

Утвержден
РДЦП.10001-07-УД

ПРОГРАММНЫЙ КОМПЛЕКС «СРЕДСТВА ВИРТУАЛИЗАЦИИ «БРЕСТ»
Руководство администратора. Часть 2
РДЦП.10001-07 95 01-2
Листов 138

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

2023

Литера О₁

АННОТАЦИЯ

Настоящий документ является руководством администратора программного изделия «Программный комплекс «Средства виртуализации «Брест» (ПК СВ «Брест») РДЦП.10001-07 (далее по тексту — ПК СВ) в части применения по назначению ПК СВ с учетом особенностей операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-37 (далее по тексту — ОС СН), под управлением которой функционирует ПК СВ.

Документ предназначен для администраторов средства виртуализации (администраторов ПК СВ) и администратора безопасности ПК СВ.

Документ не охватывает порядок установки и развертывания ПК СВ и предназначен для использования совместно с эксплуатационными документами согласно ведомости РДЦП.10001-07 20 01 «Программный комплекс «Средства виртуализации «Брест». Ведомость эксплуатационных документов».

Руководство администратора состоит из двух частей:

- РДЦП.10001-07 95 01-1 «Программный комплекс «Средства виртуализации «Брест». Руководство администратора. Часть 1»;
- РДЦП.10001-07 95 01-2 «Программный комплекс «Средства виртуализации «Брест». Руководство администратора. Часть 2».

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

Во второй части руководства представлен порядок администрирования ПК СВ с учетом ролевого управления доступа, использования среды виртуализации, обеспечения отказоустойчивости и масштабирования развернутого ПК СВ. Кроме того, руководство содержит порядок действий администратора безопасности ПК СВ части работы с журналом событий безопасности.

Порядок применения средств защиты информации ПК СВ приведен в документе РДЦП.10001-07 97 01 «Программный комплекс «Средства виртуализации «Брест». Руководство по КСЗ». Порядок применения ПК СВ пользователями, в том числе разработчиком и администратором виртуальных машин, приведен в документе РДЦП.10001-07 34 01 «Программный комплекс «Средства виртуализации «Брест». Руководство пользователя».

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

СОДЕРЖАНИЕ

1. Функции администратора ПК СВ	9
2. Инструменты управления ПК СВ	10
2.1. Общие сведения	10
2.2. Инструменты командной строки	10
2.3. Веб-интерфейс ПК СВ	10
3. Пользователи и группы	12
3.1. Общие сведения	12
3.2. Управление пользователями	12
3.2.1. Управление пользователями в интерфейсе командной строки	12
3.2.2. Управление пользователями в веб-интерфейсе ПК СВ	15
3.3. Управление группами	18
3.3.1. Общие сведения	18
3.3.2. Управление группами в интерфейсе командной строки	19
3.3.3. Управление группами в веб-интерфейсе ПК СВ	21
3.4. Управление VDC	23
3.4.1. Общие сведения	23
3.4.2. Управление VDC в интерфейсе командной строки	24
3.4.3. Управление VDC в веб-интерфейсе ПК СВ	26
3.5. Управление полномочиями	28
3.5.1. Общие сведения	28
3.5.2. Управление полномочиями в интерфейсе командной строки	29
3.5.2.1. Просмотр и изменение установленных полномочий для ресурса	29
3.5.2.2. Изменение установленных полномочий для ресурса	29
3.5.2.3. Установка полномочий по умолчанию	31
3.5.3. Управление полномочиями в веб-интерфейсе ПК СВ	32
3.5.3.1. Просмотр и изменение установленных полномочий	32
3.5.3.2. Установка полномочий, присваиваемых по умолчанию пользователю	32
3.5.4. Управление полномочиями в отношении экземпляра VM	33
3.6. Управление правилами ACL	34
3.6.1. Общие сведения	34
3.6.2. Структура правил ACL	35

3.6.3. Управление правилами ACL в интерфейсе командной строки	36
3.6.4. Управление правилами ACL в веб-интерфейсе ПК СВ	38
3.6.5. Использование правил ACL для реализации роли разработчика VM	39
4. Управление экземплярами VM	41
4.1. Статус и жизненный цикл виртуальной машины	41
4.2. Управление экземплярами VM в интерфейсе командной строки	46
4.2.1. Отображение существующих VM	46
4.2.2. Удаление экземпляров VM	47
4.2.3. Приостановка экземпляров VM	48
4.2.4. Запуск экземпляров VM	49
4.2.5. Перезагрузка экземпляров VM	49
4.2.6. Отсрочка развертывания экземпляров VM	49
4.3. Управление экземплярами VM в веб-интерфейсе ПК СВ	49
4.3.1. Отображение существующих VM	49
4.3.2. Завершение работы и приостановка экземпляров VM	50
4.3.3. Запуск экземпляра VM	51
4.3.4. Перезагрузка экземпляров VM	52
4.3.5. Отсрочка развертывания экземпляров VM	52
4.3.6. Удаление экземпляров VM	53
4.4. Управление доступом виртуальных машин к физическому и виртуальному оборудованию	53
4.4.1. Удаленное подключение USB-устройств к VM по протоколам VNC/SPICE/RDP	53
4.4.2. Ретрансляция PCI	59
4.4.2.1. Требования	59
4.4.2.2. Настройка сервера виртуализации	59
4.4.2.3. Конфигурация ядра	59
4.4.2.4. Загрузка драйвера vfio в initrd	60
4.4.2.5. Блокировка драйверов	60
4.4.2.6. Привязка устройств к vfio	60
4.4.2.7. Конфигурация qemu	61
4.4.2.8. Настройка драйвера	62
4.4.2.9. Настройка использования устройств PCI	62
4.4.3. Горячее подключение образа диска	65

4.4.3.1. В интерфейсе командной строки	65
4.4.3.2. В веб-интерфейсе ПК СВ	65
4.4.4. Перераспределение производительности ВМ	66
4.4.4.1. В интерфейсе командной строки	67
4.4.4.2. В веб-интерфейсе ПК СВ	67
4.4.5. Изменение размера дисков ВМ	68
4.4.5.1. В интерфейсе командной строки	68
4.4.5.2. В веб-интерфейсе ПК СВ	69
4.5. Управление квотами	70
4.5.1. Общие сведения	70
4.5.2. Управление квотами в интерфейсе командной строки	71
4.5.2.1. Просмотр установленных квот	71
4.5.2.2. Установка квот	72
4.5.2.3. Изменение установленных квот	75
4.5.2.4. Установка квот для нескольких пользователей/групп	76
4.5.2.5. Установка квот по умолчанию	77
4.5.3. Управление квотами в веб-интерфейсе ПК СВ	77
4.6. Миграция ВМ между серверами виртуализации	79
4.6.1. Перемещение экземпляра ВМ в интерфейсе командной строки	79
4.6.2. Перемещение экземпляра ВМ в веб-интерфейсе ПК СВ	79
4.7. Снимки состояний ВМ	80
4.7.1. Управление снимками состояний в интерфейсе командной строки	81
4.7.2. Управление снимками состояний в веб-интерфейсе ПК СВ	81
4.8. Снимки дисков ВМ	82
4.8.1. Управление снимками дисков в интерфейсе командной строки	82
4.8.2. Управление снимками дисков в веб-интерфейсе ПК СВ	83
5. Управление серверами виртуализации и кластерами	85
5.1. Серверы виртуализации	85
5.1.1. Добавление сервера виртуализации	85
5.1.1.1. Регистрация сервера виртуализации в интерфейсе командной строки	85
5.1.1.2. Регистрация сервера виртуализации в веб-интерфейсе ПК СВ	85
5.1.2. Отображение информации о сервере виртуализации и просмотр перечня серверов виртуализации	87

5.1.2.1. В интерфейсе командной строки	87
5.1.2.2. В веб-интерфейсе ПК СВ	88
5.1.3. Жизненный цикл сервера виртуализации	89
5.1.3.1. Общие сведения	89
5.1.3.2. Управление сервером виртуализации в интерфейсе командной строки	90
5.1.3.3. Управление сервером виртуализации в веб-интерфейсе ПК СВ	91
5.1.4. Удаление сервера виртуализации	91
5.1.4.1. В интерфейсе командной строки	91
5.1.4.2. В веб-интерфейсе ПК СВ	91
5.1.5. Мониторинг сервера виртуализации	92
5.1.6. Пользовательские метки сервера виртуализации и стратегии планирования	94
5.1.7. Импорт неконтролируемых виртуальных машин	94
5.1.7.1. Импорт неконтролируемых ВМ в интерфейсе командной строки	95
5.1.7.2. Импорт неконтролируемых ВМ в веб-интерфейсе ПК СВ	95
5.2. Кластеры	96
5.2.1. Управление кластером	96
5.2.1.1. В интерфейсе командной строки	96
5.2.1.2. В веб-интерфейсе ПК СВ	97
5.2.2. Добавление серверов виртуализации к кластеру	97
5.2.2.1. В интерфейсе командной строки	97
5.2.2.2. В веб-интерфейсе ПК СВ	99
5.2.3. Добавление ресурсов к кластеру	99
5.2.4. Планирование и кластеры	100
5.2.4.1. Автоматические требования	100
5.2.4.2. Требования и ранг	101
6. Настройки виртуальных сетей	102
6.1. Виртуальные сети ПК СВ	102
6.1.1. Режимы работы сети	102
6.1.2. Параметры сети	102
6.1.2.1. Параметры физической сети	103
6.1.2.2. Адресное пространство (AR)	104
6.1.2.3. Сетевые параметры контекстуализации	105
6.1.3. Использование сетей	105

6.1.4. Управление сетями в интерфейсе командной строки	106
6.1.4.1. Добавление, удаление и просмотр параметров сети	106
6.1.4.2. Изменение параметров сети	108
6.1.4.3. Управление диапазонами адресов	108
6.1.4.4. Резервирование адресов	109
6.1.5. Управление сетями в веб-интерфейсе ПК СВ	111
6.2. Сетевые группы безопасности	113
6.2.1. Параметры сетевой группы безопасности	113
6.2.2. Стандартная группа безопасности	114
6.2.3. Управление группами безопасности в интерфейсе командной строки	114
6.2.3.1. Добавление, удаление и просмотр списка групп безопасности	114
6.2.3.2. Просмотр и изменение правил группы безопасности	115
6.2.3.3. Применение группы безопасности	116
6.2.4. Управление группами безопасности в веб-интерфейсе ПК СВ	117
7. Планировщик	120
7.1. Настройка планировщика	120
7.1.1. Общие параметры планировщика	120
7.1.2. Настройка стратегии размещения	122
7.1.2.1. Параметры стратегии размещения	122
7.1.2.2. Особенности ранжирования серверов виртуализации	122
7.1.2.3. Предустановленные стратегии размещения	123
7.1.2.4. Перепланирование размещения виртуальных машин	124
7.1.2.5. Ограничение ресурсов, предоставляемых сервером виртуализации	124
7.1.3. Настройка стратегии хранения	125
7.1.3.1. Параметры стратегии хранения	125
7.1.3.2. Особенности ранжирования системных хранилищ	125
7.1.3.3. Предустановленные стратегии размещения	126
7.1.3.4. Перемещение диска VM	127
7.1.3.5. Отключение хранилища	127
7.1.4. Настройка стратегии использования сетей	127
7.1.4.1. Параметры стратегии использования сетей	128
7.1.4.2. Особенности фильтрации виртуальных сетей	128
7.2. Алгоритм работы планировщика	129

8. Руководство администратора безопасности ПК СВ	130
8.1. Регистрация событий безопасности в ПК СВ	130
8.2. Настройка регистрации событий безопасности	130
8.3. Журнал событий	131
9. Магазин приложений	132
9.1. Требования	132
9.2. Установка и настройка магазина приложений	132
9.3. Добавление приложения	133
9.3.1. Создание приложения, используя образ диска	133
9.3.2. Создание приложения, используя имеющуюся VM	135
Перечень терминов	136
Перечень сокращений	137

1. ФУНКЦИИ АДМИНИСТРАТОРА ПК СВ

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

- 1) управление учетными записями пользователей ПК СВ, включая создание и удаление учетных записей (см. 3.2);
- 2) управление правами доступа пользователей ПК СВ к виртуальным машинам (см. 3.5.4);
- 3) запуск, остановка, а также удаление экземпляров ВМ (см. 4.2 и 4.3);
- 4) управление доступом виртуальных машин к физическому и виртуальному оборудованию (см. 4.4);
- 5) управление квотами доступа ВМ к физическому и виртуальному оборудованию (см. 4.5);
- 6) управление перемещением экземпляров ВМ (см. 4.6);
- 7) создание снимков состояния виртуальных машин, включающих файл конфигурации ВМ, образа диска ВМ и образа памяти ВМ (см. 4.7), а также отдельное создание снимков состояния образа диска ВМ (см. 4.8);
- 8) управление виртуальным оборудованием ПК СВ, включая создание и удаление виртуального оборудования.

