

Утвержден

РДЦП.10001-02-УД

ПРОГРАММНЫЙ КОМПЛЕКС «СРЕДСТВА ВИРТУАЛИЗАЦИИ «БРЕСТ»

Руководство администратора. Часть 2

РДЦП.10001-02 95 01-2

Листов 148

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

2022

Литера О₁

АННОТАЦИЯ

Настоящий документ является руководством администратора программного изделия «Программный комплекс «Средства виртуализации «Брест» (ПК СВ «Брест») РДЦП.10001-02 (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 (далее по тексту — ОС СН), под управлением которой функционирует ПК СВ.

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

Руководство администратора состоит из двух частей:

- РДЦП.10001-02 95 01-1 «Программный комплекс «Средства виртуализации «Брест». Руководство администратора. Часть 1»;
- РДЦП.10001-02 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 использования среды виртуализации, обеспечения отказоустойчивости и масштабирования развернутого ПК СВ.

Дополнительная информация о порядке эксплуатации, а также варианты реализации отдельных решений приведены на официальном сайте wiki.astralinux.ru/docs.

СОДЕРЖАНИЕ

1. Инструменты управления сервисами ПК СВ	9
1.1. Инструменты командной строки	9
1.2. Веб-интерфейс ПК СВ	10
2. Управление хостами и кластерами	11
2.1. Хосты	11
2.1.1. Добавление хостов	11
2.1.1.1. Регистрация хоста в интерфейсе командной строки	11
2.1.1.2. Регистрация хоста в веб-интерфейсе ПК СВ	11
2.1.2. Отображение информации о хосте и просмотр перечня хостов	13
2.1.2.1. В интерфейсе командной строки	13
2.1.2.2. В веб-интерфейсе ПК СВ	14
2.1.3. Жизненный цикл хоста	15
2.1.3.1. Общие сведения	15
2.1.3.2. Управление хостом в интерфейсе командной строки	16
2.1.3.3. Управление хостом в веб-интерфейсе ПК СВ	17
2.1.4. Удаление хоста	17
2.1.4.1. В интерфейсе командной строки	17
2.1.4.2. В веб-интерфейсе ПК СВ	17
2.1.5. Мониторинг хоста	18
2.1.6. Импорт неконтролируемых виртуальных машин	20
2.1.6.1. Импорт неконтролируемых ВМ в интерфейсе командной строки	20
2.1.6.2. Импорт неконтролируемых ВМ в веб-интерфейсе ПК СВ	20
2.2. Кластеры	21
2.2.1. Управление кластером	21
2.2.1.1. В интерфейсе командной строки	21
2.2.1.2. В веб-интерфейсе ПК СВ	22
2.2.2. Добавление хостов к кластеру	23
2.2.2.1. В интерфейсе командной строки	23
2.2.2.2. В веб-интерфейсе ПК СВ	24
2.2.3. Добавление ресурсов к кластеру	24
3. Пользователи и группы	26

3.1. Общие сведения	26
3.2. Управление пользователями	26
3.2.1. Управление пользователями в интерфейсе командной строки	26
3.2.2. Управление пользователями в веб-интерфейсе ПК СВ	28
3.3. Управление группами	30
3.3.1. Общие сведения	30
3.3.2. Управление группами в интерфейсе командной строки	31
3.3.3. Управление группами в веб-интерфейсе ПК СВ	33
3.4. Управление VDC	35
3.4.1. Общие сведения	35
3.4.2. Управление VDC в интерфейсе командной строки	36
3.4.3. Управление VDC в веб-интерфейсе ПК СВ	38
3.5. Управление полномочиями	40
3.5.1. Общие сведения	40
3.5.2. Управление полномочиями в интерфейсе командной строки	41
3.5.2.1. Просмотр и изменение установленных полномочий для облачного ресурса	41
3.5.2.2. Изменение установленных полномочий для облачного ресурса	41
3.5.2.3. Установка полномочий по умолчанию	43
3.5.3. Управление полномочиями в веб-интерфейсе ПК СВ	44
3.5.3.1. Просмотр и изменение установленных полномочий	44
3.5.3.2. Установка полномочий, присваиваемых по умолчанию пользователю	44
3.6. Управление правилами ACL	45
3.6.1. Общие сведения	45
3.6.2. Структура правил ACL	46
3.6.3. Управление правилами ACL в интерфейсе командной строки	47
3.6.4. Управление правилами ACL в веб-интерфейсе ПК СВ	49
3.7. Управление квотами	50
3.7.1. Общие сведения	50
3.7.2. Управление квотами в интерфейсе командной строки	51
3.7.2.1. Просмотр установленных квот	51
3.7.2.2. Установка квот	52
3.7.2.3. Изменение установленных квот	55
3.7.2.4. Установка квот для нескольких пользователей/групп	57

3.7.2.5. Установка квот по умолчанию	57
3.7.3. Управление квотами в веб-интерфейсе ПК СВ	57
4. Настройки сетей ПК СВ	60
4.1. Облачные сети	60
4.1.1. Режимы работы облачной сети	60
4.1.2. Параметры облачной сети	60
4.1.2.1. Атрибуты физической сети	61
4.1.2.2. Адресное пространство (AR)	61
4.1.3. Использование облачных сетей	61
4.1.4. Управление облачными сетями в интерфейсе командной строки	62
4.1.4.1. Добавление, удаление и просмотр параметров облачной сети	62
4.1.4.2. Изменение параметров облачной сети	64
4.1.4.3. Управление диапазонами адресов	64
4.1.4.4. Резервирование адресов	66
4.1.5. Управление облачными сетями в веб-интерфейсе ПК СВ	67
4.2. Группы безопасности	69
4.2.1. Параметры группы безопасности	69
4.2.2. Стандартная группа безопасности	70
4.2.3. Управление группами безопасности в интерфейсе командной строки	70
4.2.3.1. Добавление, удаление и просмотр списка групп безопасности	70
4.2.3.2. Просмотр и изменение правил группы безопасности	71
4.2.3.3. Применение группы безопасности	72
4.2.4. Управление группами безопасности в веб-интерфейсе ПК СВ	73
5. Управление виртуальной машиной	76
5.1. Управление образами	76
5.1.1. Типы образов	76
5.1.2. Состояния образов	77
5.1.3. Создание образа	77
5.1.3.1. Общие сведения	77
5.1.3.2. Создание образа в интерфейсе командной строки	77
5.1.3.3. Создание образа в веб-интерфейсе ПК СВ	80
5.1.4. Клонирование образов	84
5.1.4.1. Общие сведения	84

5.1.4.2. Клонирование образа в интерфейсе командной строки	84
5.1.4.3. Клонирование образа в веб-интерфейсе ПК СВ	85
5.1.5. Отображение доступных образов	86
5.1.5.1. В интерфейсе командной строки	86
5.1.5.2. В веб-интерфейсе ПК СВ	87
5.1.6. Общие образы	88
5.1.6.1. Управление доступом к образу в интерфейсе командной строки	88
5.1.6.2. Управление доступом к образу в веб-интерфейсе ПК СВ	89
5.1.7. Присвоение образам атрибута «постоянный»	90
5.1.7.1. В интерфейсе командной строки	90
5.1.7.2. В веб-интерфейсе ПК СВ	90
5.1.8. Управление снимками в постоянных образах	91
5.1.8.1. В интерфейсе командной строки	91
5.1.8.2. В веб-интерфейсе ПК СВ	91
5.2. Управление шаблонами виртуальной машины	92
5.2.1. Параметры шаблона VM	92
5.2.2. Создание шаблонов VM	93
5.2.2.1. В интерфейсе командной строки	93
5.2.2.2. В веб-интерфейсе ПК СВ	94
5.2.3. Отображение доступных шаблонов и просмотр информации о шаблоне	98
5.2.3.1. В интерфейсе командной строки	98
5.2.3.2. В веб-интерфейсе ПК СВ	99
5.2.4. Изменение параметров шаблона	100
5.2.4.1. В интерфейсе командной строки	100
5.2.4.2. В веб-интерфейсе ПК СВ	100
5.2.5. Клонирование шаблонов	101
5.2.5.1. В интерфейсе командной строки	101
5.2.5.2. В веб-интерфейсе ПК СВ	101
5.2.6. Общие шаблоны	102
5.2.6.1. В интерфейсе командной строки	102
5.2.6.2. В веб-интерфейсе ПК СВ	103
5.2.7. Удаление шаблонов	104
5.2.7.1. В интерфейсе командной строки	104

5.2.7.2. В веб-интерфейсе ПК СВ	104
5.2.8. Развертывание VM из шаблона	105
5.2.8.1. В интерфейсе командной строки	105
5.2.8.2. В веб-интерфейсе ПК СВ	106
5.3. Управление виртуальными машинами	108
5.3.1. Жизненный цикл виртуальной машины	108
5.3.2. Управление экземплярами VM в интерфейсе командной строки	109
5.3.2.1. Отображение существующих VM	109
5.3.2.2. Завершение работы экземпляров VM	110
5.3.2.3. Приостановка экземпляров VM	110
5.3.2.4. Перезагрузка экземпляров VM	111
5.3.2.5. Отсрочка развертывания экземпляров VM	111
5.3.3. Управление экземплярами VM в веб-интерфейсе ПК СВ	111
5.3.3.1. Отображение существующих VM	111
5.3.3.2. Завершение работы и приостановка экземпляров VM	112
5.3.3.3. Перезагрузка экземпляров VM	113
5.3.3.4. Отсрочка развертывания экземпляров VM	114
5.3.4. Снимки состояний VM	114
5.3.4.1. Управление снимками состояний в интерфейсе командной строки	114
5.3.4.2. Управление снимками состояний в в веб-интерфейсе ПК СВ	115
5.3.5. Снимки дисков VM	116
5.3.5.1. Управление снимками дисков в интерфейсе командной строки	116
5.3.5.2. Управление снимками дисков в в веб-интерфейсе ПК СВ	117
5.3.6. Экспорт диска VM	118
5.3.6.1. В интерфейсе командной строки	118
5.3.6.2. В веб-интерфейсе ПК СВ	118
5.3.7. Горячее подключение диска	119
5.3.7.1. В интерфейсе командной строки	119
5.3.7.2. В веб-интерфейсе ПК СВ	119
5.3.8. Перераспределение производительности VM	121
5.3.8.1. В интерфейсе командной строки	121
5.3.8.2. В веб-интерфейсе ПК СВ	121
5.3.9. Изменение размера дисков VM	122

5.3.9.1. В интерфейсе командной строки	123
5.3.9.2. В веб-интерфейсе ПК СВ	124
5.3.10. Клонирование VM	124
5.3.10.1. В интерфейсе командной строки	125
5.3.10.2. В веб-интерфейсе ПК СВ	125
5.3.11. Управление полномочиями для VM	127
5.4. Доступ к рабочему столу VM веб-интерфейсе ПК СВ	127
6. Дополнительная настройка виртуальной машины	129
6.1. Контекстуализация	129
6.2. Удаленное подключение USB-устройств к VM по протоколам VNC/SPICE/RDP	129
6.3. Настройка дискреционного и мандатного управление доступом к VM	135
6.4. Отказоустойчивость виртуальной машины	136
6.5. Автостарт виртуальных машин	137
6.6. Миграции дисков VM между хранилищами	138
6.7. Автоматический ввод VM в домен через механизм контекста	140
7. Магазин приложений	143
7.1. Требования	143
7.2. Установка и настройка магазина приложений	143
7.3. Добавление приложения	144
7.3.1. Создание приложения, используя образ диска	144
7.3.2. Создание приложения, используя имеющуюся VM	146
Перечень сокращений	147

1. ИНСТРУМЕНТЫ УПРАВЛЕНИЯ СЕРВИСАМИ ПК СВ

1.1. Инструменты командной строки

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

Т а б л и ц а 1

Инструмент командной строки	Описание
onecluster	управление кластерами ПК СВ
onedatastore	управление облачными хранилищами
onedb	инструмент для миграции БД
onegroup	управление группами пользователей ПК СВ
onehook	управление хуками, применяемыми в ПК СВ
onehost	управление узлами 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 облачными сетями

ВНИМАНИЕ! Для управления сервисами ПК СВ посредством инструментов командной строки необходимо на сервере, на котором развернут сервис фронтальной машины, войти в ОС СН под учетной записью администратора с высоким уровнем целостности.

Для того чтобы получить подробное описание использования инструментов командной строки, необходимо выполнить команду:

```
<наименование_инструмента> -h
```

ВНИМАНИЕ! Перед применением инструментов командной строки необходимо в домашний каталог администратора скопировать аутентификационный файл, созданный при инициализации сервиса фронтальной машины. Для этого необходимо выполнить следующие команды:

```
mkdir ~/.one
```

```
sudo cp /var/lib/one/.one/one_auth ~/.one/
```

```
sudo chmod 755 ~/.one/one_auth
```

1.2. Веб-интерфейс ПК СВ

Для подключения к веб-интерфейсу ПК СВ необходимо в браузере Mozilla Firefox перейти по адресу: `https://<полное_доменное_имя>/`, где `<полное_доменное_имя>` — полное доменное имя сервера, на котором развернут сервис фронтальной машины.

В сервисном режиме работы ПК СВ для управления сервисами ПК СВ к веб-интерфейсе на открывшейся странице **Брест** необходимо:

- в поле **Логин** ввести `brestadmin`;
- в поле **Пароль** ввести пароль локального пользователя `brestadmin`, который был задан во время выполнения действий по установке базового сервиса ПК СВ;
- нажать на кнопку **[Войти]**.

В дискреционном режиме работы ПК СВ применяется доменная аутентификация. В связи с этим управления сервисами ПК СВ в веб-интерфейсе ПК СВ на открывшейся странице **Брест** необходимо:

- в форме аутентификации ввести логин и пароль администратора ПК СВ, которые были заданы в процессе инициализации сервиса фронтальной машины;
- нажать на кнопку **[Войти]**.

Примечание. Подключение к веб-интерфейсу ПК СВ можно осуществлять с любого компьютера, имеющего сетевой доступ к серверу, на котором развернут сервис фронтальной машины.

2. УПРАВЛЕНИЕ ХОСТАМИ И КЛАСТЕРАМИ

Хостом (Host) называется сервер, на котором развернут сервис узла виртуализации. Установка и инициализация сервиса узла виртуализации производится в соответствии с документом «Программный комплекс «Средства виртуализации «Брест» (ПК СВ «Брест») РДЦП.10001-03. Руководство администратора. Часть 1».

ПК СВ может работать с хостами, имеющими гетерогенную конфигурацию, т.е. в рамках одного облака ПК СВ можно подключать хосты с различными гипервизорами.

Кластеры (Clusters) представляют собой группы хостов с общими облачными хранилищами и облачными сетями. Более подробная информация о кластерах приведена в разделе 2.2.

2.1. Хосты

2.1.1. Добавление хостов

Для использования хостов в ПК СВ их необходимо зарегистрировать на фронтальной машине.

В дискреционном режиме функционирования ПК СВ регистрация хоста производится автоматически при инициализации сервиса узла виртуализации.

В параграфах 2.1.1.1 — 2.1.1.2 описан процесс регистрации хоста в сервисном режиме функционирования ПК СВ.

ВНИМАНИЕ! Если в сети, объединяющей серверы из состава ПК СВ, не используется сервис DNS, то перед регистрацией хоста необходимо на фронтальной машине в файле `/etc/host` указать информацию о добавляемом хосте (IP-адрес и сетевое имя).

2.1.1.1. Регистрация хоста в интерфейсе командной строки

Для регистрации хоста в интерфейсе командной строки необходимо использовать команду:

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

Процесс регистрации хоста занимает от 20 до 60 секунд.

Пример

Регистрация хоста с гипервизором KVM:

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

Пример вывода после выполнения команды:

```
ID: 1
```

2.1.1.2. Регистрация хоста в веб-интерфейсе ПК СВ

Для того чтобы зарегистрировать узел 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 хоста,
 - в) в поле **Логин администратора** ввести имя локального администратора хоста,
 - г) в поле **Пароль администратора** ввести пароль локального администратора хоста,
 - д) нажать на кнопку **[Создать]**;

The screenshot shows the 'Создать узел' (Create Node) page in the OpenNebula web interface. The page has a header with the user 'brestadmin' and the OpenNebula logo. A left sidebar contains a navigation menu with 'Узлы' (Nodes) selected. The main content area features a form with the following elements:

- Buttons: '←', 'Сброс' (Reset), and 'Создать' (Create).
- Form fields: 'Тип' (Type) set to 'KVM', 'Кластер' (Cluster) set to '0: default', 'Имя хоста' (Host Name), 'Логин администратора' (Admin Login), and 'Пароль администратора' (Admin Password).
- Checkbox: 'SSH ключ уже проброшен' (SSH key already scanned).

Рис. 1

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

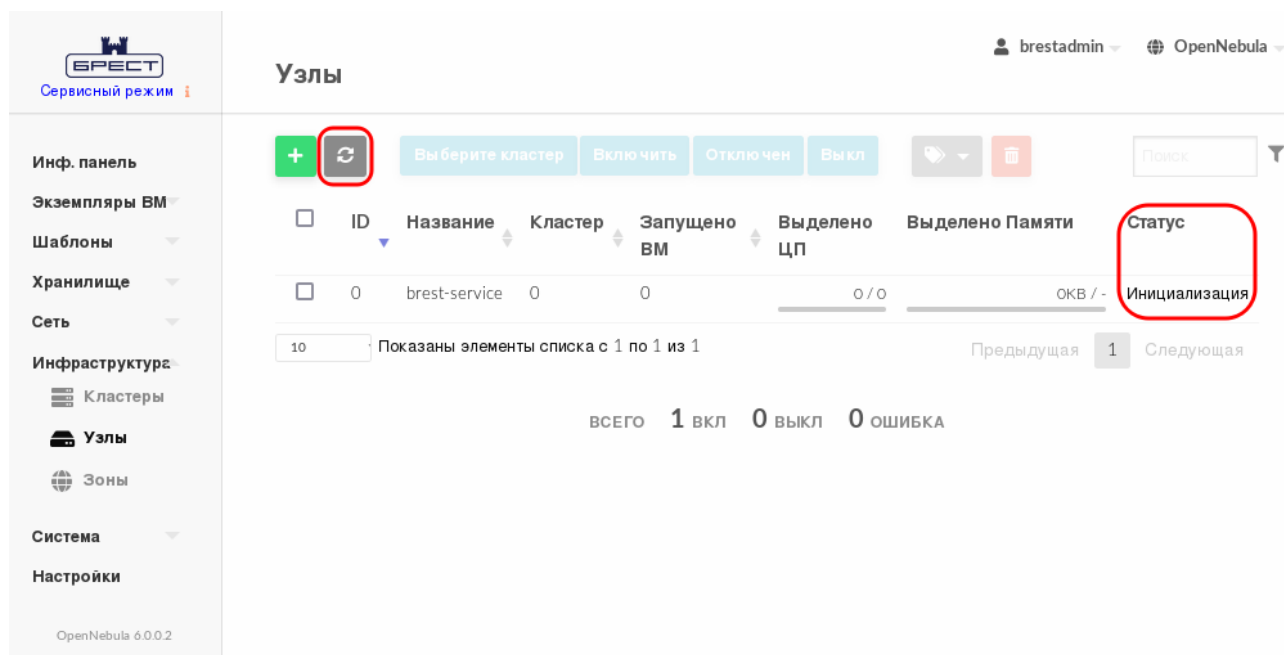


Рис. 2

2.1.2. Отображение информации о хосте и просмотр перечня хостов

2.1.2.1. В интерфейсе командной строки

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

```
onehost show <идентификатор_хоста>
```

Информация о хосте включает:

- общую информацию с указанием его названия и драйверов, которые используются для взаимодействия с ним;
- информацию о производительности (совместно используемые ресурсы хоста) для центрального процессора (ЦП) и оперативной памяти;
- информацию о подключенном облачном хранилище;
- контрольную информацию, в том числе об устройствах PCI;
- информацию о виртуальных машинах, запущенных на хостах. Неконтролируемыми (Wild) виртуальными машинами называют те, которые работают на хосте, но не они не были запущены сервисом ПК СВ. Неконтролируемые VM можно импортировать в ПК СВ.

Пример

Отображение информации о хосте 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 хостов 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	breast-service	default	0	0 / 600 (0%)	0K / 5.8G (0%)	on

2.1.2.2. В веб-интерфейсе ПК СВ

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

Для отображения информации об конкретном хосте на странице **Узлы** необходимо

выбрать соответствующий хост. После этого откроется страница с информацией о хосте (вкладка **Сведения** — см. рис. 3).

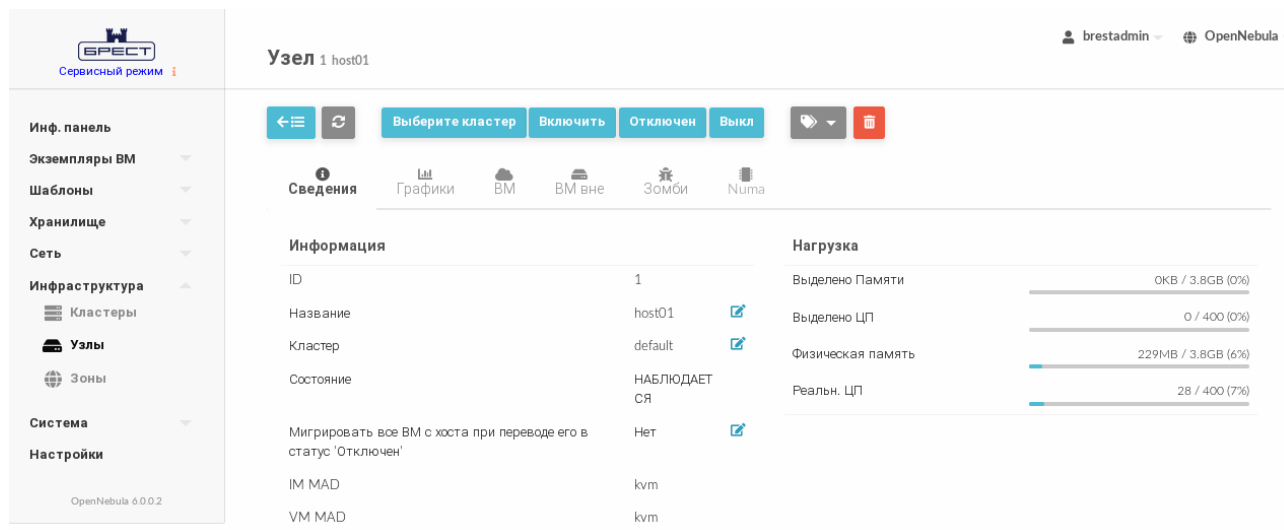


Рис. 3

2.1.3. Жизненный цикл хоста

2.1.3.1. Общие сведения

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

Таблица 2

Состояние	Контроль	Развертывание VM		Значение
		Вручную	Планир.	
Включен (on)	Да	Да	Да	Хост находится в полностью рабочем состоянии
Обновление (update)	Да	Да	Да	Обновление информации о состоянии хоста в системе мониторинга
Отключен (dsbl)	Да	Да	Нет	Отключен, например, для проведения техобслуживания
Отключен от сети (off)	Нет	Нет	Нет	Хост полностью отключен от сети
Ошибка (err)	Да	Да	Нет	При обновлении информации о состоянии хоста выявлена ошибка. Можно использовать команду <code>onehost show</code> Для просмотра описания ошибки
Повторить попытку (retry)	Да	Да	Нет	Обновление информации о хосте, который находится в состоянии ошибки

2.1.3.2. Управление хостом в интерфейсе командной строки

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

1) для отключения хоста необходимо использовать команду:

```
onehost disable <идентификатор_хоста>
```

2) чтобы снова включить хост, необходимо использовать команду:

```
onehost enable <идентификатор_хоста>
```

3) для полного отключения хоста необходимо использовать команду:

```
onehost offline <идентификатор_хоста>
```

Примеры:

1. Перевод хоста с идентификатором 1 в состояние «Отключен»

```
onehost disable 1
```

Для просмотра состояния хоста 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	breast-service	default	0	0 / 600 (0%)	0K / 5.8G (0%)	on

2. Включение хоста с идентификатором 1

```
onehost enable 1
```

Процесс включения хоста занимает от 20 до 60 секунд. Для просмотра состояния хоста 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	breast-service	default	0	0 / 600 (0%)	0K / 5.8G (0%)	on

3. Полное отключение хоста с идентификатором 1

```
onehost offline 1
```

Для просмотра состояния хоста 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	breast-service	default	0	0 / 600 (0%)	0K / 5.8G (0%)	on

Команды `disable` и `offline` не влияют на состояние ВМ, работающих на хосте.

Для того чтобы выполнить автоматическую миграцию ВМ на другие хосты, обладающие достаточным вычислительным ресурсом, необходимо выполнить команду

```
onehost flush <наименование_хоста>
```

В качестве наименования хоста можно указать перечень хостов (идентификаторов или

наименований, разделенных запятыми) или диапазон идентификаторов хостов (в качестве разделителя используются две точки — «..»).

2.1.3.3. Управление хостом в веб-интерфейсе ПК СВ

Для управления хостом в веб-интерфейсе ПК СВ необходимо:

- 1) в меню слева выбрать пункт меню «Инфраструктура — Узлы»;
- 2) на открывшейся странице **Узлы** выбрать необходимый хост.

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

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

2.1.4. Удаление хоста

2.1.4.1. В интерфейсе командной строки

Для удаления хоста в интерфейсе командной строки необходимо использовать команду:

```
onehost delete <сетевое_имя_хоста>
```

или команду:

```
onehost delete <идентификатор_хоста>
```

Пример

Удаление хоста node01:

```
onehost delete node1
```

2.1.4.2. В веб-интерфейсе ПК СВ

Для удаления хоста в веб-интерфейсе ПК СВ необходимо:

- 1) в меню слева выбрать пункт меню «Инфраструктура — Узлы»;
- 2) на открывшейся странице **Узлы** выделить необходимый хост и нажать на кнопку **[Удалить]** (см. рис. 4).

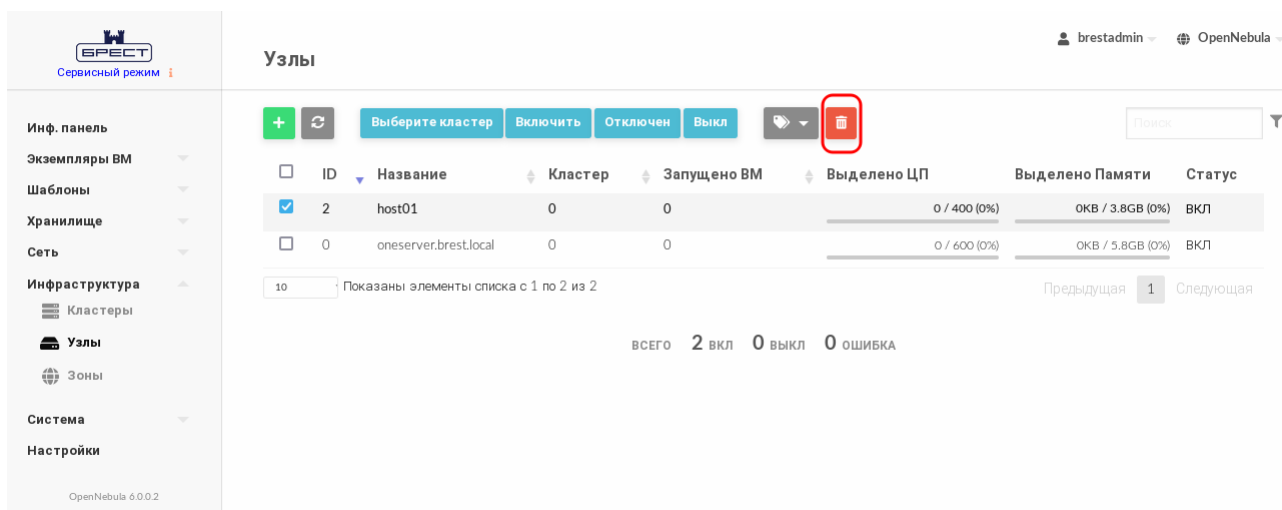


Рис. 4

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

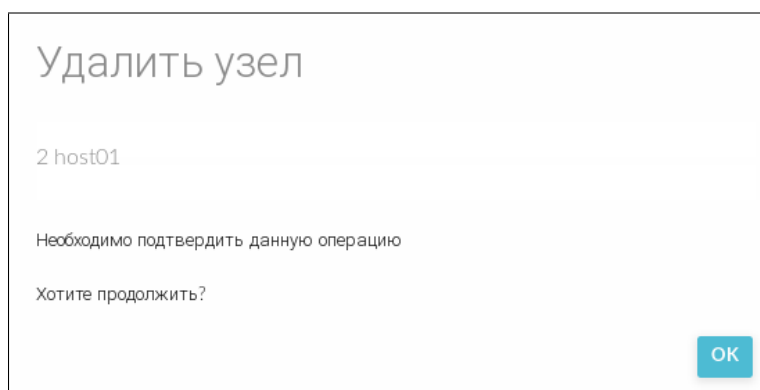


Рис. 5

2.1.5. Мониторинг хоста

В ПК СВ используется распределенная система мониторинга. На хосте функционирует агент мониторинга, который с заданной периодичностью выполняет тесты и отправляет собранные данные сервису `onemondord` на фронтальной машине.

Примечание. Функционирование системы мониторинга ПК СВ описано в документе «Программный комплекс «Средства виртуализации «Брест» (ПК СВ «Брест») РДЦП.10001-03. Руководство администратора. Часть 1».

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

Таблица 3

Параметр	Описание
HYPERVISOR	Название гипервизора хоста, применяется для выбора хостов с определенной технологией
ARCH	Архитектура ЦП хоста, например, x86_64

Продолжение таблицы 3

Параметр	Описание
MODELNAME	Название модели ЦП хоста, например, Intel(R) Core(TM) i7-2620M CPU @ 2.70GHz
CPUSPEED	Частота ЦП в МГц
HOSTNAME	Сетевое имя хоста (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. параграф 2.1.2.1)
MAX_MEM	Максимальное количество памяти, которое может использоваться для VM. Кроме того, это значение отображается в виде параметра MEMORY TOTAL в секции HOST SHARE после выполнения команды onehost show (см. параграф 2.1.2.1)
MAX_DISK	Общий объем пространства облачного 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. параграф 2.1.2.1)
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. параграф 2.1.2.1)
USED_DISK	Используемый объем пространства облачного 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 VM на данный момент, в КБ
FREE_DISK	Объем свободного пространства облачного хранилища в МБ
CPU_USAGE	Общая мощность ЦП, распределенная среди VM, запущенных на данном хосте в соответствии с запросом, который указан в параметре CPU в каждом шаблоне VM. Кроме того, это значение отображается в виде параметра CPU USED (ALLOCATED) в секции HOST SHARE после выполнения команды onehost show (см. параграф 2.1.2.1)
MEM_USAGE	Общая память, распределенная среди VM, запущенных на данном хосте в соответствии с запросом, который указан в параметре MEMORY в каждом шаблоне VM. Кроме того, это значение отображается в виде параметра MEMORY USED (ALLOCATED) в секции HOST SHARE после выполнения команды onehost show (см. параграф 2.1.2.1)
DISK_USAGE	Общий размер образов диска для VM, запущенных на хосте, рассчитанный с применением параметра SIZE каждого образа с учетом характеристик облачного хранилища
NETRX	Объем входящего сетевого трафика
NETTX	Объем исходящего сетевого трафика

Окончание таблицы 3

Параметр	Описание
WILD	Перечень VM, разделенных запятой, работающих на хосте и которые не были запущены сервисом ПК СВ и не контролируются в данный момент
ZOMBIES	Перечень VM, разделенных запятой, работающих на хосте и которые были запущены сервисом ПК СВ, но в данный момент им не контролируются

2.1.6. 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. подраздел 2.1.5). 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 сервис ПК СВ. Однако некоторые операции не могут быть выполнены на импортированной виртуальной машине, в том числе: отключение питания, отмена развертывания, перемещение, удаление или восстановление.

2.1.6.1. Импорт неконтролируемых VM в интерфейсе командной строки

Для обнаружения неконтролируемых виртуальных машин используется команда:

```
onehost show <идентификатор_хоста>
```

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_хоста> <наименование_VM>
```

2.1.6.2. Импорт неконтролируемых VM 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 хост;
- 3) на открывшейся странице хоста открыть вкладку **ВМ вне** (см. рис. 6).

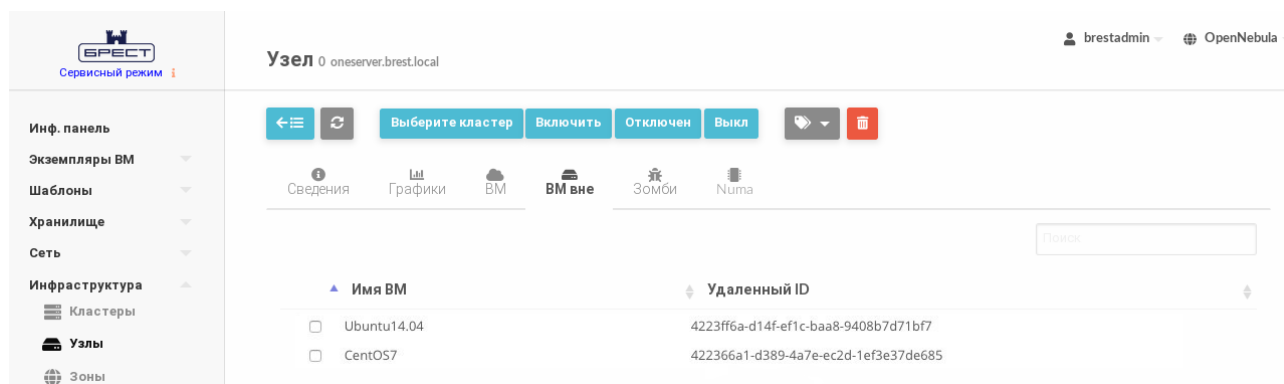


Рис. 6

2.2. Кластеры

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

2.2.1. Управление кластером

2.2.1.1. 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
```

2.2.1.2. 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).

