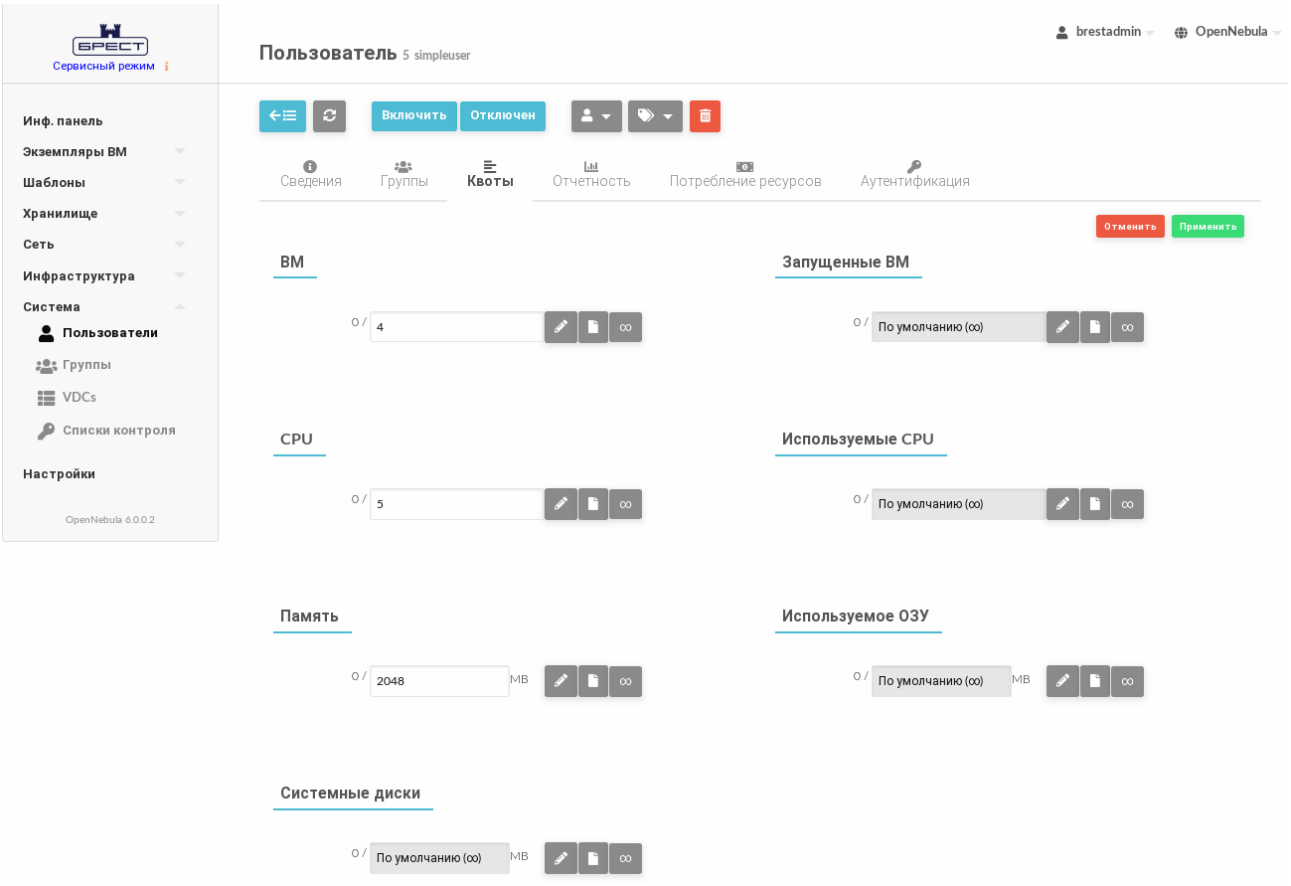

Рис. 26

Чтобы просмотреть квоты, установленные для группы пользователей, в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

1) в меню слева выбрать пункт «Система — Группы»;
2) на открывшейся странице «Группы» выбрать необходимую группу пользователей;
3) на открывшейся странице группы пользователей открыть вкладку «Квоты».

Для изменения квот, установленных для группы пользователей, в веб-интерфейсе ПК СВ необходимо выполнить такие же действия, как и при изменении квот, установленных для пользователя.

6. НАСТРОЙКИ ВИРТУАЛЬНЫХ СЕТЕЙ

Действия по созданию и настройке виртуальных сетей в ПК СВ выполняются под учетной записью администратора ПК СВ.

6.1. Виртуальные сети ПК СВ

6.1.1. Управление потоками информации

Для управления потоками информации в ПК СВ применяются следующие механизмы, обеспечивающие сетевую фильтрацию:

1) драйверы виртуальных сетей, реализованные в ПК СВ:

- драйвер «сетевой мост с группами безопасности» (Bridged with Security Groups, далее по тексту Security Group) — устанавливаются правила `iptables` для внедрения правил групп безопасности;
- драйвер VLAN — для каждой сети создается мост, к которому подключается VLAN-тегированный сетевой интерфейс (VLAN-тегирование стандарта IEEE802.1Q);
- драйвер VXLAN — для каждой сети создается мост, к которому подключается VXLAN-тегированный сетевой интерфейс. Используемый протокол VXLAN основан на UDP-инкапсуляции и групповой адресации IP.

При использовании перечисленных выше драйверов виртуальных сетей необходимо настроить группы безопасности, которые определяют правила сетевого фильтра в отношении трафика виртуальных машин. При этом следует учитывать, что группы безопасности не поддерживаются для адресации IPv6;

2) драйвер сетевых фильтров `libvirt`, реализованный в ОС СН, — обеспечивает полностью настраиваемую сетевую фильтрацию трафика на сетевых картах виртуальных машин с использованием сетевых фильтров `nwfilter`. Наборы правил для управления трафиком определяются на уровне сервера виртуализации. Затем наборы правил связываются с определенными сетевыми картами виртуальных машин. Управление сетевыми фильтрами `nwfilter` описано в документе РУСБ.10015-01 97 01-1;

3) изоляция сетей с помощью VLAN — программный многоуровневый коммутатор Open vSwitch (OVS) для виртуальных сетей из состава ОС СН обеспечивает изоляцию сети с помощью VLAN путем тегирования портов, а также фильтрацию сетевого трафика. Описание настройки и работы OVS приведено в документе РУСБ.10015-01 95 01-1.

6.1.2. Параметры сети

Параметры сети объединяются в три группы:

1) параметры физической сети, которая будет ее поддерживать, включая сетевой драйвер;

2) доступное адресное пространство. Адресами, связанными с виртуальной сетью, могут быть IPv4, IPv6, IPv4-IPv6 с двумя стеками или Ethernet;

3) параметры контекстуализации (сетевые настройки виртуальных машин, которые могут включать, например, маски сети, сервера DNS или шлюзы).

6.1.2.1. Параметры физической сети

В группу параметров физической сети входят следующие параметры, приведенные в таблице 10.

Таблица 10

Параметр	Применимость	Обязательный	Описание
NAME	Для всех режимов	Да	Наименование сети
VN_MAD	Для всех режимов	Да	Драйвер виртуальной сети, может принимать следующие значения: - bridge — для режима «сетевой мост без фильтрации» (Bridged); - fw — для режима «сетевой мост с группами безопасности» (Bridged with Security Groups); - ebtables — для режима «сетевой мост с правилами ebtables» (Bridged with ebtables isolation); - 802.1Q — для режима VLAN; - vxlan — для режима VXLAN; - ovswitch — для режима Open vSwitch.
BRIDGE	Для всех режимов	Обязательный для режимов: - bridge - fw - ebtables - ovswitch	Имя сетевого моста на серверах виртуализации
VLAN_ID	Для режимов: - 802.1Q - vxlan - ovswitch	Обязательный для режима 802.1Q	Идентификационный номер сети VLAN. Будет сгенерирован, если не указан и для параметра AUTOMATIC_VLAN_ID установлено значение YES

Окончание таблицы 10

Параметр	Применимость	Обязательный	Описание
AUTOMATIC_VLAN_ID	Для режимов: - 802.1Q - vxlan - ovswitch	Обязательный для режима 802.1Q	Игнорируется, если параметр VLAN_ID определен. Следует установить значение YES, если необходимо в автоматическом режиме генерировать идентификационный номер сети VLAN
PHYDEV	Для режимов: - 802.1Q - vxlan	Да	Имя физического сетевого устройства, которое будет подключено к сетевому мосту
MTU	Для режимов: - 802.1Q - vxlan - ovswitch	Нет	Максимальный размер в байтах пакета данных (MTU), устанавливаемый для для тегированного интерфейса и моста

Кроме того, для каждого сетевого интерфейса ВМ, подключаемого к виртуальной сети, можно настроить параметры оптимизации сетевого трафика (QoS). Применяются для ограничения средней и пиковой пропускной способности входящего и исходящего трафика, а также объема пакетных данных, которые могут передаваться на максимальной скорости. Перечень параметров приведен в таблице 11.

Таблица 11

Параметр	Описание
INBOUND_AVG_BW	Средняя скорость входящего трафика (Кбайт/с)
INBOUND_PEAK_BW	Максимальная скорость входящего трафика (Кбайт/с)
INBOUND_PEAK_KB	Объем входящего трафика, который может быть получен на максимальной скорости (Кбайт)
OUTBOUND_AVG_BW	Средняя скорость исходящего трафика (Кбайт/с)
OUTBOUND_PEAK_BW	Максимальная скорость исходящего трафика (Кбайт/с)
OUTBOUND_PEAK_KB	Объем исходящего трафика, который может быть передан на максимальной скорости (Кбайт)

6.1.2.2. Адресное пространство (AR)

IP-адреса, доступные внутри сети, определяются одним и более диапазоном адресов (AR). Каждый AR определяет непрерывный диапазон адресов и, при необходимости, опции конфигурации, которые переопределяют опции первого уровня, установленные в сети. Существует следующие типы AR:

- IP4 — для определения адресов IPv4 (бесклассовый);
- IP6 — для определения адресов IPv6 (уникальные глобальные и локальные адреса);

- IP6_STATIC — для определения адресов IPv6 (no-SLAAC);
- IP4_6 — с двумя стеками, каждый сетевой интерфейс в сети получит адрес IPv4 и адрес IPv6;
- ETHER — для ВМ формируются только MAC-адреса. Данный AR следует использовать, когда IP-адреса предоставляются внешним сервисом, например, сервером DHCP.

6.1.2.3. Сетевые параметры контекстуализации

В шаблоне виртуальной сети можно задать сетевые настройки виртуальных машин, которые будут применены в ОС виртуальной машины. Перечень параметров, значения которых можно задать для сетевого интерфейса ВМ, приведен в таблице 12.

Таблица 12

Параметр	Описание
NETWORK_ADDRESS	Идентификатор (адрес) сети
NETWORK_MASK	Маска подсети
GATEWAY	Адрес шлюза (IPv4)
GATEWAY6	Адрес шлюза (IPv6)
DNS	Адрес сервера DNS
GUEST_MTU	Максимальный размер в байтах пакета данных (MTU), устанавливаемый для сетевого интерфейса ВМ
CONTEXT_FORCE_IPV4	Применяется в случае, когда в виртуальной сети настроено использование IPv6. Необходимо установить значение «yes», чтобы для сетевого интерфейса ВМ были применены настройки IPv4
SEARCH_DOMAIN	Директива настройки сети, которая указывает возможный суффикс для DNS адресов

ВНИМАНИЕ! Для того чтобы заданные сетевые настройки применялись автоматически, в ОС виртуальной машины должен быть установлен пакет one-context.

6.1.3. Использование сетей

После настройки сети ПК СВ могут использоваться пользователями в соответствии с их полномочиями (см. 5.5).

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 Private, добавить в шаблон строку:

```
NIC = [ NETWORK = "Private" ]
```

2. При использовании идентификатора сети добавить в шаблон строку:

```
NIC = [ NETWORK_ID = 1]
```

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

Пример

Поместить ВМ в сеть Private с присвоением ей IP-адреса 10.0.0.153

```
NIC = [
NETWORK = "Private",
IP = 10.0.0.153
]
```

ВНИМАНИЕ! Пользователи могут подключать ВМ или резервировать ресурсы только той сети, в которой у них есть права доступа типа USE.

Гипервизоры могут устанавливать MAC-адрес для сетевого интерфейса ВМ, но не IP-адрес. Конфигурация IP в ВМ выполняется в процессе контекстуализации.

Для настройки сети ВМ может быть указана дополнительная информация, которая передается в ВМ во время загрузки через механизм контекстуализации. При этом могут быть переданы следующие параметры сети: маска сети, DNS-серверы или шлюзы. Параметры контекстуализации автоматически добавляются в ВМ и обрабатываются контекстными пакетами. Для этого в шаблон ВМ необходимо добавить следующий блок:

```
CONTEXT = [
   NETWORK="yes"
   ]
```

6.1.4. Управление сетями в интерфейсе командной строки

Для управления сетями используется инструмент командной строки `onevnet`.

6.1.4.1. Добавление, удаление и просмотр параметров сети

Для создания сети используется команда:

```
onevnet create <файл-шаблон>
```

где <файл-шаблон> — файл шаблона, в котором установлены значения параметров создаваемой сети.

Примеры:

1. Содержание файла шаблона `priv.net`:

```
NAME    = "Private"
VN_MAD  = "bridge"
AR=[
   TYPE = "IP4",
   IP   = "10.0.0.150",
   SIZE = "51"
```

```
]
DNS     = "10.0.0.23"
GATEWAY = "10.0.0.1"
DESCRIPTION = "Частная сеть для ВМ с доступом к сети Интернет"
```

В представленном примере описана сеть, работающая в режиме «сетевой мост» без фильтрации. Сеть предоставит IP-адреса в диапазоне от 10.0.0.150 до 10.0.0.200. Виртуальные машины в сети получат IP-адреса из указанного диапазона и настроят следующую сетевую конфигурацию:

- IP-адрес DNS-сервера: 10.0.0.23;
- IP-адрес шлюза: 10.0.0.1.

2. Создание сети с использованием файла шаблона `priv.net`:

```
onevnet create priv.net
```

Пример вывода после выполнения команды:

```
ID: 1
```

Для удаления сети используется команда:

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

В качестве наименования сети можно указать перечень сетей (идентификаторов или наименований, разделенных запятыми) или диапазон идентификаторов сетей (в качестве разделителя используются две точки — «..»).

Для отображения имеющихся сетей используется команда `onevnet list`.

Для получения подробной информации о конкретной сети используется команда:

```
onevnet show <идентификатор/наименование_сети>
```

Пример

Пример вывода после выполнения команды `onevnet show 1`:

```
VIRTUAL NETWORK 1 INFORMATION
ID : 1
NAME : Private
USER : oneadmin
GROUP : brestadmins
LOCK : None
CLUSTERS : 0
BRIDGE : onebr1
VN_MAD : bridge
AUTOMATIC VLAN ID : NO
AUTOMATIC OUTER VLAN ID : NO
USED LEASES : 0

PERMISSIONS
OWNER : um-
```

```
GROUP : ---
OTHER : ---

VIRTUAL NETWORK TEMPLATE
BRIDGE="onebr1"
BRIDGE_TYPE="linux"
DESCRIPTION="Частная сеть для ВМ с доступом к сети Интернет"
DNS="10.0.0.23"
GATEWAY="10.0.0.1"
PHYDEV=""
SECURITY_GROUPS="0"
VN_MAD="bridge"
```

6.1.4.2. Изменение параметров сети

После создания сети для изменения значений ее параметров необходимо использовать команду:

`onevnet update <идентификатор/наименование_сети> [<файл-шаблон>]`

где <файл-шаблон> — файл шаблона для настройки параметров сети. Если файл шаблона не указан, то после ввода команды откроется текстовый редактор `Vim` для формирования временного шаблона. После сохранения внесенных данных и закрытия редактора, подготовленный шаблон будет применен для настройки параметров сети, а временный файл шаблона будет удален.

Кроме того, можно изменить название сети при помощи команды:

`onevnet rename <идентификатор_сети> <новое_наименование_сети>`

6.1.4.3. Управление диапазонами адресов

Диапазон адресов представляет собой непрерывный интервал значений. При этом можно динамически добавлять или удалять AR из сети. Таким образом, можно легко добавить новые адреса в существующую сеть, если имеющиеся адреса закончились.

Новый AR можно добавить командой `onevnet addar`, указав идентификатор/наименование сети и необходимые параметры.