В ПК СВ в качестве виртуального оборудования выступают:

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

Администратор ПК СВ осуществляет управление следующим виртуальным оборудованием:

- серверами виртуализации (см. 5);
- виртуальными сетями (см. 6).

Управление образами дисков, шаблонами и экземплярами ВМ выполняется администратором ВМ и описано в документе РДЦП.10001-07 34 01.

2. ИНСТРУМЕНТЫ УПРАВЛЕНИЯ ПК СВ

2.1. Общие сведения

2.2. Инструменты командной строки

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

Таблица 1

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

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

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

```
<наименование_инструмента> -h
```

2.3. Веб-интерфейс ПК СВ

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

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

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

- в поле «Логин» ввести имя пользователя ПК СВ (например, brestadmin — имя администратора ПК СВ, который был создан во время выполнения действий по установке программных компонент ПК СВ);
- в поле «Пароль» ввести пароль пользователя ПК СВ;
- нажать на кнопку **[Войти]**.

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

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

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

3. ПОЛЬЗОВАТЕЛИ И ГРУППЫ

3.1. Общие сведения

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

Сведения об основных группах пользователей ПК СВ, реализующих функции администраторов, приведены в документе РДЦП.10001-07 97 01.

Каждый пользователь обладает уникальным идентификатором и принадлежит к группе.

При развертывании службы сервера управления автоматически создаются следующие группы:

- `brestadmins` — группа администраторов ПК СВ. При этом в этой группе автоматически создаются следующие системные пользователи:

- `oneadmin` — используется для взаимодействия всех программных компонентов ПК СВ;

- `serveradmin` — используется службой веб-интерфейса ПК СВ для взаимодействия с другими программными компонентами ПК СВ.

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

- `brestusers` — группа администраторов ВМ.

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

- в сервисном режиме функционирования ПК СВ — пользователь `brestadmin`;

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

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>
```

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

имена пользователей:

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

Кроме того, в имени пользователя не допускается использование:

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

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

```
oneuser create -h
```

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

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

Пример

Создание пользователя, принадлежащего группе администраторов ПК СВ:

```
oneuser create another-adm p@ssW0rd --group brestadmins
```

Пример вывода после успешного выполнения команды:

```
ID: 3
```

ВНИМАНИЕ! Создание пользователя, реализующего роль администратора безопасности средства виртуализации, осуществляется штатными средствами ОС СН. Порядок действий представлен в документе РДЦП.10001-07 97 01.

Примечание. Если созданный пользователь должен реализовать роль разработчика ВМ, то необходимо дополнительно настроить полномочия этого пользователя с помощью правил ACL (см. 3.6.5).

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	brestufe	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	brestufe	public	0 / -	0M /	0.0 / -
2	bre-st-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	bre-st-admin	yes	bre-stadm	public	2 / -	4G /	0.5 / -
1	serveradmin	yes	bre-stadm	server_c	0 / -	0M /	0.0 / -
0	oneadmin	yes	bre-stadm	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 «Система — Пользователи». На открывшейся странице «Пользователи» будет представлена таблица пользователей, аналогичная таблице, отображаемой в интерфейсе командной строки после выполнения команды `oneuser list` (см. рис. 1).

The screenshot shows the 'Пользователи' (Users) page in the OpenNebula web interface. The page title is 'Пользователи'. On the left is a sidebar with navigation items: 'Инф. панель', 'Экземпляры ВМ', 'Шаблоны', 'Хранилище', 'Сеть', 'Инфраструктура', 'Система', 'Пользователи' (selected), 'Группы', 'VDCs', 'Списки контроля', and 'Настройки'. The main content area shows a table of users with the following columns: ID, Название, Группа, Включено, Драйвер авторизации, ВМ, Память, and CPU. The table contains 6 rows of data. Below the table, it says 'Показаны элементы списка с 1 по 6 из 6' and '6 ВСЕГО'. The top right corner shows the user 'bre-st-admin' and the system 'OpenNebula'.

Рис. 1

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

- 1) в меню слева выбрать пункт «Система — Пользователи» и на открывшейся странице «Пользователи» нажать на кнопку **[+]**;
- 2) на открывшейся странице «Создать пользователя» (см. рис. 2) необходимо задать имя и пароль пользователя, а также, при необходимости, указать группу (по умолчанию новый пользователь будет принадлежать группе администраторов ВМ — `bre-stusers`);

Создать пользователя

← Сброс Создать

Имя пользователя
testuser

Пароль
.....

Подтвердите пароль
.....

Сменить пароль при первом входе в систему

Способ аутентификации
общий

Основная группа
1: brestusers

OpenNebula 6.0.0.2

Рис. 2

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

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

Кроме того, в имени пользователя не допускается использование:

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

ВНИМАНИЕ! Пароль пользователя должен удовлетворять следующим требованиям сложности:

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

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

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

Примечание. В дискреционном режиме функционирования ПК СВ для нового пользователя будет создана доменная учетная запись (см. рис. 3).

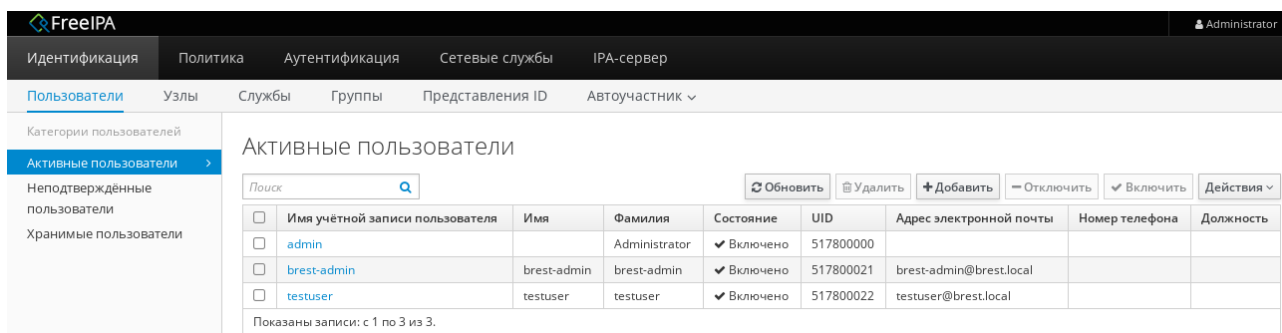


Рис. 3

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

Первичная смена пароля может быть осуществлена:

- при аутентификации пользователя в ОС сервера управления (как в графическом, так и консольном режиме);
- при аутентификации пользователя через веб-интерфейс контроллера домена (только в дискреционном режиме функционирования ПК СВ).

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

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

ВНИМАНИЕ! Создание пользователя, реализующего роль администратора безопасности средства виртуализации, осуществляется штатными средствами ОС СН. Порядок действий представлен в документе РДЦП.10001-07 97 01.

Примечание. Если созданный пользователь должен реализовать роль разработчика ВМ, то необходимо дополнительно настроить полномочия этого пользователя с помощью правил ACL (см. 3.6.5).

Для просмотра информации о конкретном пользователе на странице «Пользователи» необходимо выбрать соответствующую строку. После этого откроется страница пользователя (вкладка «Сведения» — см. рис. 4).

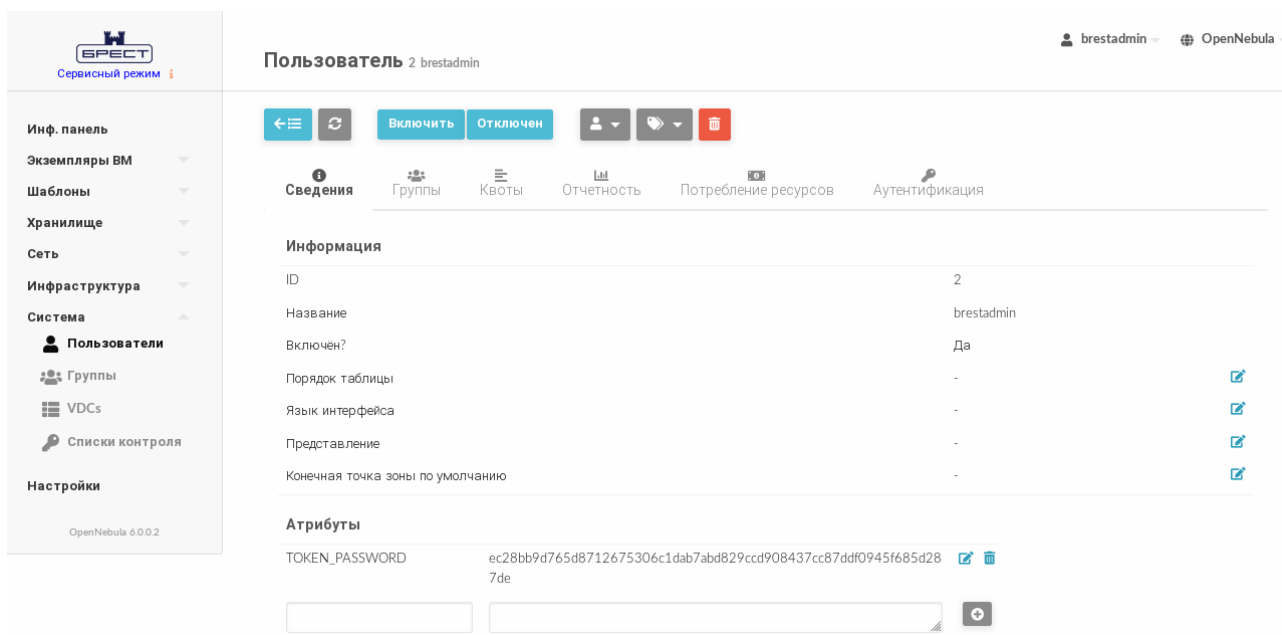


Рис. 4

Для управления учетной записью пользователя в веб-интерфейсе ПК СВ используются следующие элементы интерфейса (см. рис. 5):

- 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.

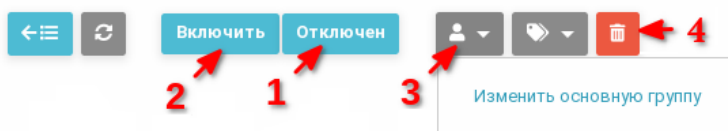


Рис. 5

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

Сведения об основных группах пользователей ПК СВ, реализующих функции администраторов, приведены в документе РДЦП.10001-07 97 01.

3.3.1. Общие сведения

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

В группах изоляция осуществляется за счет разграничения прав доступа пользова-

телей. Однако, в ПК СВ возможно разделить физические вычислительные ресурсы между группами, используя виртуальные дата-центры (VDC) — см. 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.

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

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

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

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

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 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 ресурсам пользователей группы

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

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

Примеры:

1. Создание группы с наименованием «new group»:

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

Пример вывода после выполнения команды:

```
ID: 100
```

2. Создание группы с одновременным созданием администратора группы:

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

Пример вывода после выполнения команды:

```
ID: 101
```

3. Просмотр перечня групп:

```
onegroup list
```

Пример вывода после выполнения команды:

ID	NAME	USERS	VMS	MEMORY	CPU
101	groupA	1	0 / -	0M / -	0.0 / -
100	new group	0	0 / -	0M / -	0.0 / -
1	brestartusers	0	0 / -	0M / -	0.0 / -
0	brestartadmins	3	-	-	-

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

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

Пример вывода после выполнения команды:

```
ID: 102
```

Чтобы изменить основную группу пользователя (в том числе в качестве основной указать группу `brestartadmins`), 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 `brestartusers`.

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 «Система — Группы». На открывшейся странице «Группы» будет представлена таблица групп, аналогичная таблице, отображаемой в интерфейсе командной строки после выполнения команды `onegroup list` (см. рис. 6).

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. 6

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

- 1) в меню слева выбрать пункт «Система — Группы» и на открывшейся странице «Группы» нажать на кнопку **[+]**;
- 2) на открывшейся странице «Создать группу»:
 - а) во вкладке «Общие» задать наименование группы,
 - б) если необходимо создать администратора группы, во вкладке «Администрирование» установить флаг «Создать пользователя с административными правами», задать имя и пароль пользователя,
 - в) во вкладке «Права» указать общие ресурсы, установив соответствующие флаги;
- 3) на странице «Создать группу» нажать на кнопку **[Создать]**;

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

Для просмотра информации о конкретной группе на странице «Группы» необходимо выбрать соответствующую строку. После этого откроется страница «Группа» (вкладка

«Сведения» — см. рис. 7).

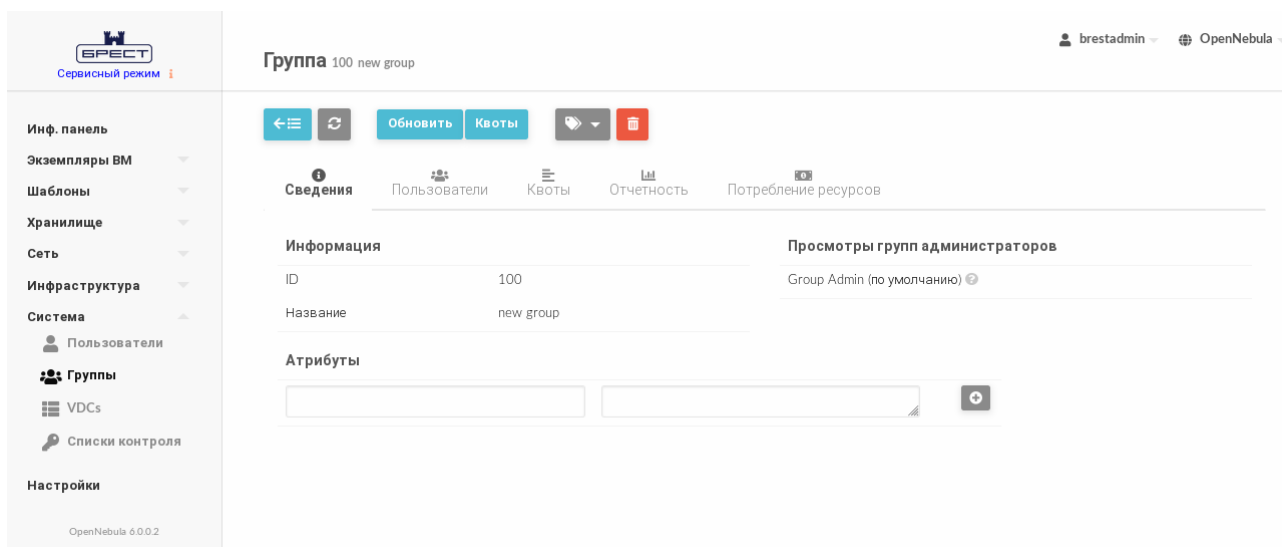


Рис. 7

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

- 1) в меню слева выбрать пункт «Система — Пользователи» и на открывшейся странице «Пользователи» выбрать необходимого пользователя;
- 2) на открывшейся странице «Пользователь» открыть вкладку «Группы» и нажать на кнопку **[Изменить]** (см. рис. 8);

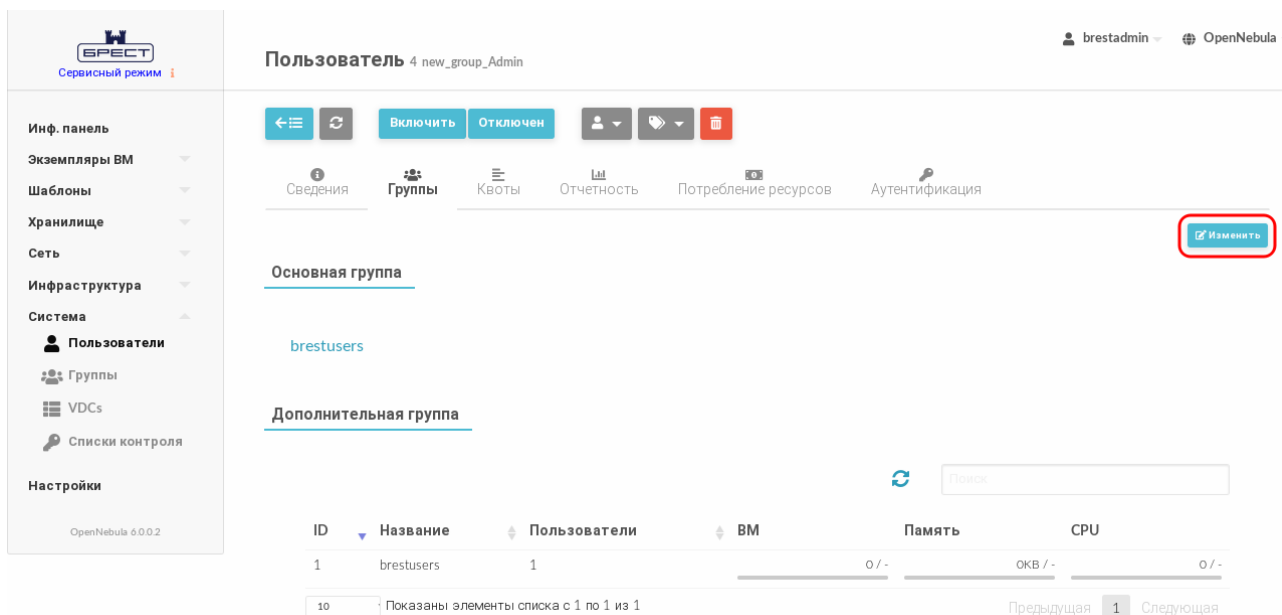


Рис. 8

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. 9).

Пользователь 4 new_group_Admin

бrestadmin OpenNebula

Инф. панель
Экземпляры VM
Шаблоны
Хранилище
Сеть
Инфраструктура
Система
Пользователи
Группы
VDCs
Списки контроля
Настройки

OpenNebula 6.0.0.2

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 / -	ОКВ / -
101	groupA	1		0 / -	ОКВ / -
100	new group	0		0 / -	ОКВ / -
1	brestusers	1		0 / -	ОКВ / -
0	brestadmins	3		-	-

Показаны элементы списка с 1 по 5 из 5

Предыдущая 1 Следующая

Применить изменения

Рис. 9

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 конфигураций.

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

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

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

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

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

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

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

- добавление сервера виртуализации:

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

- добавление виртуальной сети:

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

- добавление хранилища:

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

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

Пример

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

```
onevdc adddatastore test 0 ALL
```

Просмотр перечня VDC после добавления хранилищ:

```
onevdc list
```

Пример вывода после выполнения команды:

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

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

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 «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. 10).

Виртуальные Дата Центры

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

Показаны элементы списка с 1 по 3 из 3

3 ВСЕГО

Рис. 10

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

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

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

определенного кластера, предварительно необходимо выделить этот кластер во вкладке «Ресурсы» в секции «Кластеры» (см. рис. 11)

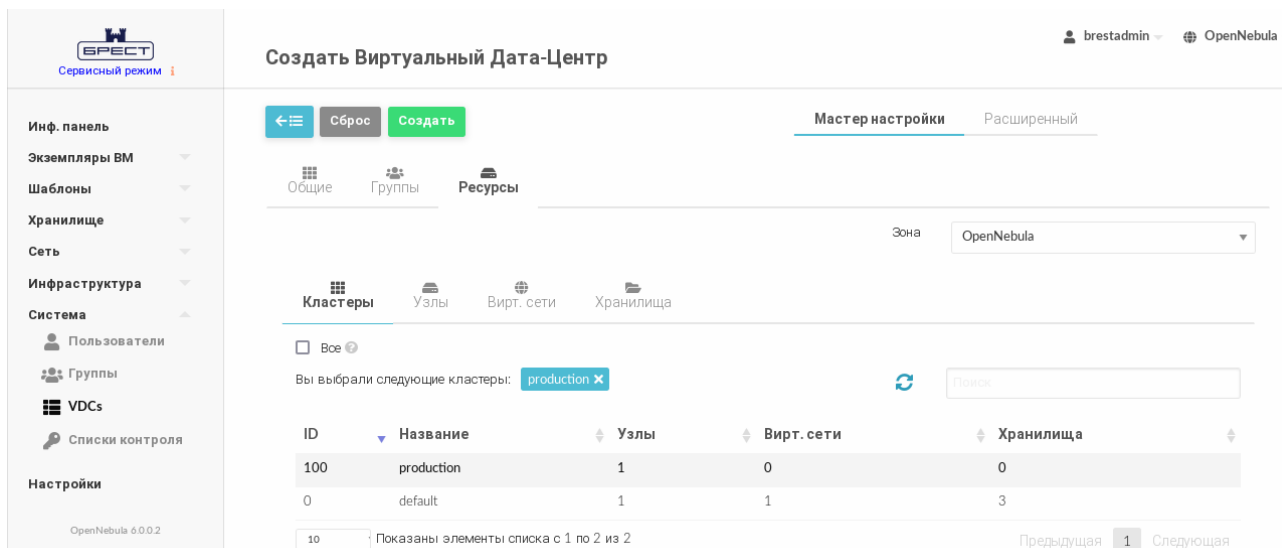


Рис. 11

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. 12).

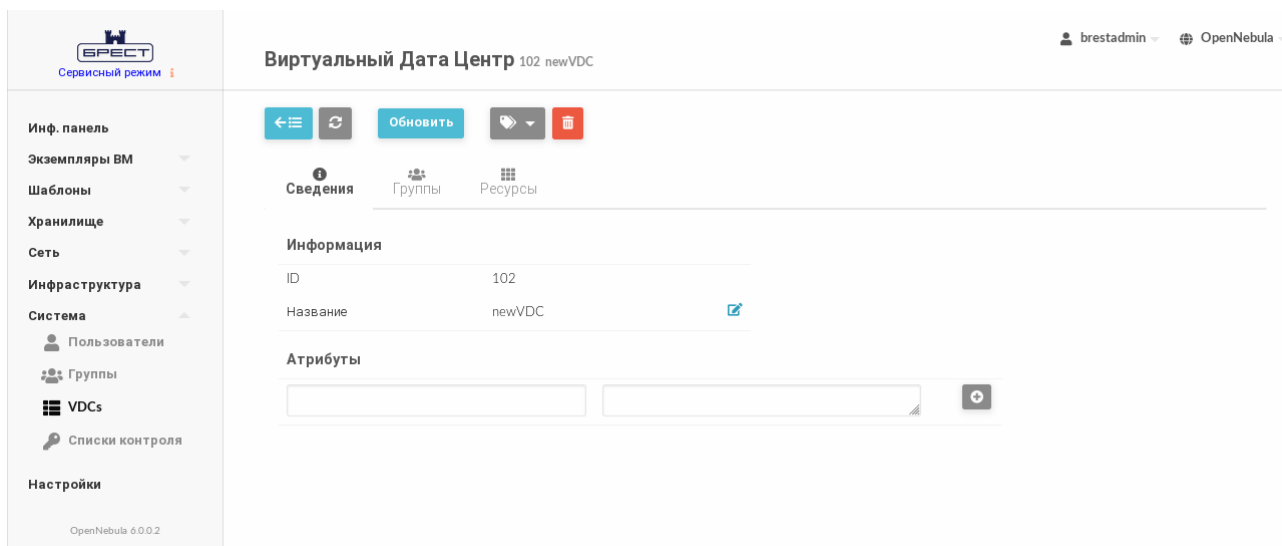


Рис. 12

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

- 1) в меню слева выбрать пункт «Система — VDCs» и на открывшейся странице «Виртуальные Дата Центры» выбрать необходимый VDC;
- 2) на открывшейся странице «Виртуальный Дата Центр» нажать на кнопку **[Обновить]**;
- 3) на странице «Виртуальный Дата Центр»:
 - а) во вкладке «Общие» изменить наименование VDC,
 - б) во вкладке «Группы» выделить необходимые группы пользователей для включения в VDC (если необходимо исключить группу — снять выделение),
 - в) во вкладке «Ресурсы» указать физические вычислительные ресурсы, которые необходимо зарегистрировать в VDC (если необходимо исключить ресурс — снять выделение);

ВНИМАНИЕ! Для того чтобы указать сервер виртуализации, сеть или хранилище из состава определенного кластера, предварительно необходимо выделить этот кластер во вкладке «Ресурсы» в секции «Кластеры» (см. рис. 11)
- 4) на странице «Виртуальный Дата Центр» нажать на кнопку **[Обновить]**.

3.5. Управление полномочиями

3.5.1. Общие сведения

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

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

Указанные выше полномочия могут быть применены в отношении следующих ресур-

сов:

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

3.5.2. Управление полномочиями в интерфейсе командной строки

3.5.2.1. Просмотр и изменение установленных полномочий для ресурса

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

Пример

Просмотр установленных полномочий шаблона с идентификатором 0