The screenshot displays the OpenNebula web interface. On the left is a navigation sidebar with the 'СЕРВЕРЫ' logo and 'Сервисный режим' indicator. The main content area is titled 'Кластер 0 default'. At the top right, it shows the user 'brestadmin' and the system 'OpenNebula'. Below the title are navigation tabs: 'Сведения' (selected), 'Узлы', 'Вирт. сети', and 'Хранилища'. The 'Сведения' tab shows the following information:

- Информация**
- ID: 0
- Название: default (with an edit icon)
- Автоматическая миграция: Выкл (with an edit icon)

Below this is the 'Переподписка' (Subscription) section, which includes two sliders and input fields:

- Зарезервировано CPU: 0% (slider at 0%, input field at 0%)
- Зарезервировано памяти: 0% (slider at 0%, input field at 0%)

A green 'Обновить' (Refresh) button is located at the top right of the main content area.

Рис. 7

2.2.2. Добавление хостов к кластеру

2.2.2.1. В интерфейсе командной строки

Хосты можно регистрировать непосредственно в кластере с помощью команды `onehost create` (см. параграф 2.1.1.1), указав в команде аргумент `--cluster <идентификатор/наименование_кластера>`.

Чтобы добавить хост в кластер необходимо выполнить команду:

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

Одновременно хост может находиться только в одном кластере.

Для удаления хоста из кластера используется команда:

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

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

Примеры:

1. Добавление хоста с наименованием «host01» в кластер с наименованием «production»: `onecluster addhost production host01`

Для просмотра информации о принадлежности хоста 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	breast-service	default	0	0 / 600 (0%)	0K / 5.8G (0%)	on

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

```
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

2.2.2.2. В веб-интерфейсе ПК СВ

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

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



Рис. 8

2.2.3. Добавление ресурсов к кластеру

В кластере можно зарегистрировать облачные хранилища и сети. В этом случае если в шаблоне VM определены идентификаторы этих облачных хранилищ и/или сетей, то VM может быть запущена на любом хосте кластера. Облачные хранилища и сети можно регистрировать одновременно в нескольких кластерах.

Для добавления/удаления облачной сети используется команда:

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

Для добавления/удаления облачного хранилища используется команда:


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

Примеры:

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

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

2. Просмотр информации о кластере с наименованием «production» после добавления облачной 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. ПОЛЬЗОВАТЕЛИ И ГРУППЫ

3.1. Общие сведения

Пользователь в ПК СВ определяется по имени и паролю. Создавать новую учетную запись в ОС СН для каждого пользователя ПК СВ не требуется. Аутентификация пользователей ПК СВ осуществляется при помощи строки сессии в каждой операции, которая проверяется ядром ПК СВ (службой `oned`).

Каждый пользователь обладает уникальным идентификатором и принадлежит к группе.

При первом запуске ПК СВ автоматически создаются следующие группы:

- `brestadmins` — администраторы ПК СВ, обладают полномочиями, чтобы выполнить любую операцию в отношении любого объекта. При этом в этой группе автоматически создаются следующие пользователи:

- `oneadmin` — используется для взаимодействия всех систем ПК СВ,
- `serveradmin` — используется сервисом веб-интерфейса ПК СВ для взаимодействия с другими сервисами ПК СВ;

- `brestusers` — пользователи инфраструктуры, имеют доступ к большей части функционала, предлагаемого ПК СВ для управления ресурсами.

Кроме того, при инициализации сервиса фронтальной машины в ПК СВ создается 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 сервиса фронтальной машины.

3.2. Управление пользователями

3.2.1. 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>
```

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	-	-	-

3.2.2. Управление пользователями в веб-интерфейсе ПК СВ

Для отображения перечня всех пользователей в веб-интерфейсе ПК СВ необходимо в меню слева выбрать пункт меню «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).

ID	Название	Группа	Включено	Драйвер авторизации	VM	Память	CPU
<input type="checkbox"/>	6	newuser	brestusers	Нет	core	0 / -	0кВ / -
<input type="checkbox"/>	5	domainuser	brestadmins	Нет	public	0 / -	0кВ / -
<input type="checkbox"/>	4	otheradmin	brestadmins	Нет	core	0 / -	0кВ / -
<input type="checkbox"/>	2	brest-admin	brestadmins	Да	public	2 / -	4GB / -
<input type="checkbox"/>	1	serveradmin	brestadmins	Да	server_cipher	0 / -	0кВ / -
<input type="checkbox"/>	0	oneadmin	brestadmins	Да	core	-	-

Рис. 9

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

- 1) в меню слева выбрать пункт меню «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);

Создать пользователя

← Сброс Создать

Имя пользователя
testuser

Пароль
••••••••

Подтвердите пароль
••••••••

Сменить пароль при первом входе в систему

Способ аутентификации
общий

Основная группа
1: brestusers

Рис. 10

- 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).

FreeIPA Administrator

Идентификация Политика Аутентификация Сетевые службы IPA-сервер

Пользователи Узлы Услуги Группы Представления ID Автоучастник

Категории пользователей

Активные пользователи

Неподтвержденные пользователи

Хранимые пользователи

Активные пользователи

Поиск

Обновить Удалить +Добавить -Отключить Включить Действия

	Имя учётной записи пользователя	Имя	Фамилия	Состояние	UID	Адрес электронной почты	Номер телефона	Должность
<input type="checkbox"/>	admin		Administrator	✓ Включено	517800000			
<input type="checkbox"/>	brest-admin	brest-admin	brest-admin	✓ Включено	517800021	brest-admin@brest.local		
<input type="checkbox"/>	testuser	testuser	testuser	✓ Включено	517800022	testuser@brest.local		

Показаны записи: с 1 по 3 из 3.

Рис. 11

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

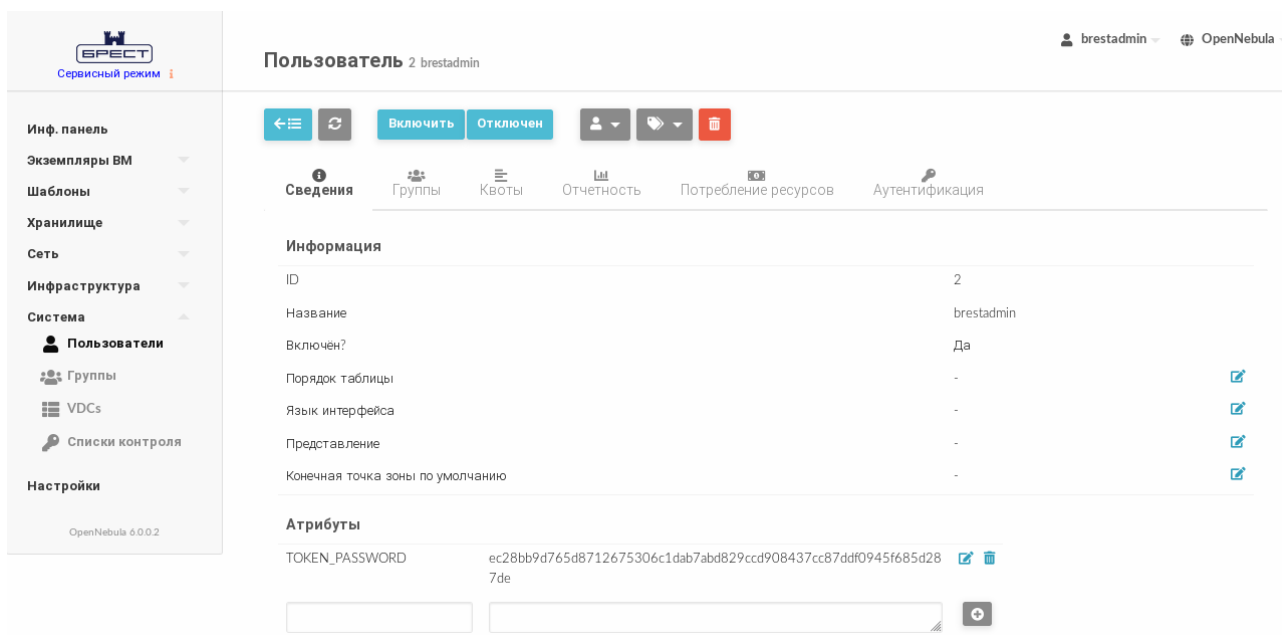


Рис. 12

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.

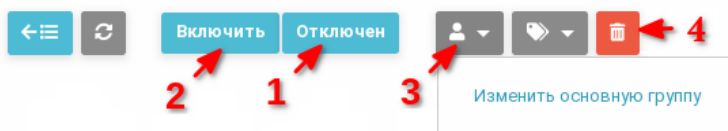


Рис. 13

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

3.3. Управление группами

3.3.1. Общие сведения

Группы в ПК СВ позволяют изолировать пользователей и ресурсы. При этом пользователь может видеть и получить доступ к облачным 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. раздел 3.4.

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.

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

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.

3.3.2. 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 облачные ресурсы. Подробная информация о правилах ACL приведена в 3.6.

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

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

Примеры:

1. Создание группы с наименованием «newuser»:

```
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 в качестве общих следующих облачных ресурсов:

VM, образы и шаблоны:

```
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 — «..»).

3.3.3. Управление группами в веб-интерфейсе ПК СВ

Для отображения перечня всех групп в веб-интерфейсе ПК СВ необходимо в меню слева выбрать пункт меню «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).

ID	Название	Пользователи	VM	Память	CPU
102	another-group	0		0 / -	0 / -
101	groupA	1		0 / -	0 / -
100	new_group	1		0 / -	0 / -
1	brestusers	1		0 / -	0 / -
0	brestadmins	3		-	-

Рис. 14

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

- 1) в меню слева выбрать пункт меню «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 облачные 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).

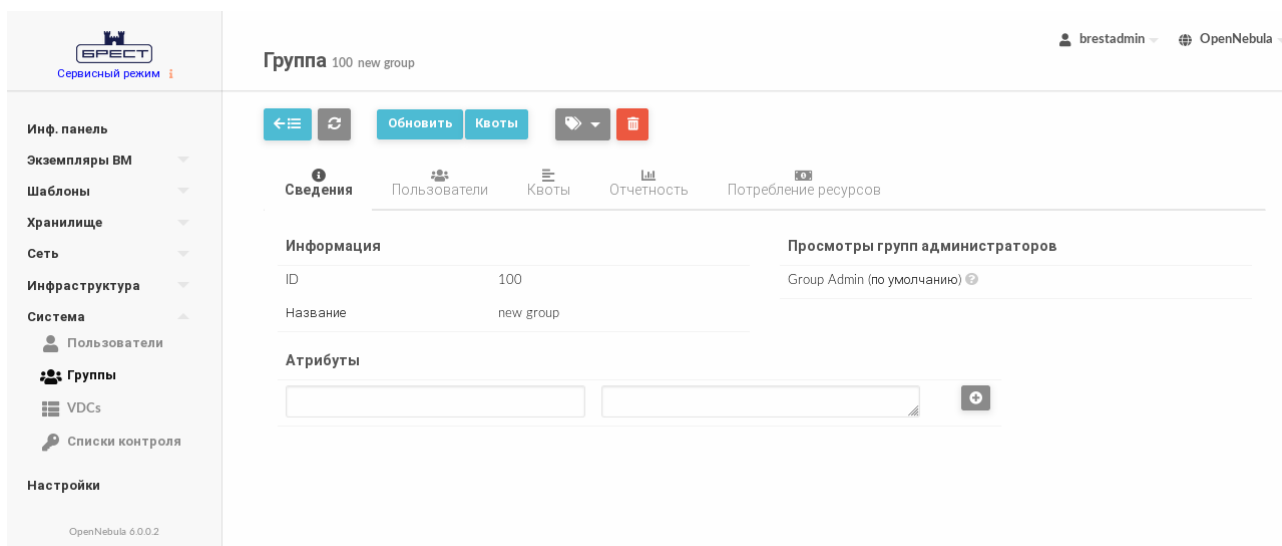


Рис. 15

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 меню «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).

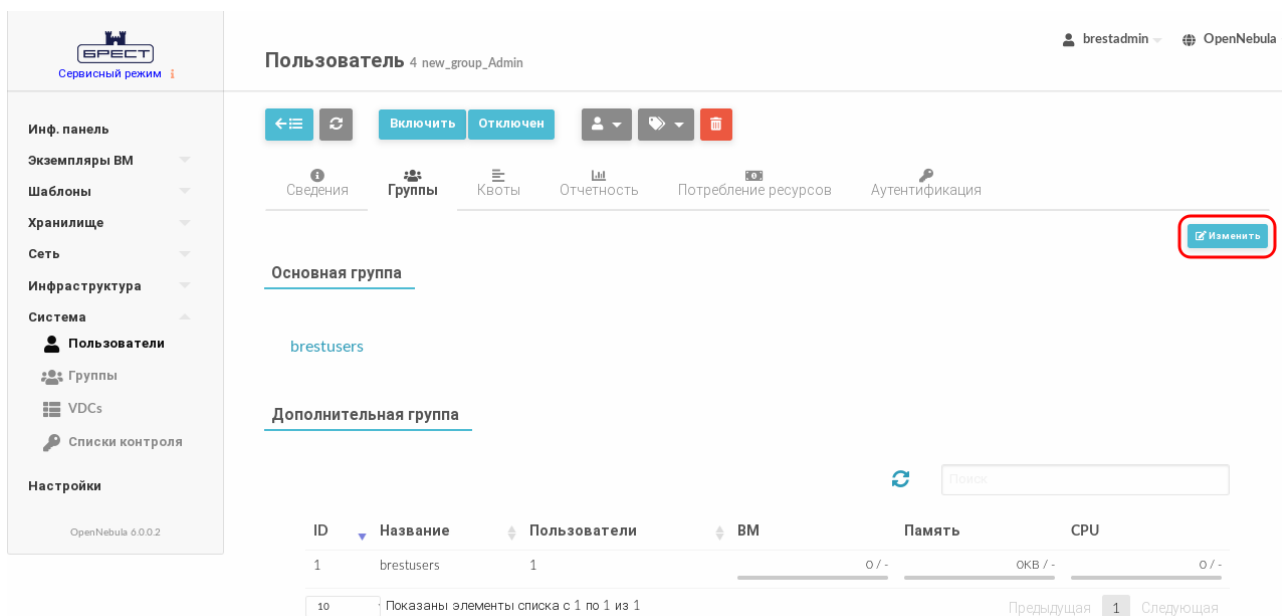


Рис. 16

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)

Пользователь 4 new_group_Admin

Информационная панель: Включить, Отключен

Сведения | Группы | Квоты | Отчетность | Потребление ресурсов | Аутентификация

Основная группа: 1: brestusers

Дополнительная группа: Вы выбрали следующие группы: brestusers, new group

ID	Название	Пользователи	VM	Память	CPU
102	another-group	0		0 / -	0КВ / -
101	groupA	1		0 / -	0КВ / -
100	new group	0		0 / -	0КВ / -
1	brestusers	1		0 / -	0КВ / -
0	brestadmins	3		-	-

Показаны элементы списка с 1 по 5 из 5

Применить изменения

Рис. 17

3.4. Управление VDC

3.4.1. 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 облачных конфигураций.

При инициализации сервиса фронтальной машины 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).

3.4.2. 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 (хосты, облачные сети и облачные хранилища). При добавлении ресурсов VDC создает правила ACL для внутренних целей, которые позволяют группам пользователей в составе VDC использовать этот пул ресурсов.

Обычно требуется добавить кластеры в VDC. Для этого используется следующая команда:

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

Для добавления отдельных хостов, облачных сетей и облачных хранилищ применяются следующие команды:

- добавление хоста:

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

- добавление виртуальной сети:

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

- добавление облачного хранилища:

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

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

Пример

Добавление всех облачных 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`.

3.4.3. Управление VDC в веб-интерфейсе ПК СВ

Для отображения перечня всех VDC в веб-интерфейсе ПК СВ необходимо в меню слева выбрать пункт меню «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).

ID	Название	Группы	Кластеры	Узлы	Вирт. сети	Хранилища
101	test	0	0	0	0	Все
100	high-performance	1	0	0	0	0
0	default	3	Все	0	0	0

Рис. 18

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

- 1) в меню слева выбрать пункт меню «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, облачную сеть или облачное хранилище

ще из состава определенного кластера, предварительно необходимо выделить этот кластер во вкладке **Ресурсы** в секции **Кластеры** (см. рис. 19)

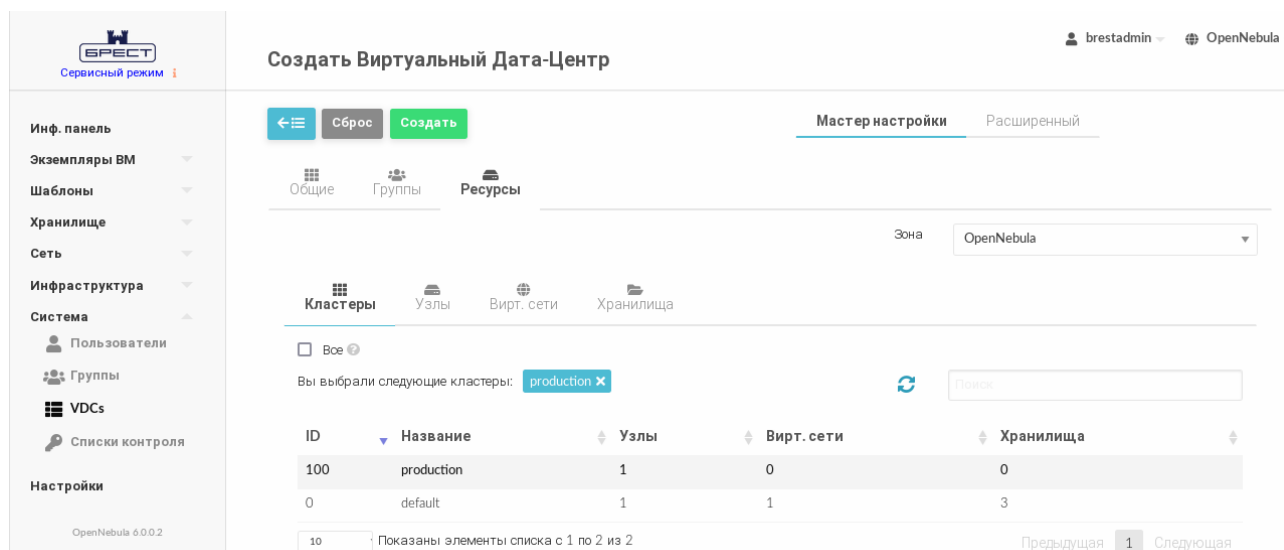


Рис. 19

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).

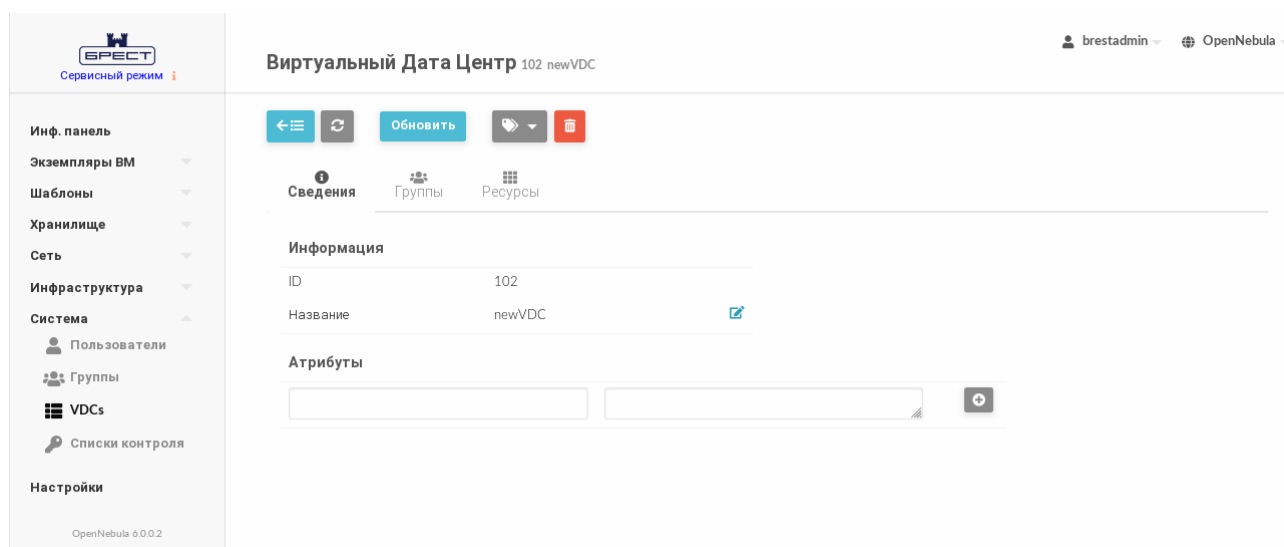


Рис. 20

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 меню «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 узел, облачную сеть или облачное 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]**.

3.5. Управление полномочиями

3.5.1. Общие сведения

У большинства облачных 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 хоста или удаление группы пользователей. В основном полномочия типа ADMIN предоставляются пользователям, которые выполняют роль администратора.

Указанные выше полномочия могут быть применены в отношении следующих облач-

ных ресурсов:

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

3.5.2. Управление полномочиями в интерфейсе командной строки

3.5.2.1. Просмотр и изменение установленных полномочий для облачного ресурса

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

Пример

Просмотр установленных полномочий шаблона с идентификатором 0

```
onetemplate show 0
```

Пример вывода после выполнения команды:

```
TEMPLATE 0 INFORMATION
ID           : 0
NAME         : else-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.

3.5.2.2. Изменение установленных полномочий для облачного ресурса

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

В качестве идентификатора облачного 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
```

3.5.2.3. 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 CH) — каждый установленный бит отменяет соответствующие полномочия для `owner`, `group` и `other`.

В таблице 4 приведены примеры соответствия маски, используемой совместно с командой `umask` и числового кода полномочий, используемого совместно с командой `chmod`.

Таблица 4

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

3.5.3. Управление полномочиями в веб-интерфейсе ПК СВ

3.5.3.1. Просмотр и изменение установленных полномочий

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

Пример

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

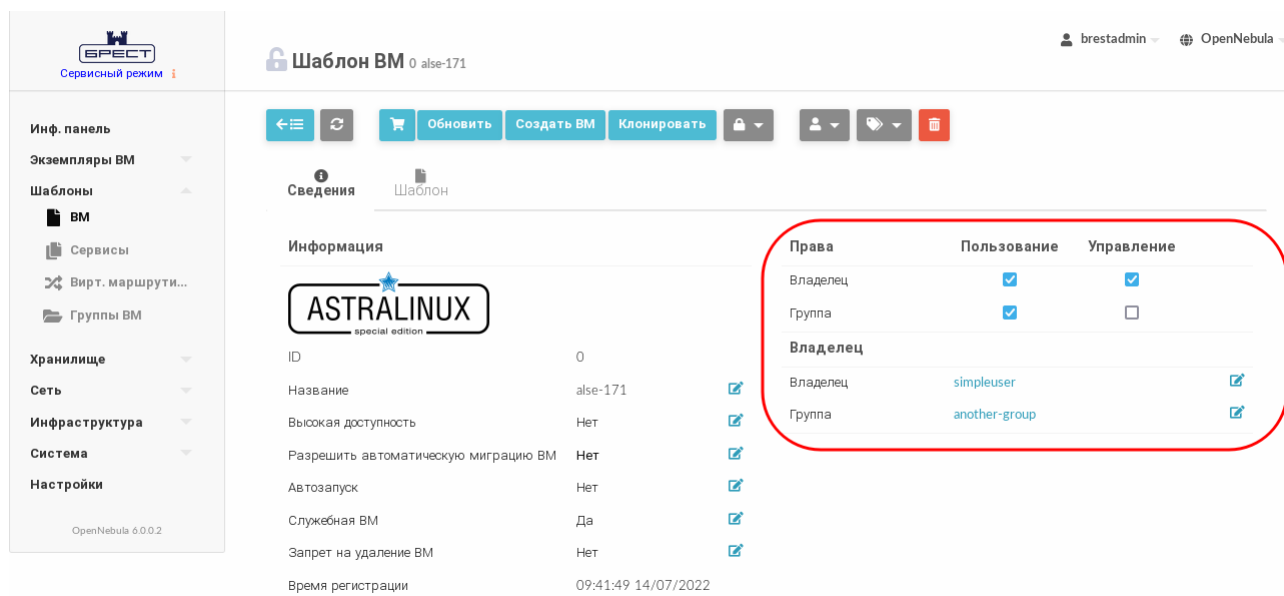


Рис. 21

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 облачного ресурса во вкладке **Сведения** установить/снять соответствующие флаги.

3.5.3.2. 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 меню «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. параграф 3.5.2.3),
- в) нажать на кнопку **[+]**.

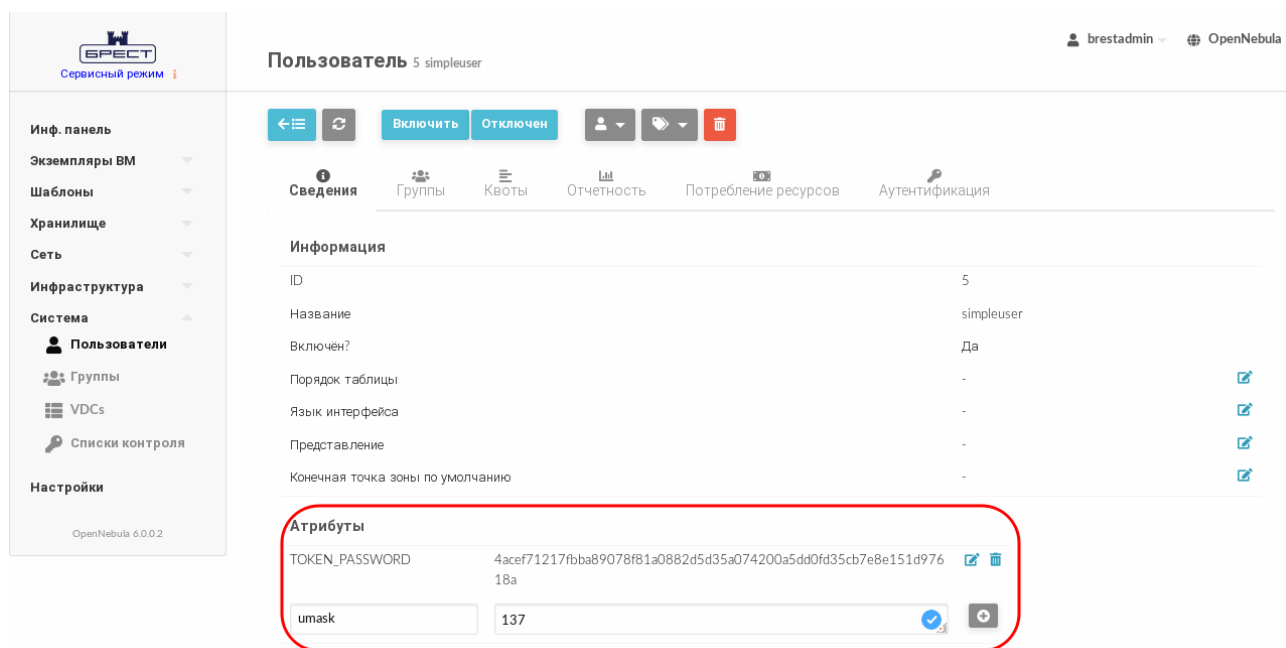


Рис. 22

3.6. Управление правилами ACL

3.6.1. 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 ядро ПК СВ (служба `oned`) может предоставить доступ или отклонить запрос.

Использование правил ACL позволяет администраторам адаптировать роли пользователей под нужды инфраструктуры. Например, при помощи правил ACL можно создать группу пользователей, которая будет видеть и использовать существующие виртуальные ресурсы, но не сможет создавать новые. Или можно предоставить определенному пользователю полномочия только для управления виртуальными сетями некоторых существующих групп.

Следует иметь в виду, что правила ACL представляют собой сложный механизм управления. В большинстве случаев рекомендуется полагаться на predefined разрешения для ресурсов и автоматически созданные правила ACL при создании группы и

добавлении физических ресурсов в VDC.

3.6.2. 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 подразделе 3.5.1);
- 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 облачного ресурса;
- 3) @<идентификатор_группы> — для группы которой принадлежит облачный ресурс;
- 4) * — для всех облачных 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 облачные 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 VM, в которых используется данная сеть

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

4. Правило дает полномочия пользователям группы с идентификатором 106 выполнять развертывание ВМ на хостах, 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 образ с идентификатором 45) не имеет смысла.

3.6.3. 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 сокращения существующих типов ресурсов. В каждом правиле указываются 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 сервиса 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 — «..»).

3.6.4. 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 меню «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).

<input type="checkbox"/>	ID	Применено к	Затрагиваемые ресурсы	№ ресурса / Принадлежит	Разрешенные действия	Зона
<input type="checkbox"/>	0	Группа brestusers	VM, Образы, Шаблоны VM, Документы, Группы безопасности, Группы VM	Все	create	Все
<input type="checkbox"/>	1	Все	Зоны	Все	use	Все
<input type="checkbox"/>	2	Все	Магазин приложений, Приложения из магазина приложений	Все	use	Все
<input type="checkbox"/>	3	Группа brestusers	Узлы	Все	manage	OpenNebula
<input type="checkbox"/>	4	Группа brestusers	Вирт. сети	Все	use	OpenNebula
<input type="checkbox"/>	5	Группа brestusers	Хранилища	Все	use	OpenNebula

Рис. 23

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

- 1) в меню слева выбрать пункт меню «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,

Создать правило контроля

Информационная панель

Экземпляры ВМ

Шаблоны

Хранилище

Сеть

Инфраструктура

Система

Пользователи

Группы

VDCs

Списки контроля

Настройки

OpenNebula 6.0.0.2

Сброс Создать

Область применения

Зоны, в которых будет действовать правило

Все

Все
 Пользователь
 Группа

Группа:

100: new group

Затрагиваемые ресурсы

Узлы
 Кластеры
 Хранилища
 ВМ

Вирт. сети
 Образы
 Шаблоны
 Пользователи

Группы
 Документы
 Зоны
 Группы безопасности

VDCs
 Вирт. маршрутизаторы
 Магазины приложений
 Приложения из магазина приложений

Группа ВМ

Подмножество ресурсов

Все
 ID
 Группа
 Кластер

Группа:

102: another-group

Разрешенные действия

Пользование
 Управление
 Администрирование
 Создать

Строка, задающая правило:

@100 IMAGE/@102 USE *

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 меню «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 **[ОК]**.

3.7. Управление квотами

3.7.1. Общие сведения

Система квот отслеживает потребление физических вычислительных ресурсов пользователями и группами и позволяют системному администратору устанавливать ограничения на применение данных ресурсов. Квоты можно установить для:

- пользователей, чтобы ограничить использование для определенного пользователя;
- групп, чтобы ограничить общее использование для всех пользователей в опре-

деленной группе. Актуально, в частности, для зон и виртуальных дата-центров ПК СВ.

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

- облачные хранилища, чтобы контролировать объем памяти, выделяемой каждому пользователю/группе в каждом облачном хранилище;
- вычислительную мощность, чтобы ограничивать общую память, работу центрального процессора или количества экземпляров VM;
- 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 VM 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.

3.7.2. Управление квотами в интерфейсе командной строки

3.7.2.1. 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.

3.7.2.2. 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 5 приведено описание параметров, необходимых для настройки каждой квоты:

Таблица 5

Параметр	Описание
Квоты на облачные хранилища. Блок параметров DATASTORE	
ID	Идентификатор облачного хранилища, для которого устанавливается квота
SIZE	Максимальный размер (в МБ), который допускается использовать в облачном хранилище

Окончание таблицы 5

Параметр	Описание
IMAGE	Максимальное количество образов, которые могут быть созданы в облачном хранилище
Квоты на вычислительную мощность. Блок параметров VM	
VMS	Максимальное количество VM, которые могут быть созданы
MEMORY	Максимальный объем памяти (в МБ), который могут запросить VM пользователя/группы
CPU	Максимальная производительность ЦП, которую могут запросить VM пользователя/группы
SYSTEM_DISK_SIZE	Максимальный размер (в МБ) системных дисков, который могут запросить VM 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 VM, которые могут одновременно использовать данный образ

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:

- общее использование облачного хранилища с идентификатором 1 ограничено диапазоном от 0 до 20 ГБ (для неограниченного количества образов);
- количество используемых виртуальных машин до четырех при максимальном объеме 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, облачных 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.