Примеры:

1. Добавление нового AR из 20 IP-адресов в сеть с наименованием «Private»

```
onevnet addar Private --ip 10.0.0.200 --size 20
```

2. Просмотр параметров сети после добавления AR. 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
```

Для удаления AR необходимо использовать команду:

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

Примеры:

1. Удаление AR с идентификатором 0 из сети с наименованием «Private»

```
onevnet rmar Private 0
```

2. Просмотр параметров сети после удаления AR. Пример вывода после выполнения команды `onevnet show Private`:

```
...
ADDRESS RANGE POOL
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
```

Для изменения значений параметров AR необходимо использовать команду:

```
onevnet updatear <идентификатор/наименование_сети> <идентификатор_AR> \
   [<файл-шаблон>]
```

где <файл-шаблон> — файл шаблона для настройки параметров AR. Если файл шаблона не указан, то после ввода команды откроется текстовый редактор `Vim` для формирования временного шаблона. После сохранения внесенных данных и закрытия редактора, подготовленный шаблон будет применен для настройки параметров AR, а временный файл шаблона будет удален.

Возможно изменить значения следующих параметров AR:

- префикс IPv6 — `GLOBAL_PREFIX` и `ULA_PREFIX`;
- любой пользовательский параметр, значение которого может отменять стандарт-

ные значения параметров сети.

6.1.4.4. Резервирование адресов

Адресам можно временно присвоить метку `hold` (зарезервировано). Они будут являться частью сети, но не будут выделяться для ВМ.

Для резервирования адреса используется команда:

```
onevnet hold <идентификатор/наименование_сети> <IP-адрес>
```

По умолчанию адрес будет поставлен на удержание во всех AR, в которые он включен. Если требуется удержать IP-адрес определенного AR, его необходимо указать с помощью аргумента `-a <идентификатор_AR>`.

Примеры:

1. Удержание IP-адреса 10.0.0.120 во всех AR сети с наименованием «Private»

```
onevnet hold Private 10.0.0.120
```

2. Удержание IP-адреса 10.0.0.123 в AR с идентификатором 1 сети с наименованием «Private»

```
onevnet hold Private 10.0.0.207 -a 1
```

3. Просмотр параметров сети после изменения AR. Пример вывода после выполнения команды `onevnet show Private`:

```
...
ADDRESS RANGE POOL
AR 1
SIZE           : 20
LEASES         : 1

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

AR 2
SIZE           : 51
LEASES         : 1

RANGE                 FIRST                 LAST
MAC      02:00:0a:00:00:64    02:00:0a:00:00:96
IP              10.0.0.100           10.0.0.150



LEASES
```

```
AR  OWNER    MAC                IP           PORT_FORWARD   IP6
1   V:-1     02:00:0a:00:00:cf  10.0.0.207   -              -
2   V:-1     02:00:0a:00:00:78  10.0.0.120   -              -
```

Для разблокировки адреса используется команда:

```
onevnet release <идентификатор/наименование_сети> <IP-адрес>
```

6.1.5. Управление сетями в веб-интерфейсе ПК СВ

Для отображения перечня всех сетей в веб-интерфейсе ПК СВ необходимо в меню слева выбрать пункт меню «Система — Вирт.сети». На открывшейся странице «Вирт. сети» будет представлена таблица сетей (см. рис. 27).

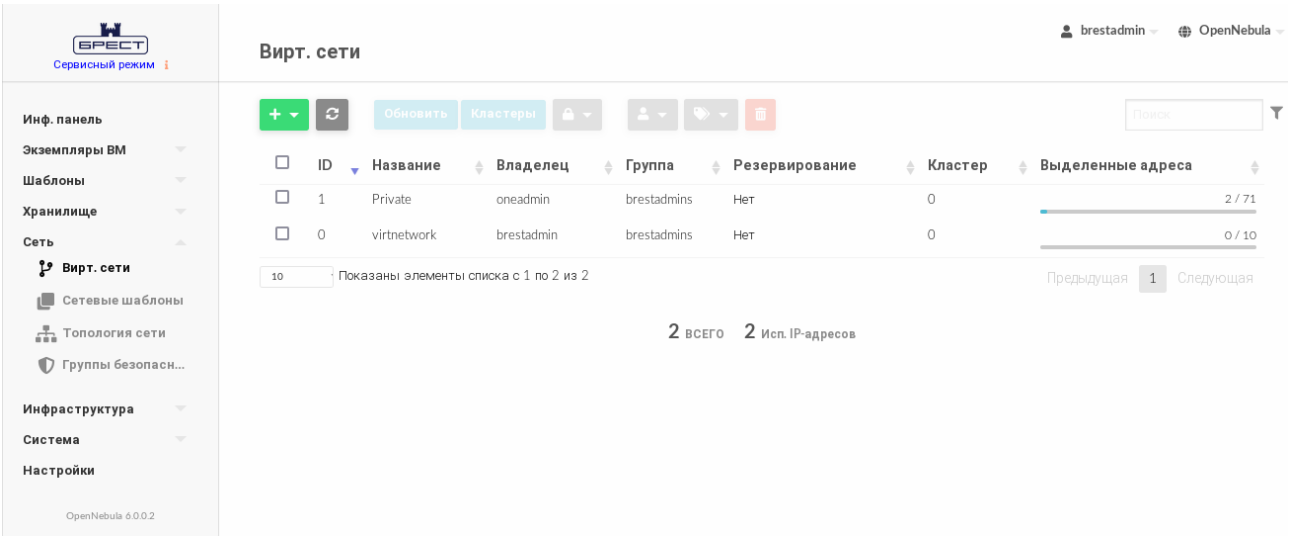

Рис. 27

Для добавления 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» нажать на кнопку **[+]**, а затем в открывшемся меню выбрать пункт «Создать»;
2) на открывшейся странице «Создать Виртуальную сеть»:
   а) во вкладке «Общие» в поле «Название» задать наименование сети;
   б) во вкладке «Конфигурация» указать режим работы сети;
   в) во вкладке «Адреса» задать диапазоны адресов (AR)
   г) нажать на кнопку **[Создать]**.

После этого на открывшейся странице «Вирт.сети» появится запись о созданной сети.

Для просмотра информации о конкретной сети на странице «Вирт.сети» необходимо выбрать соответствующую строку. После этого откроется страница сети (вкладка «Сведения» — см. рис. 28).

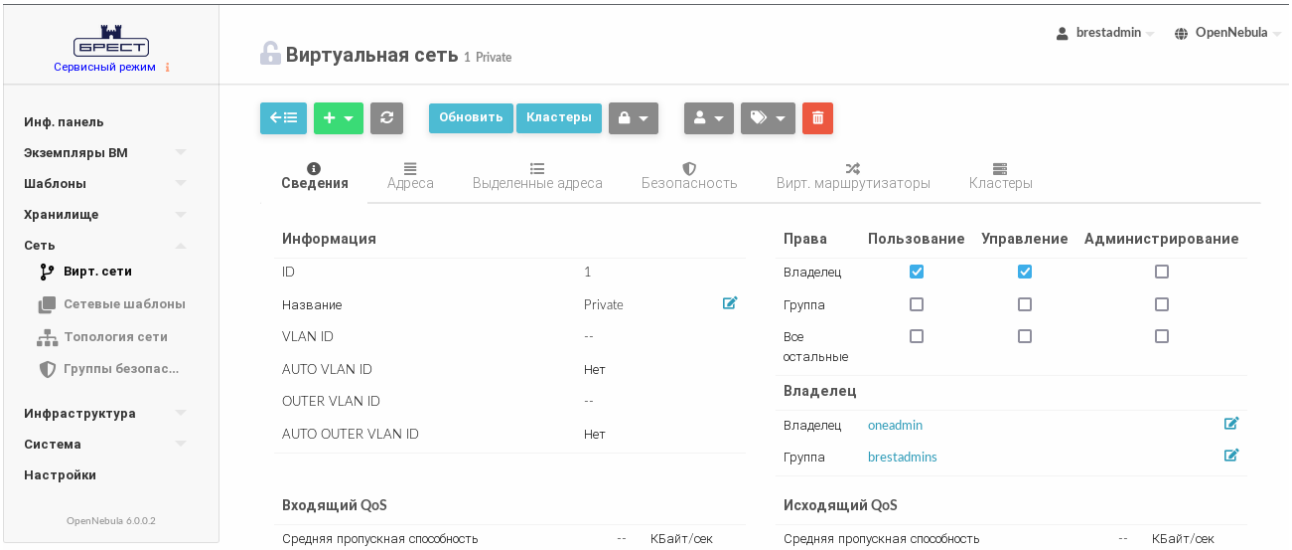

Рис. 28

Чтобы изменить параметры сети (в том числе, наименование), 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 необходимую сеть;
2) на открывшейся странице сети нажать на кнопку **[Обновить]**;
3) на открывшейся странице «Изменить виртуальную сеть»:
   а) во вкладке «Общие» скорректировать наименование сети;
   б) во вкладке «Конфигурация» скорректировать режим работы сети;
   в) во вкладке «Адреса» скорректировать диапазоны адресов (AR)
   г) нажать на кнопку **[Обновить]**.

Чтобы зарезервировать адрес, 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 необходимую сеть;
2) на открывшейся странице сети нажать на кнопку **[+]**, а затем в открывшемся меню выбрать пункт «Зарезервировано»;
3) на открывшейся странице «Резервирование из Виртуальной сети» указать адрес/адреса, которые необходимо зарезервировать и нажать на кнопку **[Зарезервировано]** (см. рис. 29).

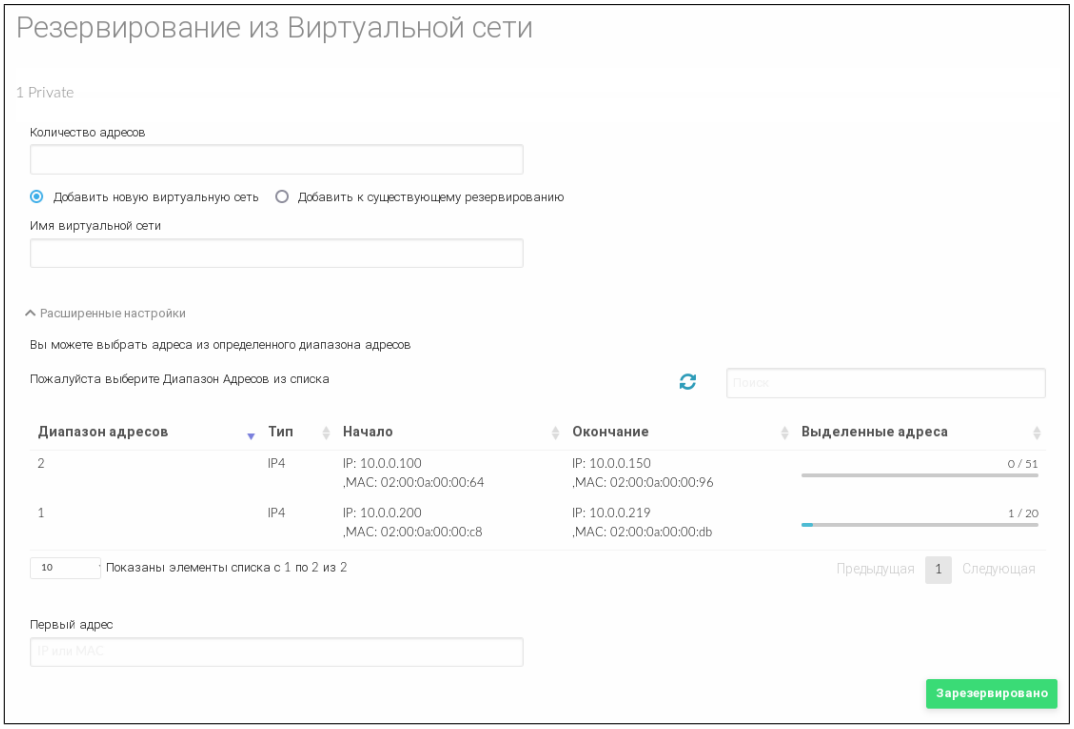

Рис. 29

6.2. Сетевые группы безопасности

Группы безопасности определяют правила сетевого фильтра, которые будут применяться в отношении виртуальных машин.

ВНИМАНИЕ! Сетевые группы безопасности не поддерживаются для сетей OpenvSwitch, а также для адресации IPv6.

6.2.1. Параметры сетевой группы безопасности

Сетевая группа безопасности состоит из нескольких правил. Каждое правило определяется параметрами, приведенными в таблице 13.

Таблица 13

Параметр	Статус	Описание	Значение
PROTOCOL	Обяз.	Определяет протокол правила	ALL, TCP, UDP, ICMP, IPSEC
RULE_TYPE	Обяз.	Определяет направление правила	INBOUND, OUTBOUND
IP	Необяз.	Используется, если правило применяется только для определенной сети. Это первый IP-адрес из диапазона IP-адресов (AR). Должен применяться совместно с параметром SIZE	Действительный IP-адрес
SIZE	Необяз.	Используется, если правило применяется только для определенной сети. Определяет размер диапазона IP-адресов (AR). Должен применяться совместно с параметром IP	Целое значение от 1

Окончание таблицы 13

Параметр	Статус	Описание	Значение
RANGE	Необяз.	Диапазон портов для фильтрации определенных портов. Работает только с TCP и UDP	Несколько портов или диапазонов портов разделяются запятой, а диапазон портов указывается при помощи двоеточия. Например, 22,53,80:90,110,1024:65535
ICMP_TYPE	Необяз.	Особый тип ICMP для правила. Если у правила несколько кодов, он включает их все. Можно использовать только с ICMP. Если отсутствует, правило повлияет на весь протокол ICMP.	0,3,4,5,8,9,10,11,12,13, 14,17,18
NETWORK_ID	Необяз.	Идентификатор сети. Используется, если правило применяется только для определенной сети.	Идентификатор существующей сети

6.2.2. Стандартная группа безопасности

По умолчанию применяется стандартная группа безопасности (с наименованием `default` и идентификатором 0). Данная группа разрешает весь входящий (INBOUND) и исходящий трафик (OUTBOUND). Если нужно ограничить соединения, необходимо изменить стандартную группу безопасности. Стандартную группу безопасности следует рассматривать как абсолютный минимум для всех ВМ. Например, может быть целесообразно установить TCP-порт 22 как входящий для SSH, а порт 80 и порт 443 — как исходящий, чтобы иметь возможность устанавливать пакеты.

Примечание. Стандартная группа безопасности добавляется во все сети при их создании, но впоследствии ее можно удалить, обновив свойства сети.

6.2.3. Управление группами безопасности в интерфейсе командной строки

Управление группами безопасности осуществляется с помощью инструмента командной строки `onesecgroup`.

6.2.3.1. Добавление, удаление и просмотр списка групп безопасности

Для создания группы безопасности используется команда:

```
onesecgroup create <файл-шаблон>
```

где <файл-шаблон> — файл шаблона с параметрами группы безопасности.

Примеры:

1. Содержание файла шаблона `sg.txt`:

```
NAME = test
RULE = [
   PROTOCOL = TCP,
   RULE_TYPE = inbound,
```

```
   RANGE = 1000:2000
]
RULE = [
   PROTOCOL= TCP,
   RULE_TYPE = outbound,
   RANGE = 1000:2000
]
RULE = [
   PROTOCOL = ICMP,
   RULE_TYPE = inbound,
   NETWORK_ID = 0
]
```

2. Создание группы безопасности с использованием файла шаблона `sg.txt`:

```
onesecgroup create sg.txt
```

Пример вывода после выполнения команды:

```
ID: 100
```

Для просмотра имеющихся групп безопасности, необходимо выполнить команду:

```
onesecgroup list
```

Пример вывода после выполнения команды:

```
ID   USER     GROUP     NAME     UPDATED   OUTDATED   ERROR
100  oneadmin brestadm  test     0         0          0
0    oneadmin brestadm  default  0         0          0
```

Для удаления группы безопасности используется команда:

```
onesecgroup delete <идентификатор/наименование_группы>
```

В качестве наименования сети можно указать перечень сетей (идентификаторов или наименований, разделенных запятыми) или диапазон идентификаторов сетей (в качестве разделителя используются две точки — «..»).

6.2.3.2. Просмотр и изменение правил группы безопасности

Для просмотра правил, установленных в группе безопасности, необходимо выполнить команду:

```
onesecgroup show <идентификатор/наименование_группы>
```

Пример вывода после выполнения команды:

```
SECURITY GROUP 100 INFORMATION
ID              : 100
NAME            : test
USER            : oneadmin
GROUP           : brestadmins
```

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

VIRTUAL MACHINES
UPDATED        :
OUTDATED       :
ERROR          :

RULES
TYPE       PROTOCOL    ICMP_TYPE    ICMVP6_TYPE    NETWORK    RANGE
inbound    TCP                                     Any        1000:2000
outbound   TCP                                     Any        1000:2000
inbound    ICMP                                    VNet 0
```

Для изменения правил необходимо использовать команду:

```
onesecgroup update <идентификатор/наименование_группы> [<файл-шаблон>]
```

где <файл-шаблон> — файл шаблона для изменения правил. Если файл шаблона не указан, то после ввода команды откроется текстовый редактор Vim для формирования временного шаблона. После сохранения внесенных данных и закрытия редактора, подготовленный шаблон будет применен для изменения правил, а временный файл шаблона будет удален.

Кроме того, можно изменить название группы безопасности при помощи команды:

```
onesecgroup rename <идентификатор_группы> <новое_наименование_группы>
```

6.2.3.3. Применение группы безопасности

Для применения групп безопасности к виртуальным машинам необходимо конкретные группы безопасности присвоить сети, используемой в ВМ. Для этого необходимо выполнить команду:

```
onevnet update <идентификатор/наименование_сети>
```

После ввода команды откроется текстовый редактор Vim в котором отобразятся параметры сети (см. 6.1.2) — для работы редактора используется временный файл шаблона. Необходимо скорректировать значение параметра SECURITY_GROUPS, указав через запятую перечень идентификаторов групп безопасности. После сохранения измененных значений параметров и закрытия редактора, измененный шаблон будет применен для установки новых значений параметров сети, а временный файл шаблона будет удален.

Также возможно настроить группы безопасности для каждого диапазона адресов (AR) сети. Для этого необходимо выполнить команду:

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

После ввода команды откроется текстовый редактор `Vim` в котором отобразятся параметры диапазона адресов (для работы редактора используется временный файл шаблона). Необходимо скорректировать значение параметра `SECURITY_GROUPS`, указав через запятую перечень идентификаторов групп безопасности. После сохранения измененных значений параметров и закрытия редактора, измененный шаблон будет применен для установки новых значений параметров диапазона адресов, а временный файл шаблона будет удален.

Кроме того, в группе параметров `NIC` каждого шаблона сети может определять перечень групп безопасности.

Пример

```
NIC = [
   NETWORK = "private-net",
   NETWORK_UNAME = "oneadmin",
   SECURITY_GROUPS = "103, 125"
]
```

ВНИМАНИЕ! Если AR или NIC шаблона определяют группы безопасности с помощью параметра `SECURITY_GROUPS`, то указанные идентификаторы не будут перезаписывать идентификаторы, определенные в сети. Все идентификаторы групп безопасности объединяются и применяются в отношении экземпляра ВМ.

Для редактирования или добавления новых правил фильтрации трафика можно обновлять группы безопасности. Эти изменения будут применяться ко всем ВМ в группе безопасности, поэтому внесение изменений может занять некоторое время. Конкретный статус ВМ можно проверить в свойствах группы безопасности, где перечислены устаревшие и текущие ВМ.

Если необходимо сбросить процесс обновления, т.е. снова применить правила, использовать команду `onesecgroup commit`.

6.2.4. Управление группами безопасности в веб-интерфейсе ПК СВ

Для отображения перечня всех групп безопасности в веб-интерфейсе ПК СВ необходимо в меню слева выбрать пункт меню «Система — Группы безопасности». На открывшейся странице «Группы безопасности» будет представлена таблица имеющихся групп безопасности (см. рис. 30).