```
onetemplate show 0
```

Пример вывода после выполнения команды:

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

```
PERMISSIONS
```

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

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

3.5.2.2. Изменение установленных полномочий для ресурса

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

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

В качестве числового кода полномочий используется трехзначное восьмеричное

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

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

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

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

Примеры:

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

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

2. Установка полномочий в отношении шаблона с идентификатором 0:

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

Для этого необходимо выполнить команду:

```
onetemplate chmod 0 664
```

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

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

3. Установка полномочий в отношении шаблона с идентификатором 0:

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

Для этого необходимо выполнить команду:

```
onetemplate chmod 0 644
```

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

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

4. Установка полномочий в отношении шаблона с идентификатором 0:

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

Для этого необходимо выполнить команду:

```
onetemplate chmod 0 607
```

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

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

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

Таблица 2

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 ресурса, необходимо перейти на страницу этого ресурса (вкладка «Сведения»).

Пример

Просмотр установленных полномочий шаблона с идентификатором 0 (см. рис. 13).

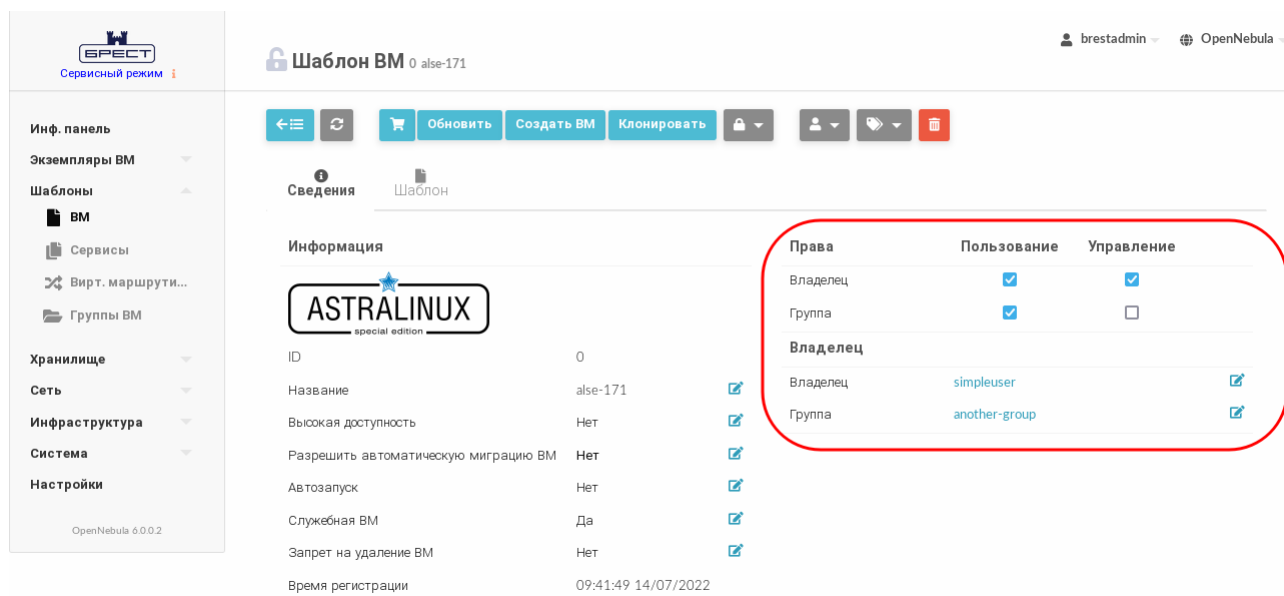


Рис. 13

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

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

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 «Система — Пользователи»;

2) на открывшейся странице «Пользователи» выбрать необходимого пользователя;
 3) на открывшейся странице пользователя во вкладке «Сведения» в секции «Атрибуты» (см. рис. 14) выполнить следующие действия:

- а) в левом поле ввести наименование атрибута: «umask»,
- б) в правом поле указать трехзначную восьмеричную маску (см. 3.5.2.3),
- в) нажать на кнопку [+].

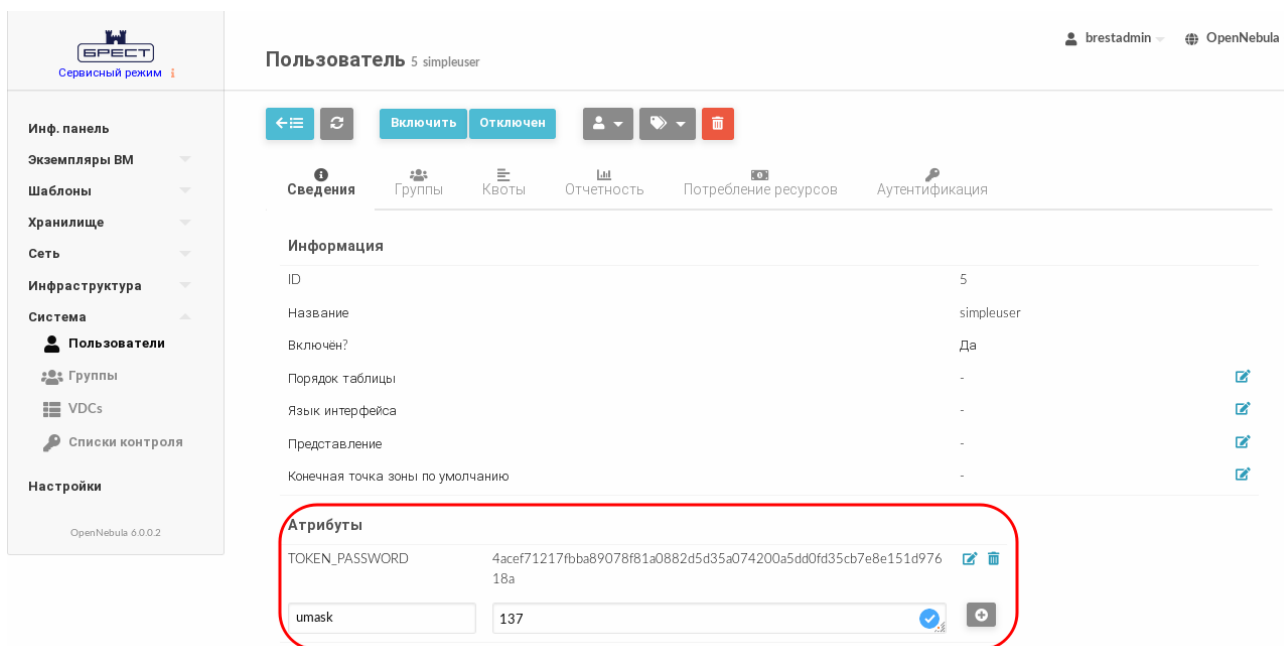


Рис. 14

3.5.4. Управление полномочиями в отношении экземпляра VM

Полномочиями в отношении экземпляра VM управляет владелец — администратор VM. Администратор VM может открыть общий доступ к экземпляру VM для других пользователей, разрешить им просматривать и использовать VM. Для этого можно воспользоваться командой `onevm chmod` или веб-интерфейсом ПК СВ.

Примеры:

1. Исходное состояние, пример вывода после выполнения команды

```
onevm show 0:
```

```
...
```

```
PERMISSIONS
```

```
OWNER           : um-
```

```
GROUP           : u--
```

```
OTHER           : ---
```

В представленном примере в отношении экземпляра VM с идентификатором 0 владелец имеет полномочия типа USE и MANAGE. Пользователи в группе, которой принадлежит владелец, имеют полномочия типа USE, а пользователи, которые не

являются владельцами или не состоят в группе, не имеют полномочий в отношении данного шаблона.

2. Установка полномочий в отношении экземпляра VM с идентификатором 0:

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

Для этого необходимо выполнить команду:

```
onevm chmod 0 664
```

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

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

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 служба сервера управления может предоставить доступ или отклонить запрос.

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

Следует иметь в виду, что правила ACL представляют собой сложный механизм управления. При администрировании и управлении полномочиями необходимо руководствоваться правилами ролевого управления доступом, изложенными в документе РДЦП.10001-07 97 01.

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 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 ресурса;
- 3) @<идентификатор_группы> — для группы которой принадлежит ресурс;
- 4) * — для всех ресурсов.

Примеры:

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

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

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

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

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

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

4. Правило дает полномочия пользователям группы с идентификатором 106 выполнять развертывание VM на серверах виртуализации, 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: пользователи группы brestadmins (администраторы ПК СВ) имеют право выполнять любую операцию.

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

Пример

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

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

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

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

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

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 условные сокращения существующих типов ресурсов. В каждом правиле указываются следующие условные сокращения типов ресурсов, к которым оно применяется:
 - V – VM
 - H – HOST
 - N – NET
 - I – IMAGE
 - U – USER
 - T – TEMPLATE
 - G – GROUP
 - D – DATASTORE
 - C – CLUSTER
 - O – DOCUMENT
 - Z – ZONE
 - S – SECURITY GROUP
 - v – VDC
 - R – VROUTER
 - M – MARKETPLACE
 - A – MARKETPLACEAPP
 - P – VMGROUP
 - t – VNTEMPLATE
- в столбце RID указан идентификатор объекта;
- в столбце Operations перечислены сокращения допустимых операций:
 - U – USE
 - M – MANAGE
 - A – ADMIN
 - C – CREATE
- в столбце Zone указаны зоны, в которых действует правило. Это может быть идентификатор отдельной зоны или всех зон.

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

Для того чтобы создать правило ACL, необходимо выполнить команду:

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

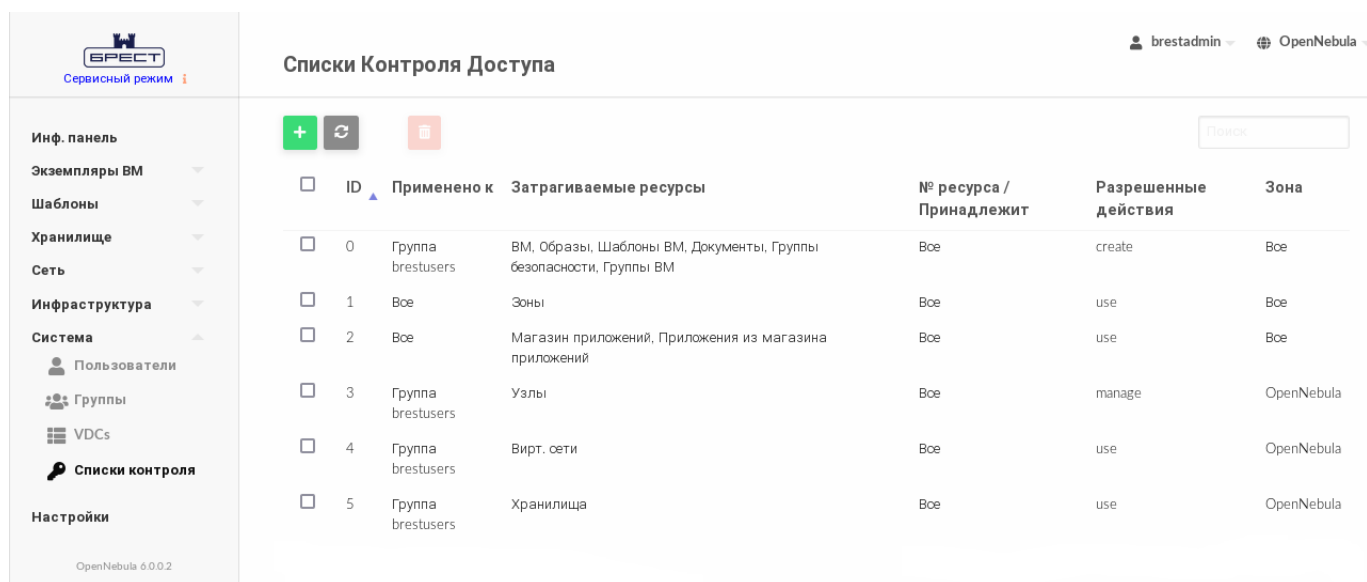
Для удаления правила ACL, необходимо выполнить команду:

`oneacl delete <идентификатор_правила>`

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

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 «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. 15).



<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. 15

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

- 1) в меню слева выбрать пункт «Система — Списки контроля» и на открывшейся странице «Списки Контроля Доступа» нажать на кнопку **[+]**;
- 2) на открывшейся странице «Создать правило контроля» (см. рис. 16):
 - 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. 16

3) на странице «Создать правило контроля» в поле Строка, задающая правило проверить корректность сформированного правила и нажать на кнопку **[Создать]**; После этого на открывшейся странице «Списки Контроля Доступа» появится запись о созданном правиле ACL.

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

- 1) в меню слева выбрать пункт «Система — Списки контроля»;
- 2) на открывшейся странице «Списки Контроля Доступа» выбрать правила, которые необходимо удалить и нажать на кнопку **[Удалить]**;
- 3) в открывшемся окне «Удалить» нажать на кнопку **[ОК]**.

3.6.5. Использование правил ACL для реализации роли разработчика ВМ

Для реализации роли разработчика ВМ необходимо выполнить следующие действия:

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

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

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

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

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

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

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

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

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


4. УПРАВЛЕНИЕ ЭКЗЕМПЛЯРАМИ VM

4.1. Статус и жизненный цикл виртуальной машины

В процессе функционирования экземпляру VM присваивается один из статусов, описание которых приведено в таблице 3.

Таблица 3

Статус	Сокращенное название статуса	Описание
INIT	init	Внутренний статус инициализации после создания VM, этот статус не виден пользователям
PENDING	pend	Ожидается выделение ресурсов виртуализации для запуска VM. VM остается в этом статусе, пока не будет развернута планировщиком или пользователем при помощи команды <code>onevm deploy</code>
HOLD	hold	Владелец поставил VM на удержание, она не доступна для развертывания в автоматическом режиме, пока не будет разблокирована. Однако ее можно развернуть вручную
ACTIVE	см. таблицу 4	VM запущена и находится в одном из состояний жизненного цикла (см. таблицу 4)
STOPPED	stop	VM остановлена. Снимок состояния VM (файл <code>checkpoint</code>) было сохранен и перенесен вместе с образами дисков в хранилище образов. Ресурсы сервера виртуализации (ЦПУ и память) освобождаются
SUSPENDED	susp	Аналогично статусу STOPPED, но снимок состояния VM (файл <code>checkpoint</code>) и образы дисков остаются на сервере виртуализации, чтобы позже возобновить на нем работу VM (т.е. нет необходимости перепланировать VM). Ресурсы сервера виртуализации (ЦПУ и память) не освобождаются
DONE	done	VM удалена. VM в этом статусе отображается при использовании команды <code>onevm list</code> , но информация о VM останется в БД. Информацию о удаленной VM можно получить с помощью команды <code>onevm show</code>
POWEROFF	poff	Аналогичен статусу SUSPENDED, но снимок состояния VM (файл <code>checkpoint</code>) не сохраняется. Образы дисков остаются на сервере виртуализации для последующего запуска VM. Ресурсы сервера виртуализации (ЦПУ и память) не освобождаются. VM получает этот статус после завершения работы гостевой ОС, установленной на этой VM
UNDEPLOYED	unde	VM выключена. Аналогичен статусу STOPPED, но снимок состояния VM (файл <code>checkpoint</code>) не сохраняется. Образы дисков переносятся в хранилище образов. VM может быть запущена позже. Ресурсы сервера виртуализации (ЦПУ и память) освобождаются

Окончание таблицы 3

Статус	Сокращенное название статуса	Описание
CLONING	clon	ВМ ожидает завершения операции клонирования образов дисков (хотя бы один образ диска все еще находится в состоянии lock)
CLONING_FAILURE	fail	В процессе клонирования ВМ произошла ошибка (хотя бы один образ диска перешел в состояние error)

После запуска жизненный цикл ВМ включает состояния, приведенные в таблице 4.

Таблица 4

Состояние	Сокращенное название состояния	Описание
LCM_INIT	init	ВМ находится в состоянии инициализации, этот внутренний статус и не виден пользователям
PROLOG	prol	Происходит перенос файлов ВМ (образы диска и файл checkpoint) на сервер виртуализации, на котором ВМ будет запущена
BOOT	boot	ПК СВ ожидает, пока сервер виртуализации создаст ВМ
RUNNING	runn	ВМ находится в работе (данное состояние включает фазы загрузки и отключения ВМ). Состояние ВМ контролируется драйвером виртуализации
MIGRATE	migr	ВМ мигрирует с одного сервера виртуализации на другой без выключения
SAVE_STOP	save	Система сохраняет файлы ВМ после завершения какой-либо операции
SAVE_SUSPEND	save	Система сохраняет файлы ВМ после приостановки какой-либо операции
SAVE_MIGRATE	save	Система сохраняет файлы ВМ для «холодной» миграции (перемещение выключенных ВМ)
PROLOG_MIGRATE	migr	Передача файлов во время «холодной» миграции (перемещение выключенных ВМ)
PROLOG_RESUME	prol	Передача файлов после возобновления действия (связан с статусом STOPPED)
EPILOG_STOP	epil	Передача файлов в хранилище образов

Продолжение таблицы 4

Состояние	Сокращенное название состояния	Описание
EPILOG	epil	Система очищает сервер виртуализации, который использовался для запуска VM, кроме того, образы постоянных дисков перемещаются обратно в хранилище образов
SHUTDOWN	shut	Система отправила сигнал ACPI для выключения VM и ожидает, пока процесс выключения завершится. Если по истечении времени ожидания VM не выключится, система будет считать, что ОС виртуальной машины проигнорировала сигнал ACPI, а статус VM изменится на RUNNING вместо DONE
CLEANUP_RESUBMIT	clea	Очистка после действия удаления/восстановления VM
UNKNOWN	unkn	Не удалось определить статус VM, она находится в неизвестном состоянии
HOTPLUG	hotp	Выполняется операция подключения/отсоединения диска
SHUTDOWN_POWEROFF	shut	Система отправила на VM сигнал ACPI о завершении работы и ожидает его выполнения. Если за время ожидания VM не исчезнет, система будет считать, что ОС виртуальной машины проигнорировала сигнал ACPI, и статус VM будет изменен на RUNNING, вместо POWEROFF
BOOT_UNKNOWN	boot	Система ожидает, пока сервер виртуализации создаст VM (связан с статусом UNKNOWN)
BOOT_POWEROFF	boot	Система ожидает, пока сервер виртуализации создаст VM (связан с статусом POWEROFF)
BOOT_SUSPENDED	boot	Система ожидает, пока сервер виртуализации создаст VM (связан с статусом SUSPENDED)
BOOT_STOPPED	boot	Система ожидает, пока сервер виртуализации создаст VM (связан с статусом STOPPED)
CLEANUP_DELETE	clea	Очистка после действия удаления
HOTPLUG_SNAPSHOT	snap	Выполняется снимок состояния

Продолжение таблицы 4

Состояние	Сокращенное название состояния	Описание
HOTPLUG_NIC	hotp	Выполняется операция подключения/отсоединения сетевого интерфейса
HOTPLUG_SAVEAS	hotp	Выполняется операция сохранения на диске
HOTPLUG_SAVEAS_POWEROFF	hotp	Выполняется операция сохранения на диске (связан с статусом POWEROFF)
HOTPLUG_SAVEAS_SUSPENDED	hotp	Выполняется операция сохранения на диске (связан с статусом SUSPENDED)
SHUTDOWN_UNDEPLOY	shut	Система отправила на VM сигнал ACPI для завершения работы и ожидает его выполнения. Если за время ожидания VM не будет удалена, система будет считать, что ОС виртуальной машины проигнорировала сигнал ACPI, и статус VM будет изменен на RUNNING, вместо UNDEPLOYED
EPILOG_UNDEPLOY	epil	Система очищает сервер виртуализации, который использовался для запуска VM, кроме того, образы постоянных дисков перемещаются обратно в хранилище образов
PROLOG_UNDEPLOY	prol	Передача файлов после возобновления действия (связан с статусом UNDEPLOY)
BOOT_UNDEPLOY	boot	Система ожидает, пока сервер виртуализации создаст VM (связан с статусом UNDEPLOY)
HOTPLUG_PROLOG_POWEROFF	hotp	Передача файлов для подключения к диску при отключении питания
HOTPLUG_EPILOG_POWEROFF	hotp	Передача файлов при отсоединении диска от источника питания
BOOT_MIGRATE	boot	Система ожидает, пока сервер виртуализации создаст VM (в результате «холодной» миграции)
BOOT_FAILURE	fail	Сбой при переводе в состояние BOOT
BOOT_MIGRATE_FAILURE	fail	Сбой при переводе в состояние BOOT_MIGRATE
PROLOG_MIGRATE_FAILURE	fail	Сбой при переводе в состояние PROLOG_MIGRATE
PROLOG_FAILURE	fail	Сбой при переводе в состояние PROLOG
EPILOG_FAILURE	fail	Сбой при переводе в состояние EPILOG

Продолжение таблицы 4

Состояние	Сокращенное название состояния	Описание
EPILOG_STOP_FAILURE	fail	Сбой при переводе в состояние EPILOG_STOP
EPILOG_UNDEPLOY_FAILURE	fail	Сбой при переводе в состояние EPILOG_UNDEPLOY
PROLOG_MIGRATE_POWEROFF	migr	Передача файлов во время «холодной» миграции (связан с статусом POWEROFF)
PROLOG_MIGRATE_POWEROFF_FAILURE	fail	Сбой при переводе в состояние PROLOG_MIGRATE_POWEROFF
PROLOG_MIGRATE_SUSPEND	migr	Передача файлов во время «холодной» миграции (связан с статусом SUSPEND)
PROLOG_MIGRATE_SUSPEND_FAILURE	fail	Сбой при переводе в состояние PROLOG_MIGRATE_SUSPEND
BOOT_UNDEPLOY_FAILURE	fail	Сбой при переводе в состояние BOOT_UNDEPLOY
BOOT_STOPPED_FAILURE	fail	Сбой при переводе в состояние BOOT_STOPPED
PROLOG_RESUME_FAILURE	fail	Сбой при переводе в состояние PROLOG_RESUME
PROLOG_UNDEPLOY_FAILURE	fail	Сбой при переводе в состояние PROLOG_UNDEPLOY
DISK_SNAPSHOT_POWEROFF	snap	Выполняется снимок состояния диска (связан с статусом POWEROFF)
DISK_SNAPSHOT_REVERT_POWEROFF	snap	Выполняется восстановление снимка состояния диска (связан с статусом POWEROFF)
DISK_SNAPSHOT_DELETE_POWEROFF	snap	Выполняется удаление снимка состояния диска (связан с статусом POWEROFF)
DISK_SNAPSHOT_SUSPENDED	snap	Выполняется снимок состояния диска (связан с статусом SUSPENDED)
DISK_SNAPSHOT_REVERT_SUSPENDED	snap	Выполняется восстановление снимка состояния диска (связан с статусом SUSPENDED)
DISK_SNAPSHOT_DELETE_SUSPENDED	snap	Выполняется удаление снимка состояния диска (связан с статусом SUSPENDED)
DISK_SNAPSHOT	snap	Выполняется снимок состояния диска (связан с статусом RUNNING)
DISK_SNAPSHOT_DELETE	snap	Выполняется удаление снимка состояния диска (связан с статусом RUNNING)

Окончание таблицы 4

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

Информацию о том, какой статус (параметр «STATE») имеет ВМ и в каком состоянии (параметр «LCM_STATE») она находится, можно получить выполнив команду `onevm show` (см. 4.2.1) или в веб-интерфейсе ПК СВ на странице ВМ во вкладке «Сведения» (см. 4.3.1).

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

4.2. Управление экземплярами ВМ в интерфейсе командной строки

4.2.1. Отображение существующих ВМ

Для отображения существующих ВМ необходимо использовать команду `onevm list`.

Пример вывода после выполнения команды:

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

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

Для просмотра полной информации о ВМ необходимо использовать команду:

```
onevm show <идентификатор_ВМ>
```

Пример вывода после выполнения команды `onevm show 1`:

VIRTUAL MACHINE 1 INFORMATION

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

VIRTUAL MACHINE MONITORING

```
ID                : 1
TIMESTAMP         : 1658214069
```

PERMISSIONS

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

4.2.2. Удаление экземпляров VM

Удаление 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, сервер виртуализации 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. ОС виртуальной машины игнорирует сигналы

ACPI, служба сервера управления снова присвоит VM статус RUNNING.

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

4.2.3. 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 том числе выделенные ресурсы, сохраняется на задействованном сервере виртуализации. При возобновлении работы приостановленной VM выполняется ее незамедлительное развертывание на том же сервере виртуализации;
- `onevm poweroff` — долгосрочная приостановка: корректно выключает электропитание работающей VM, отправляя сигнал ACPI, при этом состояние VM не сохраняется. Возобновление работы VM осуществляется на том же сервере виртуализации. 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 сервера виртуализации, которые использовала VM, будут освобождены, а сервер виртуализации очищен. Любой диск будет сохранен в хранилище образов. Следующие команды применяются при необходимости сохранить выделенные ресурсы сети и памяти, например, IP-адреса, постоянные образы диска:

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

4.2.4. Запуск экземпляров ВМ

Чтобы возобновить работу ВМ при успешной остановки или приостановки их работы, а также запустить ВМ, развертывание которых было отменено или электропитание которых было отключено, необходимо выполнить команду:

```
onevm resume <идентификатор_ВМ>
```

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

4.2.5. 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.

4.2.6. 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 `onemplate 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.

4.3. Управление экземплярами ВМ в веб-интерфейсе ПК СВ

4.3.1. Отображение существующих ВМ

Для отображения существующих ВМ в веб-интерфейсе ПК СВ необходимо в меню слева выбрать пункт «Экземпляры ВМ — ВМ». На открывшейся странице «ВМ» будет отображена таблица экземпляров ВМ (см. рис. 17)

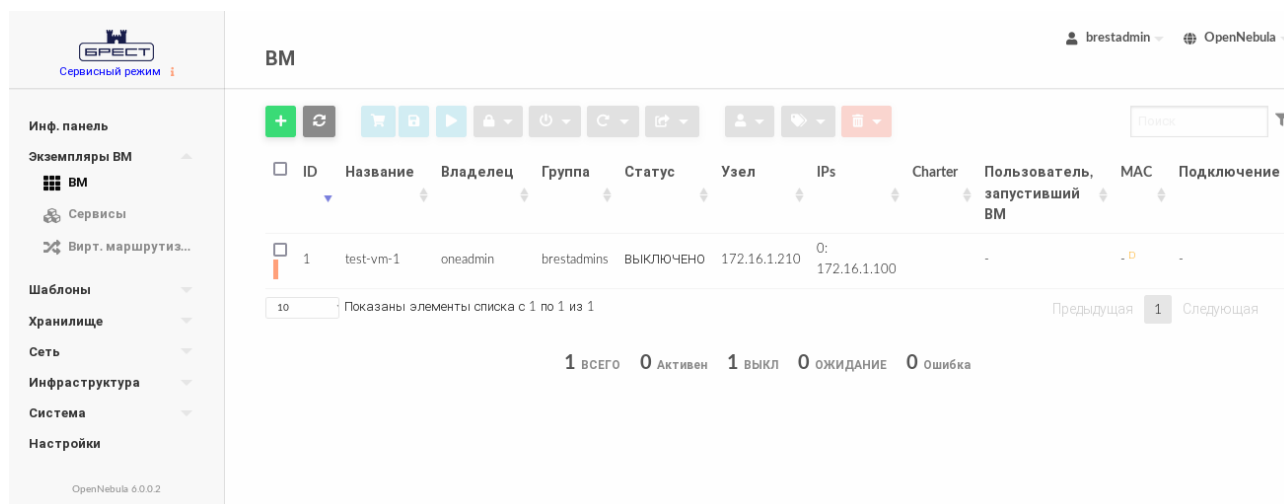


Рис. 17

Для просмотра полной информации о VM необходимо на странице «VM» выбрать необходимую VM. После этого откроется страница виртуальной машины (вкладка «Сведения») (см. рис. 18).

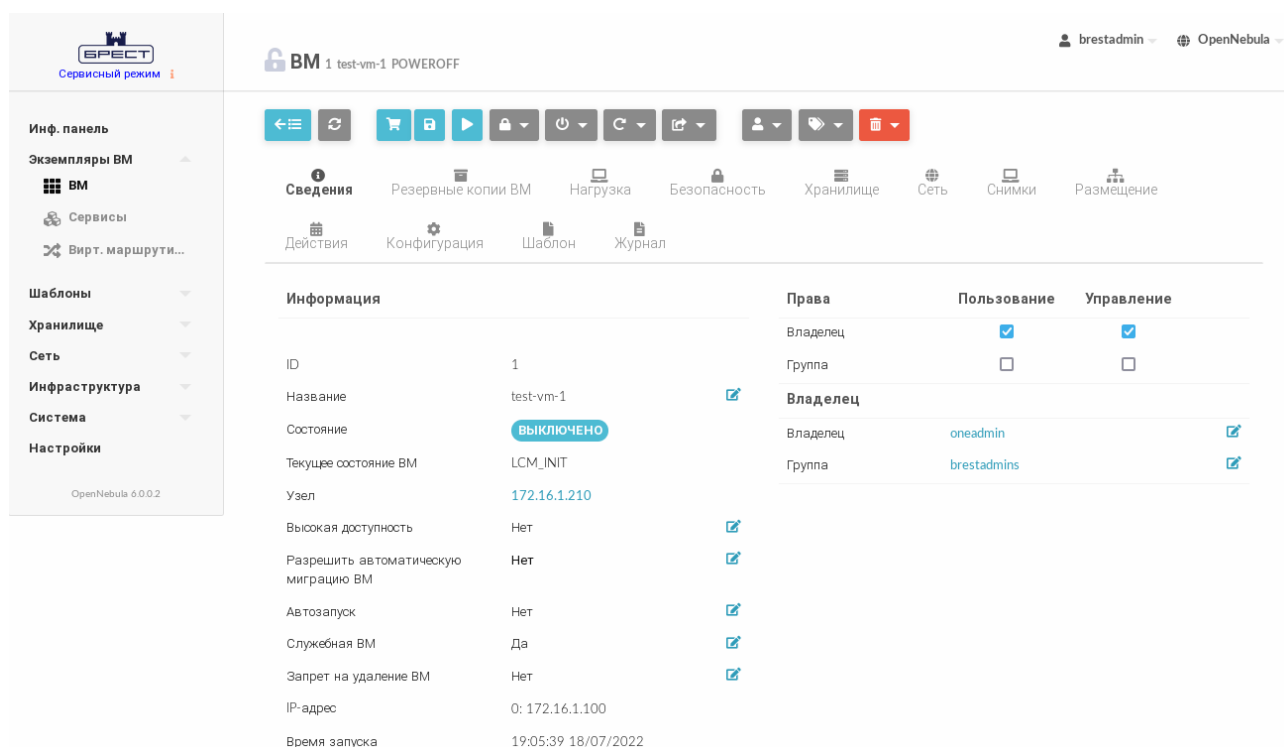


Рис. 18

4.3.2. 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. 19):

- Приостановить работу VM — краткосрочная приостановка: состояние VM, в том числе выделенные ресурсы, сохраняются на задействованном сервере вир-

туализации. При возобновлении работы приостановленной VM выполняется ее незамедлительное развертывание на том же сервере виртуализации;

- 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 сервере виртуализации;
- Отключить питание — долгосрочная приостановка: корректно выключает работающую VM, отправляя сигнал ACPI, при этом состояние VM не сохраняется. Возобновление работы VM осуществляется на том же сервере виртуализации;
- 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 сервере виртуализации;
- Отменить размещение жестко — аналогично команде Отменить размещение, но работающая VM удаляется незамедлительно.

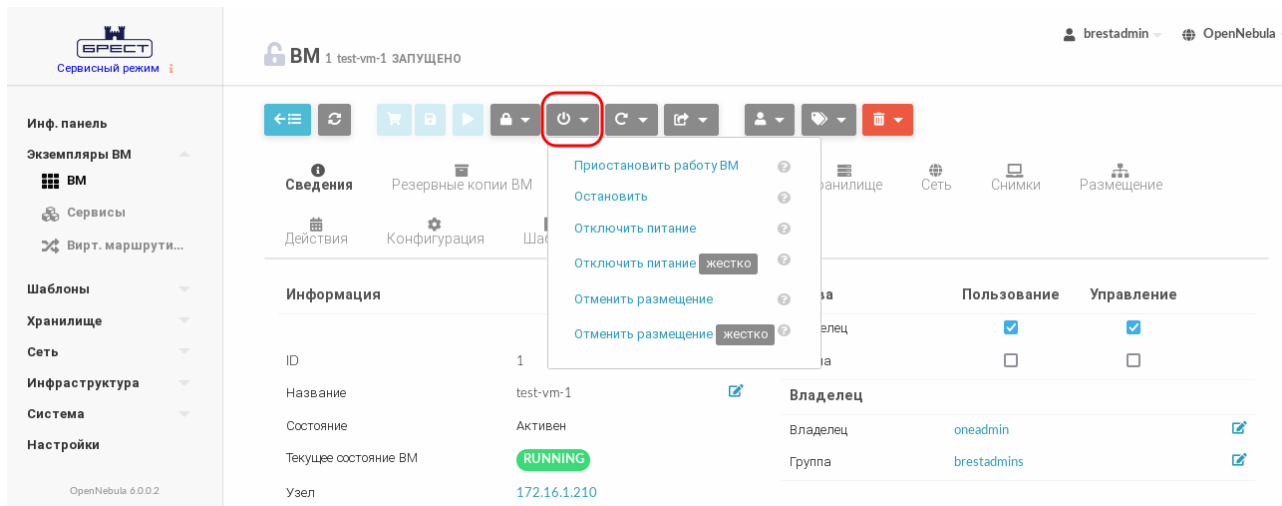


Рис. 19

4.3.3. Запуск экземпляра VM

Чтобы возобновить работу VM после успешной остановки или приостановки ее работы, а также запустить VM, развертывание которой было отменено или электропитание которых было отключено, необходимо нажать на кнопку **[Запустить]** (см. рис. 20):



Рис. 20

4.3.4. Перезагрузка экземпляров ВМ

Для перезагрузки ВМ в веб-интерфейсе ПК СВ используется кнопка **[Перезагрузка]**, после нажатия на которую откроется меню действий (см. рис. 21):

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

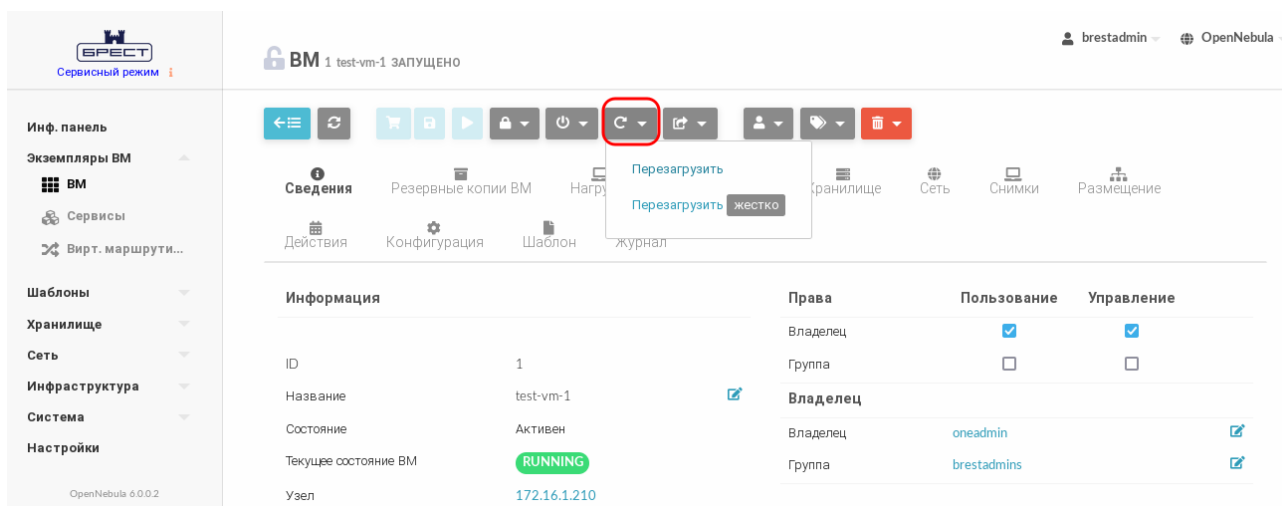


Рис. 21

4.3.5. Отсрочка развертывания экземпляров ВМ

Для управления блокировкой ВМ в веб-интерфейсе ПК СВ используется кнопка **[Блокировка]**, после нажатия на которую откроется меню действий (см. рис. 22):

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

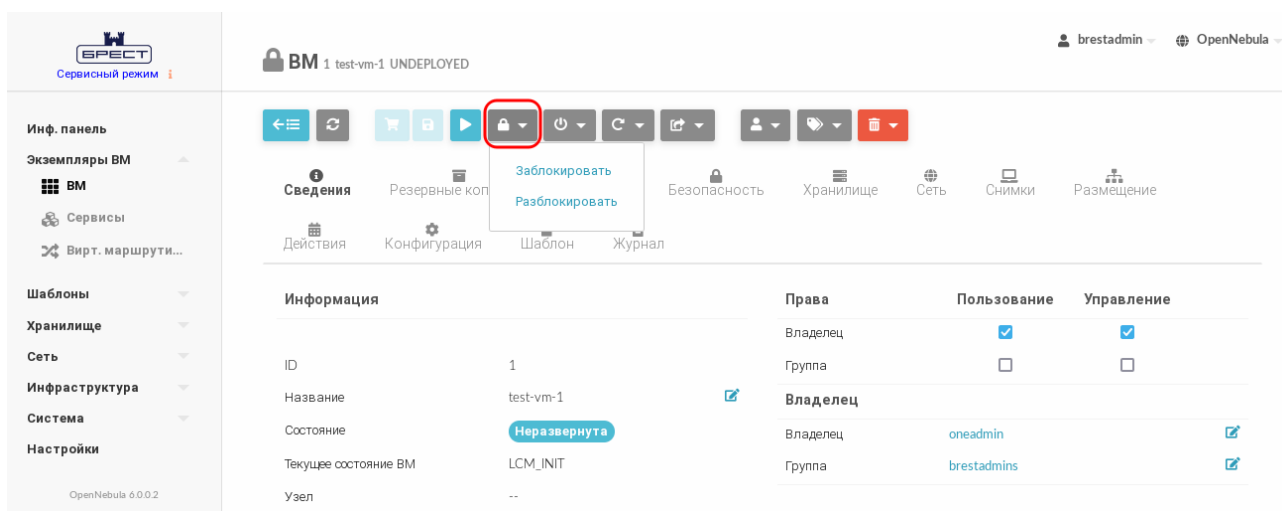


Рис. 22

4.3.6. Удаление экземпляров VM

Для удаления экземпляров VM в веб-интерфейсе ПК СВ используется кнопка **[Уничтожить]**, после нажатия на которую откроется меню действий (см. рис. 23):

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

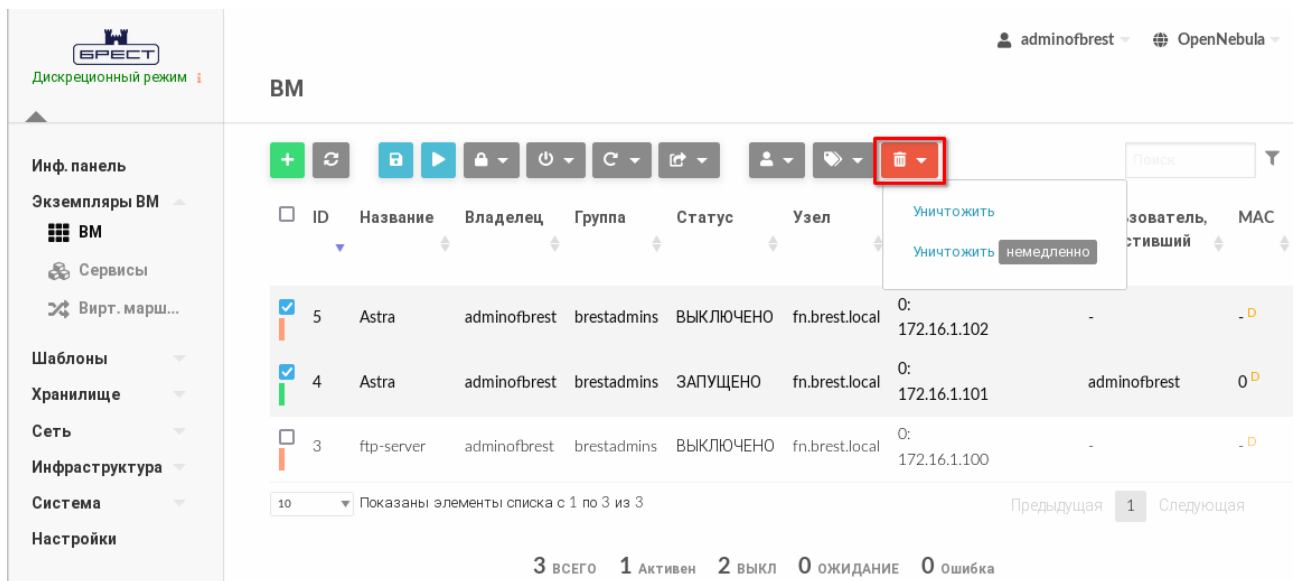


Рис. 23

4.4. Управление доступом виртуальных машин к физическому и виртуальному оборудованию

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

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

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

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