3.7.2.3. 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" ]
```


3.7.2.4. 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 — «..»).

3.7.2.5. 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.

3.7.3. 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 меню «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 меню «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):

The screenshot shows the OpenNebula web interface for a user group named '5 simpleuser'. The left sidebar contains a navigation menu with categories: 'Инф. панель', 'Экземпляры VM', 'Шаблоны', 'Хранилище', 'Сеть', 'Инфраструктура', 'Система', 'Пользователи', 'Группы', 'VDCs', 'Списки контроля', and 'Настройки'. The main content area is titled 'Пользователь 5 simpleuser' and features a top navigation bar with buttons for 'Включить', 'Отключен', and user management icons. Below this, there are tabs for 'Сведения', 'Группы', 'Квоты', 'Отчетность', 'Потребление ресурсов', and 'Аутентификация'. The 'Квоты' tab is active, showing settings for various resources:

- VM:** 4
- Запущенные VM:** По умолчанию (∞)
- CPU:** 5
- Используемые CPU:** По умолчанию (∞)
- Память:** 2048 MB
- Используемое ОЗУ:** По умолчанию (∞) MB
- Системные диски:** По умолчанию (∞) MB

 Each setting has a text input field, a '0/' indicator, and a set of control icons (edit, delete, infinity). At the top right of the main content area, there are 'Отменить' and 'Применить' buttons.

Рис. 26

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

- 1) в меню слева выбрать пункт меню «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.

4. НАСТРОЙКИ СЕТЕЙ ПК СВ

4.1. Облачные сети

4.1.1. Режимы работы облачной сети

ПК СВ поддерживает четыре сетевых режима:

- 1) режим Сетевой мост (Bridged) — VM напрямую соединяется с существующим мостом в узле виртуализации. Данный режим может быть настроен на использование групп безопасности и изоляции сети;
- 2) режим VLAN — виртуальные сети внедряются с применением технологии назначения портов на виртуальные локальные сети VLAN стандарта IEEE802.1Q (VLAN-тегирование стандарта IEEE802.1Q);
- 3) режим VXLAN — виртуальные сети задействуют сети VLAN, используя протокол VXLAN, основанный на UDP-инкапсуляции и групповой адресации IP;
- 4) режим Open vSwitch — аналогичен режиму VLAN, но использует программный коммутатор Open vSwitch (OVS) вместо сетевого моста. Группы безопасности данным режимом не поддерживаются.

ВНИМАНИЕ! Режим Open vSwitch не поддерживает классификационные метки и может использоваться только на минимальном уровне конфиденциальности.

В режиме Сетевой мост трафик VM напрямую передается через существующий сетевой мост в узлах виртуализации. При этом устанавливается один из режимов фильтрации трафика, применяемой в облачной сети:

- режим «сетевой мост без фильтрации» (Bridged);
- режим «сетевой мост с группами безопасности» (Bridged with Security Groups, далее по тексту Security Group) — устанавливаются правила iptables для внедрения правил групп безопасности;
- режим «сетевой мост с правилами ebttables » (Bridged with ebttables isolation, далее по тексту ebttables VLAN) — тоже что и для режима Security Group, но с дополнительными правилами ebttables для изоляции (L2) всех виртуальных сетей.

4.1.2. Параметры облачной сети

Параметры облачной сети объединяются в три группы:

- 1) базовая инфраструктура 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) атрибуты конфигурации для настройки виртуальной сети (сетевые настройки виртуальных машин), которые могут включать, например, маски сети, сервера DNS

или шлюзы.

4.1.2.1. Атрибуты физической сети

В группу атрибутов физической сети входят следующие параметры:

- NAME — наименование облачной сети;
- VN_MAD — сетевой режим;
- OUTBOUND_* — параметры QoS (опционально) для каждого сетевого интерфейса, подключенного к сети. Применяются для ограничения средней и пиковой пропускной способности входящего и исходящего трафика, а также объема пакетных данных, которые могут передаваться на максимальной скорости.

4.1.2.2. Адресное пространство (AR)

IP-адреса, доступные внутри облачной 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 облачной 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 VM формируются только MAC-адреса. Данный AR следует использовать, когда IP-адреса предоставляются внешним сервисом, например, сервером DHCP.

4.1.3. Использование облачных сетей

После настройки облачные сети могут использоваться пользователями в соответствии с их полномочиями (см. раздел 3.5).

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

Примеры:

1. Для определения VM с сетевым интерфейсом, подключенным к облачной сети Private, добавить в шаблон строку:

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

2. При использовании идентификатора сети добавить в шаблон строку:

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

VM также получит свободный адрес из любого адресного диапазона сети. Возможно

запросить определенный адрес, указав параметры IP или MAC в блоке параметров NIC.

Пример

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

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

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

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

Для настройки сети VM облачная сеть может включать дополнительную информацию для ввода в VM во время загрузки. Данные параметры контекстуализации могут содержать маски сети, сервера DNS или шлюзы. Параметры контекстуализации автоматически добавляются в VM и обрабатываются контекстными пакетами. Для этого в шаблон VM необходимо добавить следующий блок:

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

4.1.4. Управление облачными сетями в интерфейсе командной строки

Для управления облачными сетями используется инструмент командной строки `onevnet`.

4.1.4.1. Добавление, удаление и просмотр параметров облачной сети

Для создания облачной сети используется команда:

```
onevnet create <файл-шаблон>
```

где <файл-шаблон> — файл шаблона, в котором установлены значения параметров создаваемой облачной 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 VM с доступом к сети Интернет"

В представленном примере описана облачная 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 получают 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 облачной сети с использованием файла шаблона `priv.net`:

```
onevnet create priv.net
```

Пример вывода после выполнения команды:

```
ID: 1
```

Для удаления облачной 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 облачных сетей используется команда `onevnet list`.

Для получения подробной информации о конкретной облачной 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 VM с доступом к сети Интернет"
```

```
DNS="10.0.0.23"
```

```
GATEWAY="10.0.0.1"
```

```
PHYDEV=""
```

```
SECURITY_GROUPS="0"
```

```
VN_MAD="bridge"
```

4.1.4.2. Изменение параметров облачной сети

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

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

где <файл-шаблон> — файл шаблона для настройки параметров облачной 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 облачной сети, а временный файл шаблона будет удален.

Кроме того, можно изменить название облачной сети при помощи команды:

```
onevnet rename <идентификатор_сети> <новое_наименование_сети>
```

4.1.4.3. Управление диапазонами адресов

Диапазон адресов представляет собой непрерывный интервал значений. При этом можно динамически добавлять или удалять AR из облачной сети. Таким образом, можно легко добавить новые адреса в существующую облачную 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 облачную сеть с наименованием «Private»

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


2. Просмотр параметров облачной 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 облачной сети с наименованием «Private»

```
onevnet rmar Private 0
```

2. Просмотр параметров облачной 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 стандартные значения параметров облачной сети.

4.1.4.4. Резервирование адресов

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

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 облачной сети с наименованием «Private»

```
onevnet hold Private 10.0.0.120
```

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

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

3. Просмотр параметров облачной 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>
```

4.1.5. Управление облачными сетями в веб-интерфейсе ПК СВ

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

ID	Название	Владелец	Группа	Резервирование	Кластер	Выделенные адреса
1	Private	oneadmin	brestadmins	Нет	0	2 / 71
0	virtnetwork	brestadmin	brestadmins	Нет	0	0 / 10

Рис. 27

Для добавления облачной 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 облачной сети;
 - б) во вкладке **Конфигурация** указать режим работы облачной 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 облачной сети.

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

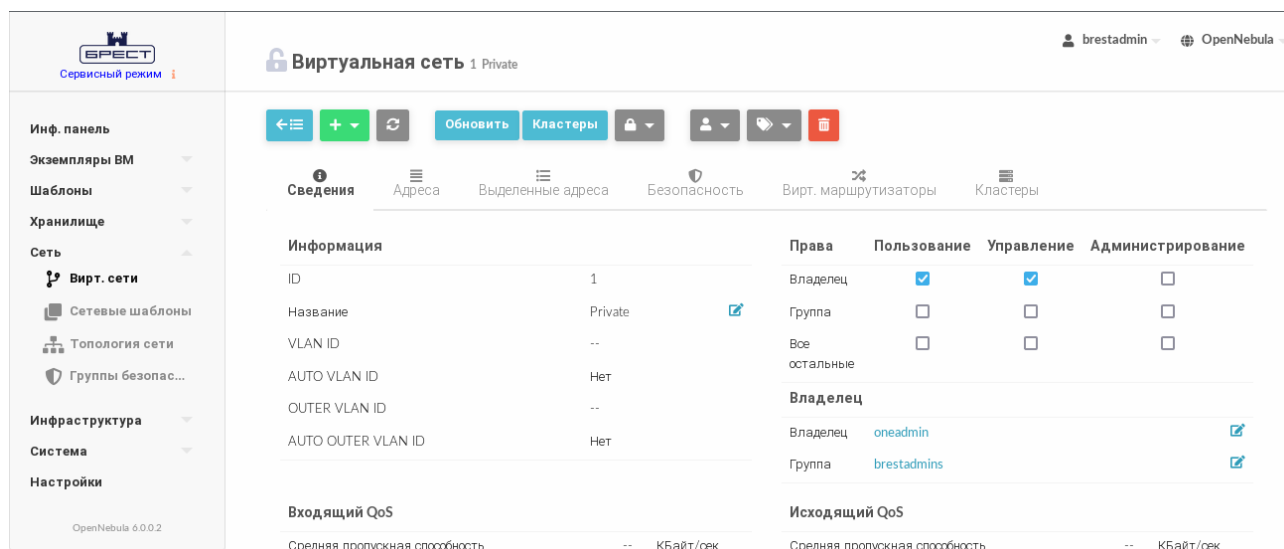


Рис. 28

Чтобы изменить параметры облачной 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 облачную сеть;
- 2) на открывшейся странице облачной сети нажать на кнопку **[Обновить]**;
- 3) на открывшейся странице **Изменить виртуальную сеть**:
 - а) во вкладке **Общие** скорректировать наименование облачной сети;
 - б) во вкладке **Конфигурация** скорректировать режим работы облачной 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 облачную сеть;
- 2) на открывшейся странице облачной 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 **[Зарезерви-**

ровано] (см. рис. 29).

Резервирование из Виртуальной сети

1 Private

Количество адресов

Добавить новую виртуальную сеть Добавить к существующему резервированию

Имя виртуальной сети

^ Расширенные настройки

Вы можете выбрать адреса из определенного диапазона адресов

Пожалуйста выберите Диапазон Адресов из списка

Поиск

Диапазон адресов	Тип	Начало	Окончание	Выделенные адреса
2	IP4	IP: 10.0.0.100 ,MAC: 02:00:0a:00:00:64	IP: 10.0.0.150 ,MAC: 02:00:0a:00:00:96	0 / 51
1	IP4	IP: 10.0.0.200 ,MAC: 02:00:0a:00:00:c8	IP: 10.0.0.219 ,MAC: 02:00:0a:00:00:db	1 / 20

10 Показаны элементы списка с 1 по 2 из 2

Предыдущая **1** Следующая

Первый адрес

Рис. 29

4.2. Группы безопасности

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

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

4.2.1. Параметры группы безопасности

Группа безопасности состоит из нескольких правил. Каждое правило определяется параметрами, приведенными в таблице 6.

Таблица 6

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

Окончание таблицы 6

Параметр	Статус	Описание	Значение
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
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 облачной сети. Используется, если правило применяется только для определенной сети.	Идентификатор существующей облачной сети

4.2.2. 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 VM. 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 облачные сети при их создании, но впоследствии ее можно удалить, обновив свойства сети.

4.2.3. Управление группами безопасности в интерфейсе командной строки

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

4.2.3.1. 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 — «..»).

4.2.3.2. 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>
```

4.2.3.3. Применение группы безопасности

Для применения групп безопасности к виртуальным машинам необходимо конкретные группы безопасности присвоить облачной 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 облачной сети (см. подраздел 4.1.2) — 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 облачной сети, а временный файл шаблона будет удален.

Также возможно настроить группы безопасности для каждого диапазона адресов (AR) облачной 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 облачной 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 облачной сети. Все идентификаторы групп безопасности объединяются и применяются в отношении экземпляра VM.

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

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

4.2.4. 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).

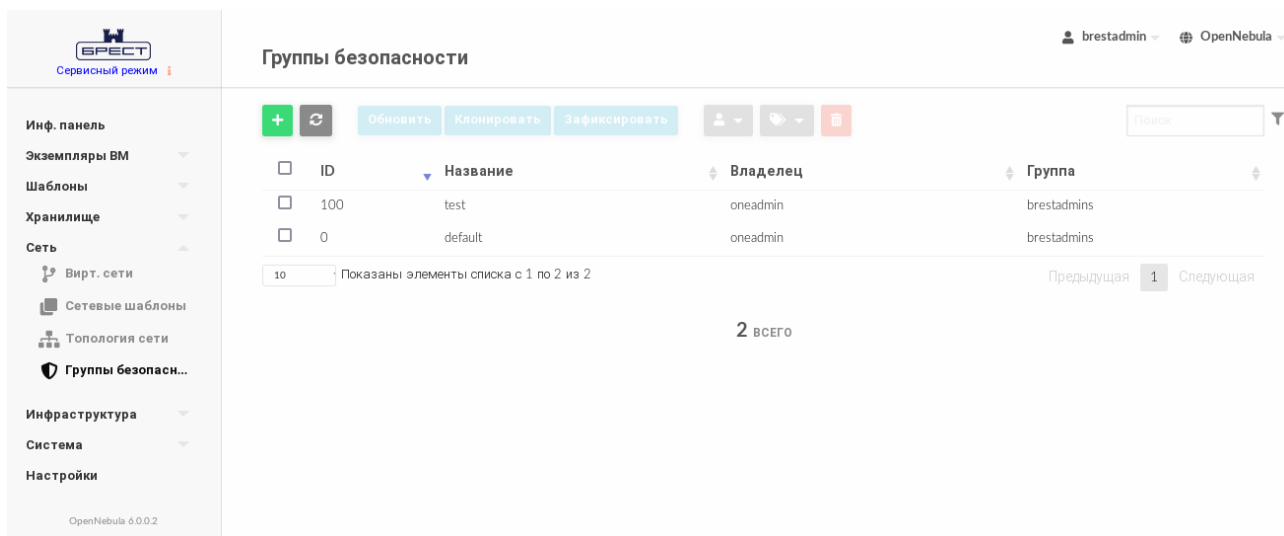


Рис. 30

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).

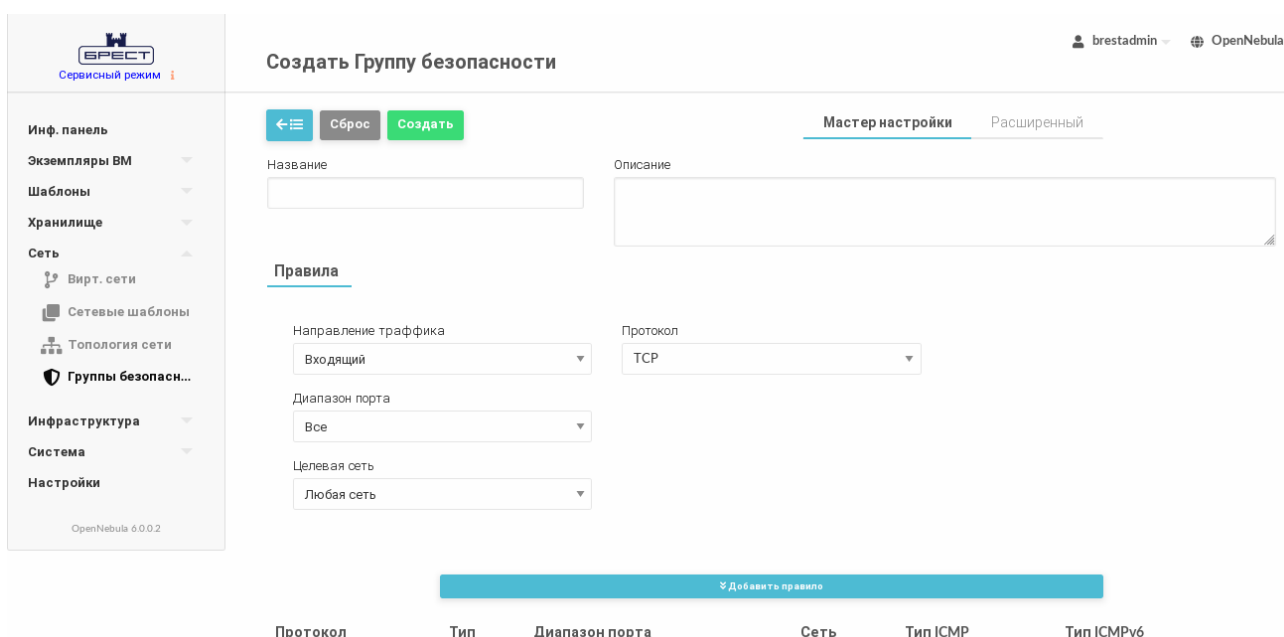


Рис. 31

После этого на открывшейся странице **Группы безопасности** появится запись о

созданной группе безопасности.

Для просмотра информации о конкретной группе безопасности на странице **Группы безопасности** необходимо выбрать соответствующую строку. После этого откроется страница группы безопасности (вкладка **Сведения** — см. рис. 32).

The screenshot shows the 'Группа безопасности 100 test' page in the OpenNebula web interface. The interface includes a sidebar menu on the left with categories like 'Инф. панель', 'Экземпляры VM', 'Шаблоны', 'Хранилище', 'Сеть', 'Вирт. сети', 'Сетевые шаблоны', 'Топология сети', 'Группы безопасн...', 'Инфраструктура', 'Система', and 'Настройки'. The main content area is titled 'Группа безопасности 100 test' and features a top navigation bar with buttons for 'Обновить', 'Клонировать', and 'Зафиксировать'. Below this, there are tabs for 'Сведения' and 'VM'. The 'Сведения' tab is active, showing a table of information for the security group 'test' (ID 100). The table includes columns for 'Информация', 'Права', 'Пользование', 'Управление', and 'Администрирование'. The 'Права' section shows checkboxes for 'Владелец', 'Группа', and 'Все остальные'. The 'Владелец' section lists 'oneadmin' and 'brestadmins' as owners. Below this, there is a 'Правила' section with a table of rules, and an 'Атрибуты' section with input fields.

Информация	Права	Пользование	Управление	Администрирование
ID: 100	Владелец: <input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Название: test	Группа: <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Все остальные: <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Протокол	Тип	Диапазон порта	Сеть	Тип ICMP
TCP	Входящий	1000:2000	Любой	
TCP	Исходящий	1000:2000	Любой	
ICMP	Входящий	Все	Виртуальная сеть 0	

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]**.

5. УПРАВЛЕНИЕ ВИРТУАЛЬНОЙ МАШИНОЙ

5.1. Управление образами

Облачное хранилище позволяет администраторам и пользователям облака ПК СВ использовать образы, которые могут являться образами дисков с установленной ОС (загрузочных дисков) или образами дисков с различными данными, используемыми в виртуальных машинах. Эти образы могут использоваться несколькими виртуальными машинами одновременно, а также быть общими для различных пользователей облака ПК СВ.

5.1.1. Типы образов

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

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

- 1) `OS` — образ загрузочного диска (с установленной ОС). Каждый шаблон VM должен определять один диск, ссылающийся на образ данного типа;
- 2) `CDROM` — образ представляет данные только для считывания. В каждом шаблоне VM может использоваться только один образ данного типа;
- 3) `DATABLOCK` — образ блока данных, является образом диска с различными данными, используемыми в виртуальных машинах. Эти образы можно создавать из уже существующих образов дисков или в качестве пустого диска.

Типы образов, которые размещены в хранилище файлов и ядер, и не могут использоваться в качестве дисков VM:

- 1) `KERNEL` — незашифрованный файл, который используется в качестве ядра (параметр `OS/KERNEL_DS` для VM);
- 2) `RAMDISK` — незашифрованный файл, который используется в качестве дискового ресурса, размещенного в оперативной памяти (параметр `OS/INITRD_DS` для VM);
- 3) `CONTEXT` — незашифрованный файл, который нужно добавить в контекстный CD-ROM (параметр `CONTEXT/FILES_DS` для VM).

5.1.2. Состояния образов

Перечень возможных состояний образов приведен в таблице 7.

Таблица 7

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

5.1.3. Создание образа

5.1.3.1. Общие сведения

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

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

При создании образа на основе имеющегося файла, исходный файл необходимо поместить на дисковый ресурс, который в настройках облачного хранилища указан в качестве разрешенного источника (параметр `SAFE_DIRS`).

5.1.3.2. Создание образа в интерфейсе командной строки

Для создания образа можно воспользоваться инструментом командной строки `oneimage`, указав команду `create`. Перечень параметров для создания образа приведен в таблице 8.

Таблица 8

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

Примеры:

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

а) выполнить команду:

```
oneimage create --datastore default --name td-alse171 --type CDROM \
  --path /var/tmp/1.7.1-22.11.2021_10.50.iso \
  --description "Технологический установочный диск ОС СН 1.7.1."
```

Пример вывода после выполнения команды:

```
ID: 4
```

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

```
oneimage show <идентификатор_образа>
```

Пример вывода после выполнения команды `oneimage show 4`:

```
IMAGE 4 INFORMATION
```

```
ID : 4
```

```
NAME : td-alse171
```

```
USER : oneadmin
```

```

GROUP : brestadmins
LOCK : None
DATASTORE : default
TYPE : CDROM
REGISTER TIME : 07/10 19:43:20
PERSISTENT : No
SOURCE : /var/lib/one//datastores/1/ce3c55d1b1737f5c365644dc7ea31335
PATH : /var/tmp/1.7.1-22.11.2021_10.50.iso
FORMAT : raw
SIZE : 3.8G
STATE : rdy
RUNNING_VMS : 0

```

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

а) выполнить команду:

```

oneimage create --datastore default --name os-alse171 \
  --type DATABLOCK --format qcow2 --prefix vd --persistent \
  --size 12288 --description "Загрузочный диск ОС СН 1.7.1."

```

В представленной выше команде были установлены следующие параметры образа:

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

Пример вывода после выполнения команды:

```
ID: 5
```

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

```
oneimage show <идентификатор_образа>
```

Пример вывода после выполнения команды `oneimage show 5`:

```

IMAGE 5 INFORMATION
ID : 5
NAME : os-alse171
USER : oneadmin
GROUP : brestadmins
LOCK : None
DATASTORE : default
TYPE : DATABLOCK
REGISTER TIME : 07/10 20:09:05
PERSISTENT : Yes

```

```

SOURCE : /var/lib/one//datastores/1/3fe0664610de3870cbdd9ba24d6a9132
FORMAT : qcow2
SIZE : 12G
STATE : rdy
RUNNING_VMS : 0

```

5.1.3.3. Создание образа в веб-интерфейсе ПК СВ

Для создания образа необходимо выполнить следующие действия:

- 1) в веб-интерфейсе ПК СВ в меню слева выбрать пункт меню «Хранилище — Образы»;
- 2) на открывшейся странице **Образы** нажать на кнопку **[+]** и в открывшемся меню выбрать пункт **Создать** (см. рис. 33)

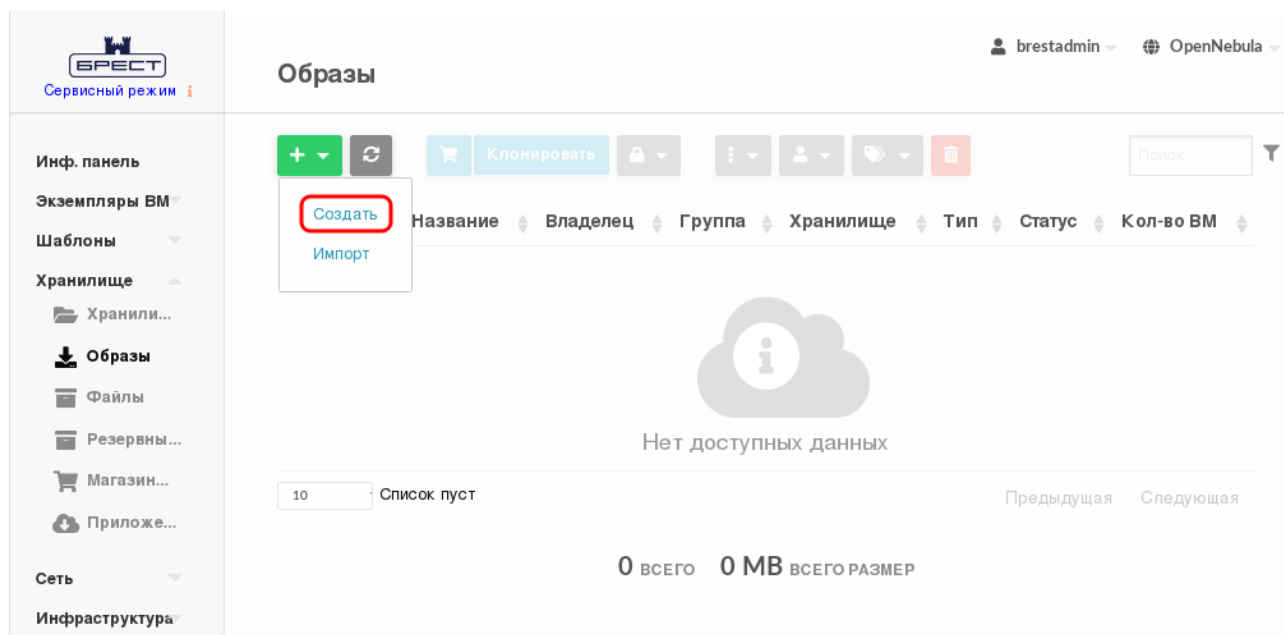


Рис. 33

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

При загрузке файла исходного образа через веб-интерфейс ПК СВ выполняется следующая последовательность действий:

- 1) клиент браузера загружает весь файл исходного образа на сервер во временный каталог;
- 2) служба `oned` регистрирует образ во время настройки пути к данному временному файлу;
- 3) служба `oned` копирует файл образа в хранилище образов;
- 4) временный файл удаляется и пользователю возвращается запрос (появляется сообщение об успешной загрузке образа).

Примечание. В случае загрузки файлов большого размера, больше 1 ГБ, и в

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

Примеры:

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

- а) в веб-интерфейсе ПК СВ в меню слева выбрать пункт меню «Хранилище — Образы»;
- б) на открывшейся странице **Образы** нажать на кнопку **[+]** и в открывшемся меню выбрать пункт **Создать**;
- в) на открывшейся странице **Укажите параметры нового образа**:
 - в поле **Название** задать наименование образа установочного носителя,
 - в выпадающем списке **Тип** выбрать значение CD-ROM только для чтения,
 - в секции **Расположение образа** установить флаг **Закачать**,
 - нажать на кнопку **[Обзор...]** (см. рис. 34);

The screenshot shows the 'Specify parameters of a new image' (Укажите параметры нового образа) page in the OpenNebula web interface. The page is titled 'Укажите параметры нового образа' and has a user 'brestadmin' and 'OpenNebula' logged in. The left sidebar contains a navigation menu with items like 'Инф. панель', 'Экземпляры ВМ', 'Шаблоны', 'Хранилище', 'Образы', 'Файлы', 'Резервны...', 'Магазин...', 'Приложе...', 'Сеть', 'Инфраструктура', 'Система', and 'Настройки'. The main content area has a 'Создать' button and a 'Образ' tab selected. Below the tabs, there are two sub-sections: 'Мастер настройки' (Master configuration) and 'Расширенный' (Advanced). The 'Мастер настройки' section contains the following fields:

- Название** (Name): A text input field containing 'td-astra171'.
- Описание** (Description): A text area containing 'Технологический установочный диск 1.7.1'.
- Тип** (Type): A dropdown menu with 'CD-ROM только для чтения' selected.
- Хранилище** (Storage): A dropdown menu with '1: default' selected.

Below these fields is the 'Расположение образа' (Image location) section, which has three radio buttons: 'Path/URL', 'Закачать' (checked), and 'Пустой образ диска'. At the bottom, there is an 'Обзор...' button and the text 'Файл не выбран.'

Рис. 34

г) в открывшемся окне **Выгрузка файла** выбрать ISO-файл образа установоч-

ного носителя и на кнопку **[Открыть]**;

д) на странице **Укажите параметры нового образа** нажать на кнопку **[Создать]**. После этого на открывшейся странице **Образы** отобразится процесс загрузки образа в облако (см. рис. 35)



Рис. 35

е) после окончания загрузки образа в хранилище необходимо дождаться момента, когда для загруженного образа в поле **Статус** значение ЗАБЛОКИРОВАНО изменится на ГОТОВО. Для обновления страницы можно воспользоваться кнопкой **[Обновить]** (см. рис. 36)

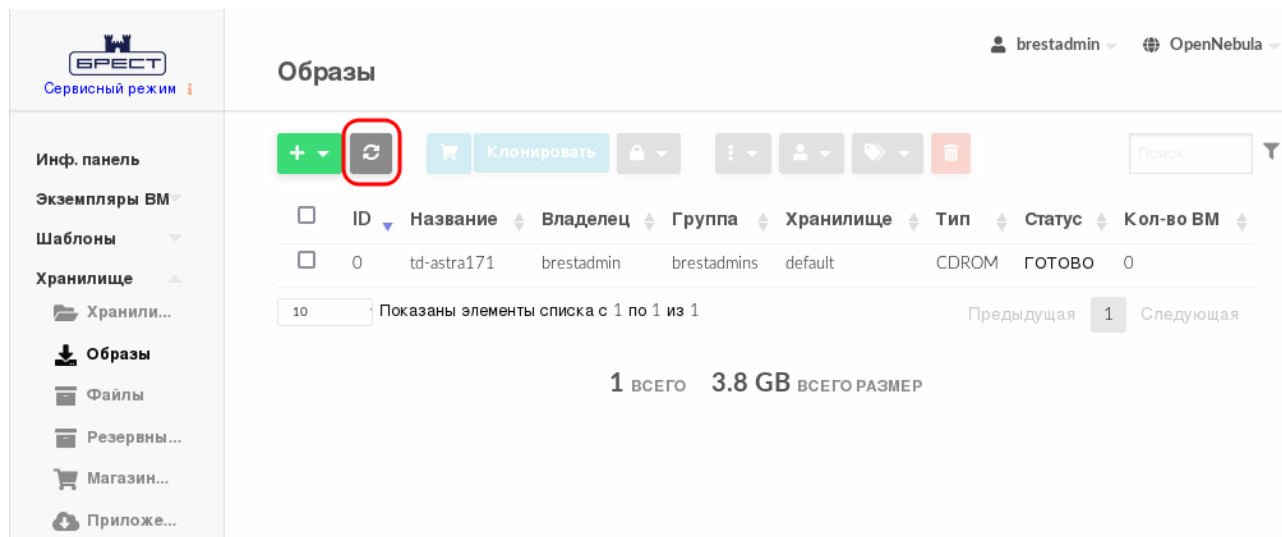


Рис. 36

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

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

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

в) на открывшейся странице **Укажите параметры нового образа**:

1) в поле **Название** задать наименование образа диска VM,

2) в выпадающем списке **Тип** выбрать значение **Общий блок данных хранилища**,

3) если планируется в дальнейшем использовать этот образ в качестве загрузочного (с установленной ОС), необходимо в выпадающем списке **Этот**

образ является постоянным выбрать значение Да,

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

5) в появившемся поле **Размер** задать требуемый размер образа (см. рис. 37);

The screenshot shows the 'Укажите параметры нового образа' (Specify parameters of a new image) page in the OpenNebula management interface. The interface includes a sidebar with navigation options like 'Инф. панель', 'Экземпляры ВМ', 'Шаблоны', 'Хранилище', 'Образы', 'Файлы', 'Резервны...', 'Магазин...', 'Приложе...', 'Сеть', 'Инфраструктура', 'Система', and 'Настройки'. The main content area has a title 'Укажите параметры нового образа' and a user profile 'brestadmin'. Below the title are buttons for '←', 'Сброс', and 'Создать'. There are two tabs: 'Образ' (selected) and 'Dockerfile'. The 'Мастер настройки' (Wizard) section is active, showing fields for 'Название' (Name: disk-171), 'Описание' (Description: Диск ВМ с ОС CH 1.7.1), 'Тип' (Type: Generic storage datablock), and 'Хранилище' (Storage: 1: default). A checkbox 'Этот образ является постоянным' (This image is permanent) is checked. Below this is the 'Расположение образа' (Image location) section with three radio buttons: 'Path/URL', 'Закачать' (Upload), and 'Пустой образ диска' (Empty disk image), which is selected. At the bottom, the 'Размер' (Size) is set to 12 GB.