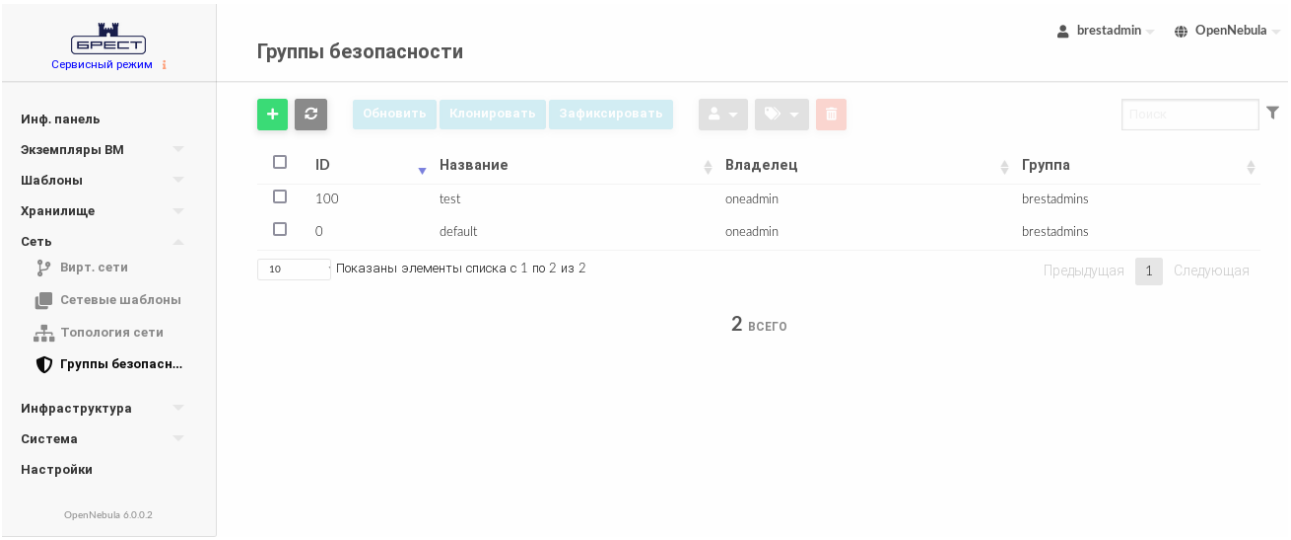

Рис. 30

Для добавления группы безопасности в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

1) в меню слева выбрать пункт меню «Сеть — Группы безопасности» и на открывшейся странице «Группы безопасности» нажать на кнопку **[+]**;
2) на открывшейся странице «Создать Группу безопасности»:
   а) в поле «Название» задать наименование группы безопасности;
   б) в секции «Правила» задать правила фильтрации трафика;
   в) нажать на кнопку **[Создать]** (см. рис. 31).

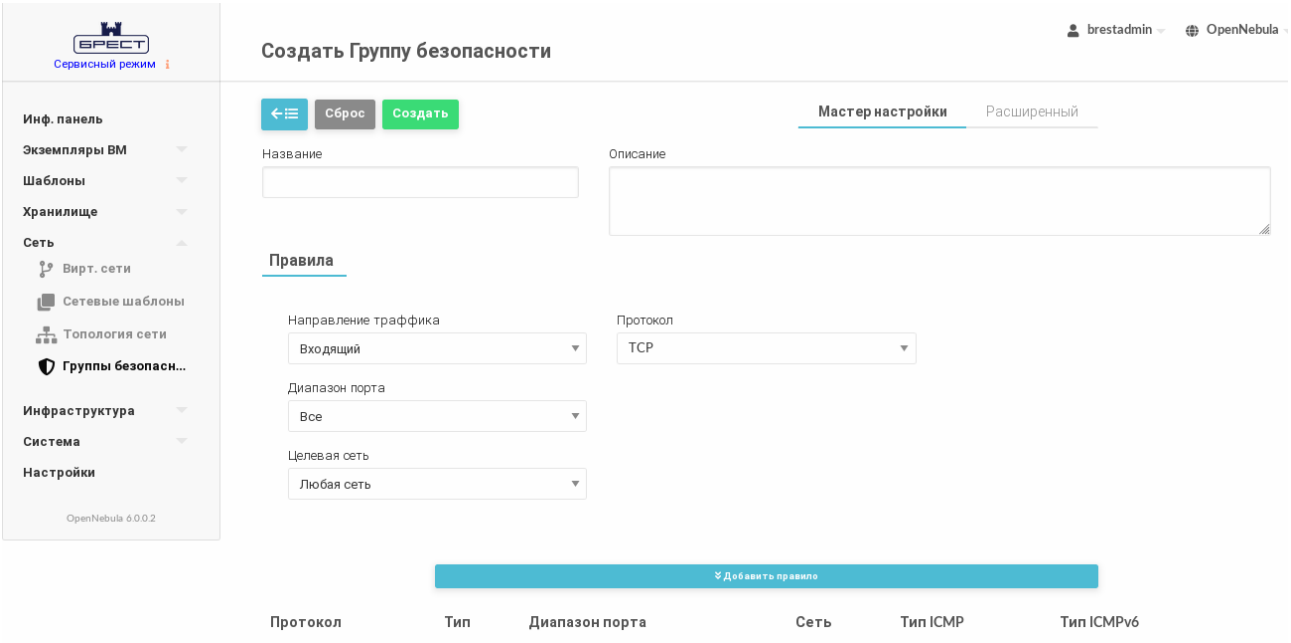

Рис. 31

После этого на открывшейся странице «Группы безопасности» появится запись о созданной группе безопасности.

Для просмотра информации о конкретной группе безопасности на странице «Груп-

пы безопасности» необходимо выбрать соответствующую строку. После этого откроется страница группы безопасности (вкладка «Сведения» — см. рис. 32).

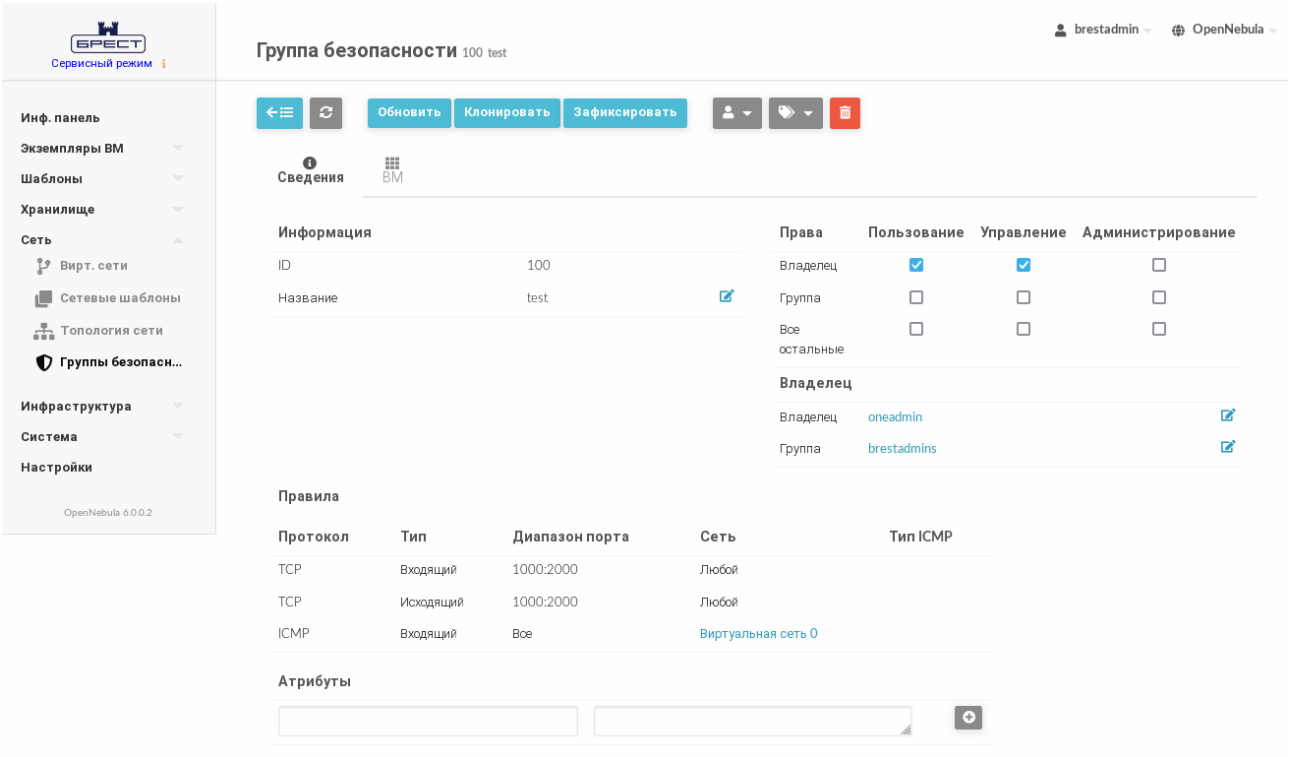

Рис. 32

Чтобы изменить правила фильтрации трафика (в том числе, установить новые), в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

1) в меню слева выбрать пункт меню «Сеть — Группы безопасности» и на открывшейся странице «Группы безопасности» выбрать необходимую группу безопасности;
2) на открывшейся странице группы безопасности нажать на кнопку **[Обновить]**;
3) на открывшейся странице «Обновить Группу безопасности» скорректировать правила фильтрации трафика и нажать на кнопку **[Обновить]**.

7. УПРАВЛЕНИЕ ВИРТУАЛЬНОЙ МАШИНОЙ

7.1. Управление экземплярами ВМ

7.1.1. Статус и жизненный цикл виртуальной машины

В процессе функционирования экземпляру ВМ присваивается один из статусов, описание которых приведено в таблице 14.

Таблица 14

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	Владелец поставил ВМ на удержание, она не доступна для развертывания в автоматическом режиме, пока не будет разблокирована. Однако ее можно развернуть вручную
ACTIVE	см. таблицу 15	ВМ запущена и находится в одном из состояний жизненного цикла (см. таблицу 15)
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
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

Окончание таблицы 14

Статус	Сокращенное название статуса	Описание
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 15.

Таблица 15

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
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

Продолжение таблицы 15

Состояние	Сокращенное название состояния	Описание
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
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

Продолжение таблицы 15

Состояние	Сокращенное название состояния	Описание
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
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

Продолжение таблицы 15

Состояние	Сокращенное название состояния	Описание
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
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)

Окончание таблицы 15

Состояние	Сокращенное название состояния	Описание
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. 7.1.2.1) или в веб-интерфейсе ПК СВ на странице ВМ во вкладке «Сведения» (см. 7.1.3.1).

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

7.1.2. Управление экземплярами ВМ в интерфейсе командной строки

7.1.2.1. 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               : ---
```

7.1.2.2. 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.

7.1.2.3. 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 т.ч. 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.

7.1.2.4. 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.

7.1.2.5. 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.

7.1.3. Управление экземплярами ВМ в веб-интерфейсе ПК СВ

7.1.3.1. 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. 33)

Рис. 33

Для просмотра полной информации о ВМ необходимо на странице «ВМ» выбрать необходимую ВМ. После этого откроется страница виртуальной машины (вкладка «Сведения») (см. рис. 34).

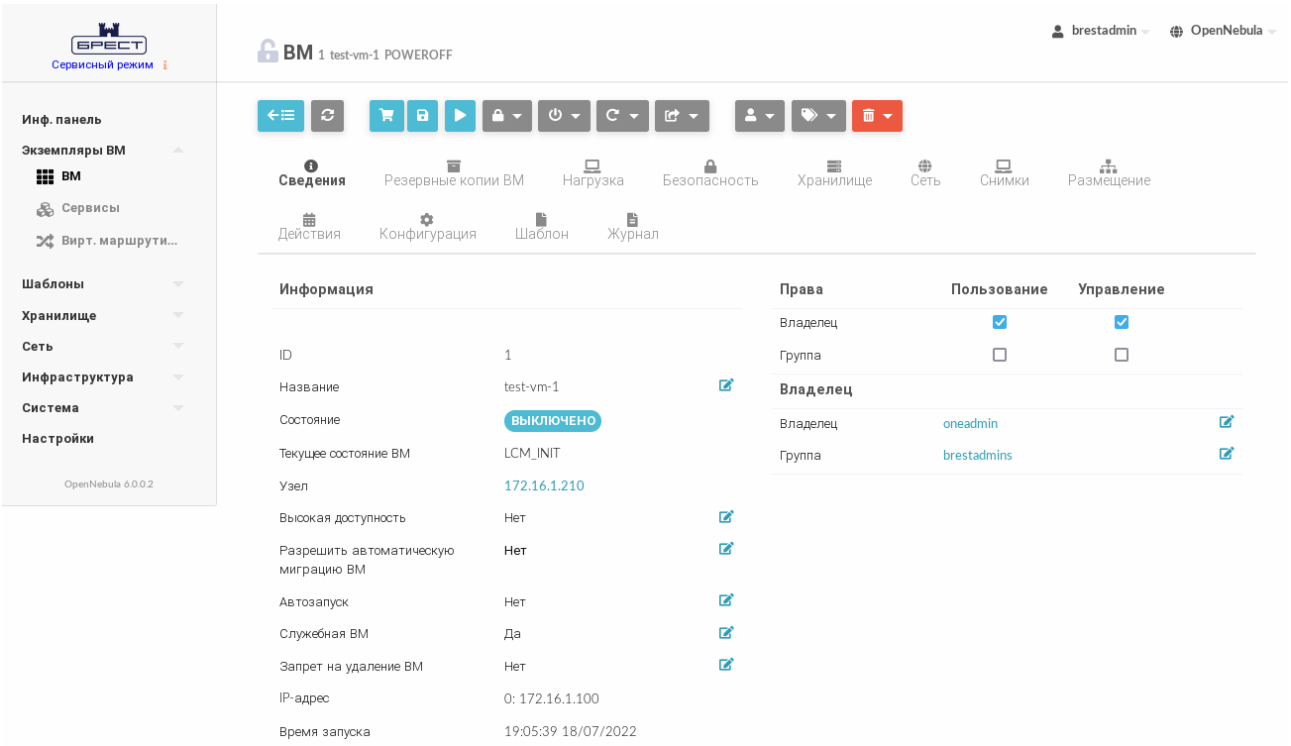

Рис. 34

7.1.3.2. 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. 35):

- `Приостановить работу ВМ` — краткосрочная приостановка: состояние ВМ, в т.ч. 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 жестко` — 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 жестко — аналогично команде Отменить размещение, но работающая ВМ удаляется незамедлительно.

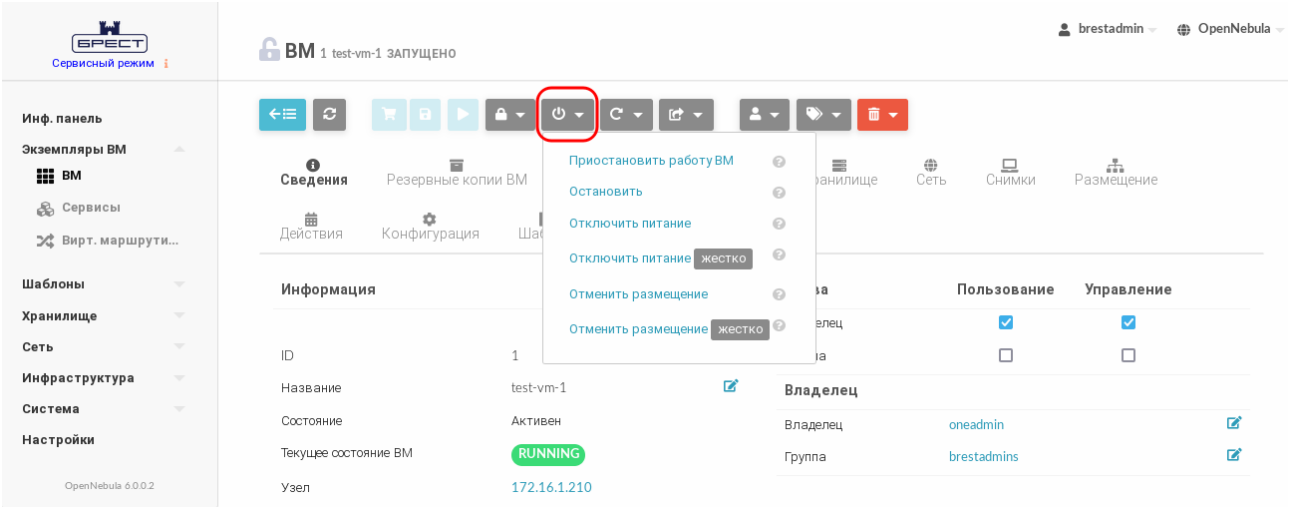

Рис. 35

7.1.3.3. Перезагрузка экземпляров ВМ

Для перезагрузки ВМ в веб-интерфейсе ПК СВ используется кнопка **[Перезагрузка]**, после нажатия на которую откроется меню действий (см. рис. 36):

- Перезагрузить — корректная перезагрузка работающей ВМ, отправляя сигнал ACPI;

- Перезагрузить жестко — принудительная перезагрузка работающей ВМ, актуально, если ВМ не поддерживает ACPI.

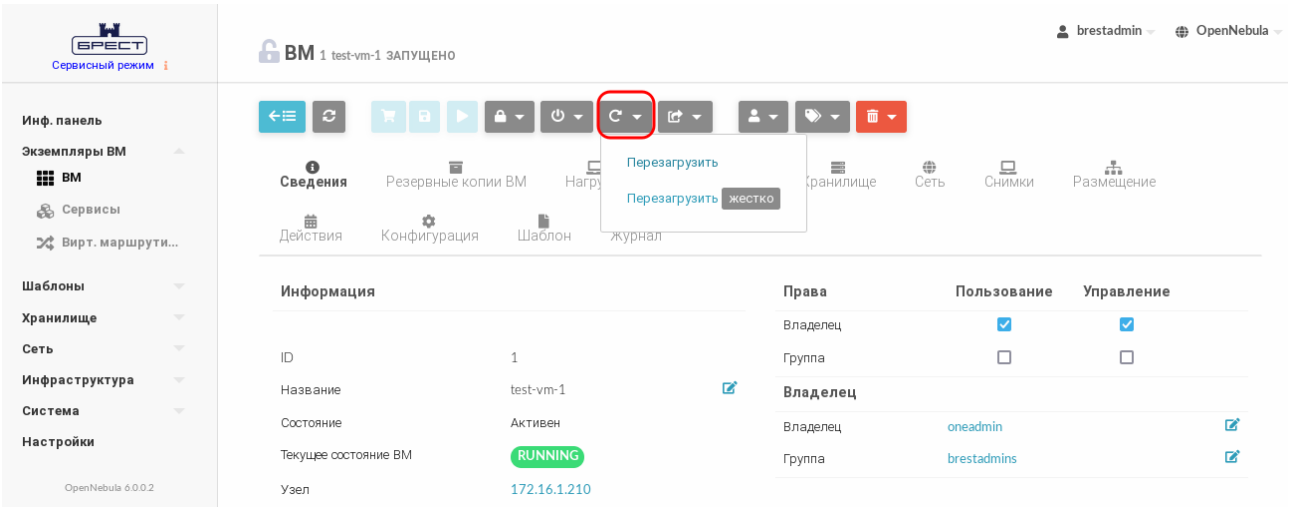

Рис. 36

7.1.3.4. 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. 37):

- Заблокировать — переводит ВМ в состояние удержания;

- Разблокировать — разблокировать ВМ, находящуюся на удержании.

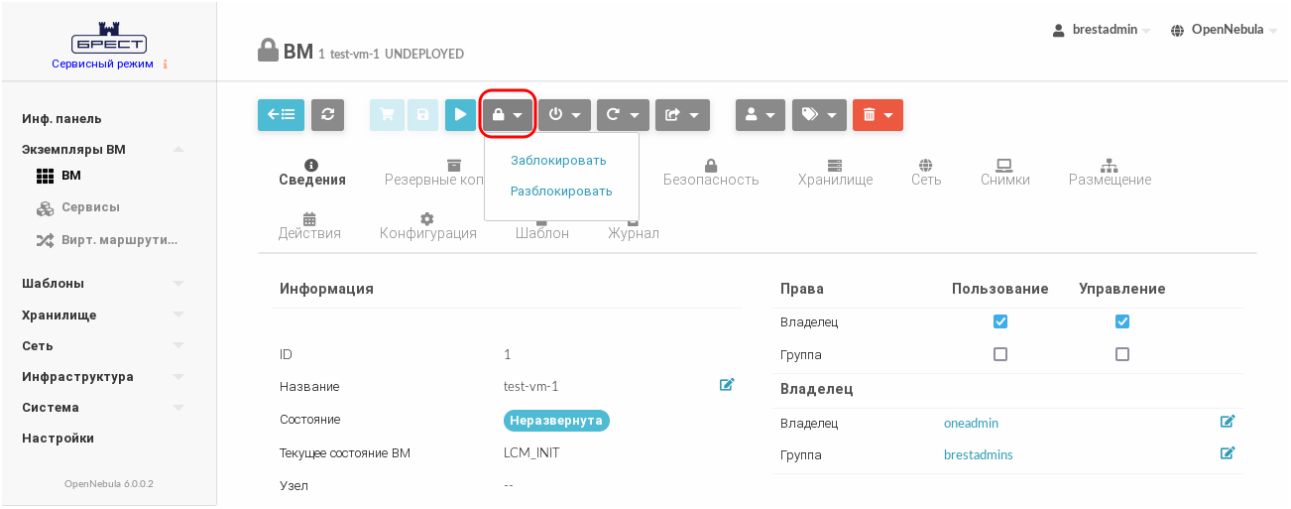

Рис. 37

7.1.3.5. Удаление экземпляров BM

Для удаления экземпляров BM в веб-интерфейсе ПК СВ используется кнопка **[Уничтожить]**, после нажатия на которую откроется меню действий (см. рис. 38):

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

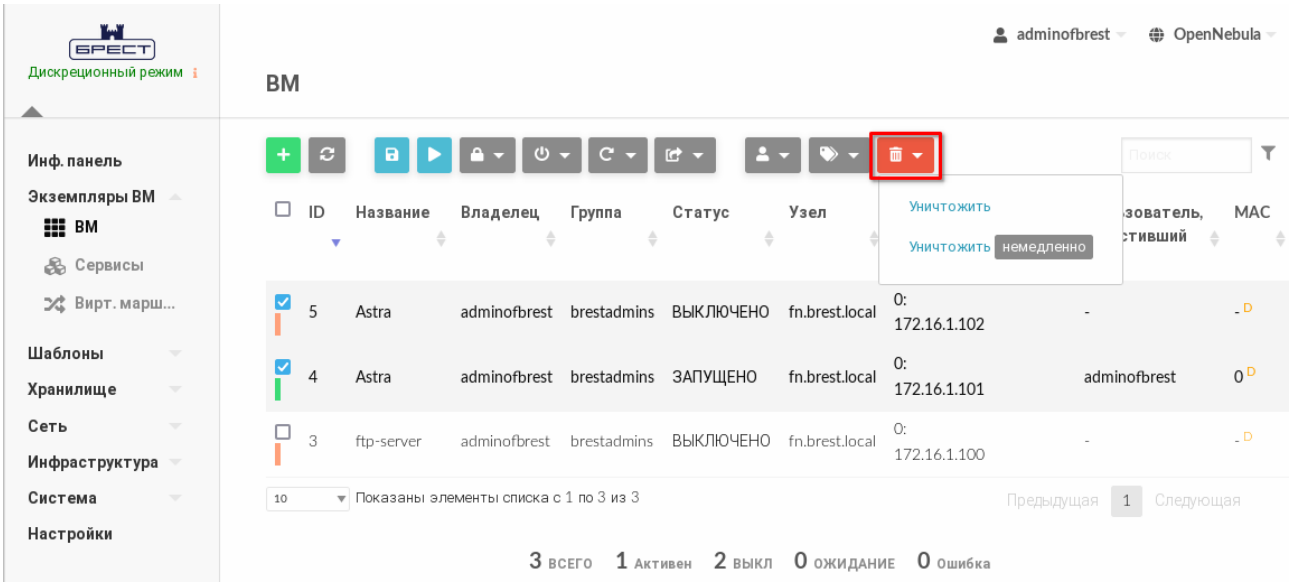

Рис. 38

7.1.4. Снимки состояний BM

Снимок состояния BM содержит снимки состояния диска и оперативной памяти BM. Пользователь может делать снимки состояния BM, только если BM в текущий момент работает (находится в состоянии RUNNING).

7.1.4.1. Управление снимками состояний в интерфейсе командной строки

Для создания снимка состояния ВМ необходимо выполнить команду:

```
onevm snapshot-create <идентификатор_ВМ> [<наименование_снимка>]
```

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

Примеры:

1. Создание снимка состояния ВМ с идентификатором 1

```
onevm snapshot-create 1 test-snapshot
```

2. Просмотр информации о ВМ, пример вывода после выполнения команды `onevm show 1`

```
VIRTUAL MACHINE 1
...
SNAPSHOTS
ID TIME          NAME                  HYPERVISOR_ID
0  07/19 12:18   после установки ОС    snap-0
1  07/19 13:14   test-snapshot         snap-1
...
```

Для возвращения ВМ к состоянию, указанному в снимке, необходимо выполнить команду:

```
onevm snapshot-revert <идентификатор_ВМ> <идентификатор_снимка>
```

Для удаления снимка состояния ВМ необходимо выполнить команду:

```
onevm snapshot-delete <идентификатор_ВМ> <идентификатор_снимка>
```

7.1.4.2. Управление снимками состояний в веб-интерфейсе ПК СВ

Для управления снимками состояний 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 «Снимки» (см. рис. 39).

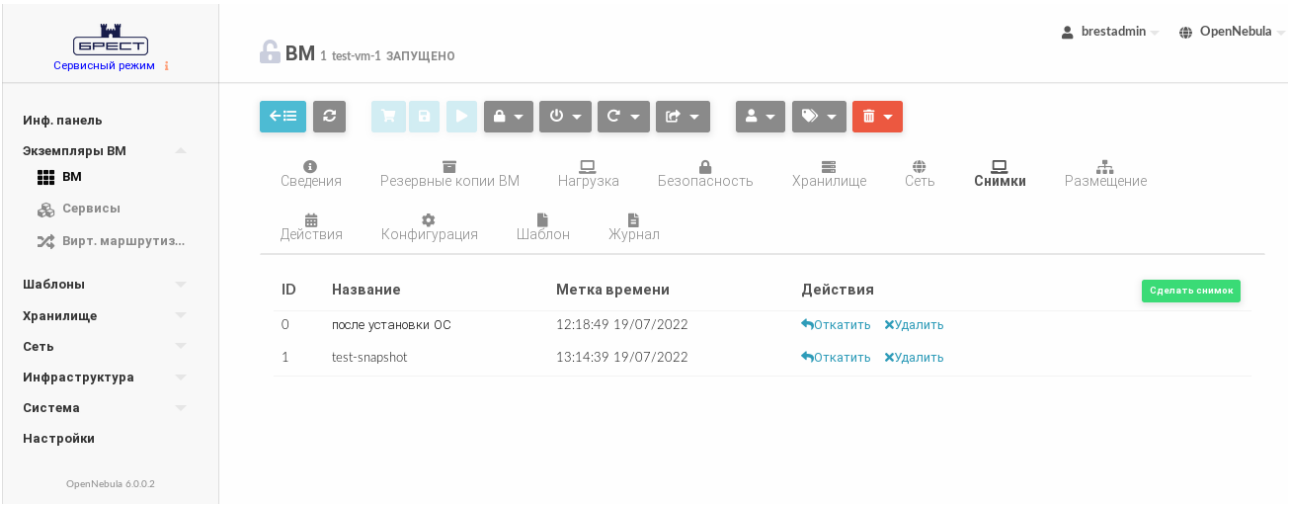

Рис. 39

На странице виртуальной машины во вкладке «Снимки»:

- для создания снимка состояния ВМ необходимо нажать на кнопку **[Сделать снимок]**;
- для возвращения ВМ к состоянию, указанному в снимке, необходимо нажать на кнопку **[Откатить]** в строке соответствующего снимка;
- для удаления снимка состояния ВМ необходимо нажать на кнопку **[Удалить]** в строке соответствующего снимка.

7.1.5. Снимки дисков ВМ

Пользователь может делать снимки состояния диска, только если ВМ в текущий момент работает (находится в состоянии RUNNING).

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.

7.1.5.1. 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.

7.1.5.2. 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 на кнопку **[Snapshot]** (см. рис. 40);

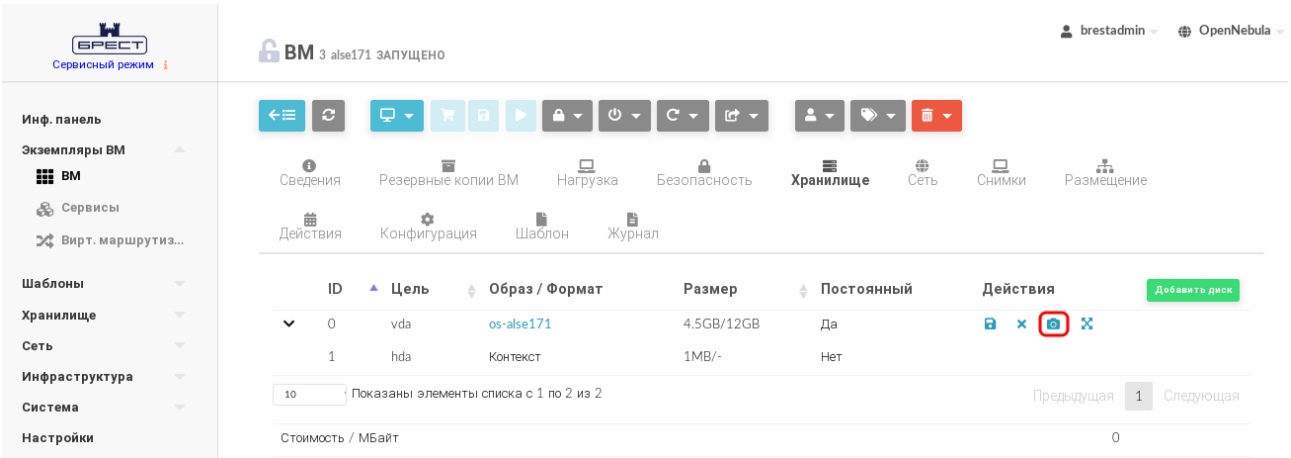

Рис. 40

4) в открывшемся окне «Снимок диска» задать наименование снимка и нажать на кнопку **[Сделать снимок]** (см. рис. 41).

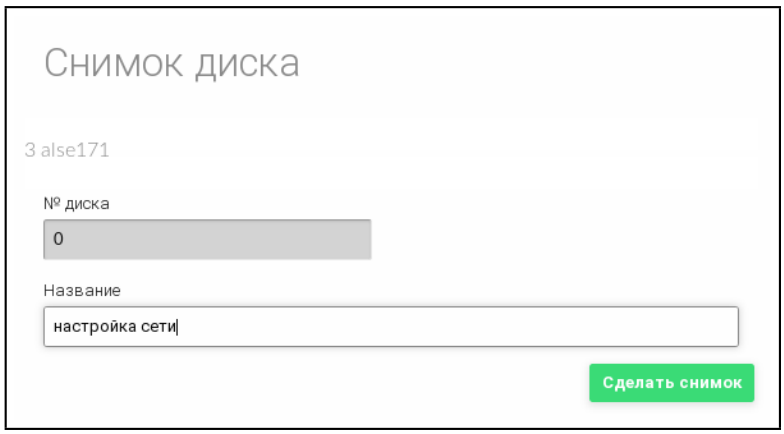

Рис. 41

На странице виртуальной машины во вкладке «Хранилище» (после остановки ВМ) — см. рис. 42:

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

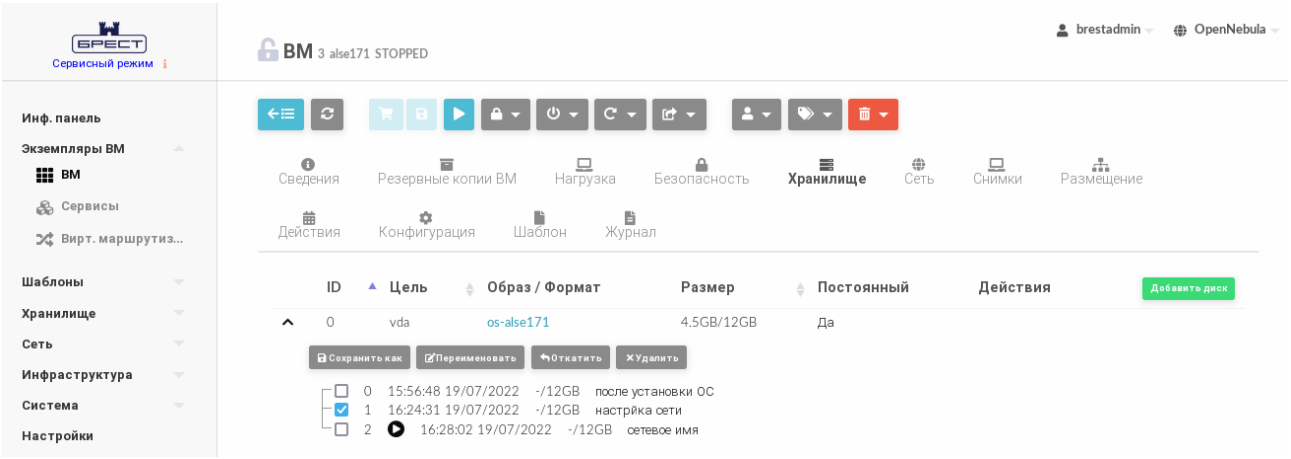

Рис. 42

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

7.1.6. Экспорт диска ВМ

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

7.1.6.1. 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.

7.1.6.2. 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 на кнопку **[Сохранить как]** (см. рис. 43);

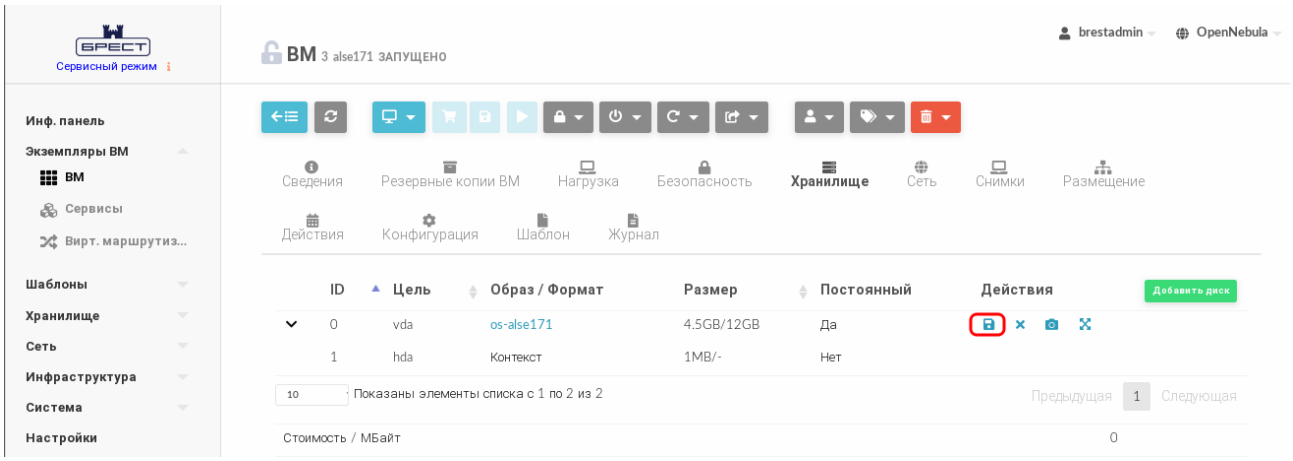

Рис. 43

4) в открывшемся окне «Сохранить диск как» задать наименование нового образа и нажать на кнопку **[Сохранить как]** (см. рис. 44).

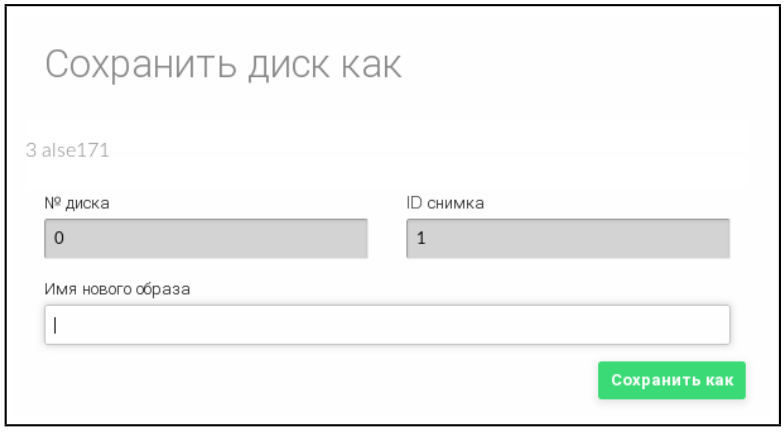

Рис. 44

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 на кнопку **[Сохранить как]** (см. рис. 42).

7.1.7. Горячее подключение диска

Возможность горячего подключения диска зависит от используемого гипервизора. Так, например, для гипервизора KVM возможно подключить только те диски, для эмуляции которых используется драйвер Virtio.

7.1.7.1. В интерфейсе командной строки

Для горячего подключения новых дисков к работающим ВМ используется команда:

```
onevm disk-attach  <идентификатор_ВМ> --image <идентификатор_образа>
```

Для отключения диска от работающей ВМ применяется команда:

```
onevm disk-detach  <идентификатор_ВМ> --image <идентификатор_образа>
```

7.1.7.2. В веб-интерфейсе ПК СВ

Для горячего подключения диска к 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 нажать на кнопку **[Добавить диск]** (см. рис. 45);

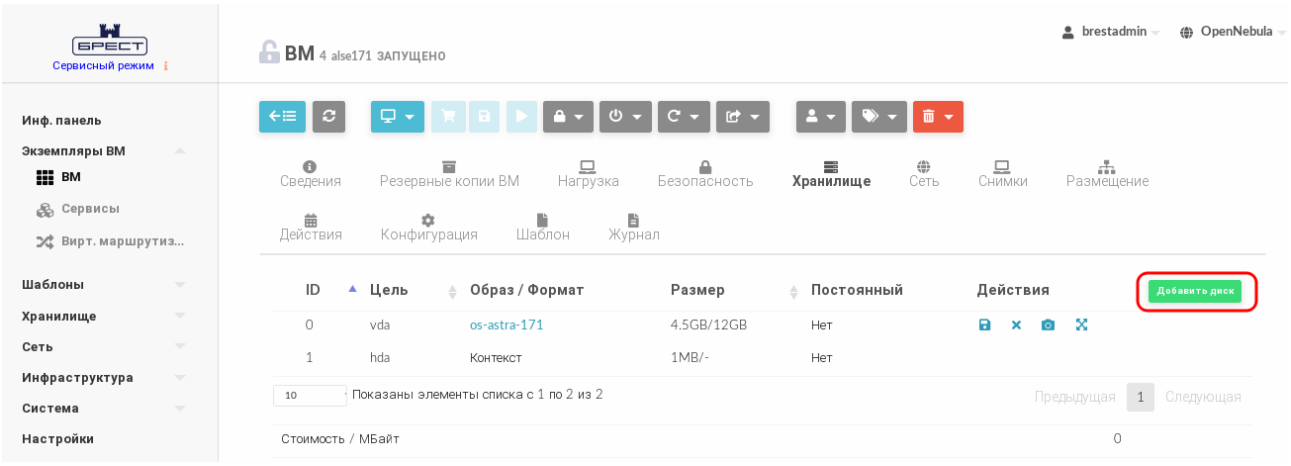

Рис. 45

4) в открывшемся окне «Присоединить диск» указать необходимый образ и нажать на кнопку **[Присоединить]** (см. рис. 46).

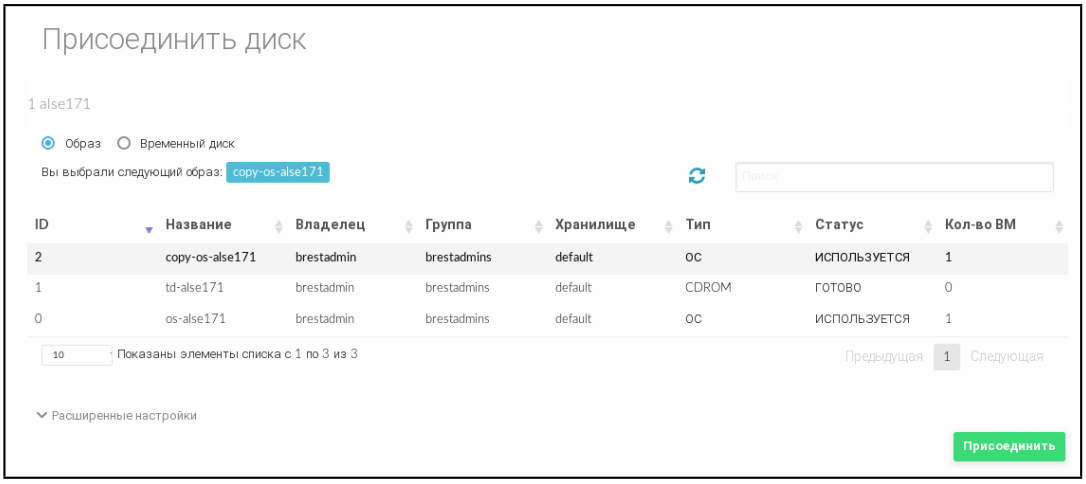

Рис. 46

Для горячего отключения диска от 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 на кнопку **[Detach]** (см. рис. 47);

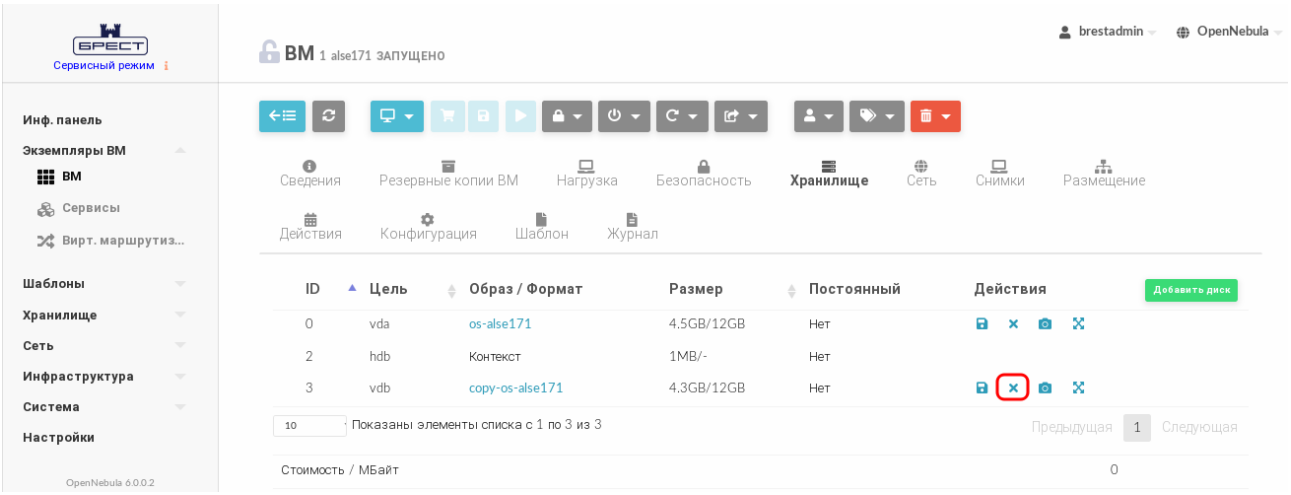

Рис. 47

4) в открывшемся окне «Подтвердить» нажать на кнопку **[OK]**.

7.1.8. Перераспределение производительности ВМ

В ПК СВ возможно перераспределить объем вычислительных ресурсов, выделяемых для ВМ в виде виртуальных ЦП и доли мощности ЦП сервера виртуализации. Перераспределение выполняется только когда ВМ находится в состоянии POWEROFF или UNDEPLOYED.

Для изменения объема вычислительных ресурсов ВМ требуется выполнить следующую последовательность действий:

- подготовить ВМ к отключению, например, остановить запущенные службы вручную;
- отключить питание ВМ;
- перераспределить ресурсы, выделяемые для ВМ;
- возобновить работу ВМ с новой производительностью.

7.1.8.1. В интерфейсе командной строки

Чтобы изменить объем вычислительных ресурсов, выделяемых для ВМ, используется команда:

```
onevm disk-attach  <наименование/идентификатор_ВМ> \
    [--cpu <доля_мощности_ЦП>] [--vcpu <кол-во_виртуальных_ЦП>]
```

Пример

Для ВМ с наименованием `alse17` выделить 50% мощности ЦП сервера виртуализации и 2 виртуальных ЦП:

```
onevm resize alse17 --cpu 0.5 --vcpu 2
```

7.1.8.2. В веб-интерфейсе ПК СВ

Для изменения объема вычислительных ресурсов 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 «Нагрузка» и нажать на кнопку **[Изменить]** (см. рис. 48);

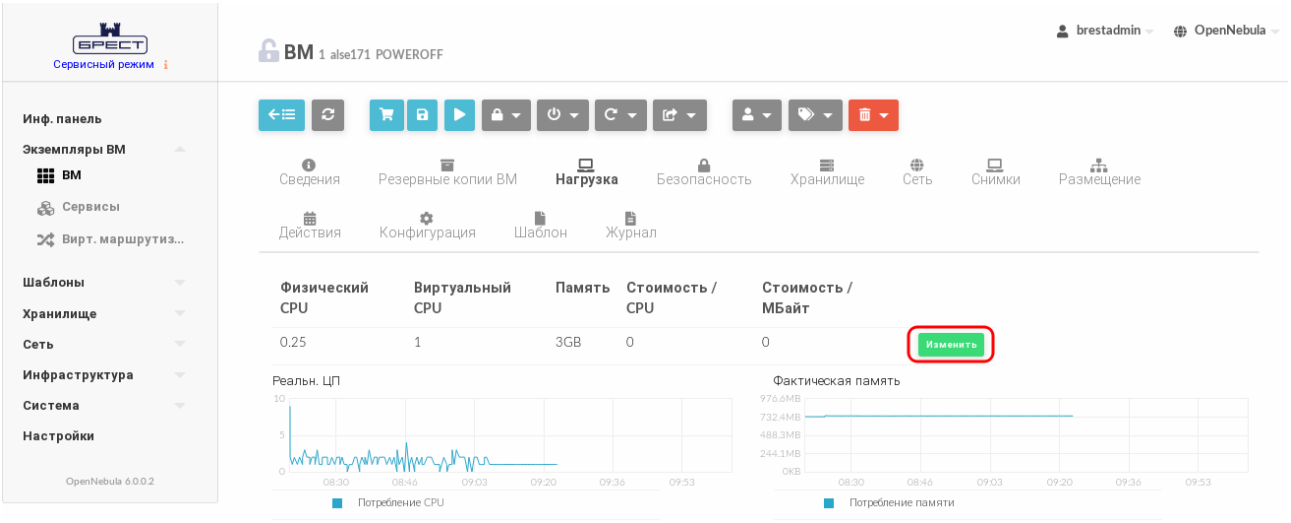

Рис. 48

4) в открывшемся окне «Изменить базовые характеристики» внести необходимые корректировки и нажать на кнопку **[Изменить]** (см. рис. 49).

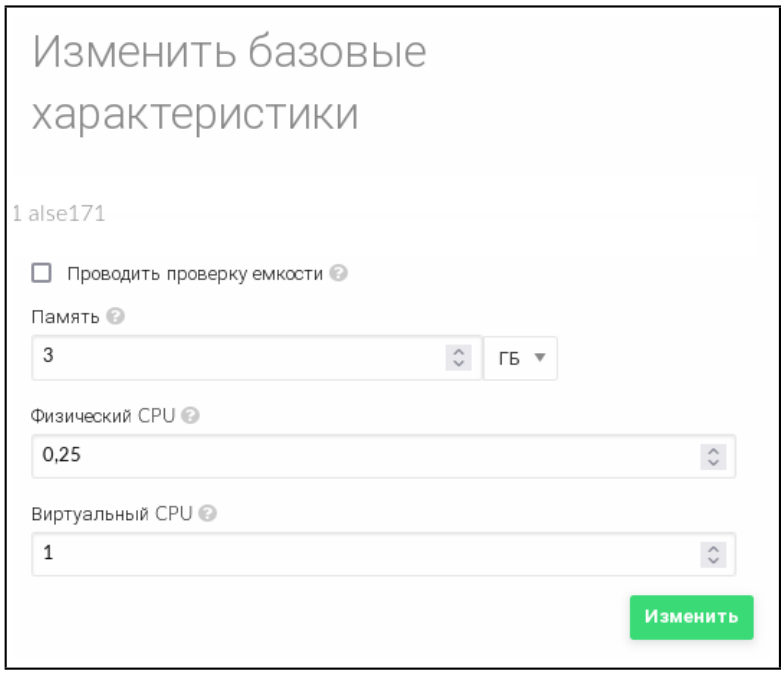

Рис. 49

7.1.9. 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.

7.1.9.1. 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
```

7.1.9.2. 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. 50)

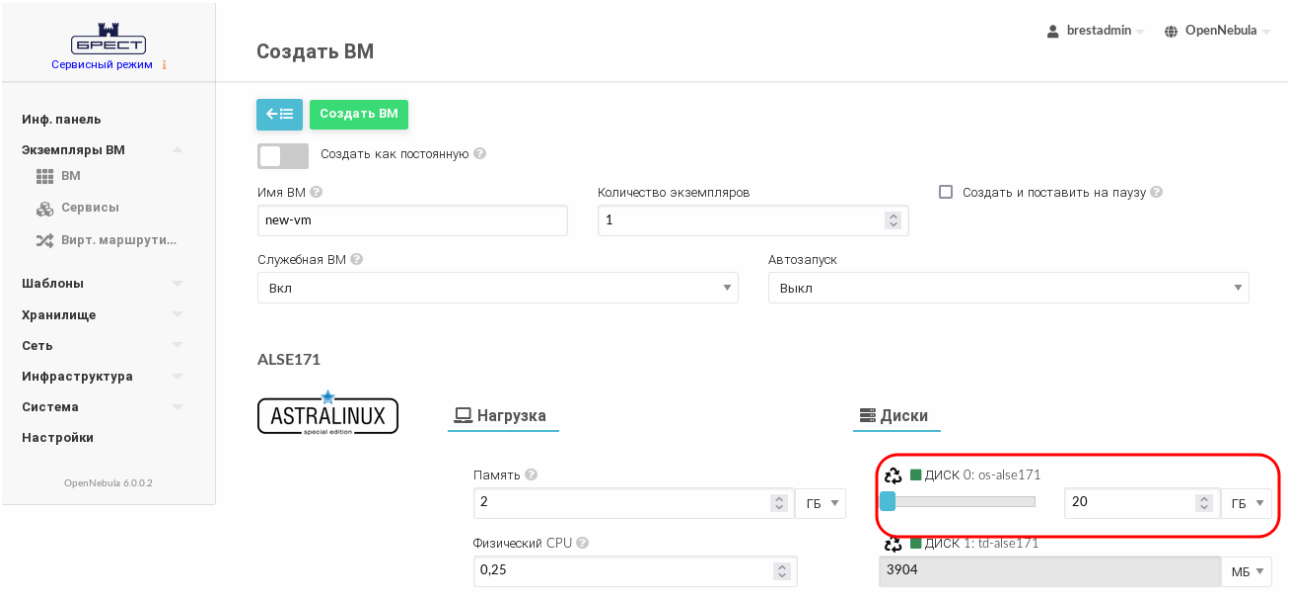

Рис. 50

7.1.10. 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 содержимое 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`. 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.