```
apt install brest-vdi-tools
```
- 2) в веб-интерфейсе ПК СВ на странице 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. 24),

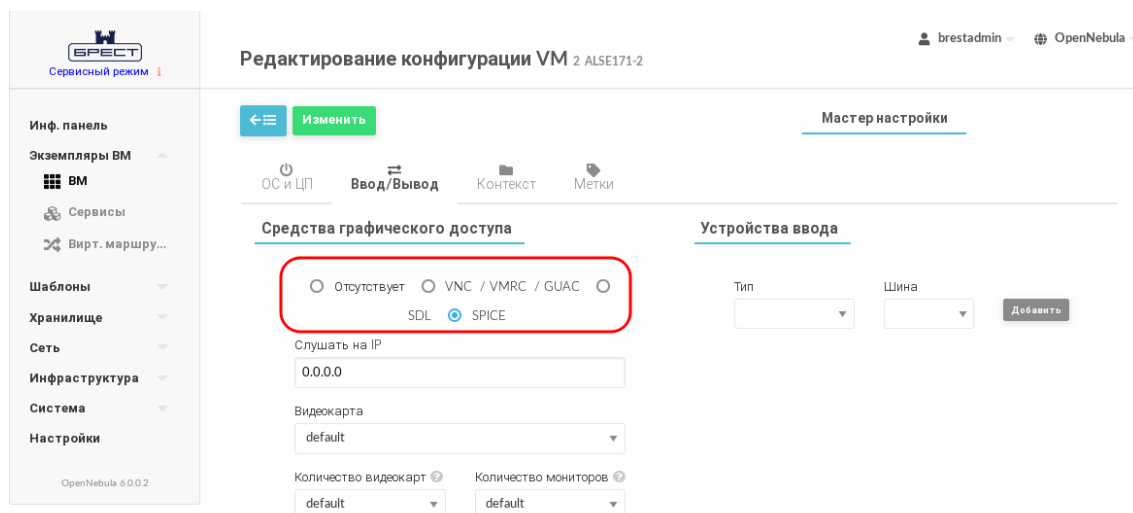


Рис. 24

- при выборе RDP — во вкладке «ОС и ЦП» в секции «Особенности» в выпадающем списке «Гостевой агент Qemu» выбрать «Да» (см. рис. 25),

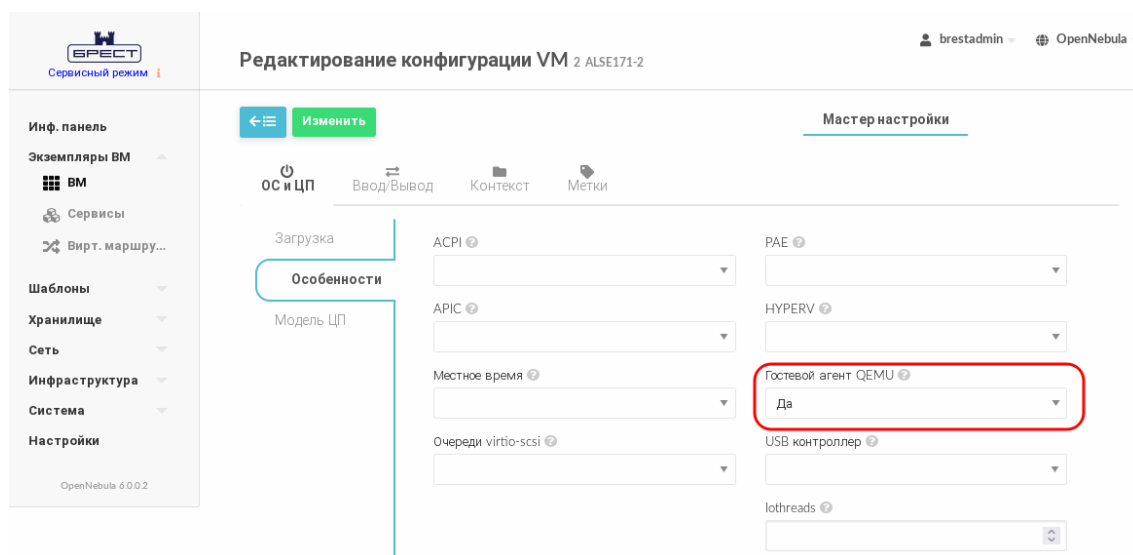


Рис. 25

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

«Особенности» в выпадающем списке «USB контроллер» выбрать «3.0» (см. рис. 25),

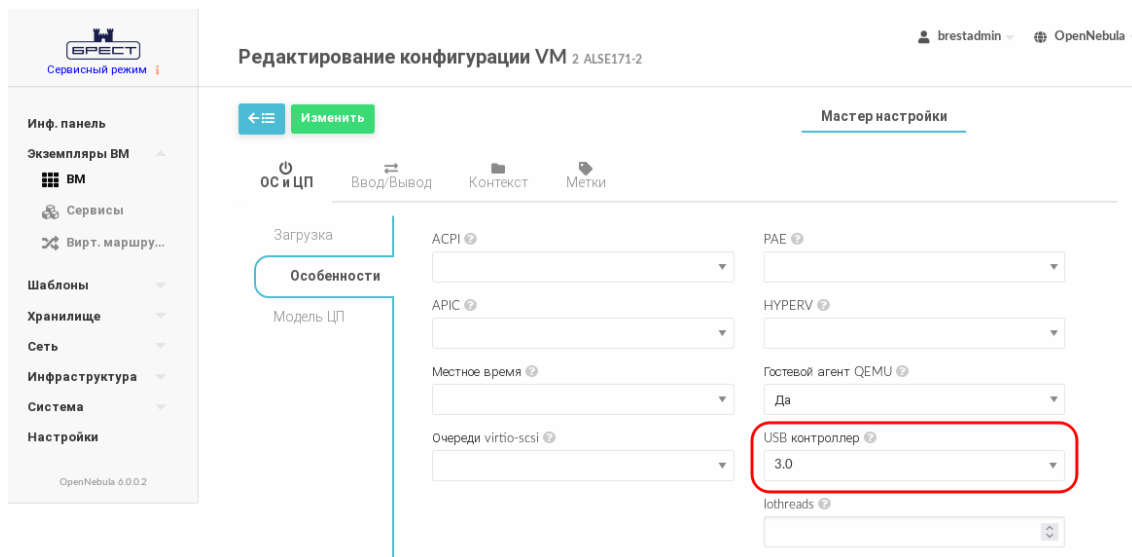


Рис. 26

- 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 сервер управления ПК СВ.

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

1) через графический интерфейс запустить приложение (права администратора не требуются): «Пуск — Сеть — Brest Usb Redirect» (см. рис. 27).

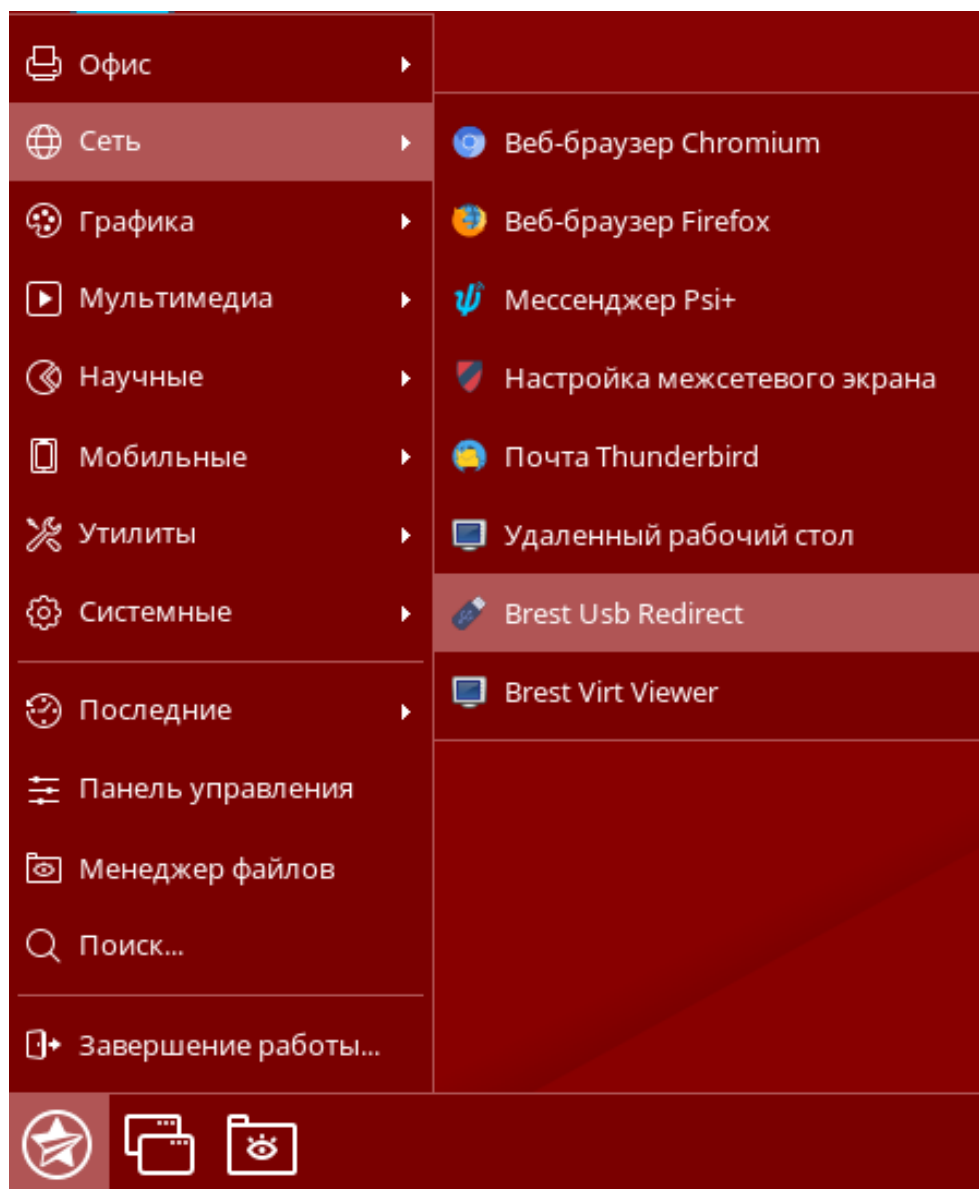
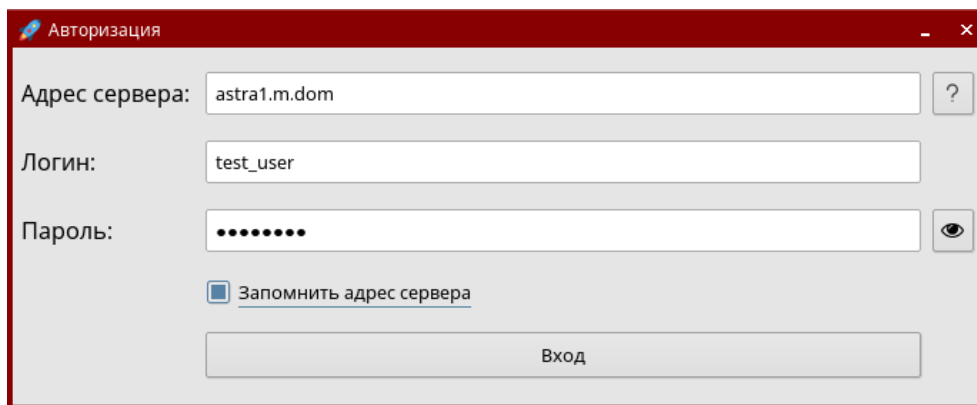


Рис. 27

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