Рис. 37

г) на странице **Укажите параметры нового образа** раскрыть секцию **Расширенные настройки**, в выпадающем списке **Шина** выбрать необходимый драйвер диска, например *Virtio*, в выпадающем списке **Формат** выбрать значение *qcow2* (см. рис. 38)

The screenshot shows the 'Расширенные настройки' (Advanced settings) section. It contains four dropdown menus: 'Шина' (Bus) set to 'Virtio', 'Целевое устройство' (Target device) which is empty, 'Формат' (Format) set to 'qcow2', and 'Файловая система' (File system) set to '--'.

Рис. 38

д) на странице **Укажите параметры нового образа** нажать на кнопку **[Создать]**. После этого на открывшейся странице **Образы** необходимо удостовериться в том, что созданный образ имеет статус ГОТОВО (см. рис. 39)

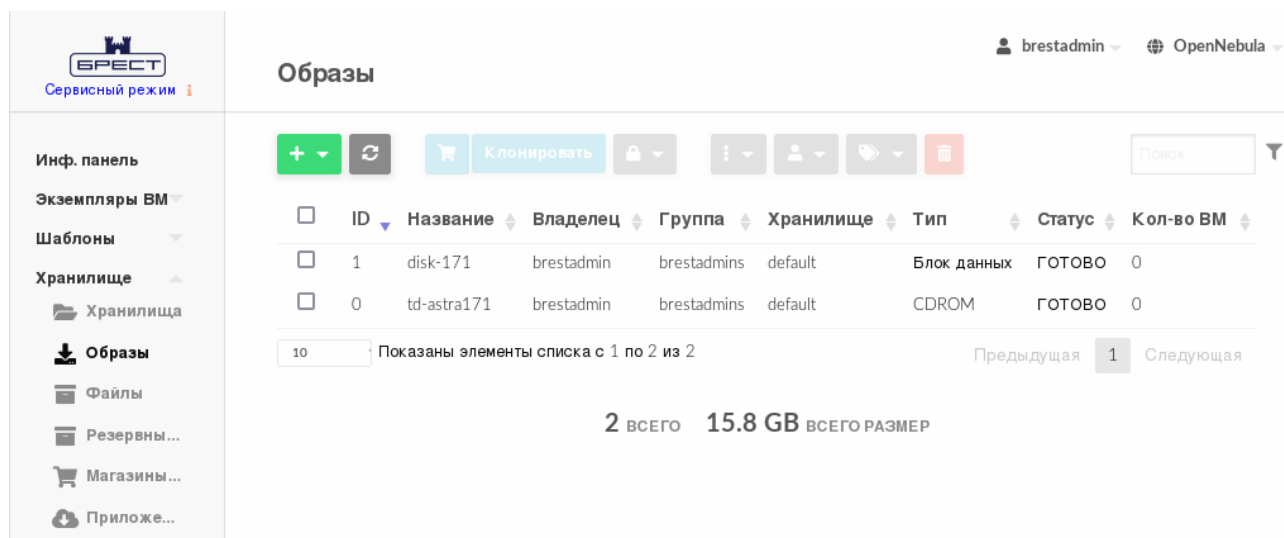


Рис. 39

5.1.4. Клонирование образов

5.1.4.1. Общие сведения

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

ВНИМАНИЕ! Нельзя клонировать постоянные образы со снимками. Для этого пользователю нужно сначала очистить его от снимков в соответствии с 5.1.8.

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

5.1.4.2. Клонирование образа в интерфейсе командной строки

Для клонирования образа в интерфейсе командной строки необходимо выполнить команду:

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

Пример

Клонирование образа блока данных с идентификатором «6»:

1) выполнить команду:

```
oneimage clone 6 another-os-also171
```

Пример вывода после выполнения команды:

```
ID: 7
```

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

```
oneimage show <идентификатор_образа>
```

Пример вывода после выполнения команды `oneimage show 7`:

```
IMAGE 7 INFORMATION
ID : 7
NAME : another-os-alse171
USER : oneadmin
GROUP : brestadmins
LOCK : None
DATASTORE : default
TYPE : DATABLOCK
REGISTER TIME : 07/10 21:12:40
PERSISTENT : Yes
SOURCE : /var/lib/one//datastores/1/e84a22fb590908a94f50e3dd06495c95
PATH : /var/lib/one//datastores/1/3fe0664610de3870cbdd9ba24d6a9132
FORMAT : qcow2
SIZE : 12G
STATE : rdy
RUNNING_VMS : 0
```

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

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

5.1.4.3. Клонирование образа в веб-интерфейсе ПК СВ

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

- 1) в меню слева выбрать пункт меню «Хранилище — Образы»;
- 2) на открывшейся странице **Образы** выбрать образ, который необходимо клонировать;
- 3) на открывшейся странице образа нажать на кнопку **[Клонировать]** (см. рис. 40)

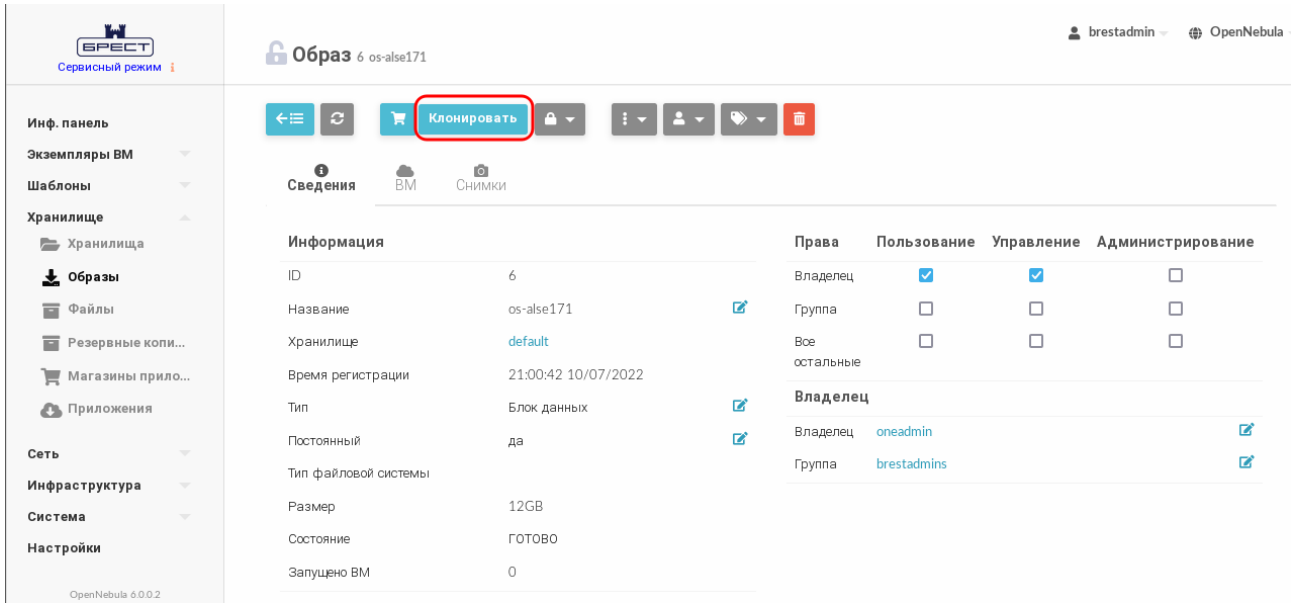


Рис. 40

4) на открывшейся странице **Клонировать образ** задать наименование нового образа. Если необходимо клонировать образ в другое хранилище, необходимо раскрыть секцию **Расширенные настройки** и выбрать новое хранилище образов (см. рис. 41)

Клонировать образ

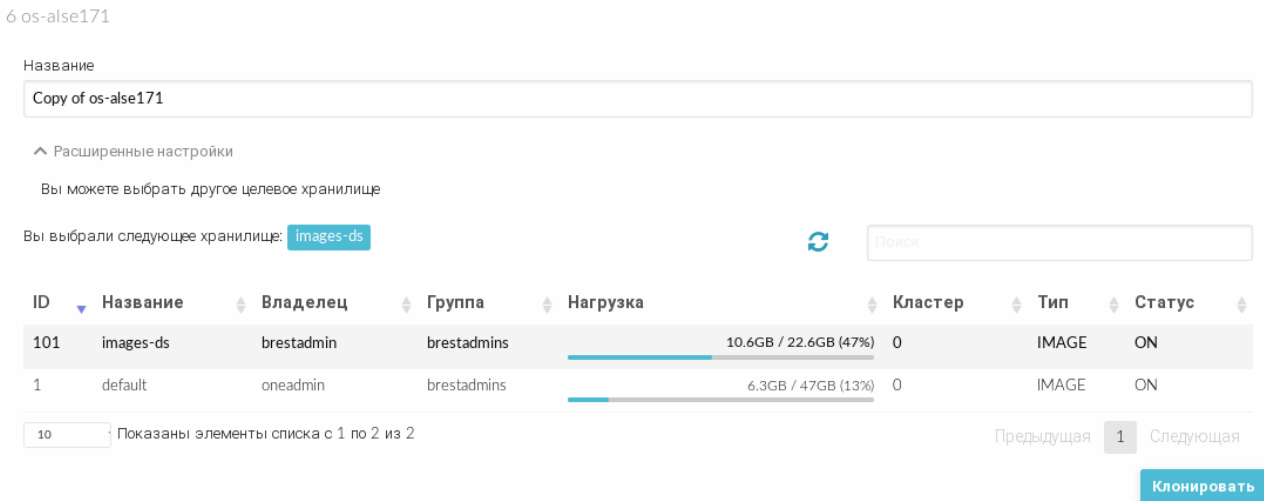


Рис. 41

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

5.1.5. Отображение доступных образов

5.1.5.1. В интерфейсе командной строки

Для отображения образов, имеющих в облачном хранилище, в интерфейсе командной строки возможно использовать команду `oneimage list` или настроить непрерывное отображение образов при помощи команды `oneimage top`. Для получения полной инфор-

мации об образе необходимо использовать команду

```
oneimage show <идентификатор_образа>
```

Пример

Вывод после выполнения команды `oneimage show 1`:

```
IMAGE 1 INFORMATION
ID : 1
NAME : td-alse171
USER : brestadmin
GROUP : brestadmins
LOCK : None
DATASTORE : default
TYPE : CDROM
REGISTER TIME : 07/18 16:18:44
PERSISTENT : No
SOURCE : /var/lib/one//datastores/1/5c31df1e4e28a9969e4c1a84f77c9c28
PATH : /var/tmp/4093640704-171-22112021_1050iso
FORMAT : raw
SIZE : 3.8G
STATE : rdy
RUNNING_VMS : 0

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

IMAGE TEMPLATE
DEV_PREFIX="hd"
```

5.1.5.2. В веб-интерфейсе ПК СВ

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

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

- 1) в меню слева выбрать пункт меню «Хранилище — Образы»;
- 2) на открывшейся странице **Образы** выбрать необходимый образ. После этого откроется страница с параметрами выбранного образа (вкладка **Сведения**) — см. рис. 42

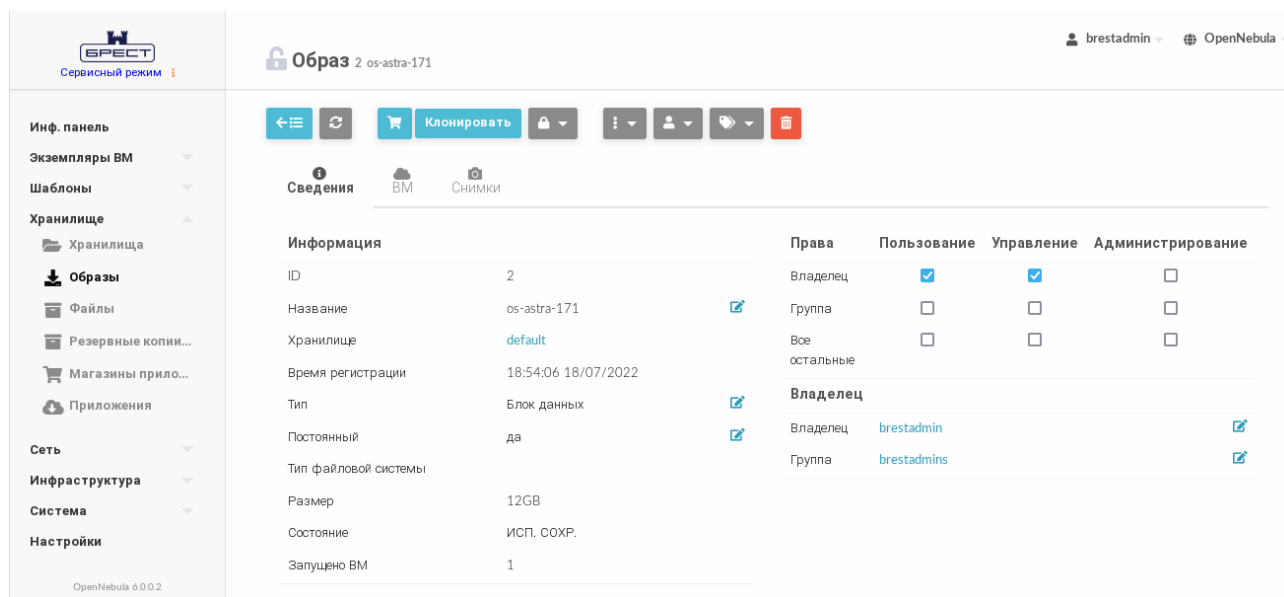


Рис. 42

5.1.6. Общие образы

Пользователи могут предоставлять общий доступ к своим образам другим пользователям в своей группе или всем пользователям ПК СВ в соответствии с установленными полномочиями (см. раздел 3.5).

5.1.6.1. Управление доступом к образу в интерфейсе командной строки

Управление доступом осуществляется с помощью команды `oneimage chmod` путем настройки битов прав доступа (см. параграф 3.5.2.2).

Примеры:

1. Предоставление пользователям в группе общего доступ к образу 0 путем настройки бита прав типа USE для GROUP.

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

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

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

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

```
...
PERMISSIONS
OWNER : um-
```


GROUP : u--

OTHER : ---

...

2. Предоставление пользователям в одной группе прав типа USE и MANAGE на образ 0, а остальным пользователям только права типа USE

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

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

...

PERMISSIONS

OWNER : um-

GROUP : um-

OTHER : u--

...

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

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

Пример

Просмотр установленных разрешений для образа с идентификатором 2 (см. рис. 43).

The screenshot shows the OpenNebula web interface. The left sidebar contains a navigation menu with items like 'Инф. панель', 'Экземпляры VM', 'Шаблоны', 'Хранилище', 'Образы', 'Файлы', 'Резервные копии...', 'Магазины прило...', 'Приложения', 'Сеть', 'Инфраструктура', 'Система', and 'Настройки'. The main content area displays details for image '2 os-astra-171'. A table titled 'Права' (Permissions) is highlighted with a red rounded rectangle. The table has four columns: 'Права', 'Пользование', 'Управление', and 'Администрирование'. The rows are 'Владелец' (Owner), 'Группа' (Group), and 'Все остальные' (All others). The 'Владелец' row has checked boxes for 'Пользование' and 'Управление'. The 'Группа' and 'Все остальные' rows have unchecked boxes for all three categories. Below the table, the 'Владелец' (Owner) is listed as 'brestadmin' and the 'Группа' (Group) as 'brestadmins'.

Права	Пользование	Управление	Администрирование
Владелец	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Группа	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Все остальные	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Владелец
 Владелец: [brestadmin](#)
 Группа: [brestadmins](#)

Рис. 43

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

полномочий в отношении данного образа.

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

5.1.7. Присвоение образам атрибута «постоянный»

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

5.1.7.1. В интерфейсе командной строки

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

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

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

5.1.7.2. В веб-интерфейсе ПК СВ

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

- 1) в меню слева выбрать пункт меню «Хранилище — Образы»;
- 2) на открывшейся странице **Образы**:
 - а) выбрать необходимые образы,
 - б) нажать кнопку изменения атрибутов образ и в открывшемся меню выбрать пункт «Сделать постоянным» / «Сделать непостоянным» (см. рис. 44).

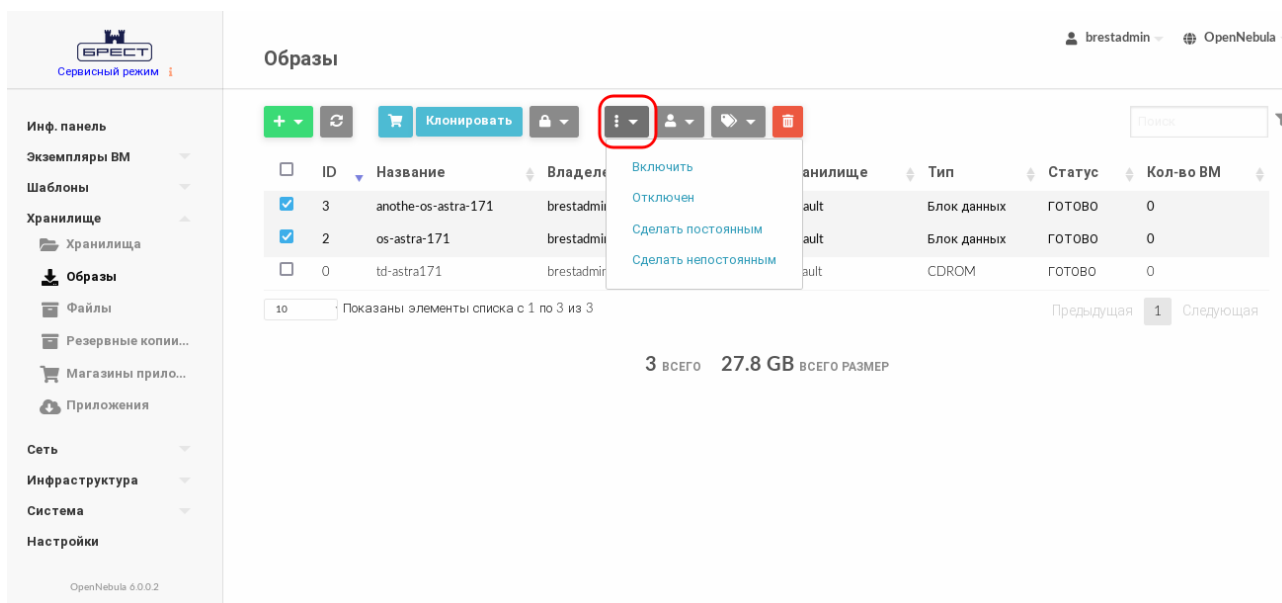


Рис. 44

5.1.8. Управление снимками в постоянных образах

Постоянные образы могут иметь снимки состояния, создаваемые пользователем во время работы ВМ, которая использует данный постоянный образ (см. подраздел 5.3.5). Снимки состояния постоянного образа сохраняются после удаления ВМ.

5.1.8.1. В интерфейсе командной строки

Ниже представлены команды, которые позволяют пользователю напрямую управлять снимками.

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

```
oneimage snapshot-revert <идентификатор_образа> <идентификатор снимка>
```

Команда удаляет все несохраненные данные.

Для преобразования в образ без снимков используется команда:

```
oneimage snapshot-flatten <идентификатор_образа> <идентификатор снимка>
```

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

Для удаления снимка используется команда:

```
oneimage snapshot-delete <идентификатор_образа> <идентификатор снимка>
```

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

5.1.8.2. В веб-интерфейсе ПК СВ

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

- 1) в меню слева выбрать пункт меню «Хранилище — Образы»;
- 2) на открывшейся странице **Образы** выбрать необходимый образ;
- 3) на странице образа открыть вкладку **Снимки** (см. рис. 45).

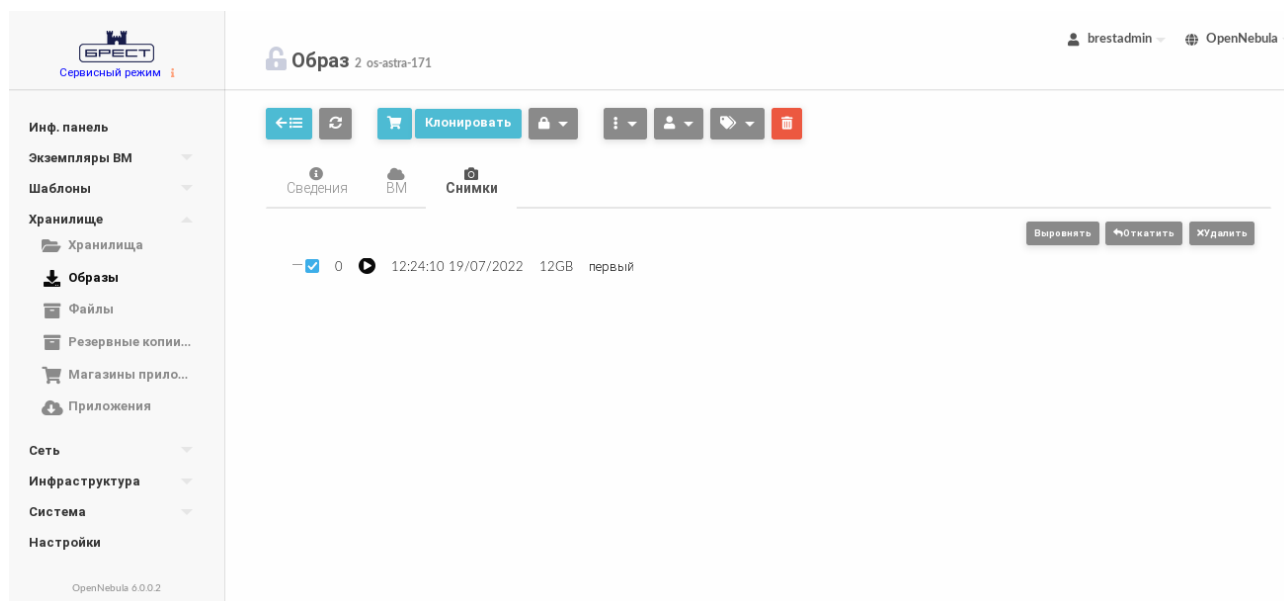


Рис. 45

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]**.

5.2. Управление шаблонами виртуальной машины

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

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

5.2.1. Параметры шаблона VM

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

- наименование и производительность VM, включает следующие обязательные параметры:

- NAME — наименование шаблона/VM (если из шаблона разворачивается несколько экземпляров VM, то наименования VM будут иметь вид:

<наименование_шаблона>-<идентификатор_VM>),

- MEMORY — объем памяти (в МБ),

- CPU — процент используемой мощности ЦП (в сотых долях). Например, если для VM зарезервировано 50% мощности ЦП узла виртуализации, то значение

составит «0,5»,

- VCPU — количество виртуальных ЦП;
- блок параметров диска VM (DISK) обязательно должен содержать параметр IMAGE (наименование образа), а также может содержать такие необязательные параметры, как IMAGE_UNAME (имя владельца образа) или DISK_TYPE (тип образа). Блок параметров DISK указывается для каждого образа, подключаемого к VM;
- блок параметров сетевого интерфейса (NIC) обязательно должен содержать параметр NETWORK_ID (идентификатор облачной сети). Кроме того можно указать те параметры облачной сети, которые необходимо переопределить при создании VM (например IP-адрес или MAC-адрес). Блок параметров NIC указывается для каждого сетевого интерфейса в создаваемой VM;
- необязательные блоки параметров, например, средства графического доступа, порядок загрузки, контекстная информация.

5.2.2. Создание шаблонов VM

5.2.2.1. В интерфейсе командной строки

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

Примеры:

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

а) создать файл `alse.tmp1` следующего содержания:

```
NAME = test-vm
MEMORY = 2048
CPU = "0.25"
DISK = [
    IMAGE = "os-astra-171",
    IMAGE_UNAME = "brestadmin" ]
DISK = [
    IMAGE = "td-astra171",
    IMAGE_UNAME = "brestadmin" ]
NIC = [
    NETWORK = "virtnetwork",
    NETWORK_UNAME = "brestadmin",
    SECURITY_GROUPS = "0" ]
OS = [
```

```
BOOT = "disk0,disk1" ]
```

б) создать шаблон с использованием файла `alse.tpl`:

```
onetemplate create alse.tpl
```

Пример вывода после выполнения команды:

```
ID: 2
```

в) просмотр перечня шаблонов. Пример вывода после выполнения команды

```
onetemplate list:
```

ID	USER	GROUP	NAME	REGTIME
2	oneadmin	brestdadm	test-vm	07/18 14:40:22
1	brestdadm	brestdadm	ALSE-171	07/18 12:45:38

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

а) выполнить следующую команду:

```
onetemplate create --name test-vm2 --memory 2048 --cpu "0.25" \
  --disk "anothe-os-astra-171" --nic Public
```

Пример вывода после выполнения команды:

```
ID: 3
```

б) просмотр перечня шаблонов. Пример вывода после выполнения команды

```
onetemplate list:
```

ID	USER	GROUP	NAME	REGTIME
2	oneadmin	brestdadm	test-vm2	07/18 14:50:27
2	oneadmin	brestdadm	test-vm	07/18 14:40:22
1	brestdadm	brestdadm	ALSE-171	07/18 12:45:38

5.2.2.2. В веб-интерфейсе ПК СВ

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

- 1) в меню слева выбрать пункт меню «Шаблоны — VM»;
- 2) на открывшейся странице **Шаблоны VM** нажать на кнопку **[+]** и в открывшемся меню выбрать пункт **Создать**;
- 3) на открывшейся странице **Создать шаблон VM** во вкладке **Общие** в поле **Название** задать наименование шаблона, в секции **Гипервизор** установить соответствующий флаг (например **KVM**) и указать основные параметры VM (память, процессор и т.п.) — (см. рис. 46)

Создать шаблон VM

бrestadmin OpenNebula

Сервисный режим

Инф. панель

Экземпляры VM

Шаблоны

VM

Сервисы

Вирт. мар...

Группы VM

Хранилище

Сеть

Инфраструктура

Система

Настройки

OpenNebula 6.0.0.2

Мастер настройки

Расширенный

Общие Хранилище Сеть ОС и ЦП Ввод/Вывод Действия Контекст

Расписание Группа VM Метки NUMA

Название: Astra171

Гипервизор: KVM vCenter LXC Firecracker

Описание:

Логотип:

Память: 2 ГБ

Enable hot resize?: нет

Модификация ОЗУ: любое

Physical CPU: 0,25

Модификация CPU: любое

Virtual CPU: 1

Enable hot resize?: нет

Модификация VCPU: любое

Рис. 46

4) на странице **Создать шаблон VM** во вкладке **Хранилище**:

- а) для Диска 0 указать загрузочный диск VM,
- б) если необходимо подключить CDRом, то в левом поле нажать на кнопку **[+]** и для Диска 1 указать соответствующий образ (см. рис. 47)

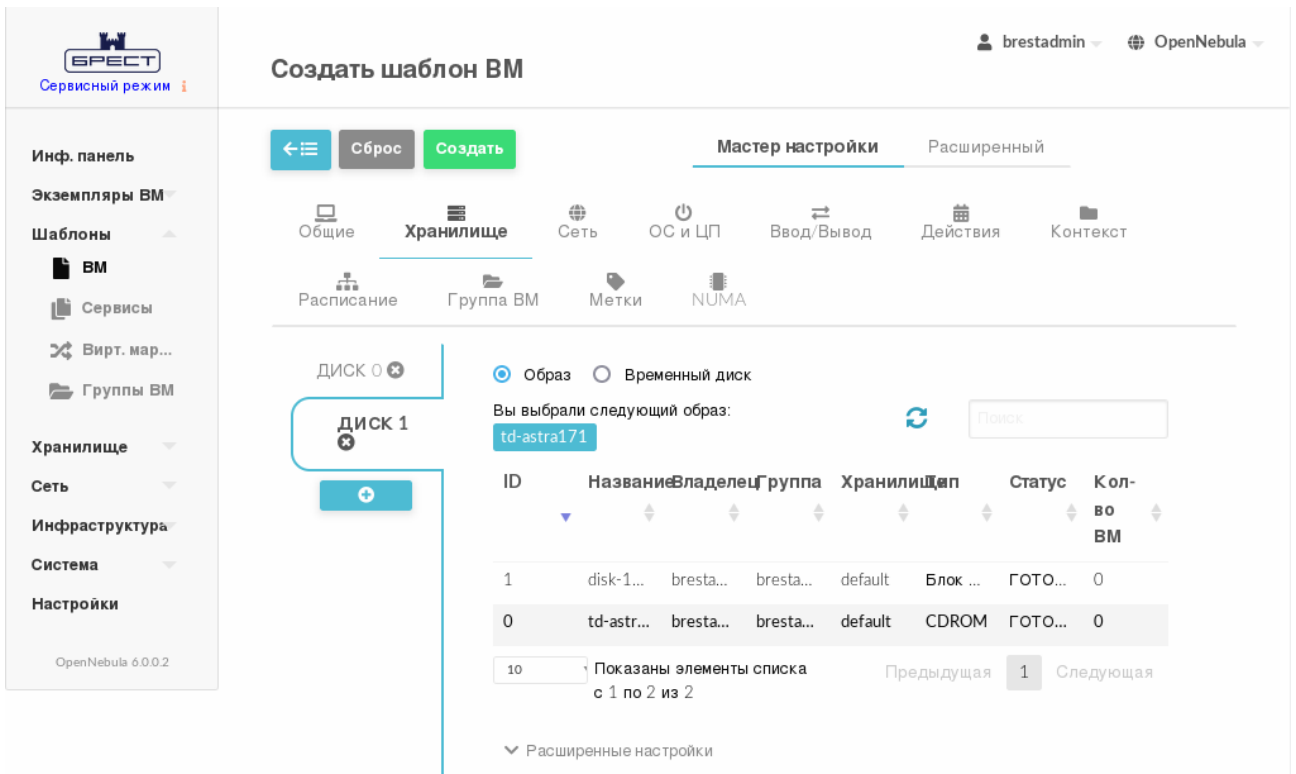


Рис. 47

5) на странице **Создать шаблон VM** во вкладке **Сеть** указать облачную сеть (см. рис. 48)

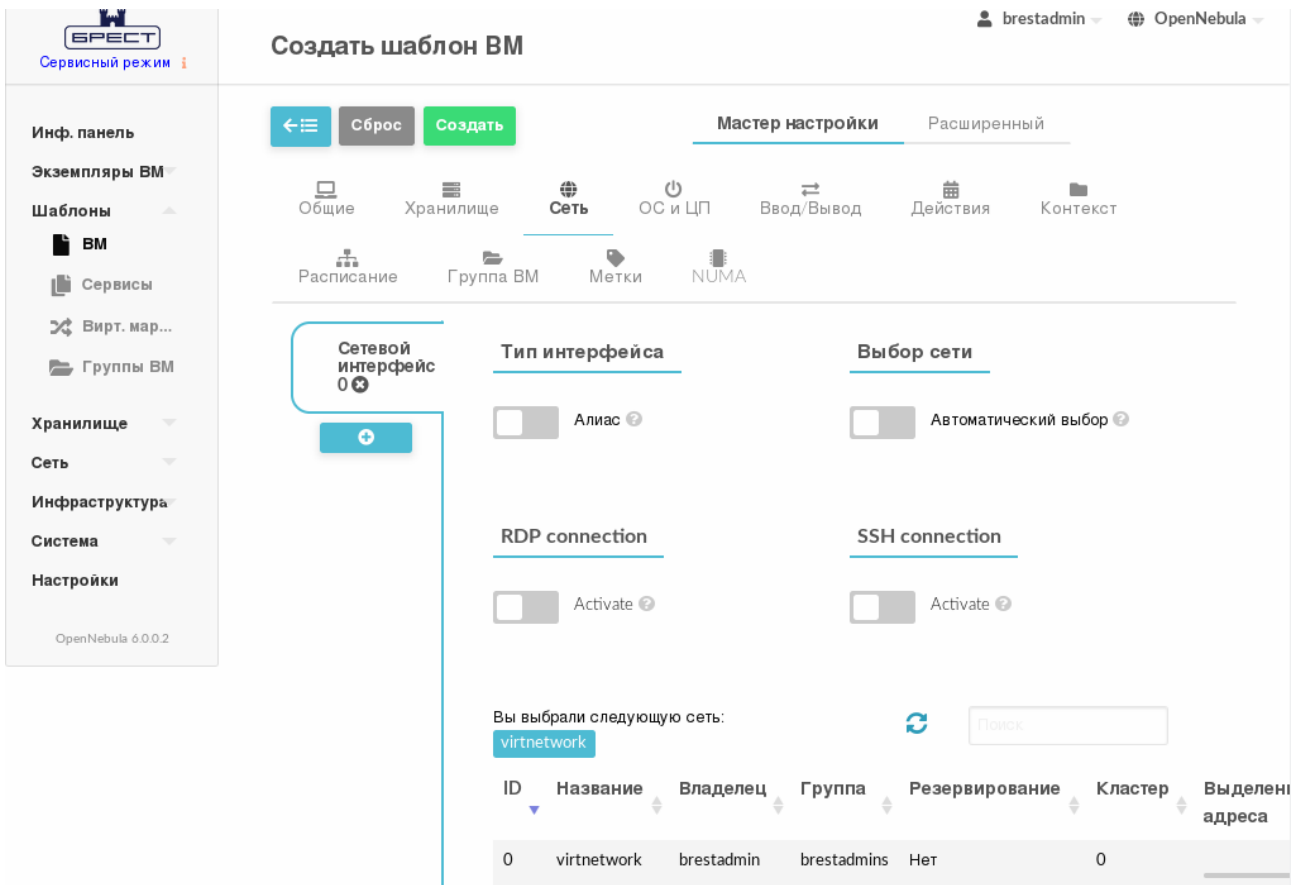


Рис. 48

- б) на странице **Создать шаблон VM** во вкладке **ОС и ЦП**:
- а) в секции **Загрузка** определить очередность использования образов при загрузке ОС (см. рис. 49)