7.1.10.1. 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
```

7.1.10.2. 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. 51).

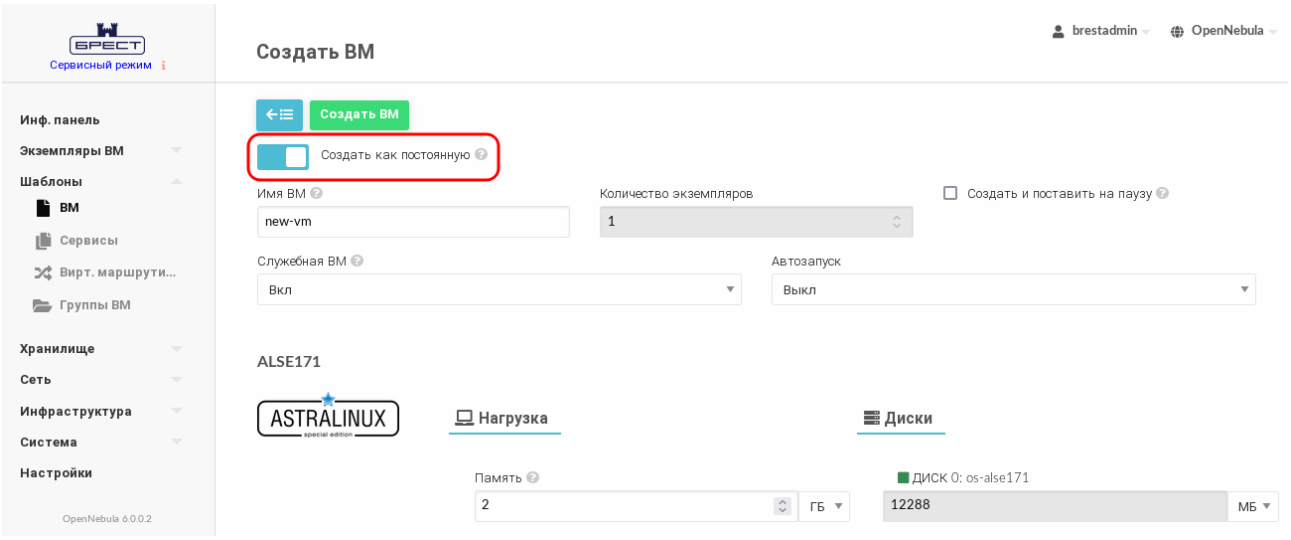

Рис. 51

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

1) на странице выключенной ВМ нажать на кнопку **[Сохранить как]** (см. рис. 52);

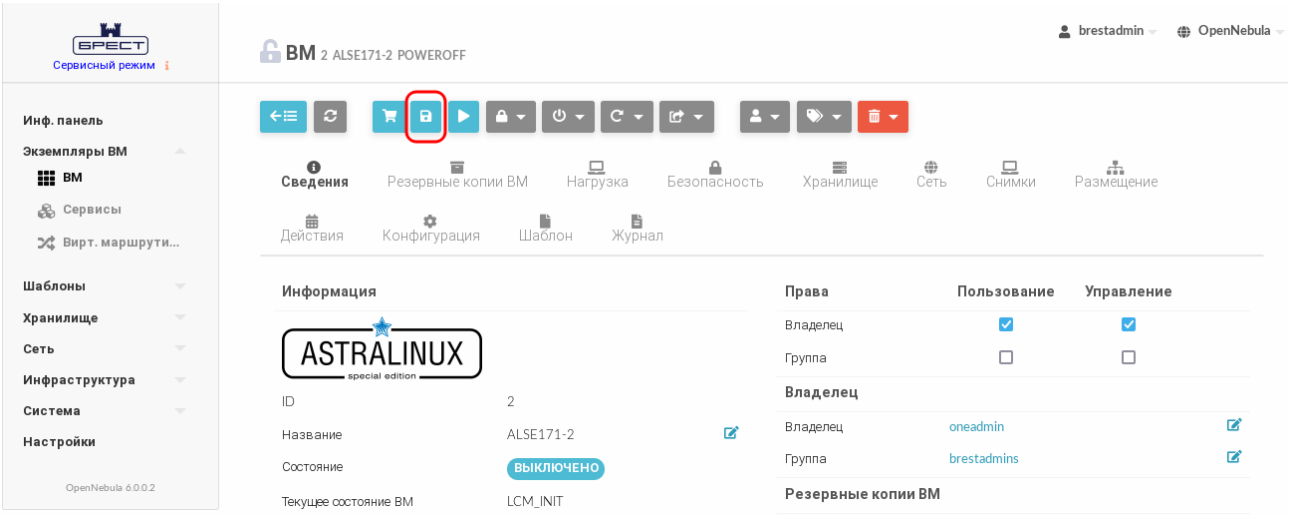

Рис. 52

2) в открывшемся окне «Сохранить как шаблон» (см. рис. 53):
   а) задать наименование нового шаблона,
   б) установить флаг «Сделать новый образ постоянным»,
   в) нажать на кнопку **[Сохранить как шаблон]**.

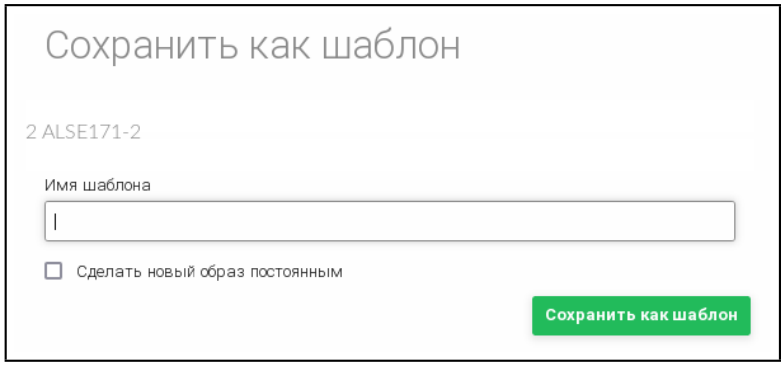

Рис. 53

7.1.11. Управление полномочиями для ВМ

В ПК СВ реализован механизм полномочий на основе правил ACL, предназначенный для администраторов. Также для каждого экземпляра ВМ существуют неявные полномочия, которыми управляет владелец ВМ. Например, владелец ВМ может открыть общий доступ к экземпляру ВМ для других пользователей, разрешить им просматривать и использовать ВМ.

Управление полномочиями описано в 5.5

7.1.12. 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`).

7.1.12.1. 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.

7.1.12.2. 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 на кнопку **[Добавить действие]**;

4) на открывшейся странице внести необходимые настройки и нажать на кнопку **[Добавить]** (см. рис. 54.

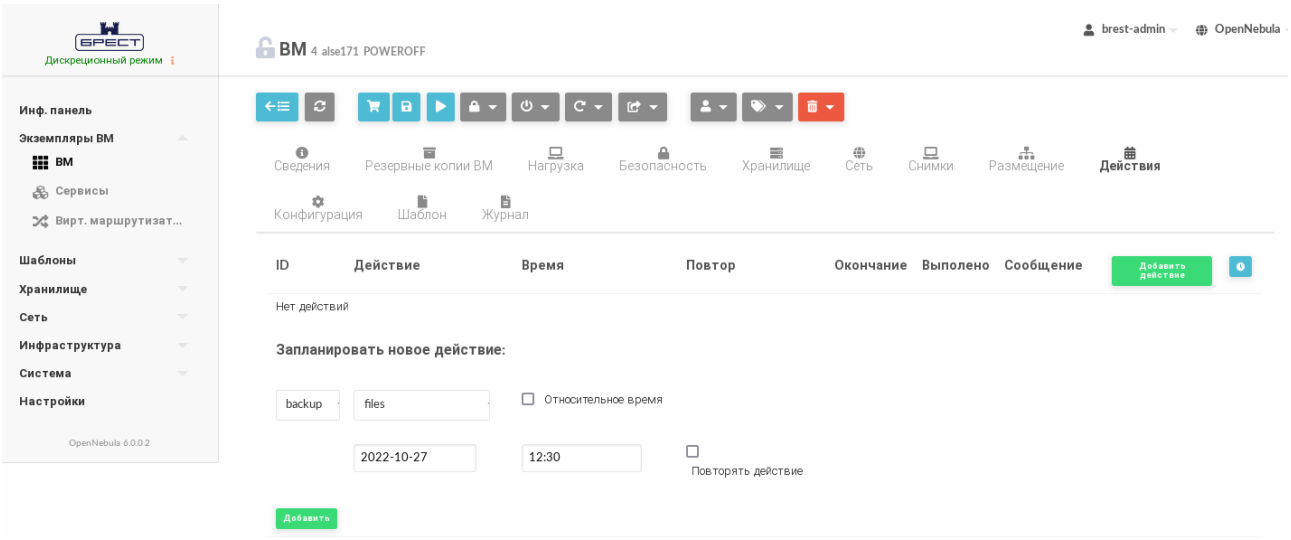

Рис. 54

7.1.13. Снимки дисков ВМ

Пользователь может делать снимки состояния диска, только если ВМ в текущий момент работает (находится в состоянии RUNNING). 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.

7.1.13.1. 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.

7.1.13.2. 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. 55).

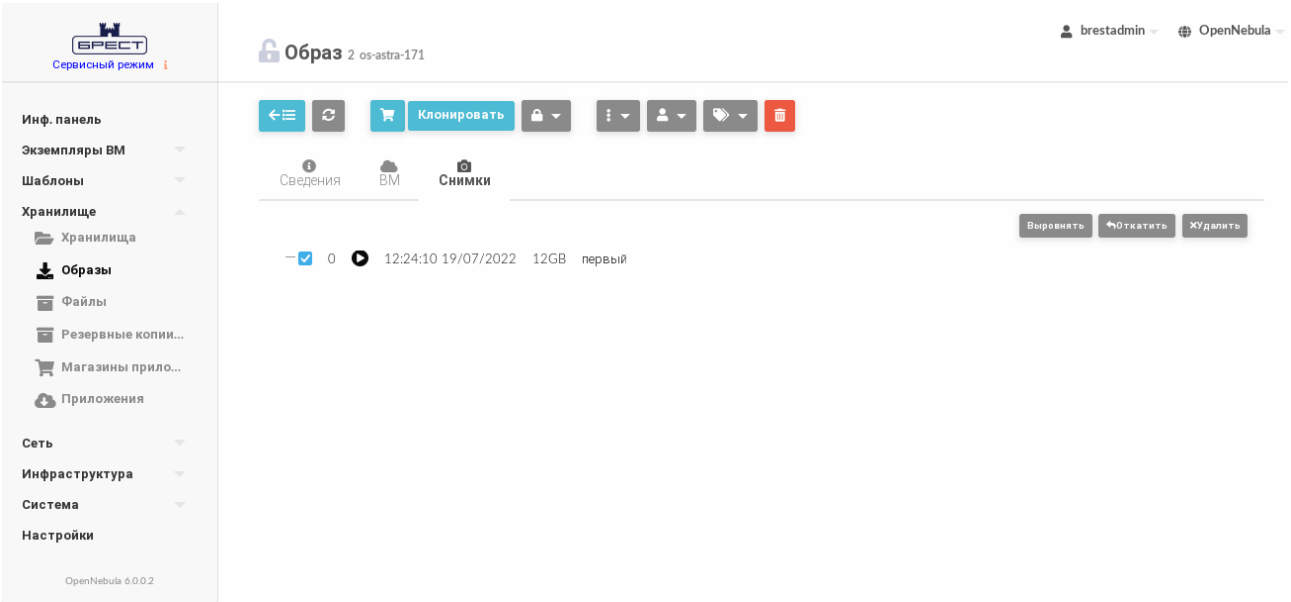

Рис. 55

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]**.

7.2. Доверенная загрузка виртуальных машин

Доверенная загрузка виртуальных машин осуществляется с использованием следующих механизмов:

- механизм контроля конфигурации виртуального оборудования виртуальных машин;
- механизм контроля файлов виртуальной базовой системы ввода-вывода (первичного загрузчика виртуальной машины);

- механизм контроля целостности исполняемых файлов гостевой операционной системы виртуальной машины.

7.2.1. Контроль целостности исполняемых файлов гостевой операционной системы

В ПК СВ используется механизм контроля исполняемых целостности файлов гостевой операционной системы, реализованный в ОС СН. Подробное описание этого механизма приведено в документе РУСБ.10015-01 97 01-1.

Для обеспечения контроля целостности исполняемых файлов гостевой операционной системы в ПК СВ необходимо на каждом компьютере, выполняющем функцию сервера виртуализации, выполнить следующие действия:

1) установить пакет `astra-kvm-secure` командой:

```
sudo apt install astra-kvm-secure
```

2) включить механизм контроля целостности исполняемых файлов гостевой операционной системы. Для этого в конфигурационном файле `/etc/libvirt/libvirtd.conf` для параметра `file_integrity_check_period_s` значение периода проверки в секундах, например «60». Конфигурирование настроек `libvirt` рекомендуется выполнять в интерактивном режиме, с использованием команды:

```
virsh -c qemu:///system config --edit-config /etc/libvirt/libvirtd.conf
```

3) включить режим принудительного выключения виртуальной машины в случае нарушения целостности установленных на контроль файлов гостевой операционной системы. Для этого в конфигурационном файле `/etc/libvirt/libvirtd.conf` для параметра `file_integrity_check_shutdown_domain` установить значение «1»;

4) перезапустить службу `libvirt` командой:

```
sudo systemctl restart libvirtd
```

7.2.2. Контроль конфигурации виртуального оборудования виртуальных машин

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. Подробное описание реализации управления доступом к информации в защищенной СУБД PostgreSQL

приведено в документе РУСБ.10015-01 97 01-1.

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

7.2.3. Контроль файлов виртуальной базовой системы ввода-вывода

Контроль файлов виртуальной базовой системы ввода-вывода (первичного загрузчика виртуальной машины) обеспечивается механизмом контроля целостности с использованием алгоритма работы с контрольными суммами («отпечатка конфигурации»), реализованном в ОС СН. Подробное описание механизма контроля целостности «отпечаток конфигурации» приведено в документе РУСБ.10015-01 97 01-1.

Для обеспечения контроля файлов виртуальной базовой системы ввода-вывода в ПК СВ необходимо на каждом компьютере, выполняющем функцию сервера виртуализации, выполнить следующие действия:

1) установить пакеты ovmf и astra-kvm-secure командой:

```
sudo apt install ovmf astra-kvm-secure
```

2) включить механизм контроля целостности «отпечаток конфигурации». Для этого в конфигурационном файле `/etc/libvirt/libvirtd.conf` для параметра `integrity_control` установить значение «1». Конфигурирование настроек libvirt рекомендуется выполнять в интерактивном режиме, с использованием команды:

```
virsh -c qemu:///system config --edit-config /etc/libvirt/libvirtd.conf
```

3) перезапустить службу libvirt командой:

```
sudo systemctl restart libvirtd
```

7.3. 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. 56).

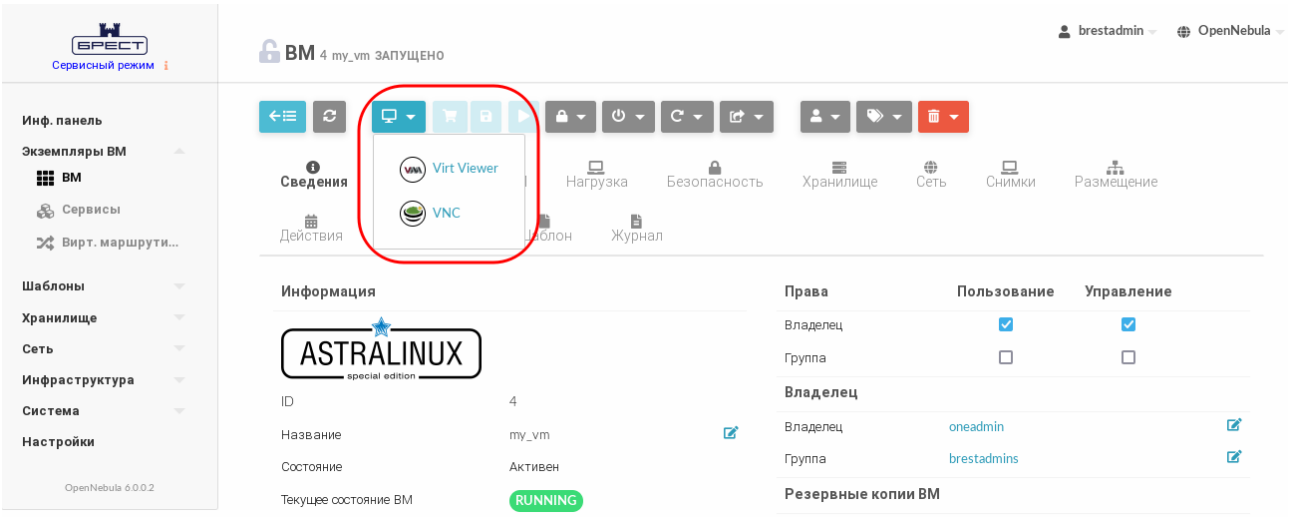

Рис. 56

При появлении в браузере firefox панели с предупреждением нажать на кнопку **[Настройки]** и выбрать пункт `Разрешить всплывающие окна` (см. рис. 57).

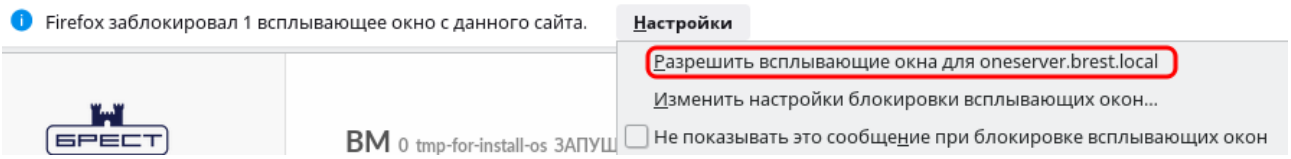

Рис. 57

После этого откроется страница с подключенным удаленным рабочим столом ВМ (см. рис. 58).

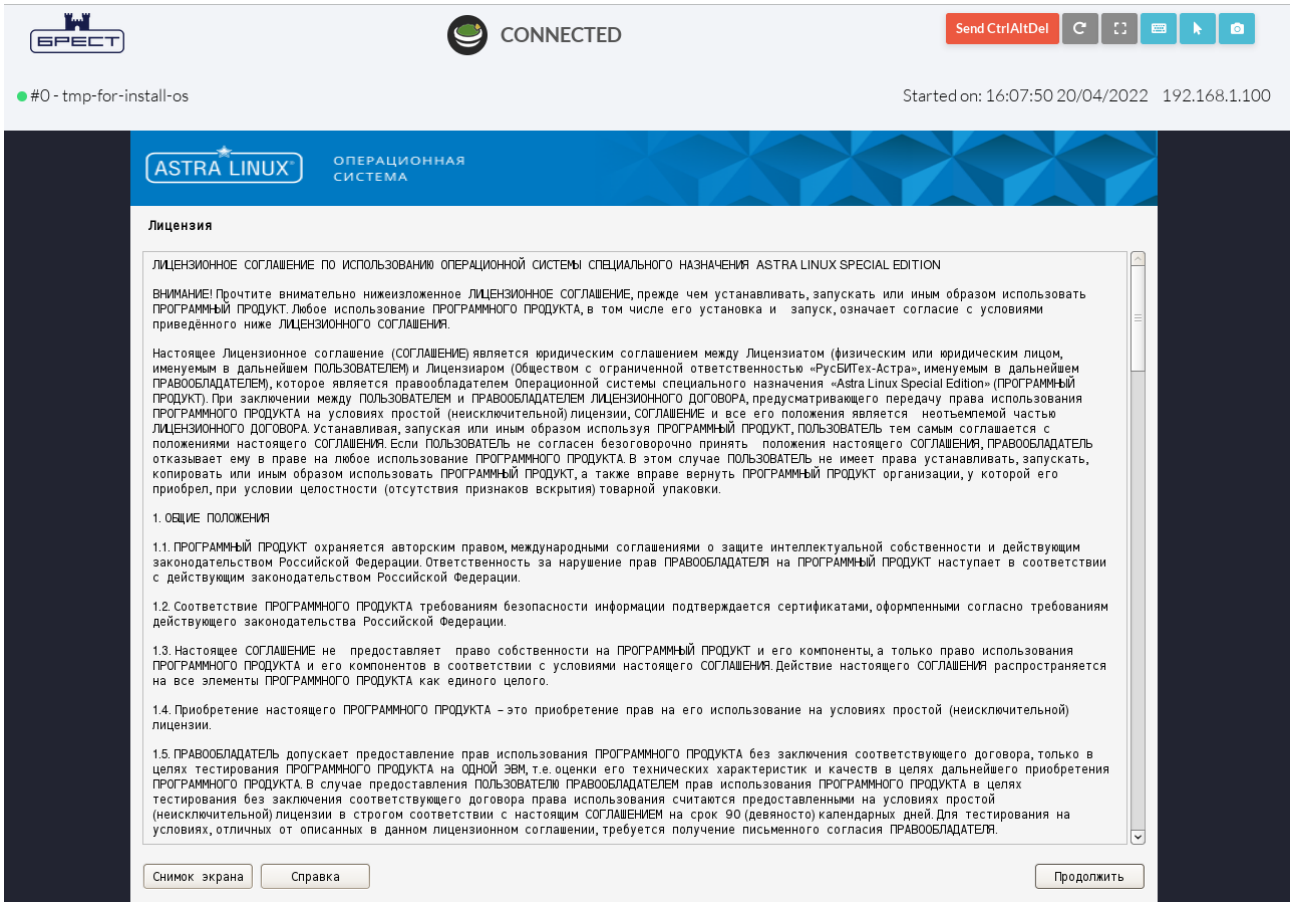

Рис. 58

7.4. Резервное копирование и восстановление экземпляра ВМ

В ПК СВ обеспечивается резервное копирование:

- образов виртуальных машин и конфигурации виртуального оборудования виртуальных машин;
- параметров настройки средства виртуализации;
- сведений о событиях безопасности.

Резервное копирование параметров настройки средства виртуализации реализуется с использованием следующих встроенных в ОС СН средств резервного копирования:

- комплекс программ Bacula;
- утилита копирования rsync;
- утилиты архивирования и копирования: tar, cpio, gzip, cp.

Описание указанных средств резервного копирования приведено в документе РУСБ.10015-01 95 01-1 «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора. Часть 1». Дополнительная настройка ПК СВ не требуется.

Резервное копирование сведений о событиях безопасности реализуется с использованием встроенных в ОС СН средств ротации и архивации журанлов logrotate, и при необходимости встроенных в ОС СН средств резервного копирования, указанных выше. Настройка ротации возможна с использованием утилиты fly-admin-events («Настройка регистрации системных событий»), которая установлена в ОС СН по умолчанию. Дополнительная настройка ПК СВ не требуется. Описание утилиты fly-admin-events приведено в электронной справке ОС СН.

7.4.1. 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, на-

стройки 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.

7.4.2. 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 на кнопку **[Управление размещением]** и в открывшемся меню выбрать пункт «Резервная копия» (см. рис. 59);

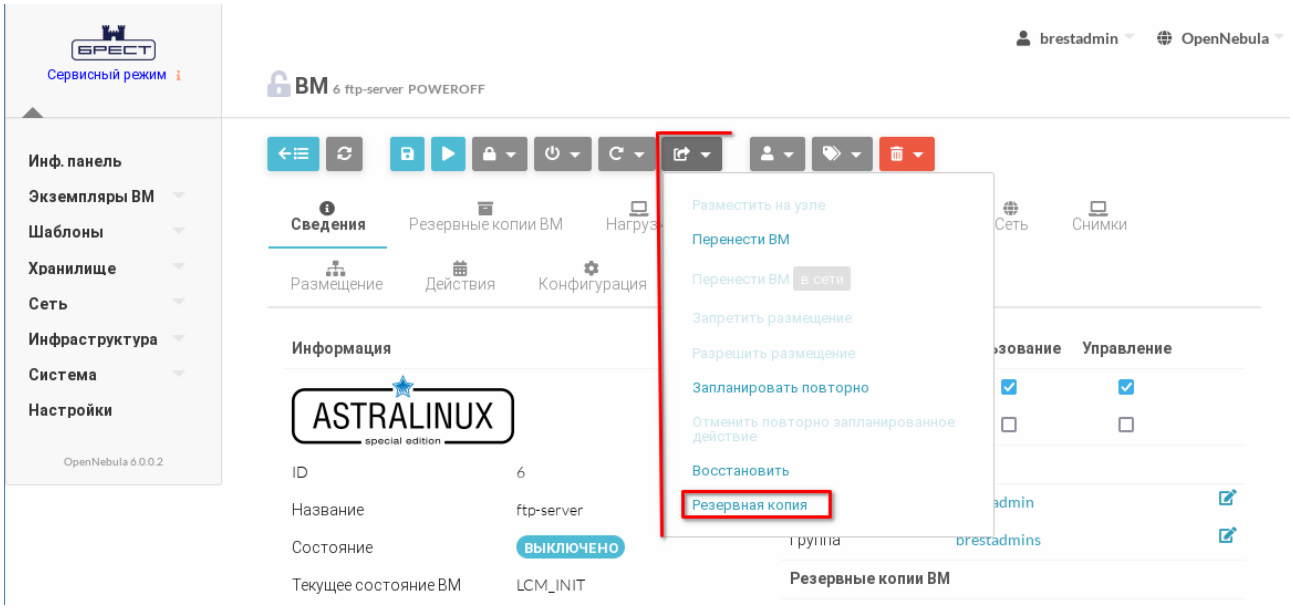

Рис. 59

4) в открывшемся окне «Резервная копия ВМ» (см. рис. 60):

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 на кнопку **[Резервная копия]**.

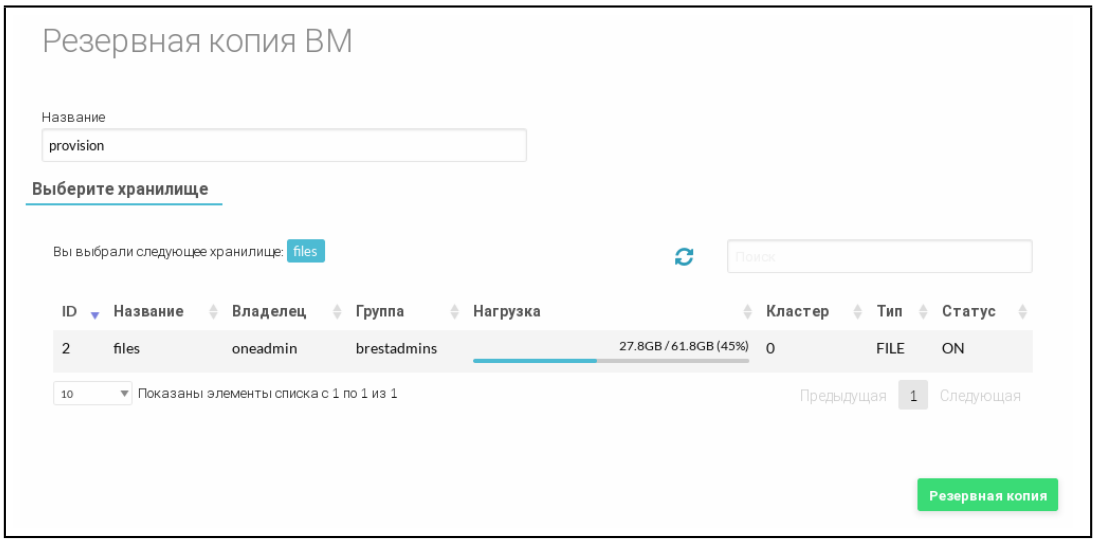

Рис. 60

7.4.3. Отображение резервных копий экземпляра ВМ

Для отображения существующих резервных копий ВМ необходимо на странице этой виртуальной машины открыть вкладку «Резервные копии ВМ» (см. рис. 61).

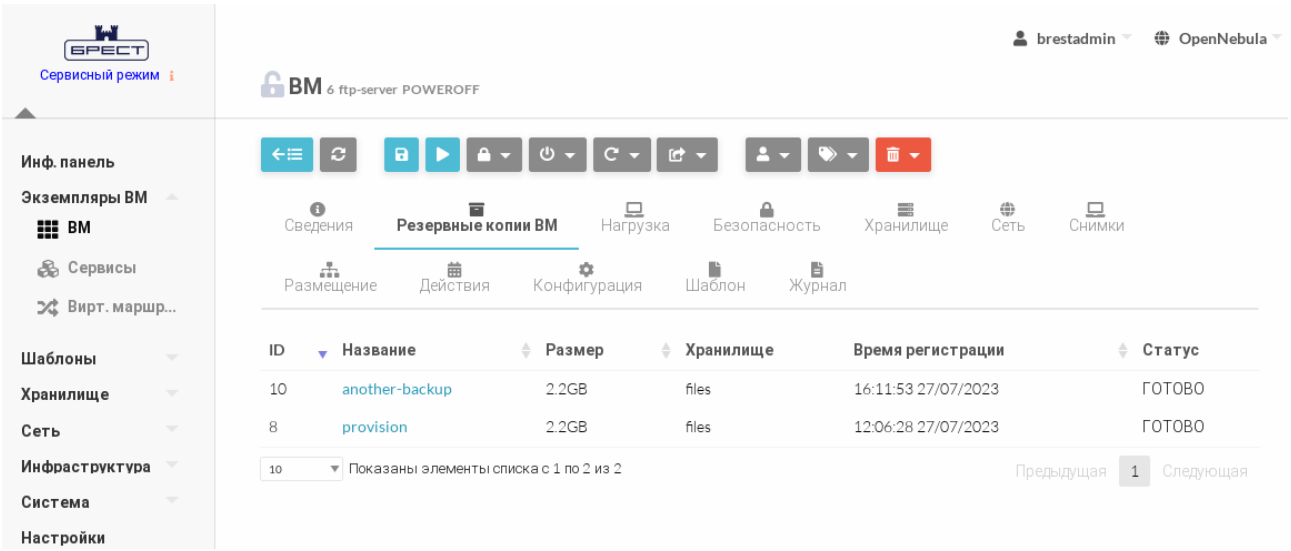

Рис. 61

Для просмотра полной информации о резервной копии ВМ необходимо нажать на соответствующую ссылку в поле «Название». После этого откроется страница «Резервная копия» (см. рис. 62).

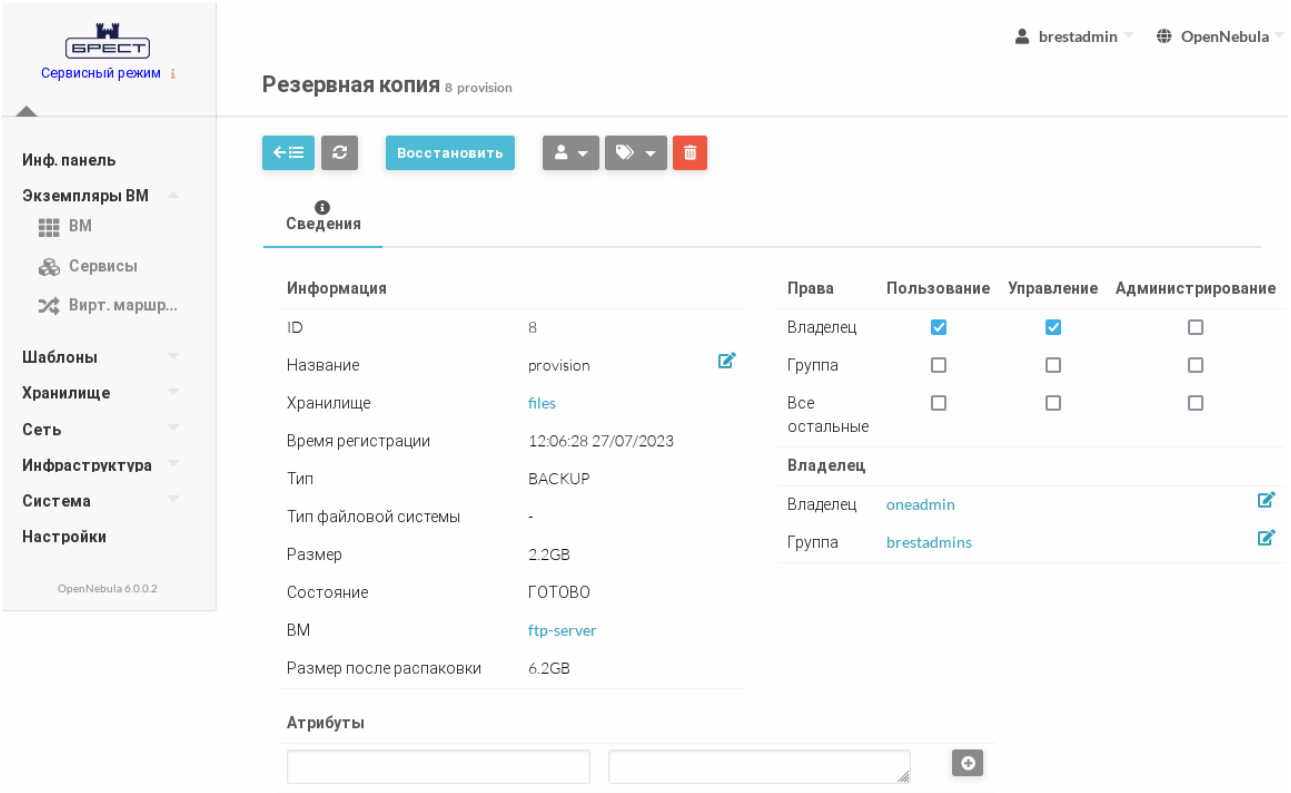

Рис. 62

7.4.4. Отображение всех резервных копий, имеющихся в ПК СВ

Для отображения всех существующих резервных копий ВМ необходимо в веб-интерфейсе ПК СВ в меню слева выбрать пункт «Хранилище — Резервные копии ВМ». На открывшейся странице «Резервные копии ВМ» будет отображена таблица резервных копий ВМ (см. рис. 63)

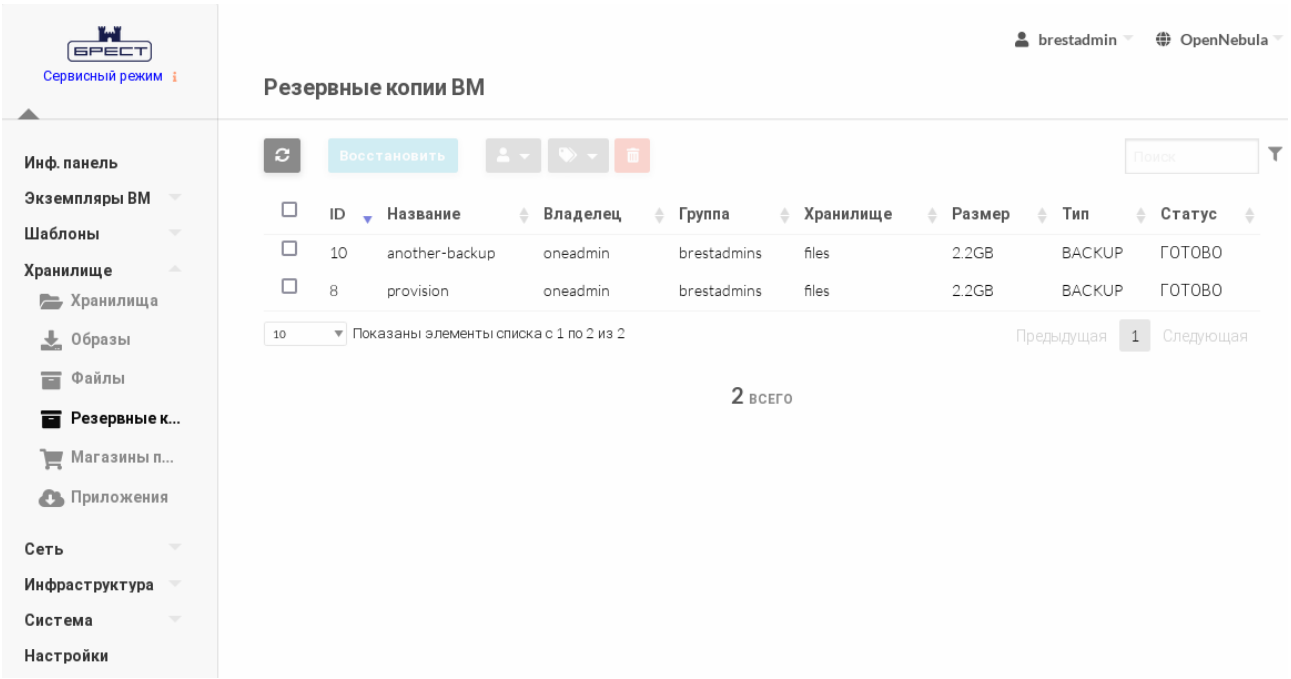

Рис. 63

Для просмотра полной информации о резервной копии ВМ необходимо нажать на соответствующую строку таблицы. После этого откроется страница «Резервная копия» (см. рис. 62).

7.4.5. 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 на кнопку **[Восстановить]**;
3) в открывшемся окне «Восстановление резервной копии» (см. рис. 64):
   а) в поле «Имя восстанавливаемой машины» задать наименование ВМ;
   б) выбрать системное хранилище, в котором будут размещена ВМ;
   в) нажать на кнопку **[Восстановить]**.

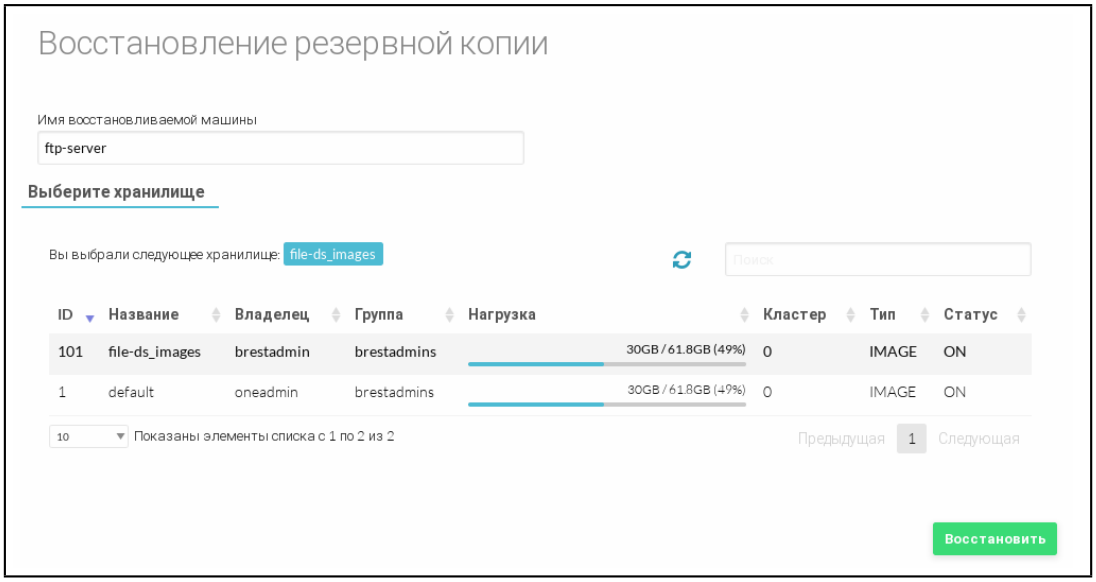

Рис. 64

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]**.

8. МАГАЗИН ПРИЛОЖЕНИЙ

Магазин приложений выступает в качестве удаленного хранилища приложений ПК СВ. Приложение — это логическое объединение образа диска и шаблона виртуальной машины.

8.1. Требования

В качестве магазина приложений можно использовать любой сервер виртуализации. При этом на сервере виртуализации, который будет использоваться в качестве магазина приложений, должен быть установлен пакет `apache2`.

8.2. Установка и настройка магазина приложений

На сервере управления необходимо установить пакет `brest-marketplace`, выполнив в терминале команду:

```
sudo apt install brest-marketplace
```

ВНИМАНИЕ! Если в ПК СВ для обеспечения отказоустойчивости сервера управления применяется технология Raft, пакет `brest-marketplace` должен быть установлен на каждом экземпляре сервера управления. При этом первоначальная настройка магазина приложений должно происходить на «лидере».

Примечание. Алгоритм Raft описан в документе РДЦП.10001-03 95 01-1.

Для первоначальной настройки и/или подключения магазина приложений необходимо запустить мастер настройки, выполнив в терминале команду:

```
sudo brest-marketplace-configure
```

Во время работы мастера настройки необходимо указать IP-адрес (полное доменное имя) сервера виртуализации, выступающего в качестве магазина приложений, имя магазина приложений и режим доступа. Доступ к магазину приложений возможен в двух режимах:

1) «Доступ на управление» — позволяет добавлять, удалять и скачивать приложения;
2) «Отказ от доступа» — позволяет только скачивать приложения.

ВНИМАНИЕ! При первоначальной настройке магазина приложений необходимо выбрать режим «Доступ на управление».

К одному магазину приложений можно подключить несколько экземпляров ПК СВ, при этом режим «Доступ на управление» может иметь только один экземпляр ПК СВ. Для изменения режима доступа необходимо повторно запустить мастер настройки `brest-marketplace-configure` на сервере управления того ПК СВ, для которого необходимо изменить режим доступа.

По окончании работы мастера настройки в веб-интерфейсе ПК СВ появится информация о добавленном магазине приложений (см. рис. 65).

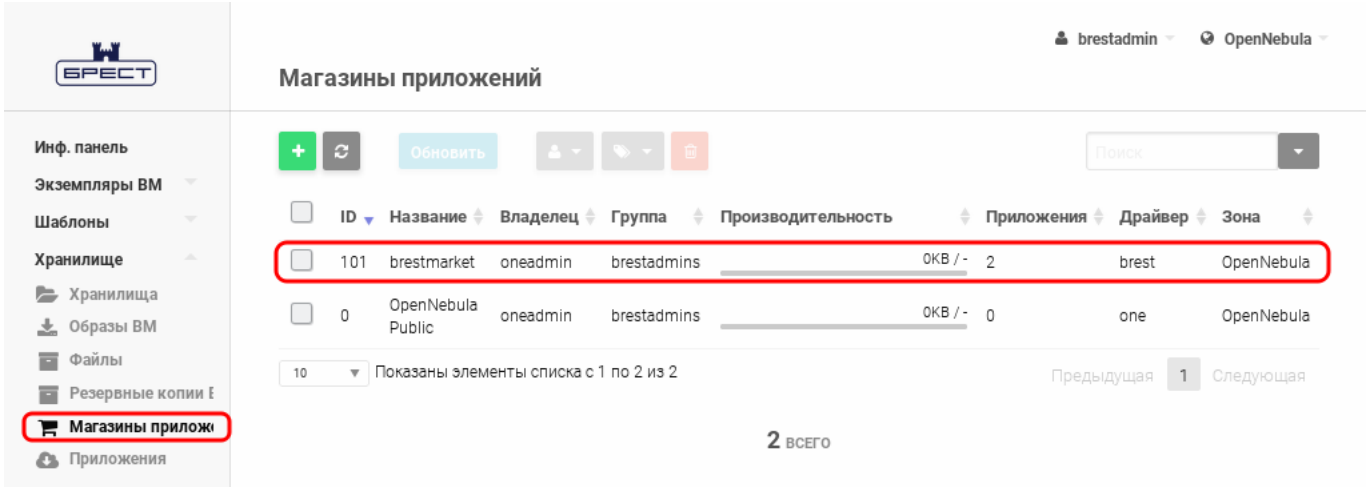

Рис. 65

8.3. Добавление приложения

Создать приложение и добавить его в магазин приложений можно используя образ диска из хранилища образов или имеющуюся виртуальную машину.

8.3.1. Создание приложения, используя образ диска

Для того чтобы создать приложение и добавить его в магазин приложений, в веб-интерфейсе ПК СВ необходимо:

1) в меню слева выбрать пункт «Хранилище — Приложения» и на открывшейся странице «Приложения» нажать на кнопку **[+]** (см. рис. 66);

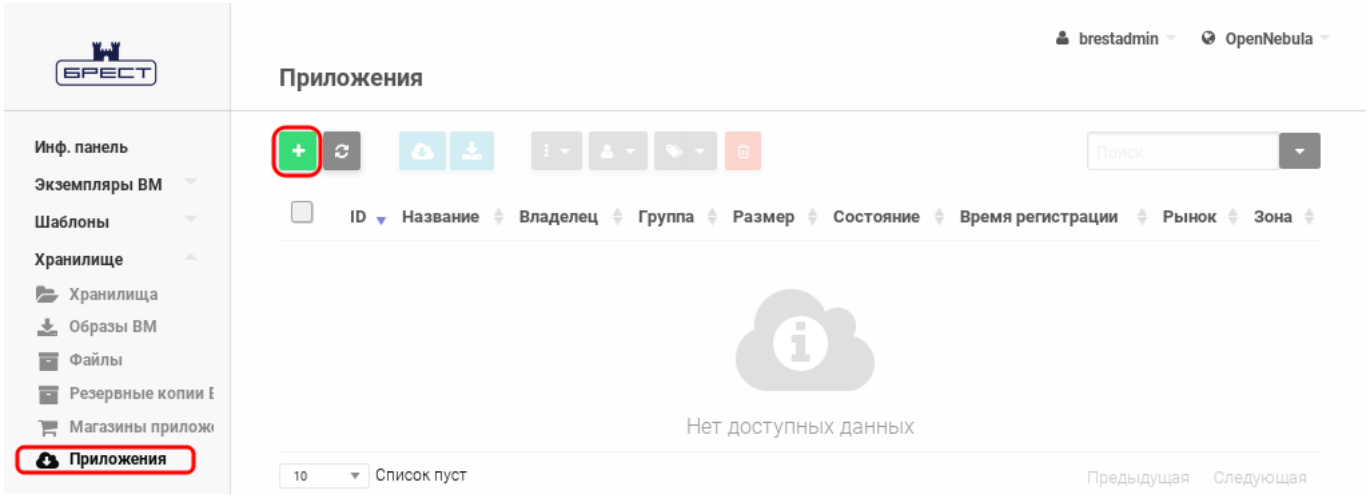

Рис. 66

2) на открывшейся странице «Создать приложение в магазине приложений» (см. рис. 67) выполнить следующие действия:

- в поле «Название» задать наименование приложения,
- выбрать образ для создания приложения,
- выбрать магазин приложений, в который необходимо добавить созданное приложение,

- нажать на кнопку **[Создать]**.

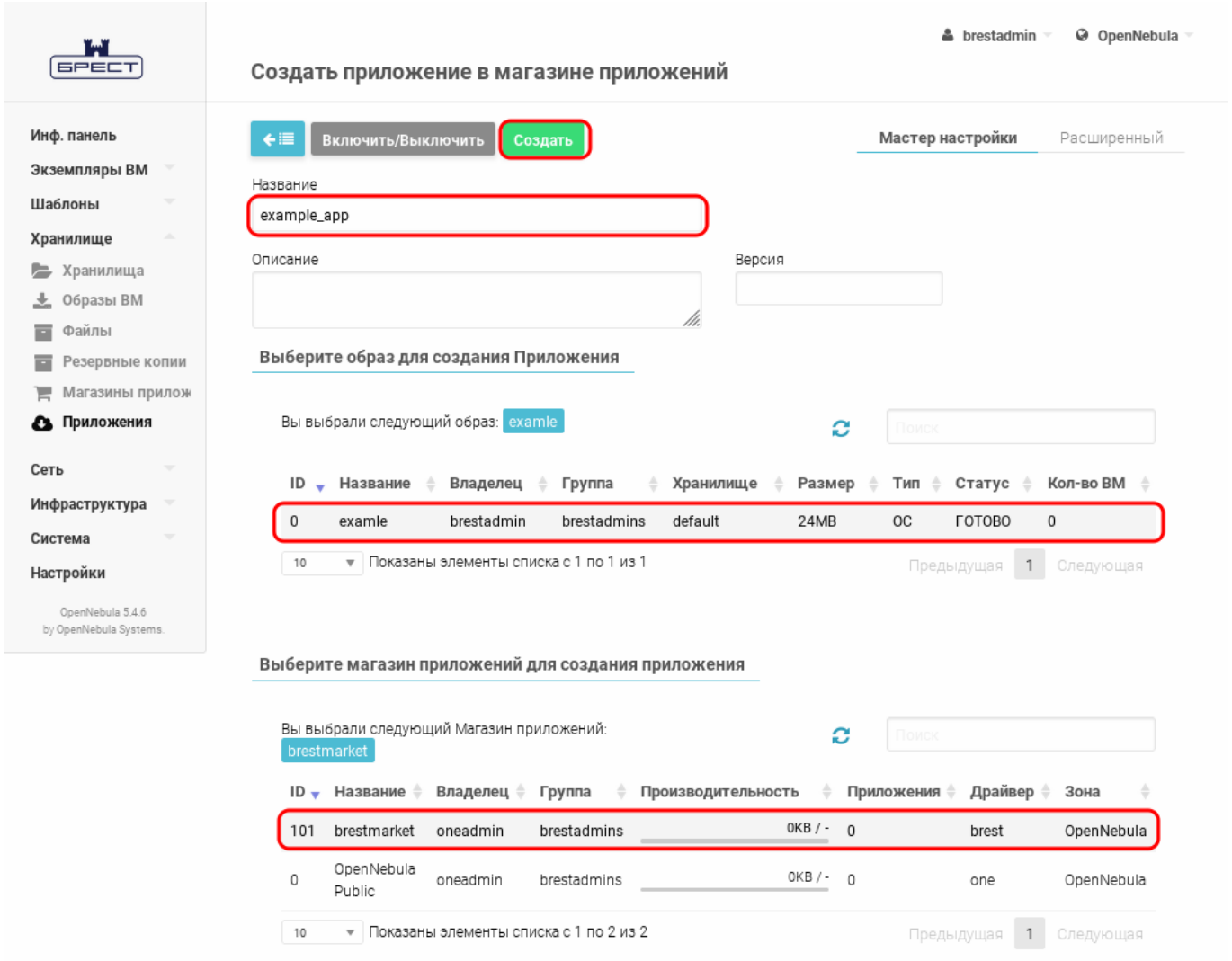

Рис. 67

Созданное приложение будет отображено в веб-интерфейсе ПК СВ на странице «Приложения» (см. рис. 68).

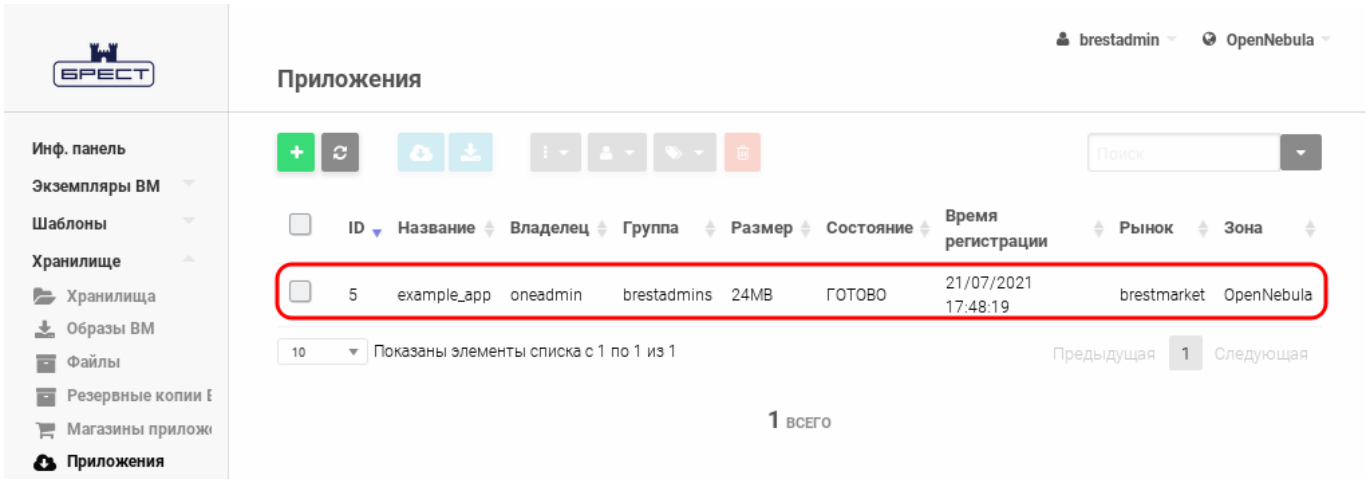

Рис. 68

Примечание. После создания и завершения загрузки приложения в магазин

приложений оно исчезнет из веб-интерфейса и в течении одной минуты появится.

8.3.2. Создание приложения, используя имеющуюся ВМ

Для того чтобы создать приложение, используя имеющуюся ВМ, и добавить его в магазин приложений, необходимо на сервере управления в терминале выполнить команду:

```
sudo one-vmtomarket <идентификатор_ВМ> <идентификатор_магазина приложений> \
    [<наименование_приложения>]
```

ВНИМАНИЕ! Виртуальная машина должна содержать только один диск и находиться в выключенном состоянии.

Пример

Создание приложения «test app» из ВМ с идентификатором «1» и добавление его в магазин приложений с идентификаторм «101»:

```
sudo one-vmtomarket 1 101 "test app"
```

Созданное приложение будет отображено в веб-интерфейсе ПК СВ на странице «Приложения» (см. рис. 69).

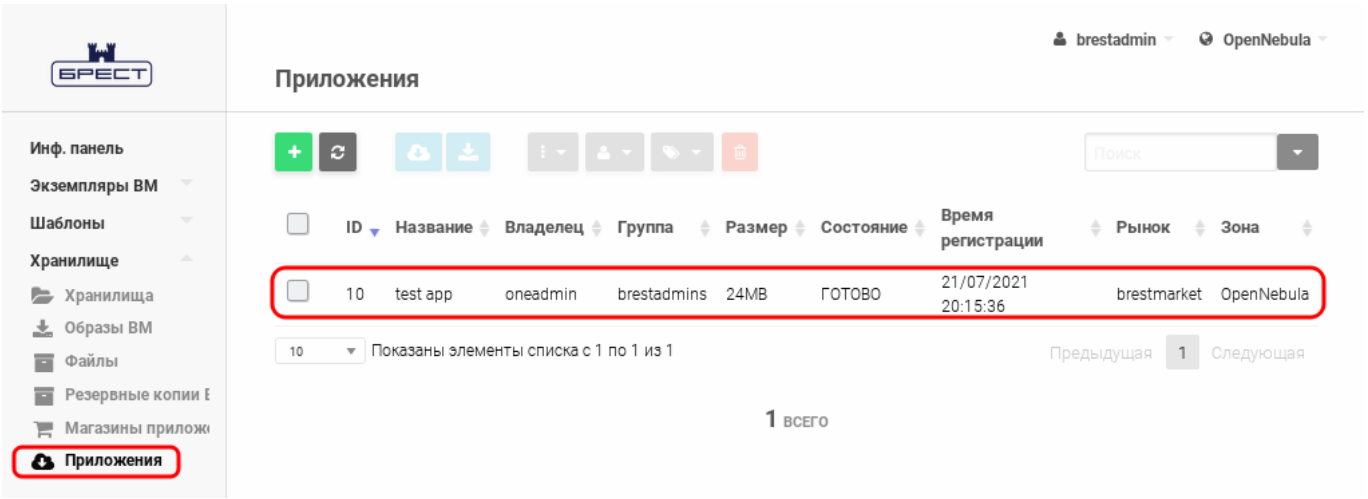

Рис. 69

ПЕРЕЧЕНЬ ТЕРМИНОВ

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 — администратор средства виртуализации, входящий в группу `brestadmins`, которому предоставляются права для выполнения действий по управлению вычислительными ресурсами ПК СВ.

Локальный администратор компьютера — администратор ОС СН, установленной на компьютере.

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 сопро-водительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					