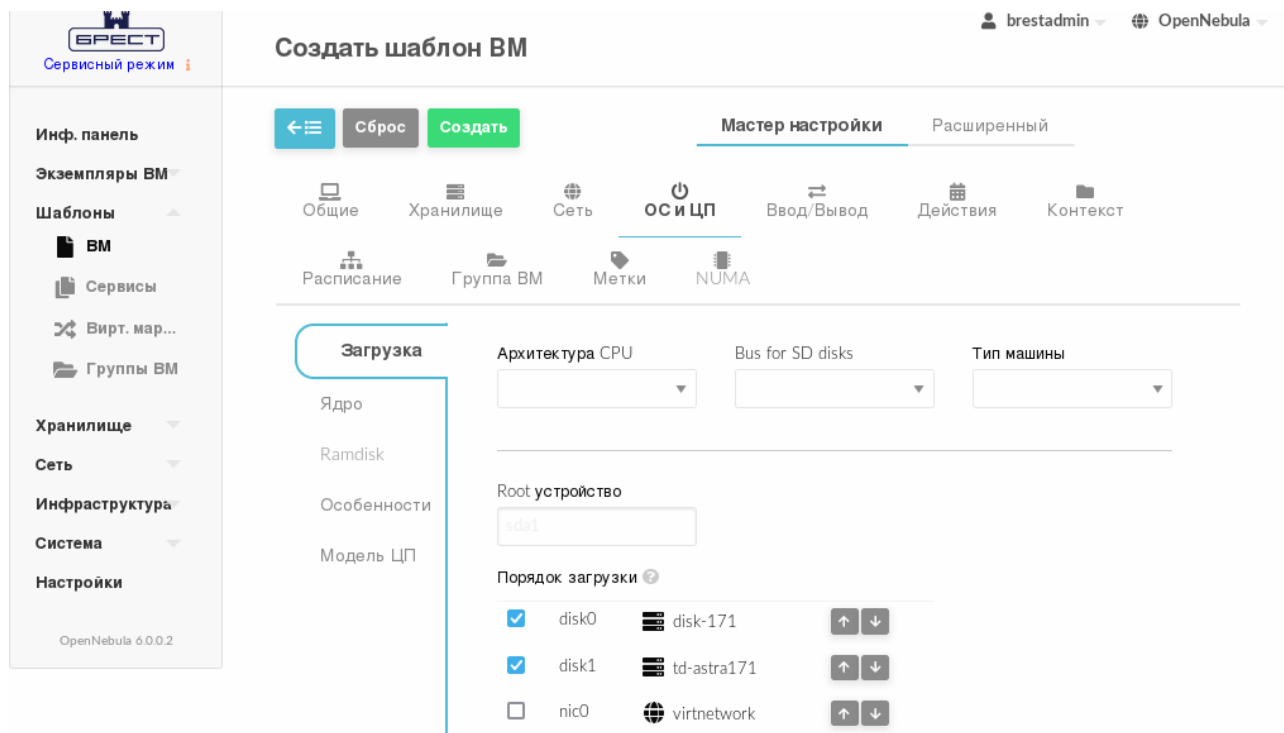


Рис. 49

- б) для обеспечения функционирования контекстуализации, в секции **Особенности** в выпадающем списке **Гостевой агент QEMU** выбрать значение Да (см. рис. 50)

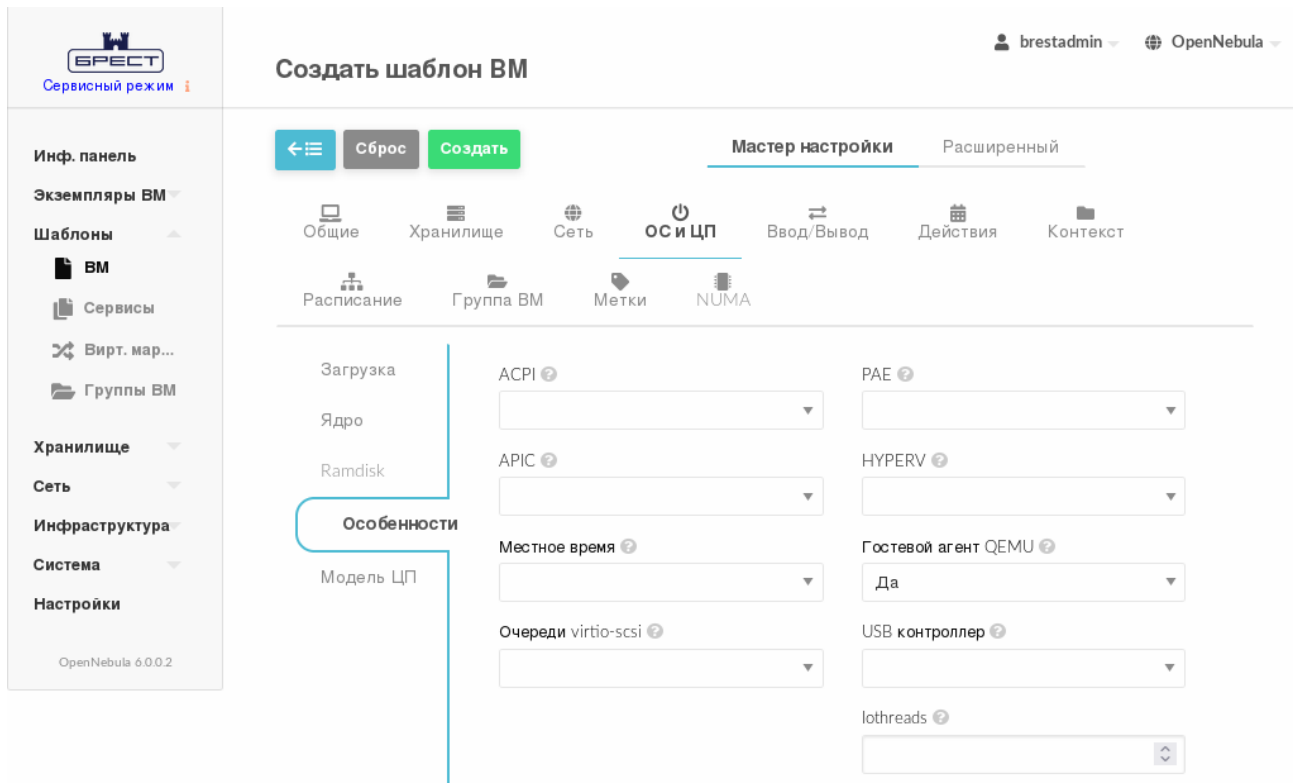


Рис. 50

7) на странице **Создать шаблон VM** нажать на кнопку **[Создать]**. После этого на открывшейся странице **Шаблоны VM** отобразится созданный шаблон (см. рис. 51)

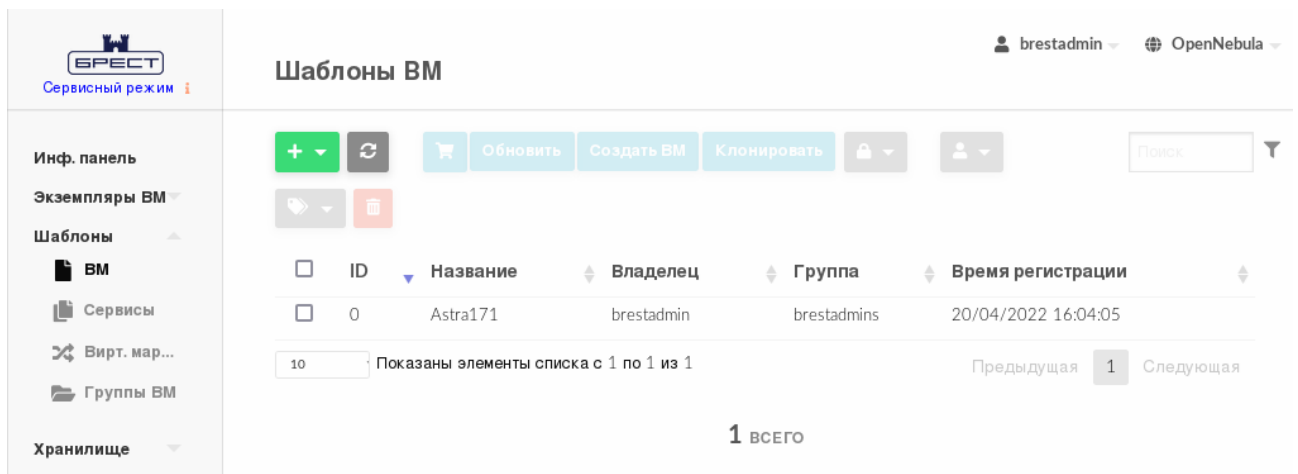


Рис. 51

5.2.3. Отображение доступных шаблонов и просмотр информации о шаблоне

5.2.3.1. В интерфейсе командной строки

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

```
ID USER      GROUP      NAME      REGTIME
2  oneadmin  brestadm  test-vm2  07/18 18:58:19
1  oneadmin  brestadm  test-vm   07/18 18:56:50
0  brestadm  brestadm  ALSE171   07/18 16:22:18
```

Для просмотра полной информации о шаблоне необходимо использовать команду:

```
onetemplate show <идентификатор_шаблона>
```

Пример вывода после выполнения команды `onetemplate show 2`:

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

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

```
TEMPLATE CONTENTS
CPU="0.25"
DISK=[
    IMAGE="os-astra-171" ]
HOT_RESIZE=[
    CPU_HOT_ADD_ENABLED="NO",
    MEMORY_HOT_ADD_ENABLED="NO" ]
INPUTS_ORDER=""
MEMORY="2048"
MEMORY_UNIT_COST="MB"
NIC=[
    NETWORK="virtnetwork",
    NETWORK_UNAME="brestadmin",
    SECURITY_GROUPS="0" ]
```

5.2.3.2. В веб-интерфейсе ПК СВ

Для отображения шаблонов, доступных пользователю, в веб-интерфейсе ПК СВ необходимо в меню слева выбрать пункт меню «Шаблоны — ВМ». На открывшейся странице **Шаблоны ВМ** будет отображена таблица шаблонов (см. рис. 52)

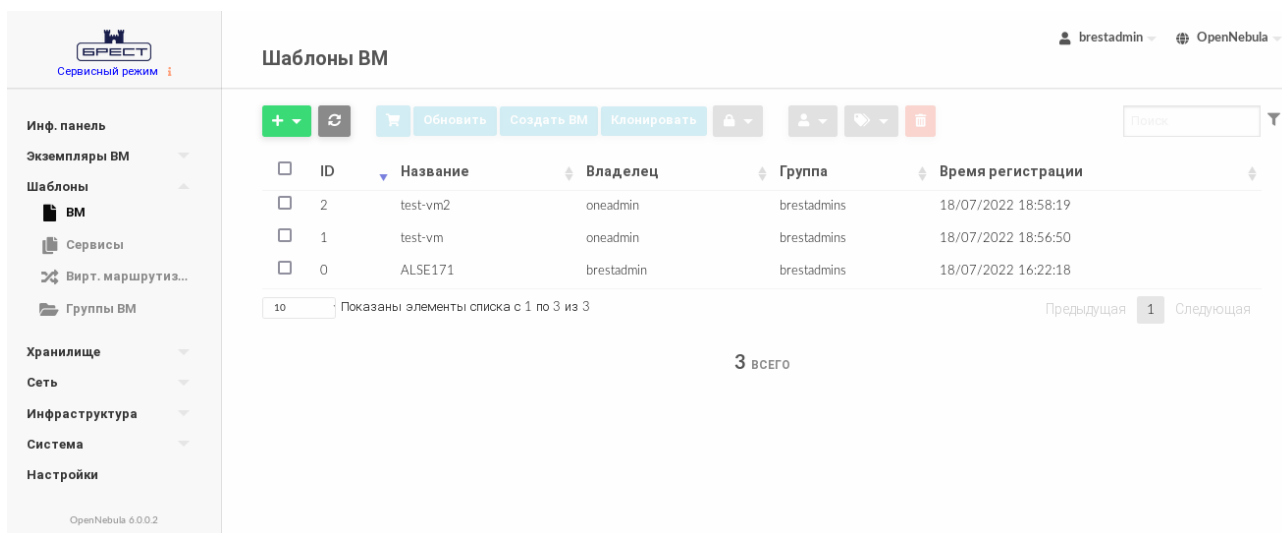


Рис. 52

Для просмотра информации о конкретном шаблоне необходимо на странице **Шаблоны VM** выбрать необходимый шаблон. После этого откроется страница шаблона (вкладка **Сведения**) — см. рис. 53.

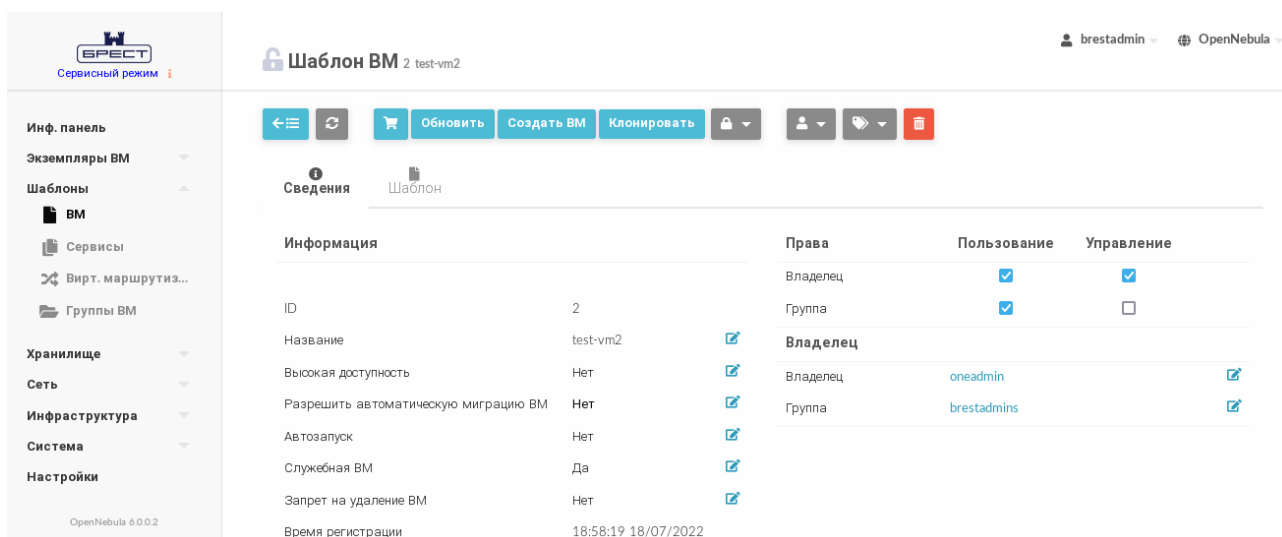


Рис. 53

5.2.4. Изменение параметров шаблона

5.2.4.1. В интерфейсе командной строки

Для изменения параметров шаблона необходимо использовать команду `onetemplate update <идентификатор_шаблона> [<файл_параметров>]` где `<файл_параметров>` — файл в котором перечислены параметры VM, заменяющие значения, которые были ранее определены в шаблоне. Если файл параметров не указан, то после ввода команды откроется текстовый редактор Vim для редактирования шаблона VM.

5.2.4.2. В веб-интерфейсе ПК СВ

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

- 1) в меню слева выбрать пункт меню «Шаблоны — ВМ» и на открывшейся странице **Шаблоны ВМ** выбрать необходимый шаблон;
- 2) на открывшейся странице **Шаблон ВМ** нажать на кнопку **[Обновить]**;
- 3) на открывшейся странице **Изменить шаблон ВМ** внести необходимые изменения и нажать на кнопку **[Обновить]**.

5.2.5. Клонирование шаблонов

5.2.5.1. В интерфейсе командной строки

Клонировать существующий шаблон возможно с помощью команды:

```
onetemplate clone <идентификатор_шаблона> <наименование_нового_шаблона>
```

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

Примеры:

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

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

Пример вывода после выполнения команды:

```
VM ID: 4
```

2. Просмотр перечня образов. Пример вывода после выполнения команды

```
oneimage list:
```

ID	USER	GROUP	NAME	DATASTORE	SIZE	TYPE	PER
4	oneadmin	brestdadm	clone_template-disk-1	default	3.8G	CD	No
3	oneadmin	brestdadm	clone_template-disk-0	default	12G	DB	Yes
2	brestdadm	brestdadm	os-astra-171	default	12G	DB	Yes
1	brestdadm	brestdadm	td-alse171	default	3.8G	CD	No
0	brestdadm	brestdadm	os-alse171	default	12G	DB	Yes

5.2.5.2. В веб-интерфейсе ПК СВ

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

- 1) в меню слева выбрать пункт меню «Шаблоны — ВМ» и на открывшейся странице **Шаблоны ВМ** выбрать необходимый шаблон;
- 2) на открывшейся странице **Шаблон ВМ** нажать на кнопку **[Клонировать]**;
- 3) на открывшейся странице **Клонировать шаблон ВМ**:
 - а) задать наименование нового шаблона,
 - б) нажать на кнопку **[Клонировать]** или на кнопку **[Клонировать с образами]**, если также необходимо клонировать все образы, указанные в шаблоне.

5.2.6. Общие шаблоны

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

5.2.6.1. В интерфейсе командной строки

Изменить установленные полномочия можно при помощи команды `chmod` с указанием идентификатора шаблона и числового кода полномочий. Описание числового кода полномочий представлено в разделе 3.5.

Примеры:

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

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

2. Установка полномочий в отношении шаблона с идентификатором 0:

- владельцу установить биты USE и MANAGE (разрешить применение и управление);
- пользователям группы установить биты USE и MANAGE;
- остальным пользователям установить бит USE.

Для этого необходимо выполнить команду:

```
onetemplate chmod 0 664
```

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

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

3. Установка полномочий в отношении шаблона с идентификатором 0:

- владельцу установить биты USE и MANAGE (разрешить применение и управление);
- пользователям группы установить бит USE;
- остальным пользователям установить бит USE.

Для этого необходимо выполнить команду:

```
onetemplate chmod 0 644
```

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

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

4. Установка полномочий в отношении шаблона с идентификатором 0:

- владельцу установить биты USE и MANAGE (разрешить применение и управление);
- пользователям группы снять все биты (отозвать все полномочия);
- остальным пользователям установить биты USE, MANAGE и ADMIN (разрешить применение, управление и администрирование).

Для этого необходимо выполнить команду:

```
onetemplate chmod 0 607
```

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

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

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

5.2.6.2. В веб-интерфейсе ПК СВ

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

Пример

Просмотр полномочий, установленных в отношении шаблона с идентификатором 0 (см. рис. 54).

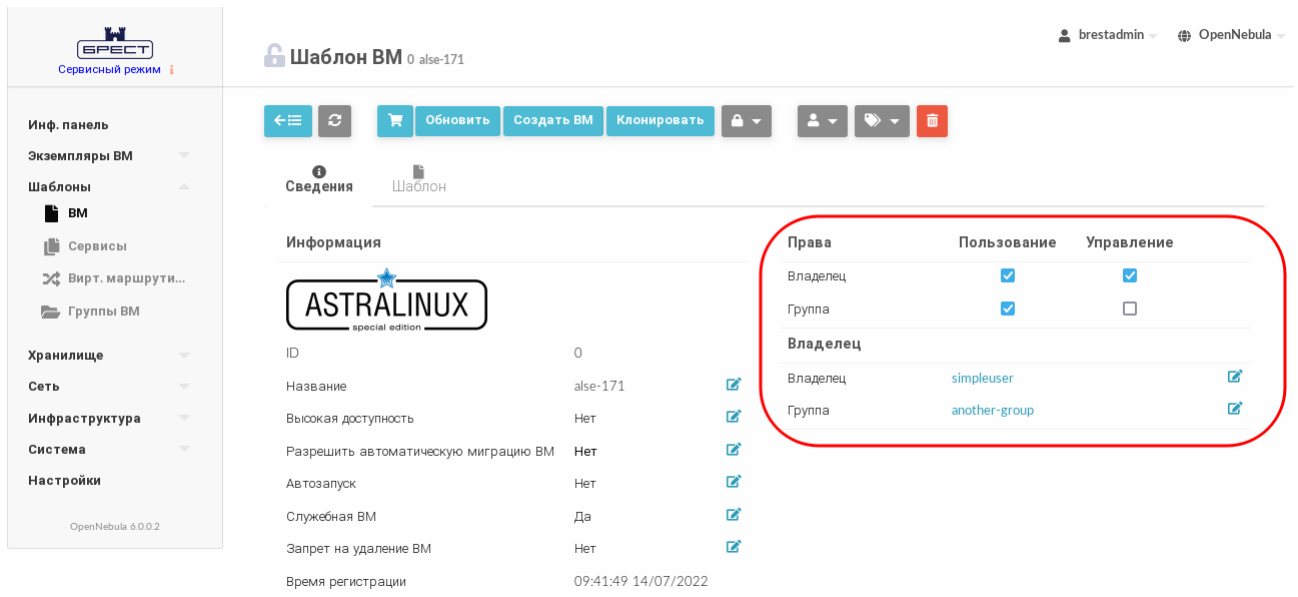


Рис. 54

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 шаблона во вкладке **Сведения** установить/снять соответствующие флаги.

5.2.7. Удаление шаблонов

5.2.7.1. В интерфейсе командной строки

Для удаления шаблона необходимо выполнить команду:

```
onetemplate delete <идентификатор_шаблона>
```

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

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

5.2.7.2. В веб-интерфейсе ПК СВ

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

- 1) в меню слева выбрать пункт меню «Шаблоны — VM»;
- 2) на открывшейся странице **Шаблоны VM** отметить необходимые шаблоны и нажать на кнопку **[Удалить]** (см. рис. 55).

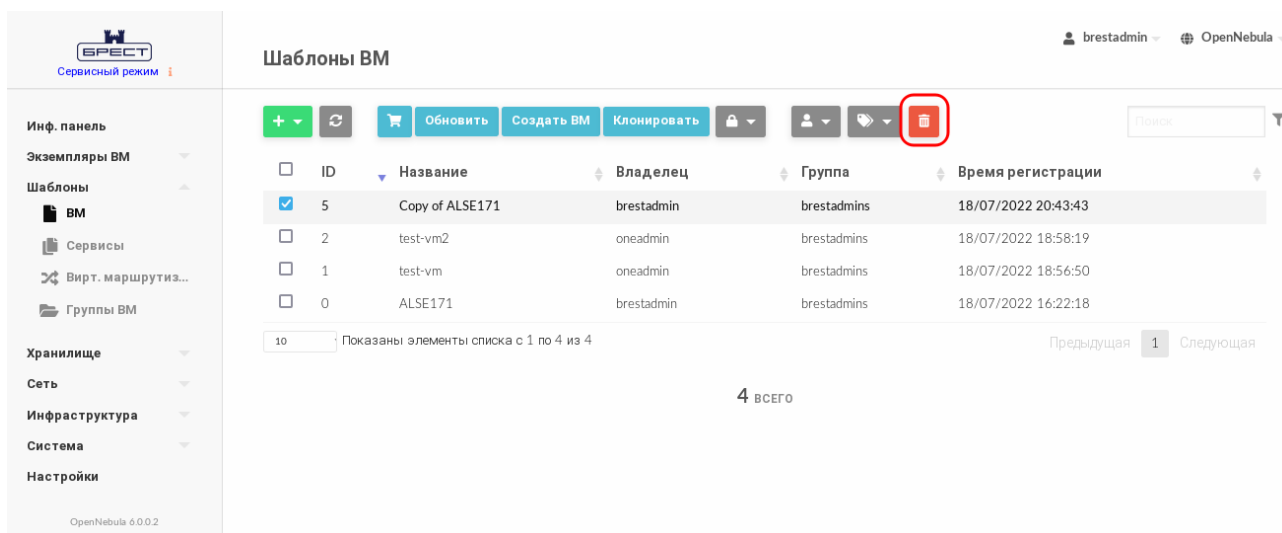


Рис. 55

3) в открывшемся окне нажать на кнопку **[Удалить]** или **[Удалить все образы]**, если также необходимо удалить все образы, указанные в шаблоне. (см. рис. 56).

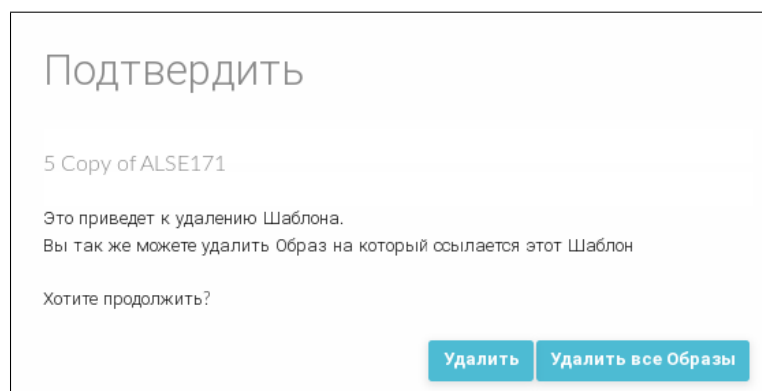


Рис. 56

5.2.8. Развертывание VM из шаблона

5.2.8.1. В интерфейсе командной строки

Для развертывания VM из шаблона можно воспользоваться командой:

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

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

Примеры:

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

```
onemplate instantiate 2 --memory 3072
```

Пример вывода после выполнения команды:

```
VM ID: 1
```

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

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

С помощью аргумента `--multiple <количество_VM>` можно создать более одного экземпляра одновременно. При этом наименования VM будут иметь вид:

`<наименование_шаблона>-<идентификатор_VM>`

Пример

Развертывание двух VM из шаблона с идентификатором 0:

```
onemplate instantiate 0 --multiple 2
```

5.2.8.2. В веб-интерфейсе ПК СВ

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

- 1) в меню слева выбрать пункт меню «Шаблоны — VM»;
- 2) на открывшейся странице **Шаблоны VM** выбрать необходимый шаблон;
- 3) на открывшейся странице **Шаблон VM** нажать на кнопку **[Создать VM]** (см. рис. 57)

The screenshot shows the OpenNebula web interface. On the left is a navigation menu with 'Шаблоны' selected. The main area displays 'Шаблон VM 0 Astra171'. A toolbar contains buttons for 'Обновить', 'Создать VM' (highlighted with a red circle), and 'Клонировать'. Below the toolbar are tabs for 'Сведения' and 'Шаблон'. The 'Сведения' tab is active, showing a table with VM details and permissions.

Информация		Права	Пользование	Управление
ID	0	Владелец	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Название	Astra171	Группа	<input type="checkbox"/>	<input type="checkbox"/>
Высокая доступность	Нет	Владелец	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Разрешить автоматическую миграцию VM	Нет	Группа	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Автозапуск	Нет			
Службная VM	Да			
Время регистрации	16:04:05 20/04 /2022			

Рис. 57

- 4) на открывшейся странице **Создать VM** в поле **Имя VM** задать наименование и количество экземпляров VM и нажать на кнопку **[Создать VM]** (см. рис. 58)

Создать VM

Создать как постоянную

Имя VM: tmp-for-install-os

Количество экземпляров: 1

Службная VM: Вкл

Автозапуск: Выкл

Astra171

Нагрузка

Диски

Память: 2 ГБ

Physical CPU: 0.25

Virtual CPU: 1

ДИСК 0: disk-171: 12288 МБ

ДИСК 1: td-astra171: 3904 МБ

Рис. 58

5) в веб-интерфейсе в меню слева выбрать пункт меню «Экземпляры VM – VM» и дождаться пока в поле **Статус** для созданной на предыдущем шаге VM значение Инициализация не изменится на **ВЫКЛЮЧЕНО** (промежуточные значения: Ожидание и Пролог). Для обновления значения статуса можно воспользоваться кнопкой **[Обновить]** (см. рис. 59)

VM

ID	Название	Владелец	Группа	Статус	Узел	IPs	Charter	Пользователь, запустивший VM
0	tmp-for-install-os	brestadmin	brestadmins	Пролог	brest-service	192.168.1.100		

Показаны элементы списка с 1 по 1 из 1

1 ВСЕГО 1 Активен 0 ВЫКЛ 0 ОЖИДАНИЕ 0 Ошибка

Рис. 59

5.3. Управление виртуальными машинами

5.3.1. Жизненный цикл виртуальной машины

Жизненный цикл ВМ в системе ПК СВ включает состояния, приведенные в таблице 9.

Таблица 9

Состояние	Сокращенное название состояния	Описание
PENDING	pend	По умолчанию ВМ начинает работать в состоянии ожидания запуска ресурса. Остается в этом состоянии, пока не будет развернута планировщиком или пользователем при помощи команды <code>onevm deploy</code>
HOLD	hold	Владелец поставил ВМ на удержание, она не доступна для развертывания в автоматическом режиме, пока не будет разблокирована. Однако ее можно развернуть вручную
CLONING	clon	ВМ ожидает один или более образов диска для завершения операции клонирования (образ все еще находится в состоянии lock)
PROLOG	prol	Система переносит файлы ВМ (образы диска и файл восстановления) на хост, в котором ВМ будет работать
BOOT	boot	ПК СВ ожидает, пока гипервизор создаст ВМ
RUNNING	runn	ВМ находится в работе (данное состояние включает фазы загрузки и отключения ВМ). Периодически контролируется драйвером виртуализации
MIGRATE	migr	ВМ переносится с одного ресурса на другой. Это может быть динамический перенос или холодный перенос (ВМ сохраняется, а файлы ВМ переносятся на новый ресурс)
HOTPLUG	hotp	Выполнение операции подключения/отключения диска или сетевого интерфейса
SNAPSHOT	snap	Выполняется снимок состояния
SAVE	save	Система сохраняет файлы ВМ после переноса, операции остановки или приостановки
EPILOG	epil	Система очищает хост, который использовался для виртуализации ВМ, кроме того, образы дисков, которые нужно сохранить, копируются обратно в хранилище образов
SHUTDOWN	shut	Система отправила сигнал ACPI для отключения ВМ и ожидает, пока процесс отключения завершится. Если по истечении времени ожидания ВМ не отключится, система будет считать, что ОС виртуальной машины проигнорировала сигнал ACPI, а состояние машины изменится на RUNNING (в работе) вместо DONE (выполнено)
STOPPED	stop	ВМ остановлена. Состояние ВМ было сохранено и перенесено вместе с образами диска обратно в хранилище образов

Окончание таблицы 9

Состояние	Сокращенное название состояния	Описание
SUSPENDED	susp	Аналогично состоянию STOPPED, но файлы остаются на хосте, чтобы позже возобновить на нем ВМ (т.е. нет необходимости перепланировать ВМ)

5.3.2. Управление экземплярами ВМ в интерфейсе командной строки

5.3.2.1. 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 2`:

```
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          : ---
```

5.3.2.2. Завершение работы экземпляров VM

Завершение работы экземпляра VM из любого состояния выполняется командой:

```
onevm terminate <идентификатор_VM>
```

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

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

Если по истечении определенного времени после выполнения команды `onevm terminate VM` все еще работает, т.е. гостевое устройство игнорирует сигналы ACPI, OpenNebula вернет VM в состояние RUNNING.

Если экземпляр VM находится в состоянии RUNNING, для завершения его работы в команде можно указать аргумент `--hard`. В этом случае экземпляр VM будет удален незамедлительно. Следует использовать данную опцию, если VM не поддерживает ACPI.

5.3.2.3. Приостановка экземпляров VM

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

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

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

Возможно запланировать долгосрочную приостановку. В этом случае ресурсы хоста, которые использовала VM, будут освобождены, а хост 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 остановке или приостановке их работы, а также ВМ, развертывание которых было отменено или электропитание которых было отключено.

5.3.2.4. 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.

5.3.2.5. 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.

5.3.3. Управление экземплярами ВМ в веб-интерфейсе ПК СВ

5.3.3.1. Отображение существующих ВМ

Для отображения существующих ВМ в веб-интерфейсе ПК СВ необходимо в меню слева выбрать пункт меню «Экземпляры ВМ — ВМ». На открывшейся странице **ВМ** будет отображена таблица экземпляров ВМ (см. рис. 60)

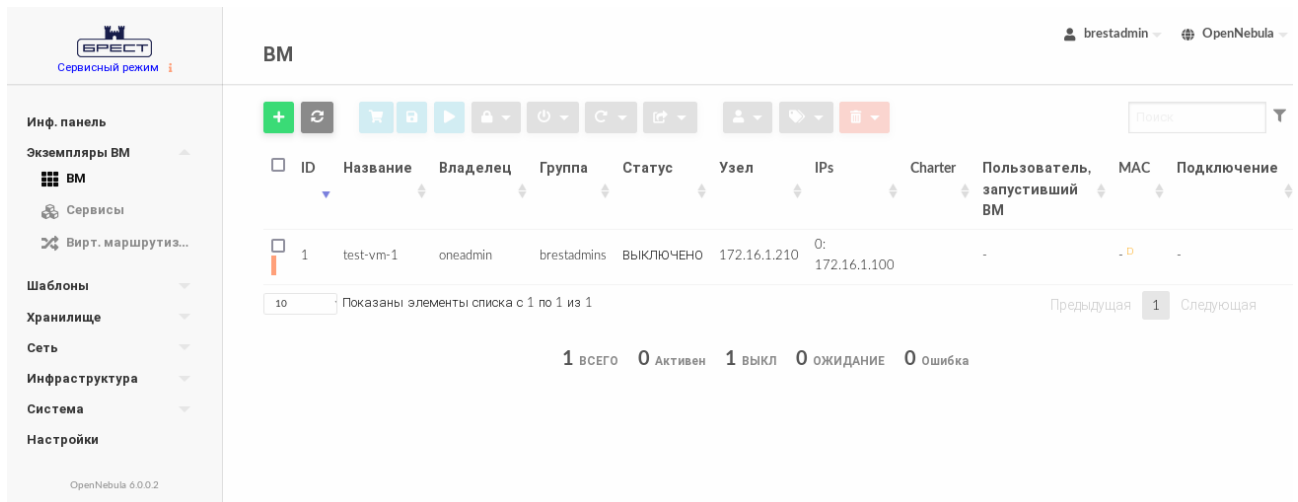


Рис. 60

Для просмотра полной информации о VM необходимо на странице **VM** выбрать необходимую VM. После этого откроется страница виртуальной машины (вкладка **Сведения**) (см. рис. 61).

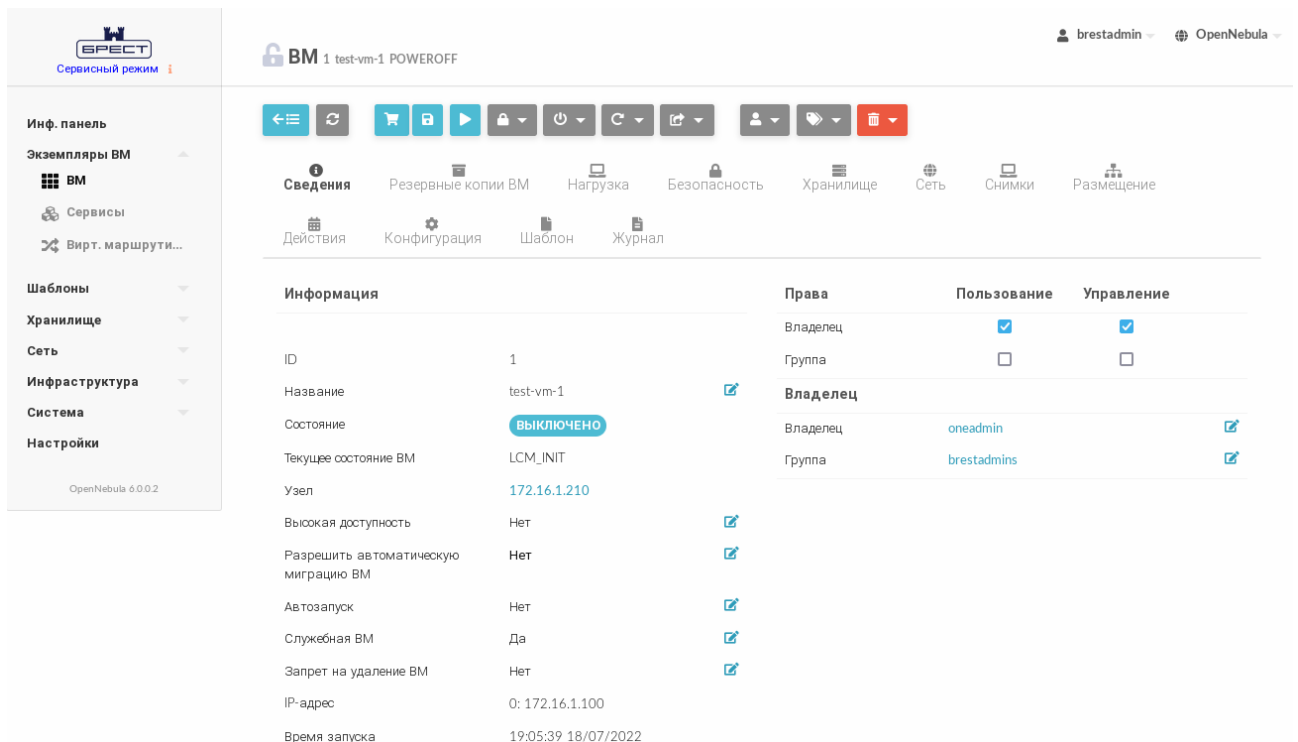


Рис. 61

5.3.3.2. Завершение работы и приостановка экземпляров VM

Для завершения работы экземпляра VM или его приостановки в веб-интерфейсе ПК СВ используется кнопка **[Управление питанием]**, после нажатия на которую откроется меню действий (см. рис. 62):

- Приостановить работу VM — краткосрочная приостановка: состояние VM, в т.ч. выделенные ресурсы, сохраняется на рабочем хосте. При возобновлении работы

приостановленной VM выполняется ее незамедлительное развертывание на том же хосте;

- **Остановить** — корректно выключает работающую VM, отправляя сигнал ACPI. Диски VM перемещаются в хранилище образов, при этом сохраняется состояние VM. Возобновление работы VM осуществляется на любом доступном хосте;
- **Отключить питание** — долгосрочная приостановка: корректно выключает работающую VM, отправляя сигнал ACPI, при этом состояние VM не сохраняется. Возобновление работы VM осуществляется на том же хосте;
- **Отключить питание жестко** — незамедлительно отключить электропитание VM. Использование данной опции актуально, если VM не поддерживает ACPI;
- **Отменить размещение** — корректно выключает работающую VM, отправляя сигнал ACPI. Диски VM перемещаются в хранилище образов, при этом состояние VM не сохраняется. Возобновление работы VM осуществляется на любом доступном хосте;
- **Отменить размещение жестко** — аналогично команде **Отменить размещение**, но работающая VM удаляется незамедлительно.

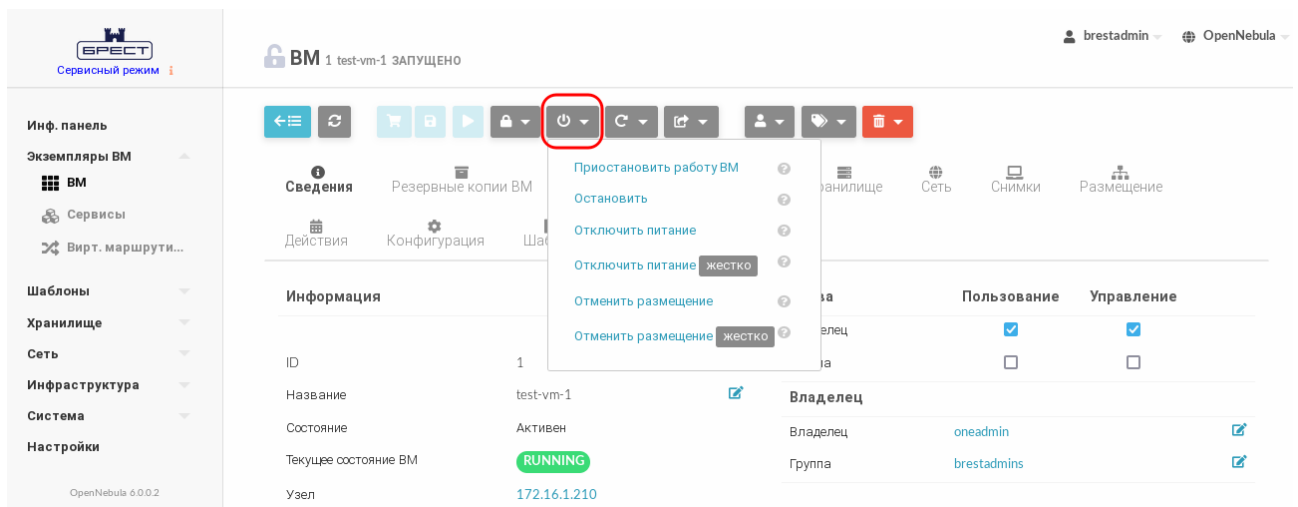


Рис. 62

5.3.3.3. Перезагрузка экземпляров VM

Для перезагрузки VM в веб-интерфейсе ПК СВ используется кнопка **[Перезагрузка]**, после нажатия на которую откроется меню действий (см. рис. 63):

- **Перезагрузить** — корректная перезагрузка работающей VM, отправляя сигнал ACPI;
- **Перезагрузить жестко** — принудительная перезагрузка работающей VM, актуально, если VM не поддерживает ACPI.

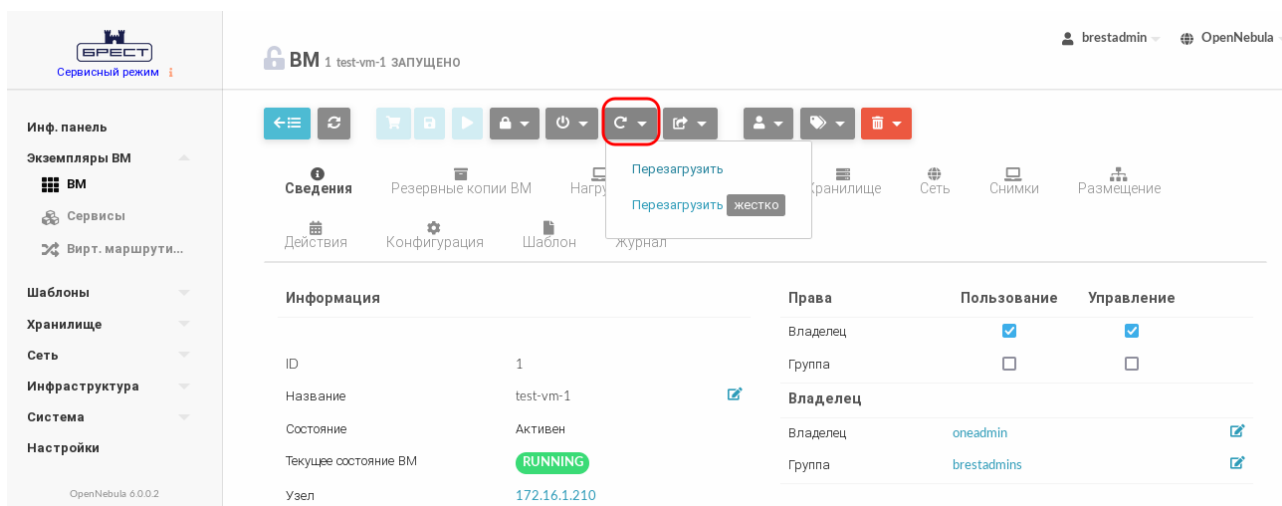


Рис. 63

5.3.3.4. Отсрочка развертывания экземпляров VM

Для управления блокировкой VM в веб-интерфейсе ПК СВ используется кнопка **[Блокировка]**, после нажатия на которую откроется меню действий (см. рис. 64):

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

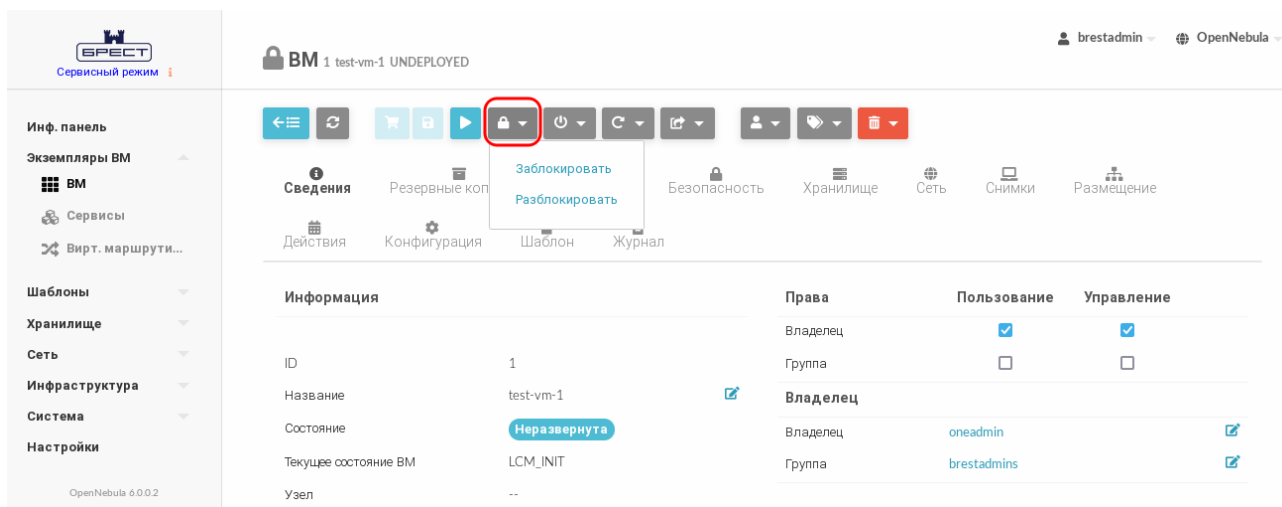


Рис. 64

5.3.4. Снимки состояний VM

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

5.3.4.1. Управление снимками состояний в интерфейсе командной строки

Для создания снимка состояния VM необходимо выполнить команду:

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

В качестве идентификатора VM можно указать перечень идентификаторов, разделенных запятыми или диапазон идентификаторов (в качестве разделителя используются две точки

— «..»)

Примеры:

1. Создание снимка состояния VM с идентификатором 1

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

2. Просмотр информации о VM, пример вывода после выполнения команды `onevm show 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 VM к состоянию, указанному в снимке, необходимо выполнить команду:

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

Для удаления снимка состояния VM необходимо выполнить команду:

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

5.3.4.2. Управление снимками состояний в веб-интерфейсе ПК СВ

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

- 1) в меню слева выбрать пункт меню «Экземпляры VM — VM»;
- 2) на открывшейся странице **VM** выбрать необходимую виртуальную машину;
- 3) на странице виртуальной машины открыть вкладку **Снимки** (см. рис. 65).

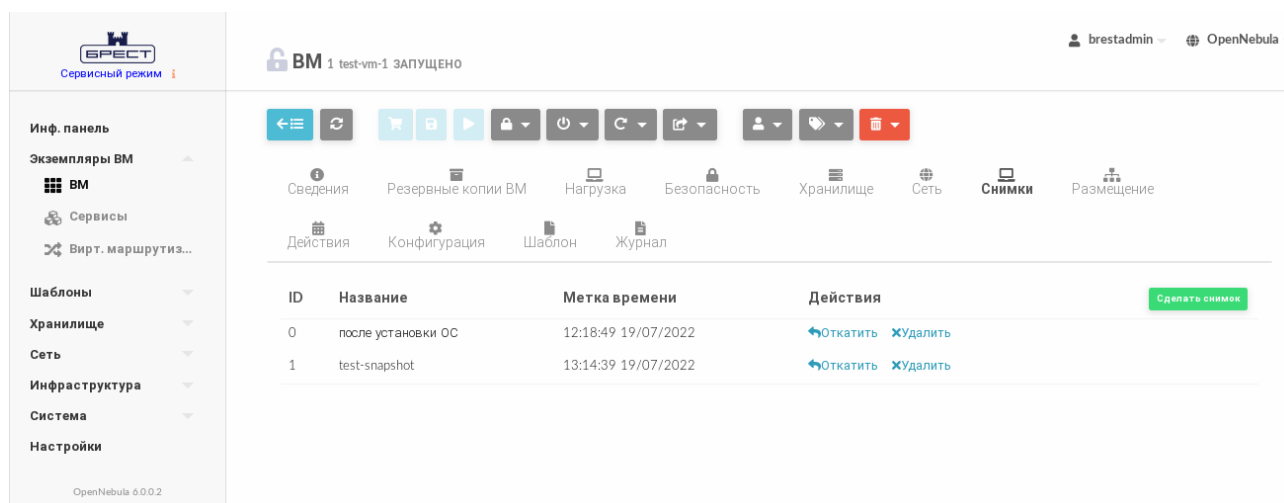


Рис. 65

На странице виртуальной машины во вкладке **Снимки**:

- для создания снимка состояния VM необходимо нажать на кнопку **[Сделать сн-**

мок];

- для возвращения VM к состоянию, указанному в снимке, необходимо нажать на кнопку **[Откатить]** в строке соответствующего снимка;

- для удаления снимка состояния VM необходимо нажать на кнопку **[Удалить]** в строке соответствующего снимка.

5.3.5. Снимки дисков VM

Пользователь может делать снимки состояния диска, только если VM 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 роли родительского элемента для следующего снимка. Снимки, которые не являются активными и не имеют дочерних элементов, можно удалять.

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

5.3.5.1. Управление снимками дисков в интерфейсе командной строки

Для создания снимка состояния диска необходимо выполнить команду:

```
onevm disk-snapshot-create <идентификатор_VM> \
<идентификатор_диска_VM> <наименование_снимка>
```

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

```
onevm disk-snapshot-revert <идентификатор_VM> \
<идентификатор_диска_VM> <идентификатор_снимка>
```

Команда будет выполнена только в том случае, если VM 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_VM> \
<идентификатор_диска_VM> <идентификатор_снимка>
```

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

5.3.5.2. Управление снимками дисков в в веб-интерфейсе ПК СВ

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

- 1) в меню слева выбрать пункт меню «Экземпляры VM — VM»;
- 2) на открывшейся странице **VM** выбрать необходимую виртуальную машину;
- 3) на странице виртуальной машины открыть вкладку **Хранилище** и в строке необходимого диска нажать на кнопку **[Snapshot]** (см. рис. 66).

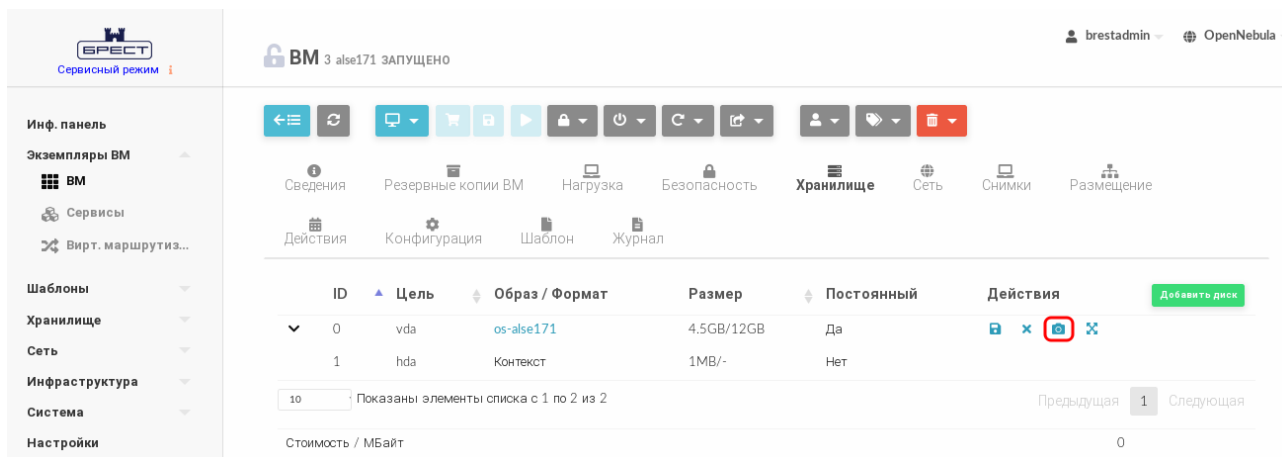


Рис. 66

- 4) в открывшемся окне **Снимок диска** задать наименование снимка и нажать на кнопку **[Сделать снимок]** (см. рис. 67).

Снимок диска

3 alse171

№ диска

Название

Сделать снимок

Рис. 67

На странице виртуальной машины во вкладке **Хранилище** (после остановки VM) — см. рис. 68:

- 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]**.

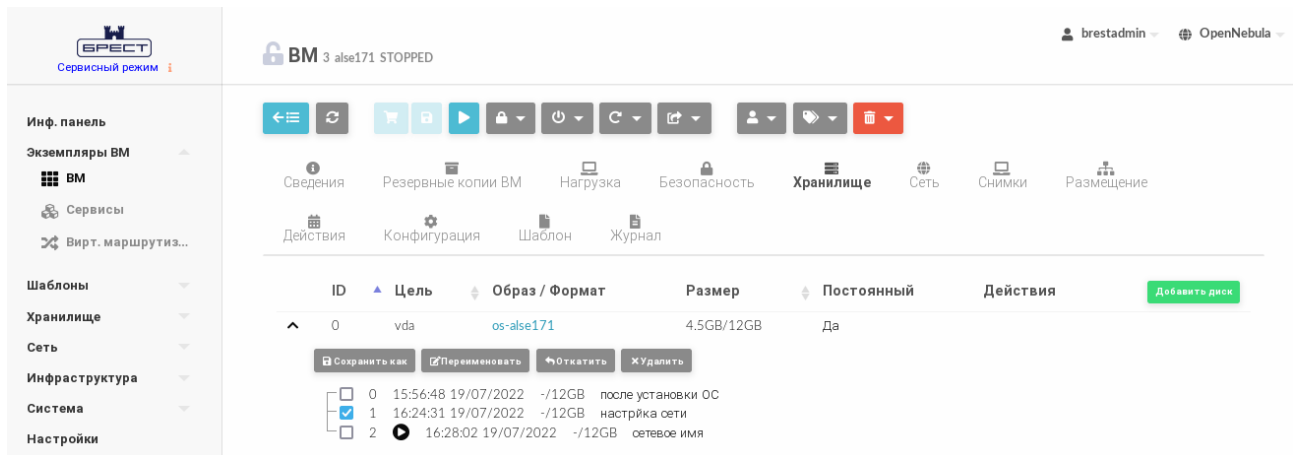


Рис. 68

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

5.3.6. Экспорт диска VM

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

5.3.6.1. В интерфейсе командной строки

Для экспорта диска VM необходимо выполнить команду:

```
onevm disk-saveas <идентификатор_VM> <идентификатор_диска_VM> \
<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_VM> <идентификатор_диска_VM> \
<наименование_нового_образа> --snapshot <идентификатор_диска>
```

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

5.3.6.2. В веб-интерфейсе ПК СВ

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

- 1) в меню слева выбрать пункт меню «Экземпляры VM — VM»;
- 2) на открывшейся странице **VM** выбрать необходимую виртуальную машину;
- 3) на странице виртуальной машины открыть вкладку **Хранилище** и в строке необходимого диска нажать на кнопку **[Сохранить как]** (см. рис. 69).

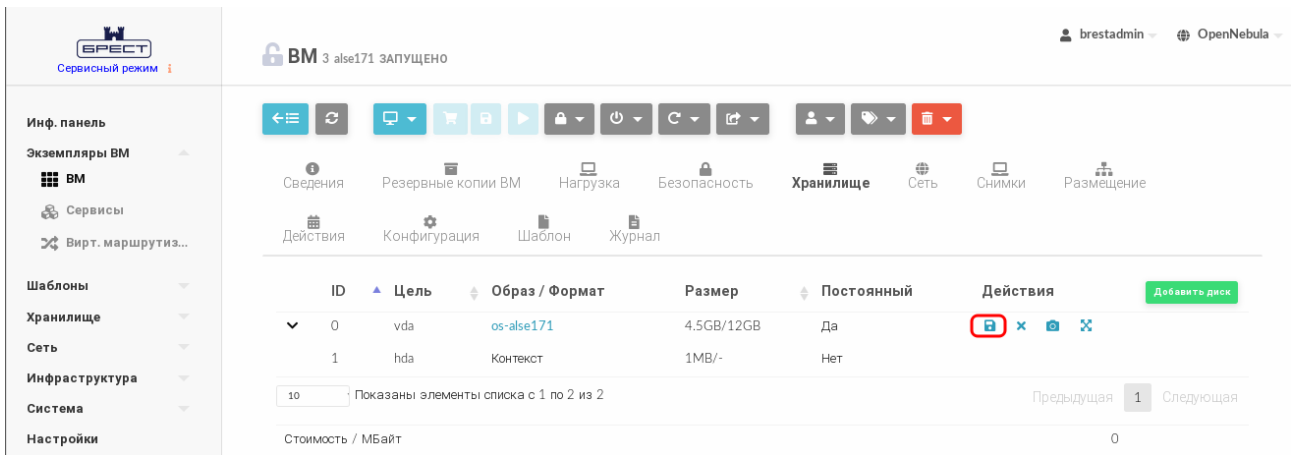


Рис. 69

4) в открывшемся окне **Сохранить диск как** задать наименование нового образа и нажать на кнопку **[Сохранить как]** (см. рис. 70).

Рис. 70

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. 68).

5.3.7. 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.

5.3.7.1. В интерфейсе командной строки

Для горячего подключения новых дисков к работающим VM используется команда:

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

Для отключения диска от работающей VM применяется команда:

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

5.3.7.2. В веб-интерфейсе ПК СВ

Для горячего подключения диска к VM в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

- 1) в меню слева выбрать пункт меню «Экземпляры VM — VM»;
- 2) на открывшейся странице **VM** выбрать необходимую виртуальную машину;
- 3) на странице виртуальной машины открыть вкладку **Хранилище** и нажать на кнопку **[Добавить диск]** (см. рис. 71).

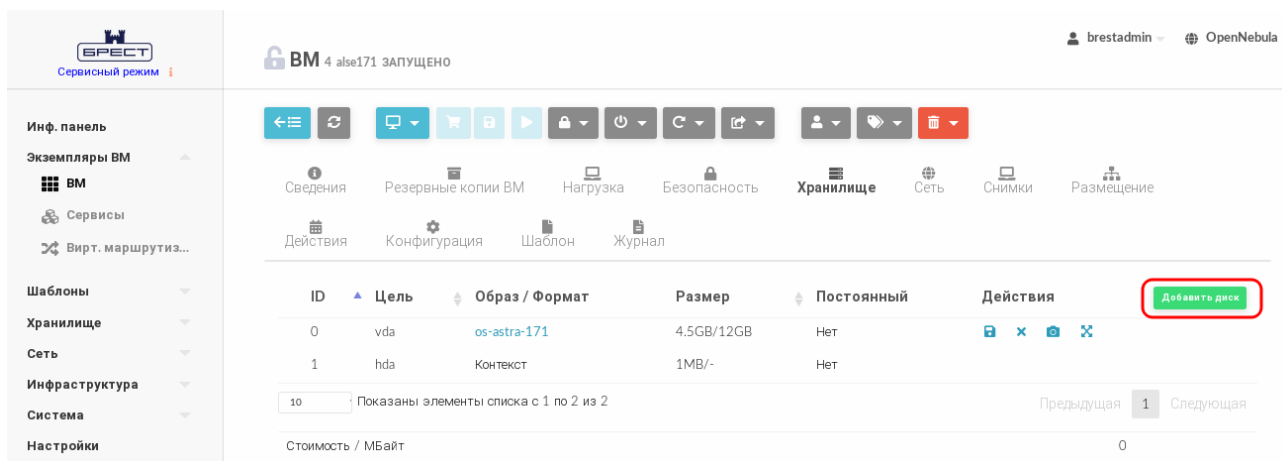


Рис. 71

- 4) в открывшемся окне **Присоединить диск** указать необходимый образ и нажать на кнопку **[Присоединить]** (см. рис. 72).

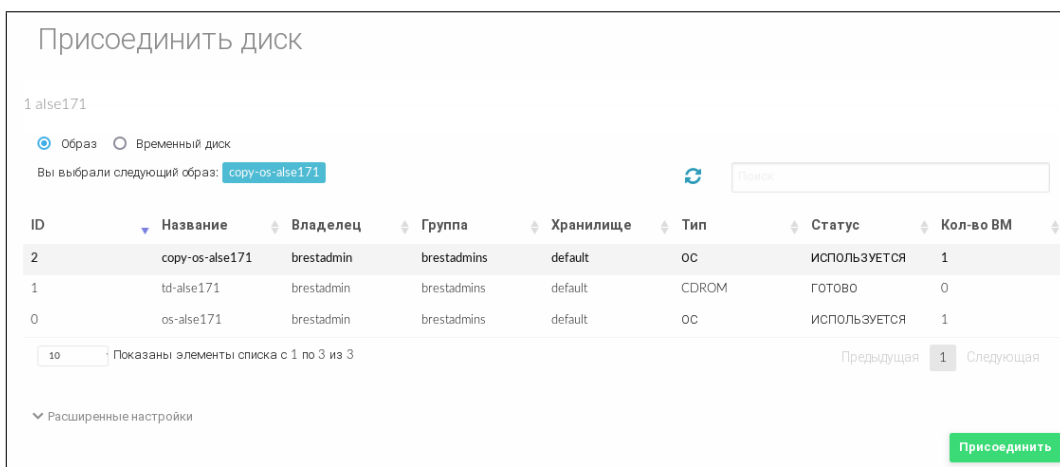


Рис. 72

Для горячего отключения диска от VM в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

- 1) в меню слева выбрать пункт меню «Экземпляры VM — VM»;
- 2) на открывшейся странице **VM** выбрать необходимую виртуальную машину;
- 3) на странице виртуальной машины открыть вкладку **Хранилище** и в строке необходимого диска нажать на кнопку **[Detach]** (см. рис. 73).

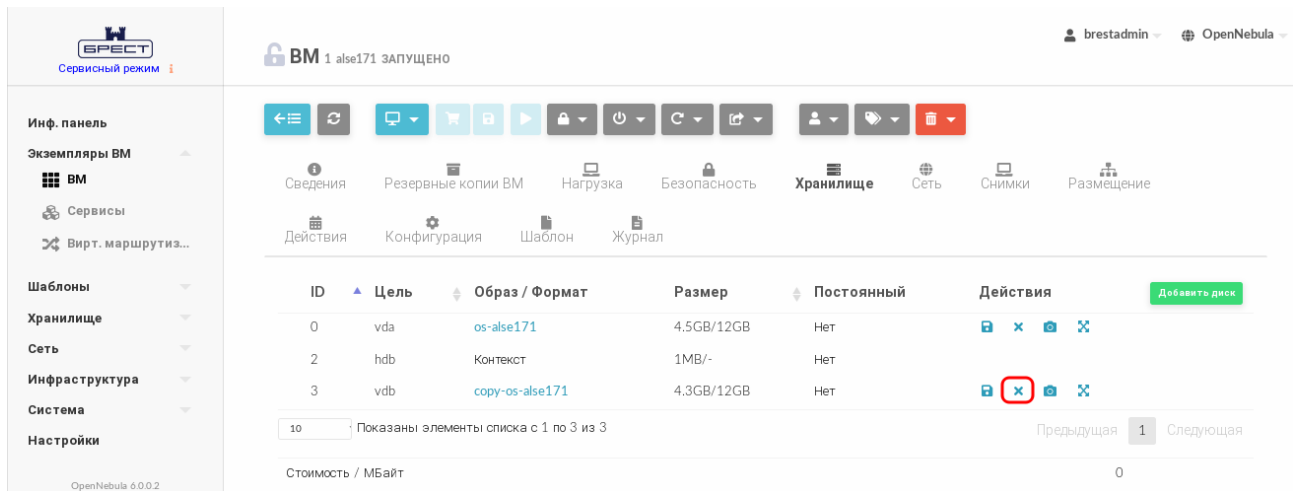


Рис. 73

4) в открывшемся окне **Подтвердить** нажать на кнопку **[ОК]**.

5.3.8. Перераспределение производительности VM

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

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

- подготовить VM к отключению, например, остановить сервисы вручную;
- отключить питание VM;
- перераспределить ресурсы, выделяемые для VM;
- возобновите работу VM с новой производительностью.

5.3.8.1. В интерфейсе командной строки

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

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

Пример

Для VM с наименованием `alse171` выделить 50% мощности ЦП хоста и 2 виртуальных ЦП:

```
onevm resize alse171 --cpu 0.5 --vcpu 2
```

5.3.8.2. В веб-интерфейсе ПК СВ

Для изменения объема вычислительных ресурсов VM в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

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

3) на странице виртуальной машины открыть вкладку **Нагрузка** и нажать на кнопку **[Изменить]** (см. рис. 74).

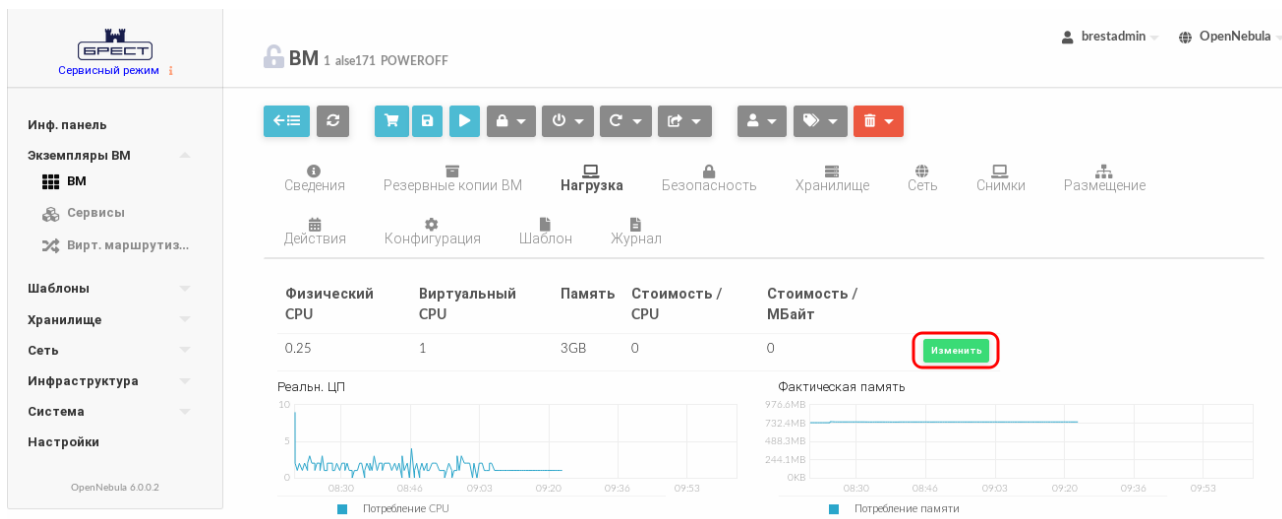


Рис. 74

4) в открывшемся окне **Изменить базовые характеристики** внести необходимые корректировки и нажать на кнопку **[Изменить]** (см. рис. 75).

Изменить базовые характеристики

1 else171

Проводить проверку емкости ?

Память ?

3 ГБ

Физический CPU ?

0,25

Виртуальный CPU ?

1

Изменить

Рис. 75

5.3.9. Изменение размера дисков VM

Увеличение объема дисков, выделенных для VM, возможно выполнить во время развертывания VM 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 VM. Для того чтобы в ОС виртуальной машины

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

5.3.9.1. В интерфейсе командной строки

Чтобы изменить объем диска, выделяемого для VM 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 VM, создаваемом на основе образа с идентификатором 2, будет установлен объем 20 ГБ (размер образа — 12 ГБ).

2. Развернуть VM на основе шаблона с наименованием `ALSE171` и с использованием файла параметров `disk.txt`:

```
onetemplate instantiate ALSE171 disk.txt
```

Пример вывода после выполнения команды:

```
VM ID: 3
```

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

```
VIRTUAL MACHINE 3 INFORMATION
ID                : 3
NAME              : ALSE171-3
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-alse171     -/20G  file  NO
```

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

Пример

Развернуть VM на основе шаблона с наименованием ALSE171, при этом для диска VM, создаваемом на основе образа с идентификатором 2, будет установлен объем 20 ГБ:
`onemplate instantiate ALSE171 --disk 2:size=20480`

5.3.9.2. В веб-интерфейсе ПК СВ

Чтобы изменить объем диска, выделяемого для VM, при развертывании из шаблона в веб-интерфейсе ПК СВ необходимо на странице **Создать VM** в секции **Диски** задать новое значение (см. рис. 76)

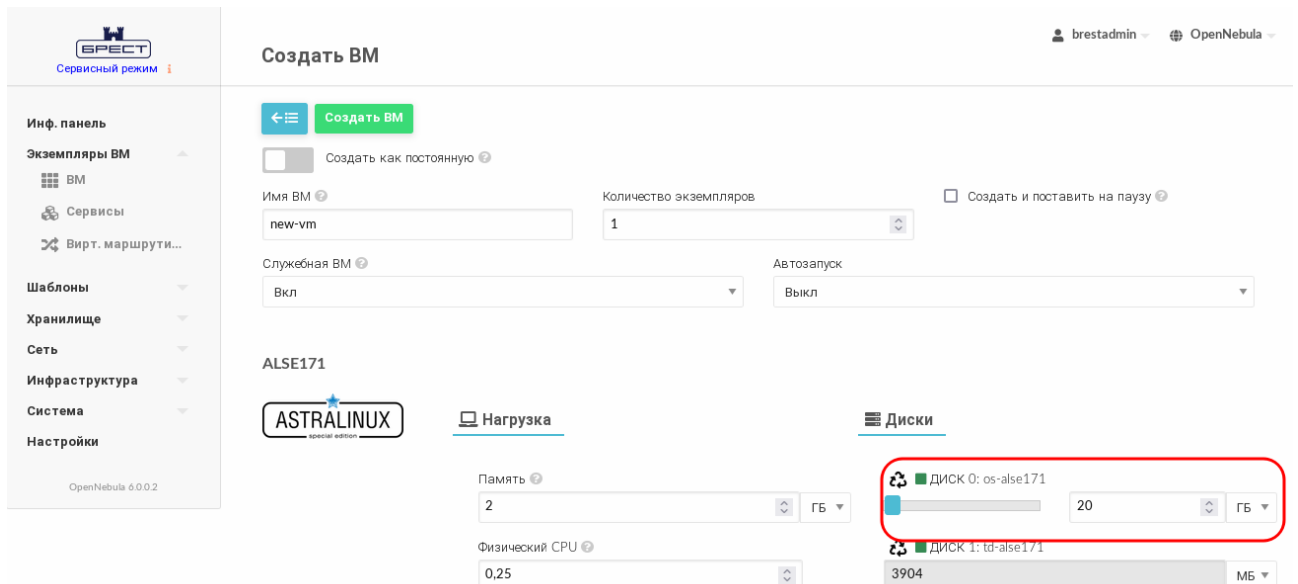


Рис. 76

5.3.10. Клонирование VM

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

Существует два способа создания постоянной частной копии VM:

- реализовать шаблон в качестве постоянного;
- сохранить существующий экземпляр VM 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 VM. Клонированный шаблон VM будет содержать определение для пустого энергозависимого диска.

При сохранении ВМ в качестве шаблона выполняется клонирование исходного шаблона ВМ с заменой дисков на снимки текущих дисков. Если для экземпляра ВМ выполнялось перераспределение ресурсов, будет использоваться текущая производительность. Новые клонированные образы можно дополнительно сделать постоянными, установив атрибут `--persistent` (см. подраздел 5.1.7). Сетевые интерфейсы (блок параметров NIC) также будут перезаписаны на полученные от экземпляра ВМ.

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

5.3.10.1. 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 ALSE171 и на его основе создать постоянный шаблон с наименованием my_vm:

```
onetemplate instantiate ALSE171 --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	brestdadm	my_vm	07/20 12:21:42
1	brestdadm	brestdadm	Copy of ALSE171	07/20 10:49:49
0	brestdadm	brestdadm	ALSE171	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	brestdadm	my_vm	runn	0.25	2G	oneserver	0d 00h07
2	oneadmin	brestdadm	ALSE171-2	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
```

5.3.10.2. 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. 77)

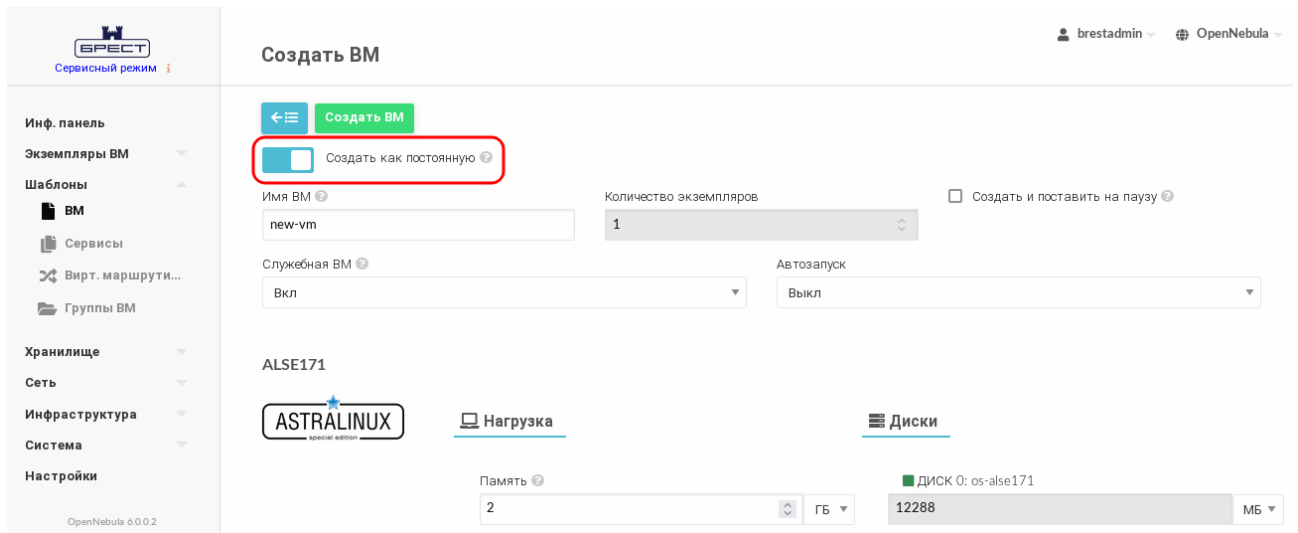


Рис. 77

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

- 1) на странице выключенной VM нажать на кнопку **Сохранить как** (см. рис. 78)

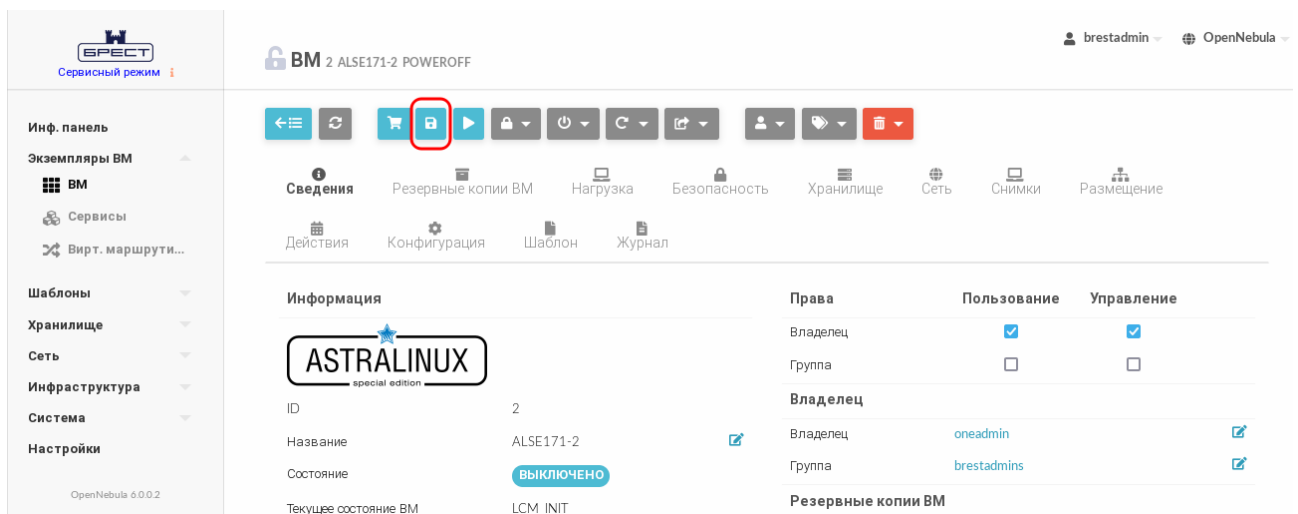


Рис. 78

- 2) в открывшемся окне **Сохранить как шаблон** (см. рис. 79):
 - а) задать наименование нового шаблона,
 - б) установить флаг **Сделать новый образ постоянным**,
 - в) нажать на кнопку **[Сохранить как шаблон]**.

Сохранить как шаблон

2 ALSE171-2

Имя шаблона

Сделать новый образ постоянным

[Сохранить как шаблон](#)

Рис. 79

5.3.11. Управление полномочиями для VM

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

Управление полномочиями описано в разделе 3.5

5.4. Доступ к рабочему столу VM веб-интерфейсе ПК СВ

Если VM поддерживает VNC или Spice и находится в состоянии RUNNING, то во вкладке просмотра VM отображается иконка доступа к рабочему столу VM (см. рис. 80)

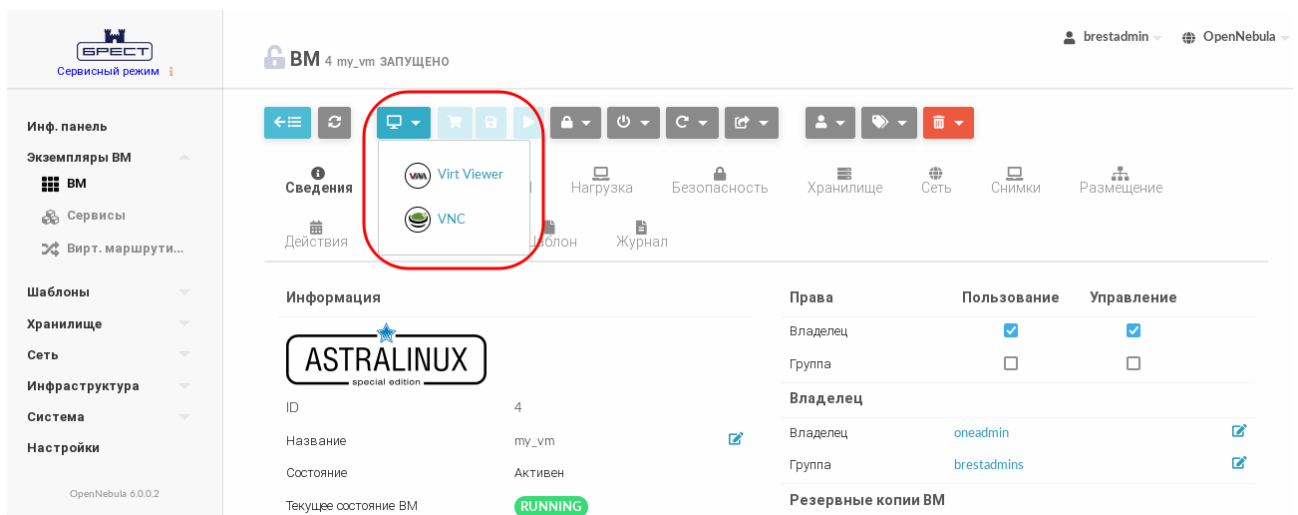


Рис. 80

При появлении в браузере firefox панели с предупреждением нажать на кнопку [Настройки] и выбрать пункт Разрешить всплывающие окна (см. рис. 81)

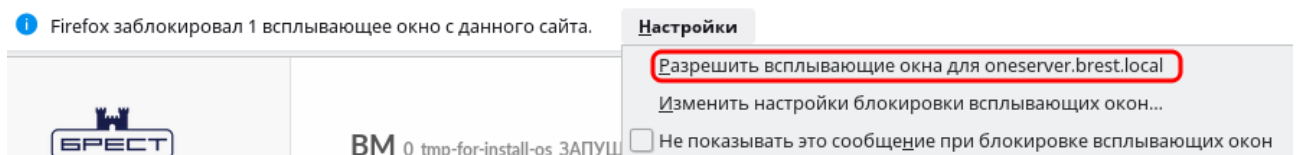


Рис. 81

После этого откроется страница с подключенным удаленным рабочим столом VM (см. рис. 82).

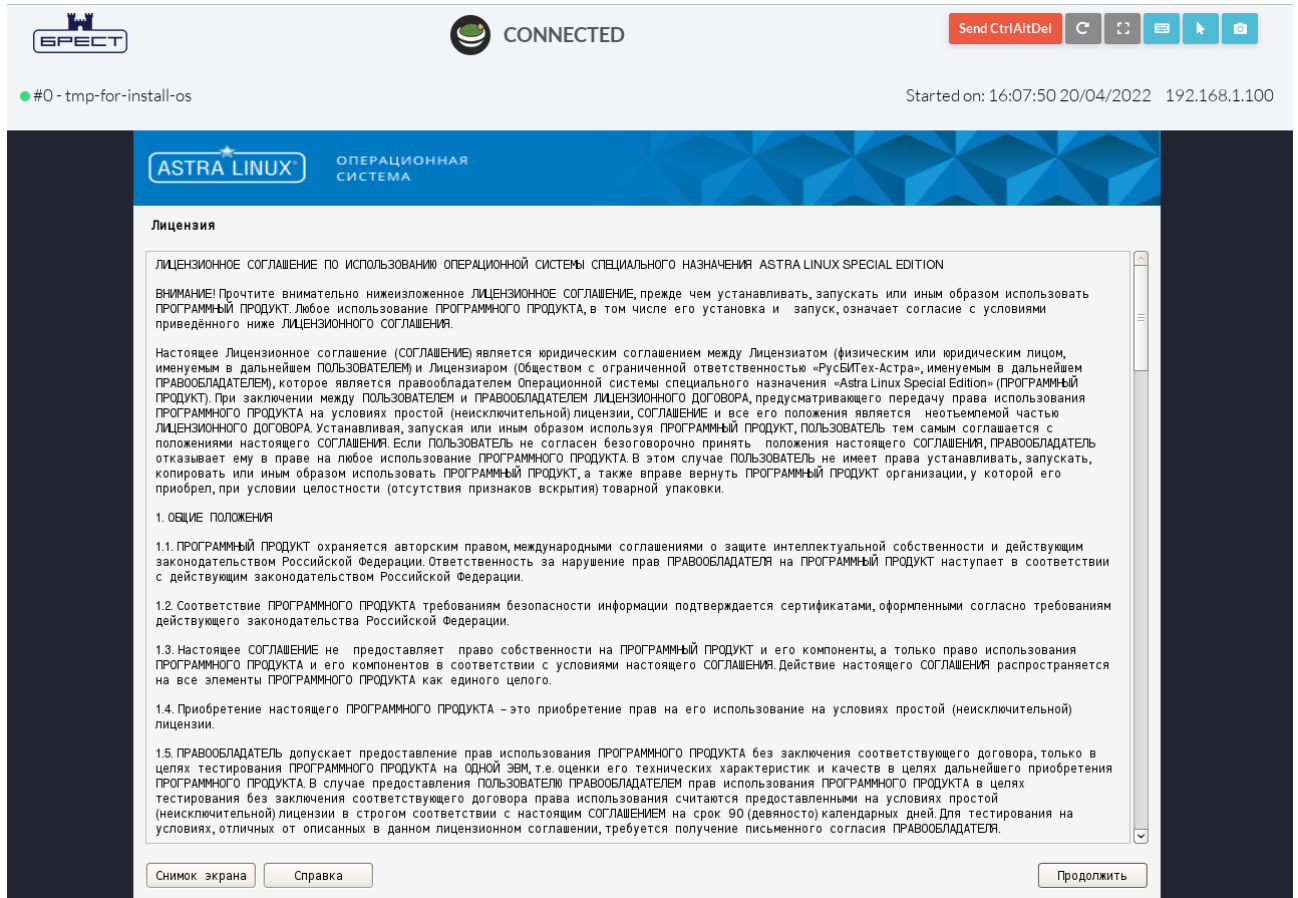


Рис. 82

6. ДОПОЛНИТЕЛЬНАЯ НАСТРОЙКА ВИРТУАЛЬНОЙ МАШИНЫ

6.1. Контекстуализация

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

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

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

Пример

Раздел `CONTEXT` шаблона VM

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

В данном примере задаются следующие настройки VM:

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

6.2. Удаленное подключение USB-устройств к VM по протоколам VNC/SPICE/RDP

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

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

- 1) на фронтальной машине ПК СВ установить пакет `breast-vdi-tools`, для этого в терминале выполнить команду:

```
apt install breast-vdi-tools
```

- 2) в веб-интерфейсе ПК СВ на странице VM, на которую необходимо перенаправить

USB-устройство:

- а) открыть вкладку **Конфигурация** и нажать на кнопку **[Изменить конфигурацию]**;
- б) на открывшейся странице **Редактирование конфигурации VM** указать один из протоколов удаленного доступа. Для этого:
 - при выборе VNC или SPICE — во вкладке **Ввод/Вывод** в секции **Средства графического доступа** выбрать необходимый протокол (см. рис. 83),

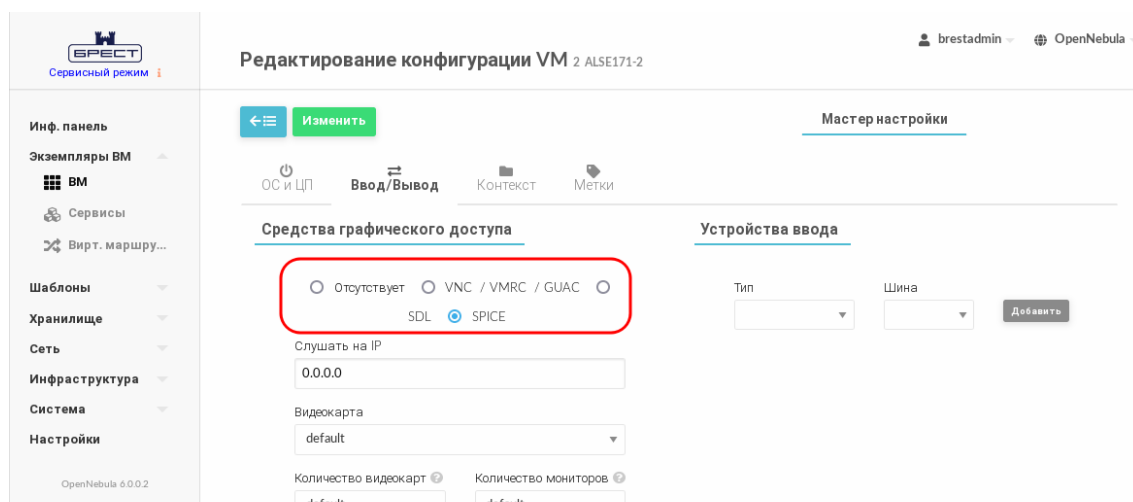


Рис. 83

- при выборе RDP — во вкладке **ОС и ЦП** в секции **Особенности** в выпадающем списке **Гостевой агент Qemu** выбрать «Да» (см. рис. 84)

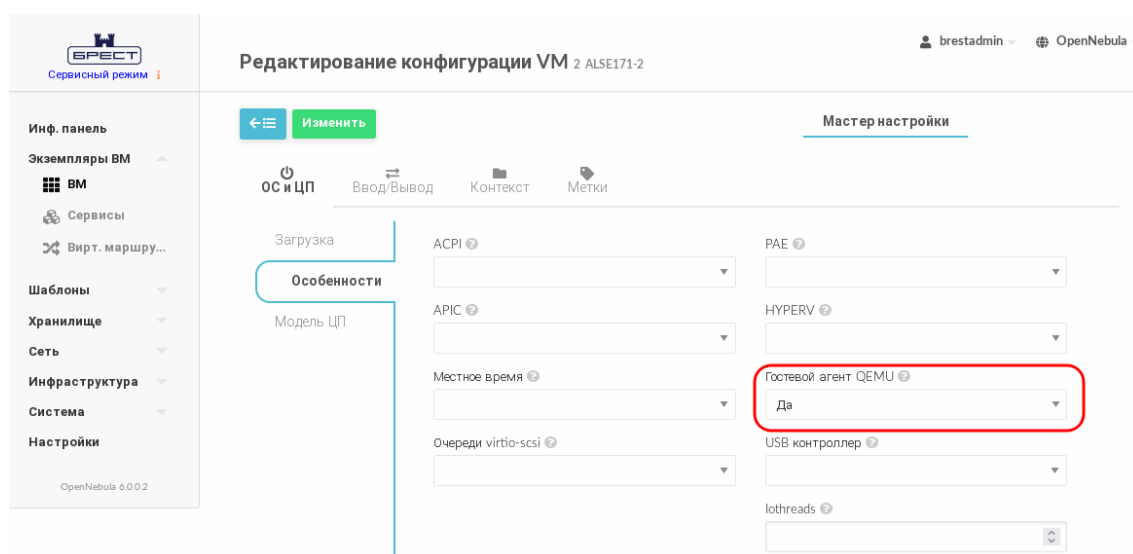


Рис. 84

- при необходимости скорректировать тип USB-контроллера в настройках виртуальной машины, на которую будет перенаправлено USB-устройство (по умолчанию задействован контроллер USB 2.0). Если необходимо перенаправить устройство USB 3.0 и выше, то во вкладке **ОС и ЦП** в сек-

ции **Особенности** в выпадающем списке **USB контроллер** выбрать «3.0» (см. рис. 84)

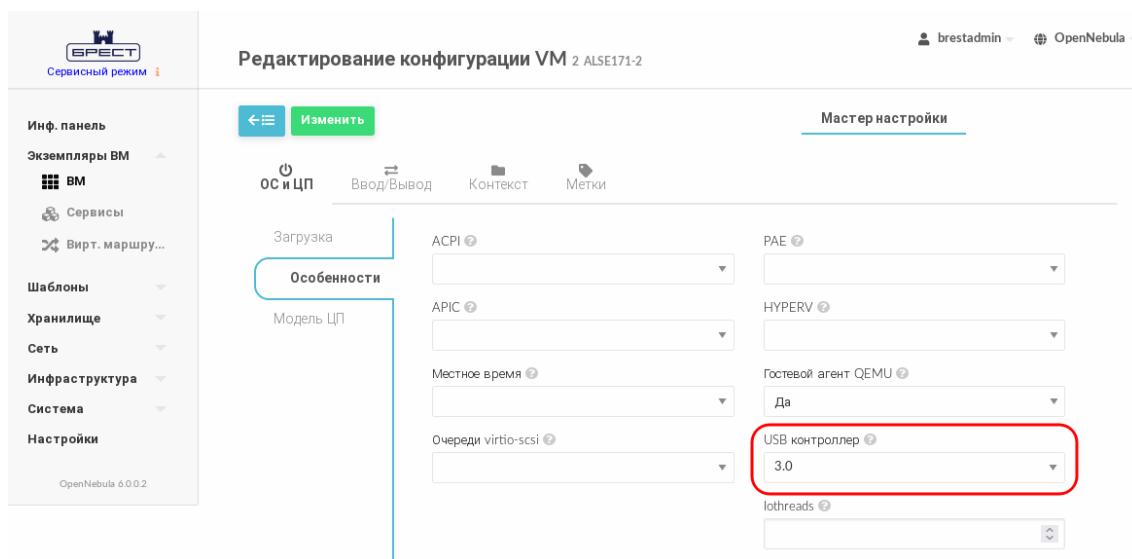


Рис. 85

- на странице **Редактирование конфигурации VM** нажать на кнопку **[Изменить]**;

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

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

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

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

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

Для того чтобы перенаправить подключенное USB-устройство на VM, необходимо выполнить следующие действия:

1) через графический интерфейс запустить приложение (права администратора не требуются): «Пуск — Сеть — Brest Usb Redirect» (см. рис. 86).

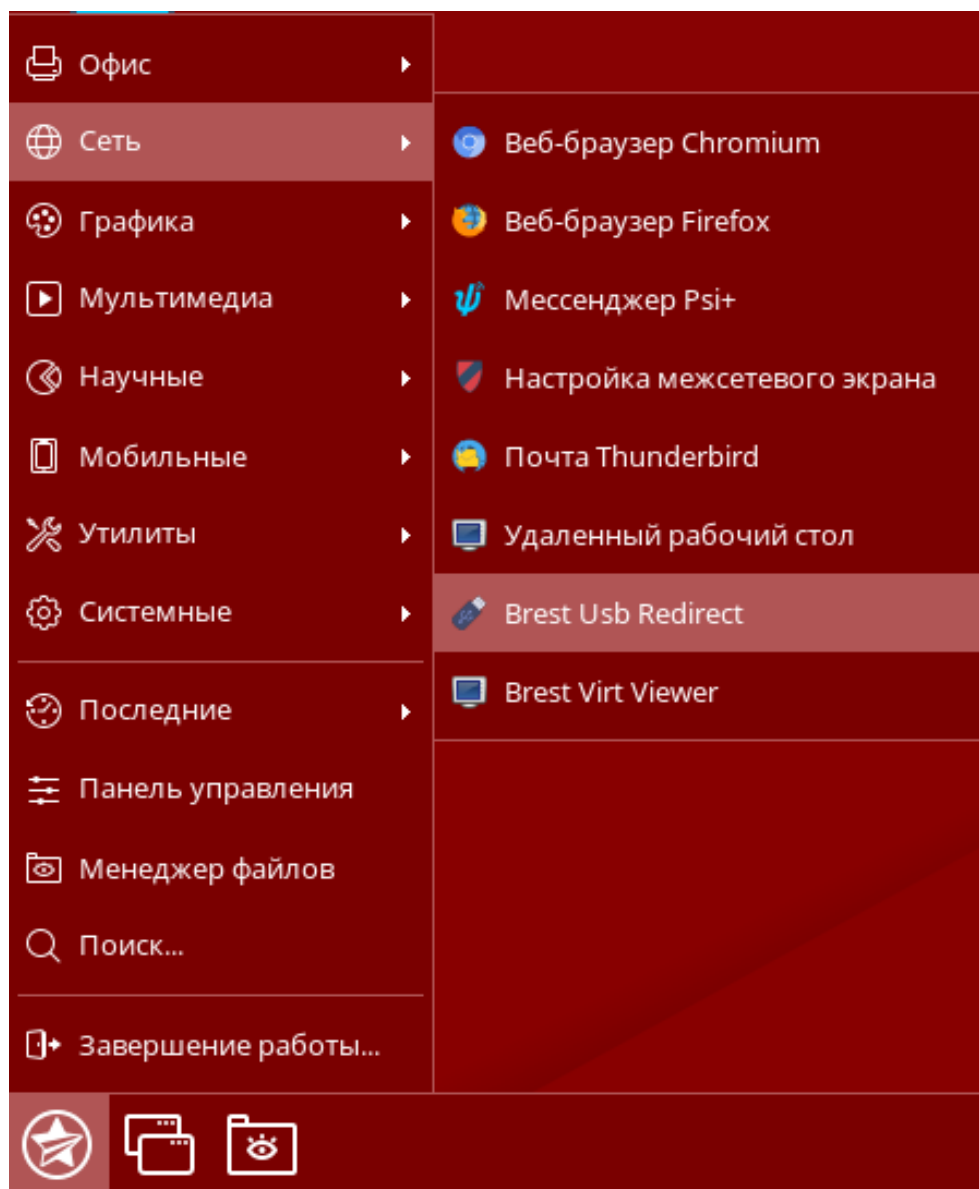
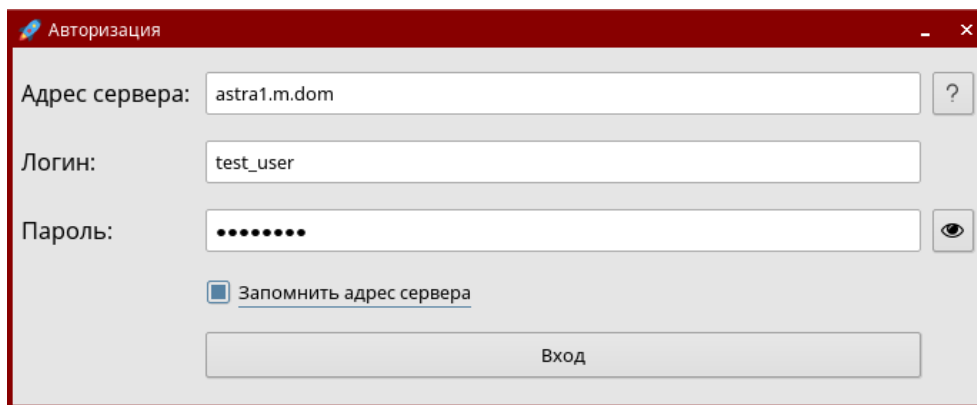


Рис. 86

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

2) в открывшемся окне «Авторизация» (см. рис. 87) указать авторизационные параметры для доступа к виртуальной машине, на которую необходимо перенаправить USB-устройство:

- «Адрес сервера» — полное доменное имя фронтальной машины ПК СВ;
- «Логин» — имя учетной записи пользователя домена, имеющего доступ к виртуальной машине;
- «Пароль» — пароль учетной записи пользователя домена, имеющего доступ к виртуальной машине;



Адрес сервера: astra1.m.dom

Логин: test_user

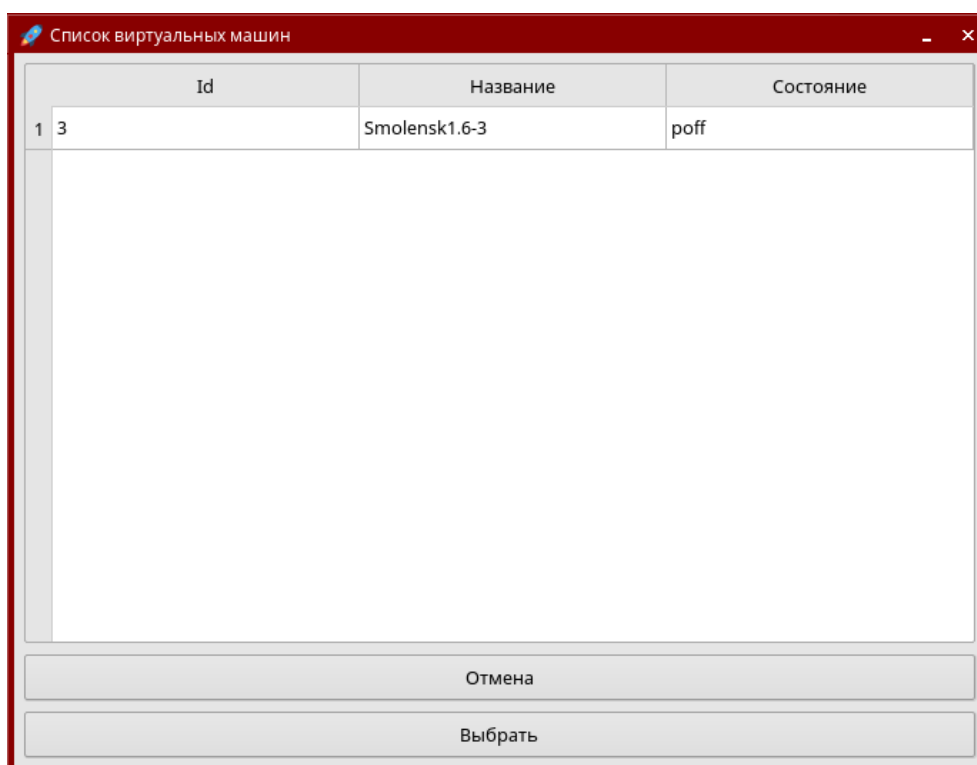
Пароль:

Запомнить адрес сервера

Вход

Рис. 87

3) в открывшемся окне «Список виртуальных машин» (см. рис. 88) указать виртуальную машину, на которую необходимо перенаправить USB-устройство.



Id	Название	Состояние
1 3	Smolensk1.6-3	poff

Отмена

Выбрать

Рис. 88

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

4) в открывшемся окне «Список usb-устройств» (см. рис. 89) выбрать одно или несколько USB-устройств, которые необходимо перенаправить;

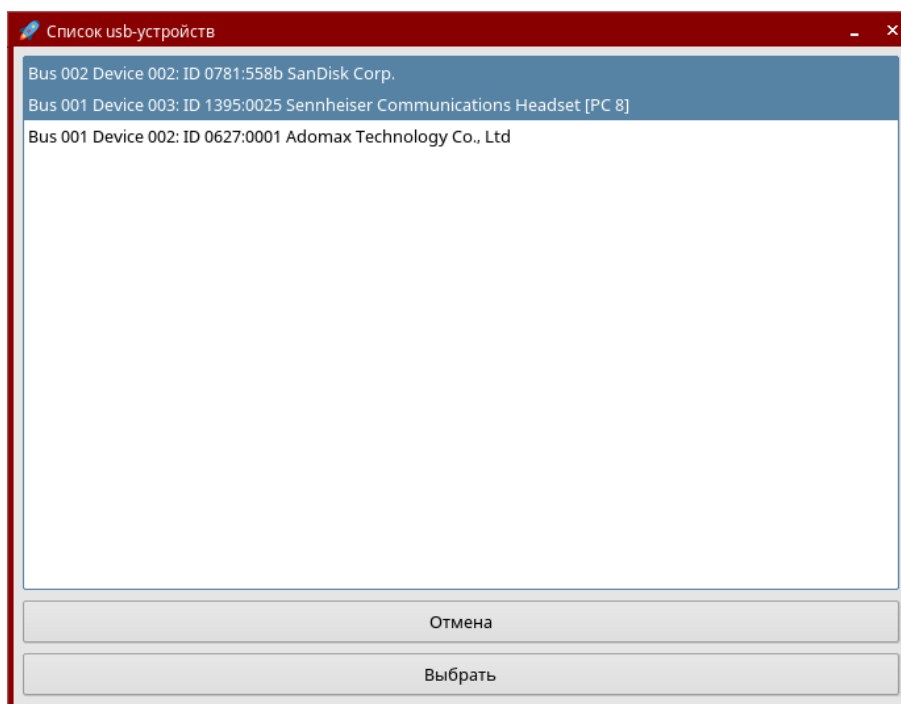


Рис. 89

5) в открывшемся окне «Доступные подключения» (см. рис. 90) выбрать протокол подключения.

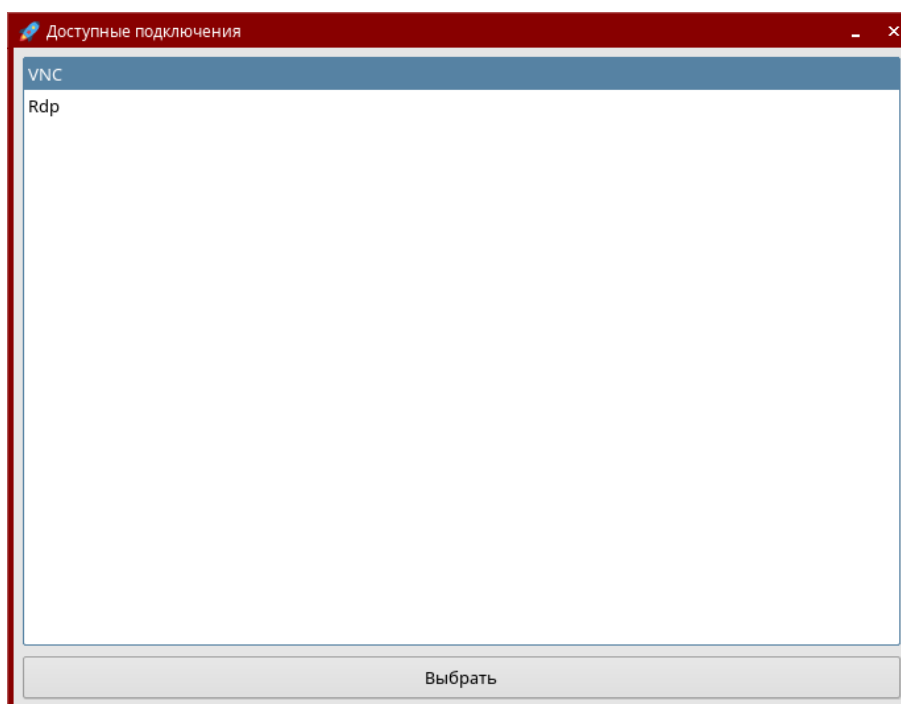


Рис. 90

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

```
lsusb
```

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

USB-устройство (см. рис. 91).

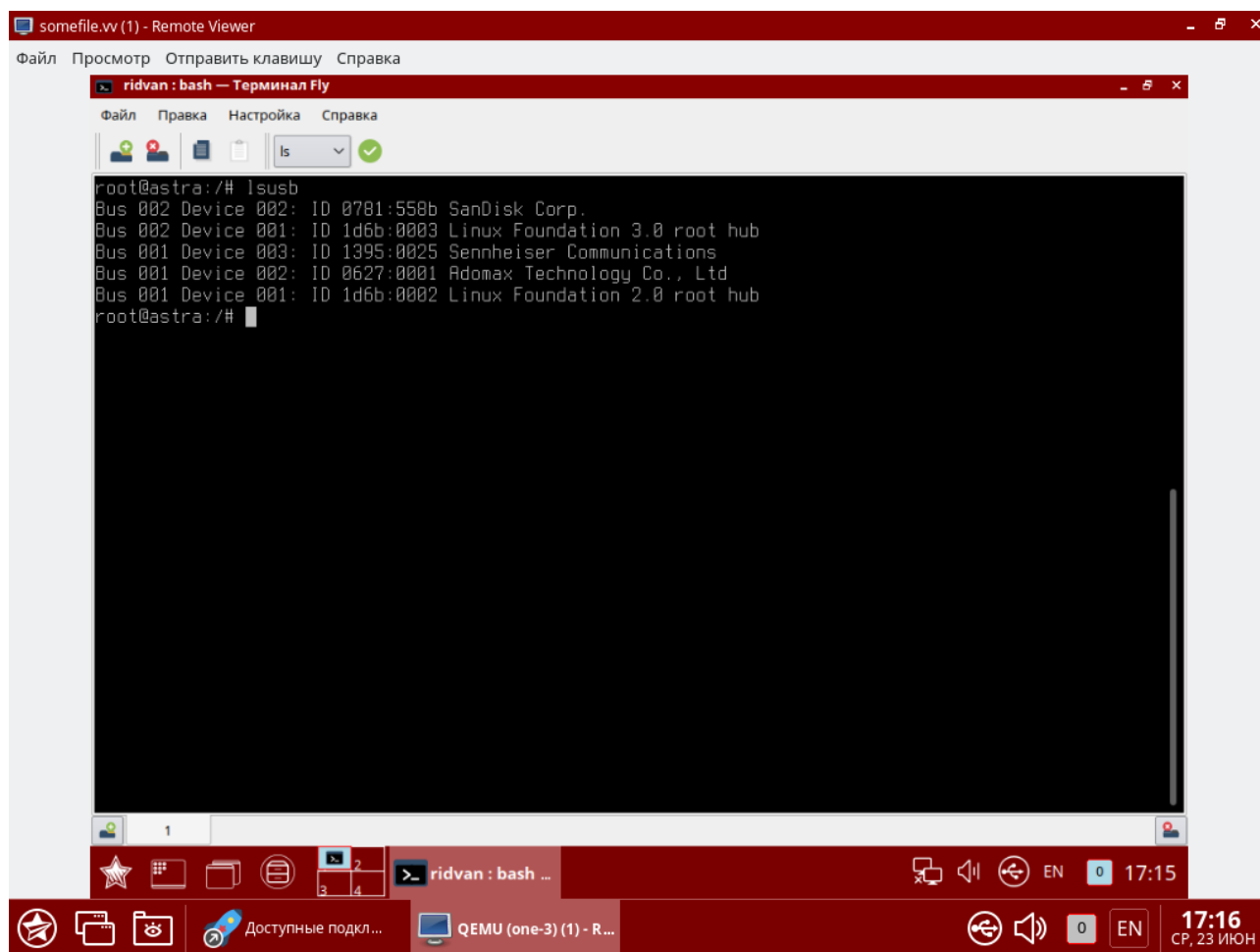


Рис. 91

6.3. Настройка дискреционного и мандатного управление доступом к ВМ

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

Для настройки мандатного контроля целостности, дискреционного и мандатного управления доступом виртуальной машины необходимо в веб-интерфейсе ПК СВ для этой ВМ открыть вкладку **Безопасность** и выполнить следующие действия (см. рис. 92.):

- в секции **Модель PARSEC** в выпадающем списке **Тип** выбрать тип модели мандатного управления доступом (динамический или статический). При выборе статического типа модели в поле **Метка** необходимо задать мандатную метку;
- в секции **Дискреционный контроль доступа** следует:
 - в выпадающем списке **Тип** выбрать тип субъекта (пользователь или группа);
 - в выпадающем списке **Субъект** выбрать соответствующего субъекта (пользователя или группу);
 - в выпадающем списке **Права доступа** выбрать типа доступа к виртуальной машине:

- «Управление» — разрешен полный доступ к VM, включая запуск, правку ее свойств и управление правами доступа к ней;
- «Использование» — разрешен только просмотр свойств, запуск и работа с виртуальной машиной.

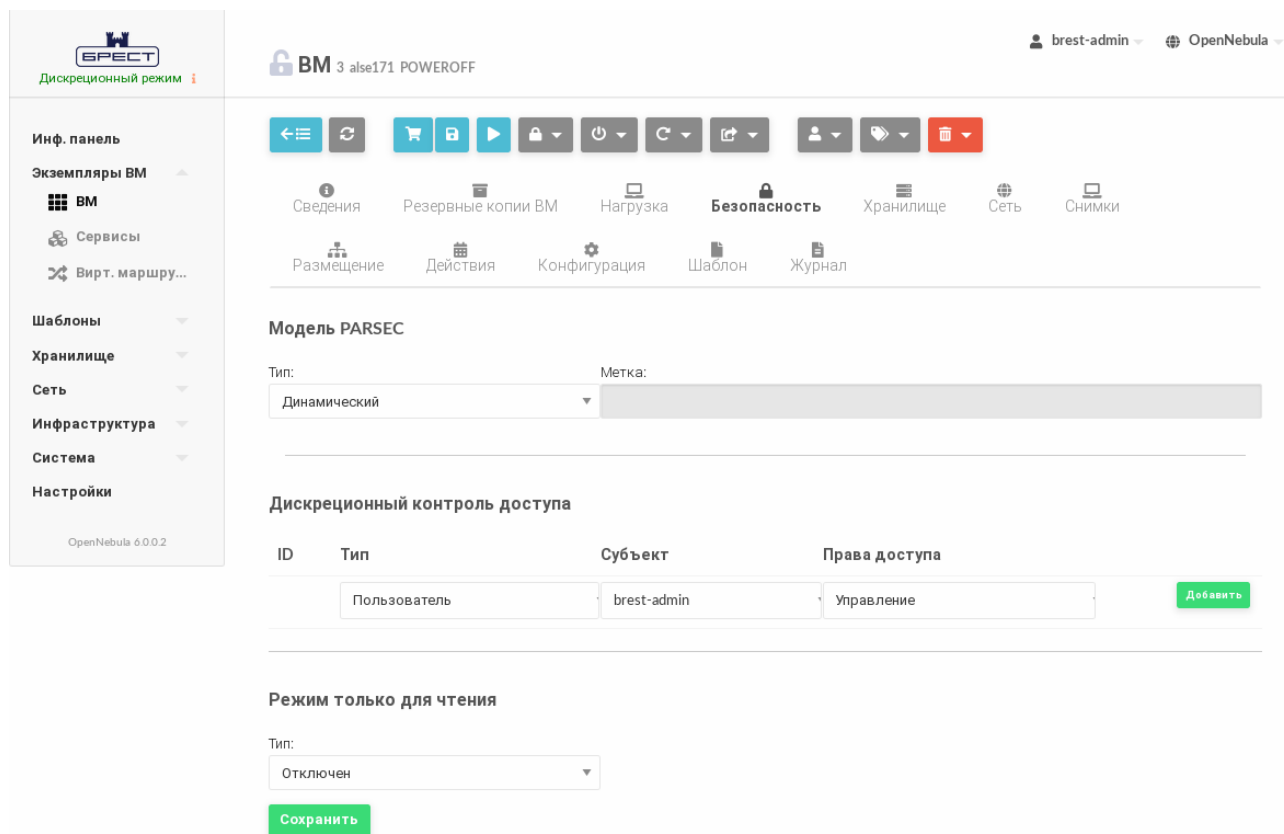


Рис. 92

После внесения изменений необходимо нажать на кнопку **[Сохранить]**.
ВНИМАНИЕ! Настройка доступа возможно только при выключенной VM.

6.4. Отказоустойчивость виртуальной машины

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

Для работы модуля необходимо соблюдение следующих условий:

- наличие в кластере минимум двух рабочих узлов виртуализации;
- общее хранилище дисков VM, доступное на каждом из узлов;
- поддержка со стороны узлов технологии IPMI (Intelligent Platform Management Interface). Данные для авторизации по IPMI должны быть указаны в настройках каждого узла виртуализации;
- для VM должен быть установлен признак отказоустойчивости (Высокая доступность) — см. рис. 93.

The screenshot shows the OpenNebula web interface for a VM named 'alse171'. The VM is currently in a 'POWEROFF' state. The 'Information' (Сведения) tab is active, showing details such as ID (3), Name (alse171), and State (ВЫКЛЮЧЕНО). A red box highlights the 'High Availability' (Высокая доступность) setting, which is set to 'Yes' (Да). Other settings include 'Current State' (Текущее состояние VM) as LCM_INIT and 'Node' (Узел) as oneserver.brest.local.

Информация	Права	Пользование	Управление
Владелец		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Группа		<input type="checkbox"/>	<input type="checkbox"/>
Владелец			
Владелец		brest-admin	<input checked="" type="checkbox"/>
Группа		brestadmins	<input checked="" type="checkbox"/>
Резервные копии VM			
Частота		-	
ID магазина приложений		-	

Рис. 93

В процессе работы модуля:

- ПК СВ получает сигнал о неисправности узла виртуализации;
- считывается список запущенных на неисправном узле VM с установленным признаком отказоустойчивости (Высокая доступность);
- считываются сохранившиеся атрибуты безопасности VM (мандатная метка и имя пользователя, запустившего виртуальную машину) и производится ее перезапуск на рабочем узле.

6.5. Автостарт виртуальных машин

Механизм автостарта VM позволяет автоматически запустить VM, настроенные на автостарт, на узлах при восстановлении облака после аварийного отключения.

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

Автостарт происходит следующим образом:

- 1) при восстановлении работы ПК СВ фронтальная машина запускается в первую очередь;
- 2) фронтальная машина проверяет состояние узлов, ожидая их запуска;
- 3) фронтальная машина проверяет наличие на запущенных узлах VM, для которых настроен автостарт;
- 4) если такие VM присутствуют, фронтальная машина автоматически запускает их.

ВНИМАНИЕ! Если в ПК СВ для обеспечения отказоустойчивости сервиса фронтальной машины применяется технология Raft, то для корректной работы автостарта необхо-

димом в файл `/lib/systemd/system/libvirtd.service`, находящийся на фронтальной машине, добавить строку:

```
After=opennebula.service
```

Примечание. Алгоритм Raft описан в документе «Программный комплекс «Средства виртуализации «Брест» (ПК СВ «Брест») РДЦП.10001-03. Руководство администратора. Часть 1».

6.6. Миграции дисков VM между хранилищами

Миграции дисков VM может быть осуществлена только между одинаковыми типами хранилищ (например из LVM_LVM в LVM_LVM или из Qcow2 в Qcow2) и только в рамках одного узла виртуализации.

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

- 1) на странице VM нажать на кнопку управления размещением и в открывшемся меню выбрать пункт «Перенести VM» (см. рис. 94).



Рис. 94

- 2) в открывшемся окне **Мигрировать виртуальную машину** следует выполнить следующие шаги:

- а) в секции **Выберите Узел** выбрать тот же узел, на котором запущена VM (см. рис. 95);

Мигрировать виртуальную машину

VM 84 brest-stend в настоящее время запущено на Узле srv-01.example.dom, № хранилища - 103

Выбрать узел

Выберите Узел из списка



ID	Название	Кластер	Запущенные VM	Выделено ЦП	Выделено Памяти	Статус	VM MAD
5	srv-03.example.dom	default	6	440 / 1600 (28%)	75GB / 125.8GB (60%)	Вкл	kvm
4	srv-02.example.dom	default	5	390 / 1600 (24%)	72GB / 125.8GB (57%)	Вкл	kvm
3	srv-01.example.dom	default	4	250 / 1600 (16%)	48GB / 125.8GB (38%)	Вкл	kvm

Показаны элементы списка с 1 по 4 из 4

Предыдущая

1

Следующая

Расширенные настройки

Перенести VM

Рис. 95

б) в открывшейся секции **Выберите хранилище** выбрать хранилище такого же типа, как хранилище, в котором на текущий момент хранится диск VM (см. рис. 96);

Мигрировать виртуальную машину

VM 84 brest-stand в настоящее время запущено на Узле srv-01.example.dom, № хранилища - 103

Выбрать узел

Вы выбрали следующий Узел: **srv-01.example.dom**

ID	Название	Кластер	Запущенные VM	Выделено ЦП	Выделено Памяти	Статус	VM MAD
8	usb-test.example.dom	default	0	0 / 800 (0%)	0KB / 7.1GB (0%)	ОШИБКА	kvm
5	srv-03.example.dom	default	6	440 / 1600 (28%)	75GB / 125.8GB (60%)	Вкл	kvm
4	srv-02.example.dom	default	5	390 / 1600 (24%)	72GB / 125.8GB (57%)	Вкл	kvm
3	srv-01.example.dom	default	4	250 / 1600 (16%)	48GB / 125.8GB (38%)	Вкл	kvm

10 Показаны элементы списка с 1 по 4 из 4

Предыдущая 1 Следующая

Расширенные настройки

Проверка

Выберите хранилище

Пожалуйста выберите хранилище из списка

ID	Название	Владелец	Группа	Производительность	Кластер	Тип	Статус
103	lvm-lvm-system	oneadmin	brestadmins	48.6GB / 1.8TB (3%)	0	Системный	Вкл
104	lvm-lvm 1	oneadmin	brestadmins	48.6GB / 1.8TB (3%)	0	Системный	Вкл

10 Показаны элементы списка с 1 по 1 из 1 (отфильтровано из 2 элементов списка)

Предыдущая 1 Следующая

Рис. 96

в) нажать на кнопку **[Перенести VM]**.

6.7. Автоматический ввод VM в домен через механизм контекста

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

- 1) создать базовую VM, на основе которой будет подготовлен шаблон;
- 2) в базовой VM выполнить следующие шаги:
 - а) установить ОС CH;
 - б) установить пакет `one-context`;
 - в) в конфигурационном файле `/etc/one/oned.conf` раскомментировать следующую строку:


```
ONEGATE_ENDPOINT = ...
```
 - г) выключить базовую VM сохранить ее как постоянный шаблон (см. подраздел 5.3.10);
- 3) на фронтальной машине перезапустить службу `opennebula`, выполнив команду:


```
sudo systemctl restart opennebula
```

- 4) в веб-интерфейсе ПК СВ для созданного шаблона выполнить следующие шаги:
- на странице шаблона нажать на кнопку **[Обновить]**,
 - на открывшейся странице **Изменить шаблон VM** во вкладке **Контекст** в секции **Конфигурация** установить флаг **Добавить токен OneGate** (см. рис. 97)

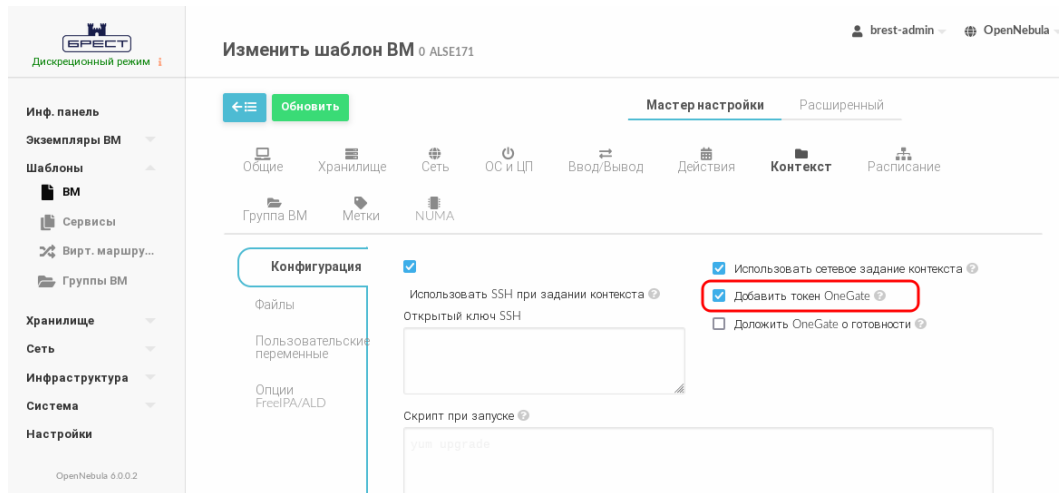


Рис. 97

- в) на странице **Изменить шаблон VM** во вкладке **Контекст** в секции **Опции FreeIPA/ALD** (см. рис. 98) указать параметры контроллера домена:

- переключатель «Контролер домена» предназначен для выбора типа домена (FreeIPA/ALD),
- в поле «Доменное имя (REALM)» — указывается наименование домена,
- в поле «Полное доменное имя сервера (FQDN)» — указывается полное доменное имя контроллера домена FreeIPA/ALD,
- в поле «IP адрес сервера» — указывается IP-адрес контроллера домена FreeIPA/ALD,
- в поле «Логин администратора» — указывается имя администратора домена FreeIPA/ALD,
- в поле «Пароль администратора» — указывается пароль администратора домена FreeIPA/ALD,
- в поле «Установить префикс для имени VM» опционально можно указать префикс, который будет добавляться к имени (hostname) создаваемой VM;

Изменить шаблон VM 0 ALSE171

Мастер настройки

Общие Хранилище Сеть ОС и ЦП Ввод/Вывод Действия Контекст Расписание

Группа VM Метки NUMA

Конфигурация

Файлы

Пользовательские переменные

Опции FreeIPA/ALD

Контроллер домена

Не использовать FreeIPA ALD

Доменное имя (REALM) *

brest.local

Полное доменное имя сервера (FQDN) *

dc.brest.local

IP-адрес сервера *

172.16.1.10

Логин администратора *

testuser

Пароль администратора *

Показать пароль

Установить префикс для имени VM (optional)

alse

Рис. 98

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

г) на странице **Изменить шаблон VM** нажать на кнопку **[Обновить]**.

7. МАГАЗИН ПРИЛОЖЕНИЙ

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

7.1. Требования

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

7.2. Установка и настройка магазина приложений

На фронтальной машине необходимо установить пакет `brest-marketplace`, выполнив в терминале команду:

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

ВНИМАНИЕ! Если в ПК СВ для обеспечения отказоустойчивости сервиса фронтальной машины применяется технология Raft, пакет `brest-marketplace` должен быть установлен на каждом сервере с ролью фронтальной машины. При этом первоначальная настройка магазина приложений должно происходить на «лидере».

Примечание. Алгоритм Raft описан в документе «Программный комплекс «Средства виртуализации «Брест» (ПК СВ «Брест») РДЦП.10001-03. Руководство администратора. Часть 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) узла, выступающего в роли 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 ПК СВ, при этом режим «Доступ на управление» может иметь только один ПК СВ. Для изменения режима доступа необходимо повторно запустить мастер настройки `brest-marketplace-configure` на фронтальной машине 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. 99).

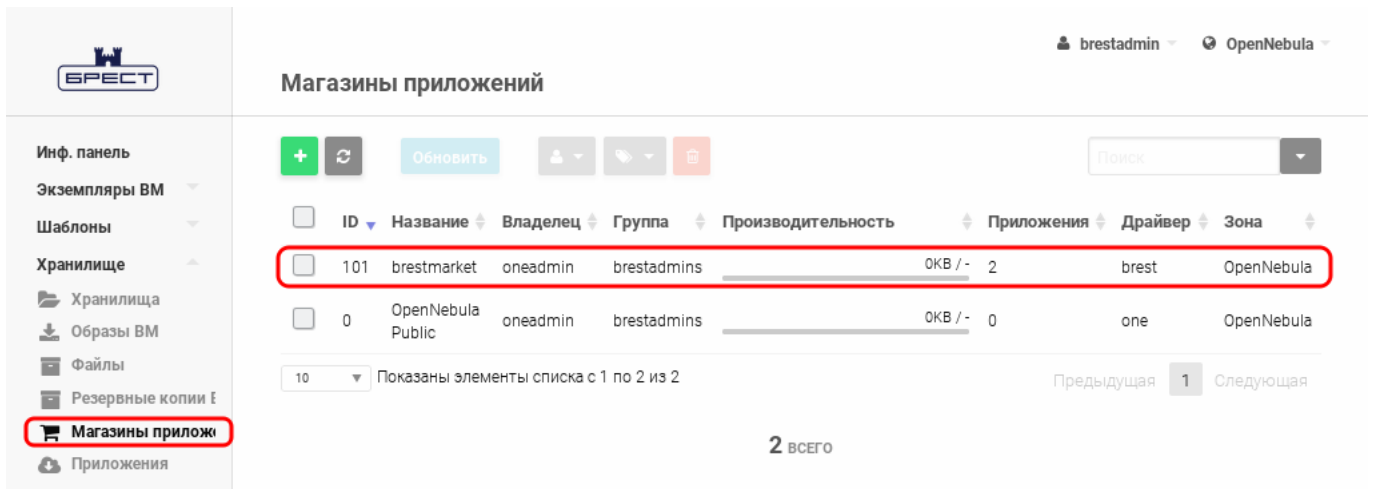


Рис. 99

7.3. Добавление приложения

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

7.3.1. 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 меню «Хранилище — Приложения» и на открывшейся странице **Приложения** нажать на кнопку **[+]** (см. рис. 100);

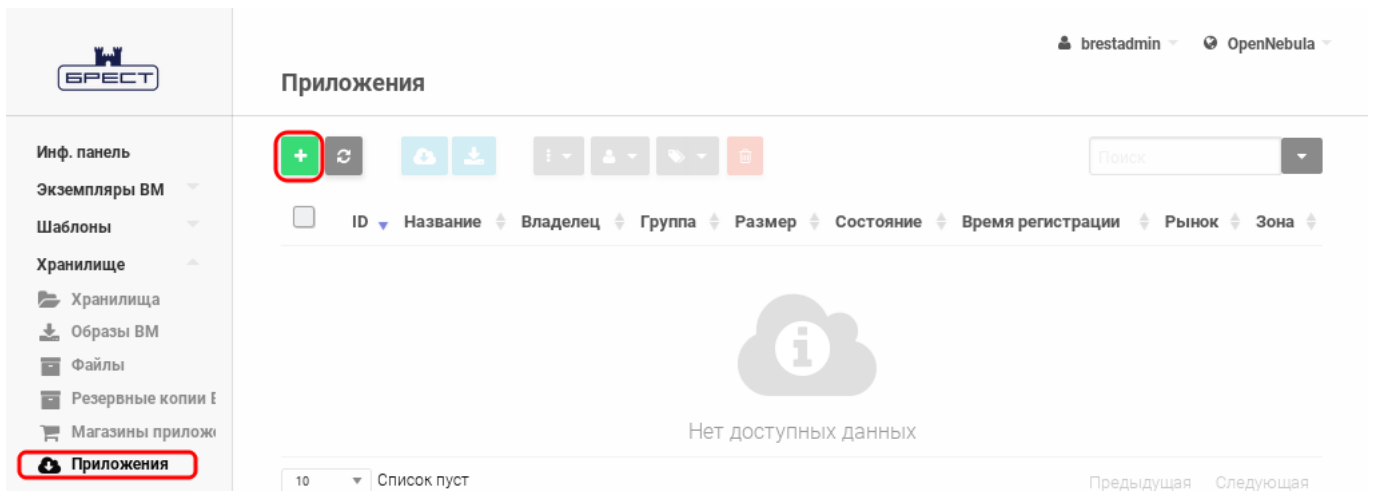


Рис. 100

- 2) на открывшейся странице **Создать приложение в магазине приложений** (см. рис. 101) 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]**.

Создать приложение в магазине приложений

Мастер настройки | Расширенный

Включить/Выключить **Создать**

Название:

Описание:

Версия:

Выберите образ для создания Приложения

Вы выбрали следующий образ: **examlе**

ID	Название	Владелец	Группа	Хранилище	Размер	Тип	Статус	Кол-во VM
0	examlе	brestadmin	brestadmins	default	24MB	ОС	ГОТОВО	0

Показаны элементы списка с 1 по 1 из 1

Выберите магазин приложений для создания приложения

Вы выбрали следующий Магазин приложений: **brestmarket**

ID	Название	Владелец	Группа	Производительность	Приложения	Драйвер	Зона
101	brestmarket	oneadmin	brestadmins	ОКВ / -	0	brest	OpenNebula
0	OpenNebula Public	oneadmin	brestadmins	ОКВ / -	0	one	OpenNebula

Показаны элементы списка с 1 по 2 из 2

Рис. 101

Созданное приложение будет отображено в веб-интерфейсе ПК СВ на странице **Приложения** (см. рис. 102).

Приложения

ID	Название	Владелец	Группа	Размер	Состояние	Время регистрации	Рынок	Зона
5	example_app	oneadmin	brestadmins	24MB	ГОТОВО	21/07/2021 17:48:19	brestmarket	OpenNebula

Показаны элементы списка с 1 по 1 из 1

1 всего

Рис. 102

Примечание. После создания и завершения загрузки приложения в магазин

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

7.3.2. Создание приложения, используя имеющуюся VM

Для того чтобы создать приложение, используя имеющуюся VM, и добавить его в магазин приложений, необходимо на фронтальной машине в терминале выполнить команду:

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

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

Пример

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

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

Созданное приложение будет отображено в веб-интерфейсе ПК СВ на странице **Приложения** (см. рис. 103).

The screenshot displays the 'Приложения' (Applications) page in the OpenNebula web interface. The page features a table of applications with the following columns: ID, Название (Name), Владелец (Owner), Группа (Group), Размер (Size), Состояние (Status), Время регистрации (Registration Time), Рынок (Market), and Зона (Zone). A single application is listed with ID 10, name 'test app', owner 'oneadmin', group 'brestadmins', size '24MB', and status 'ГОТОВО'. The application is highlighted with a red box. The left sidebar shows the navigation menu with 'Приложения' selected. The top right shows the user 'brestadmin' and the OpenNebula logo.

ID	Название	Владелец	Группа	Размер	Состояние	Время регистрации	Рынок	Зона
10	test app	oneadmin	brestadmins	24MB	ГОТОВО	21/07/2021 20:15:36	brestmarket	OpenNebula

Рис. 103

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
AR	— Address Ranges (диапазон IP-адресов)
VDC	— Virtual Data Center (виртуальный дата-центр)