2) в открывшемся окне «Авторизация» (см. рис. 28) указать авторизационные параметры для доступа к виртуальной машине, на которую необходимо перенаправить USB-устройство:

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



Адрес сервера: astra1.m.dom

Логин: test_user

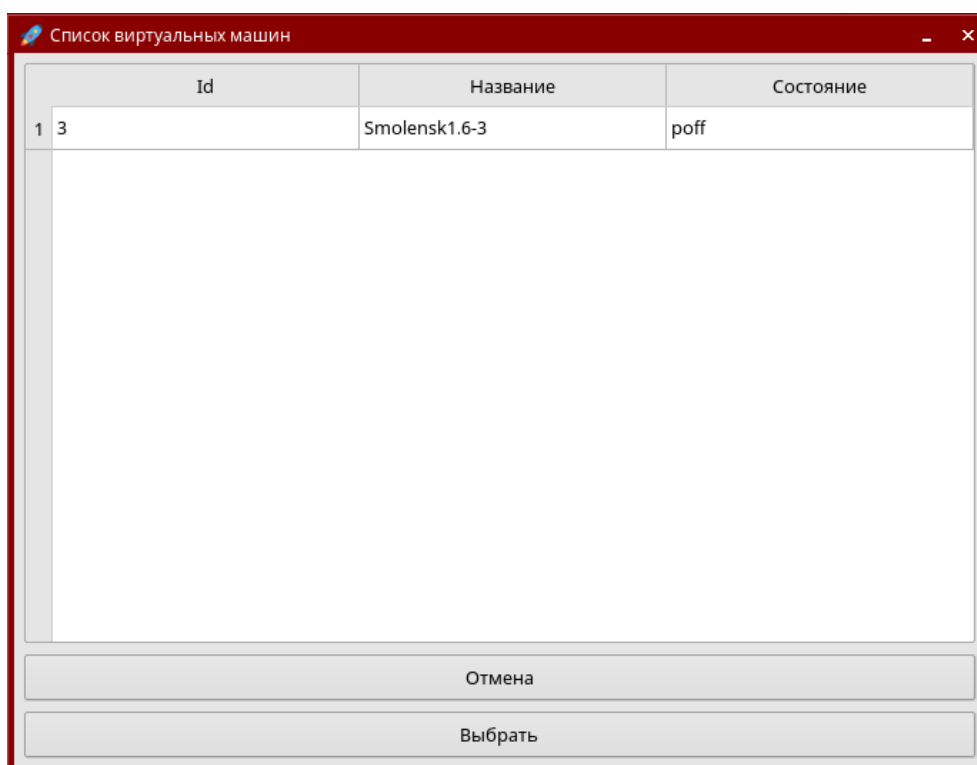
Пароль:

Запомнить адрес сервера

Вход

Рис. 28

3) в открывшемся окне «Список виртуальных машин» (см. рис. 29) указать виртуальную машину, на которую необходимо перенаправить USB-устройство.



Id	Название	Состояние
1 3	Smolensk1.6-3	poff

Отмена

Выбрать

Рис. 29

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

4) в открывшемся окне «Список usb-устройств» (см. рис. 30) выбрать одно или несколько USB-устройств, которые необходимо перенаправить;

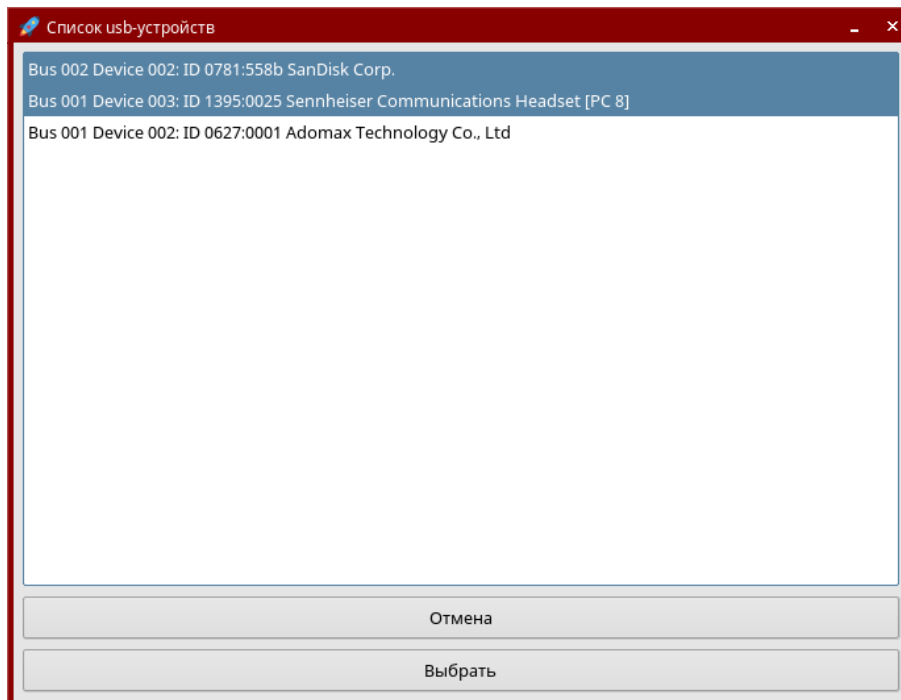


Рис. 30

5) в открывшемся окне «Доступные подключения» (см. рис. 31) выбрать протокол подключения;

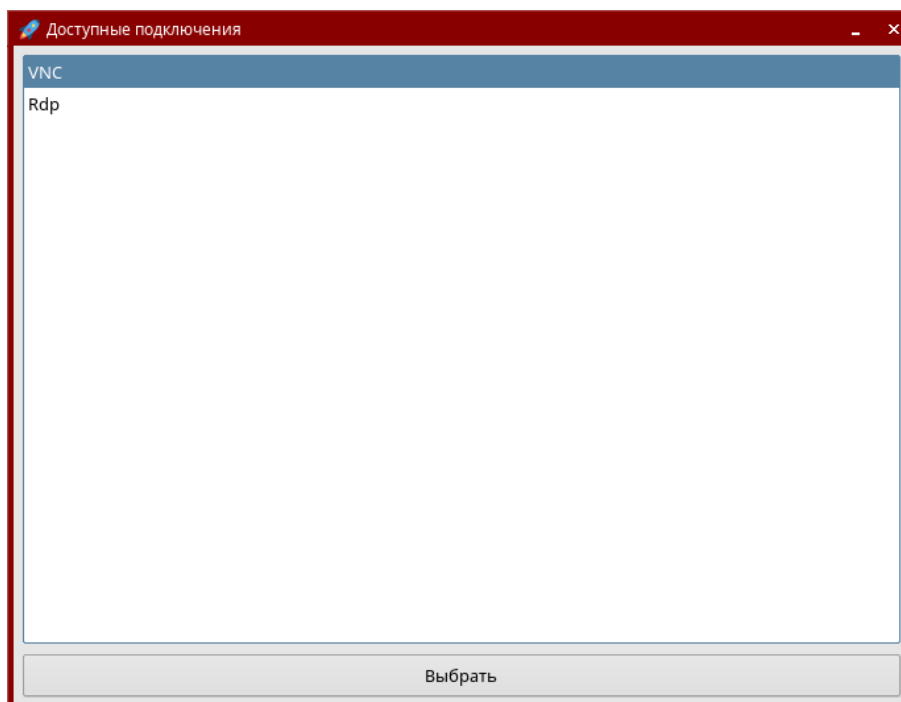


Рис. 31

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

```
lsusb
```

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

USB-устройство (см. рис. 32).

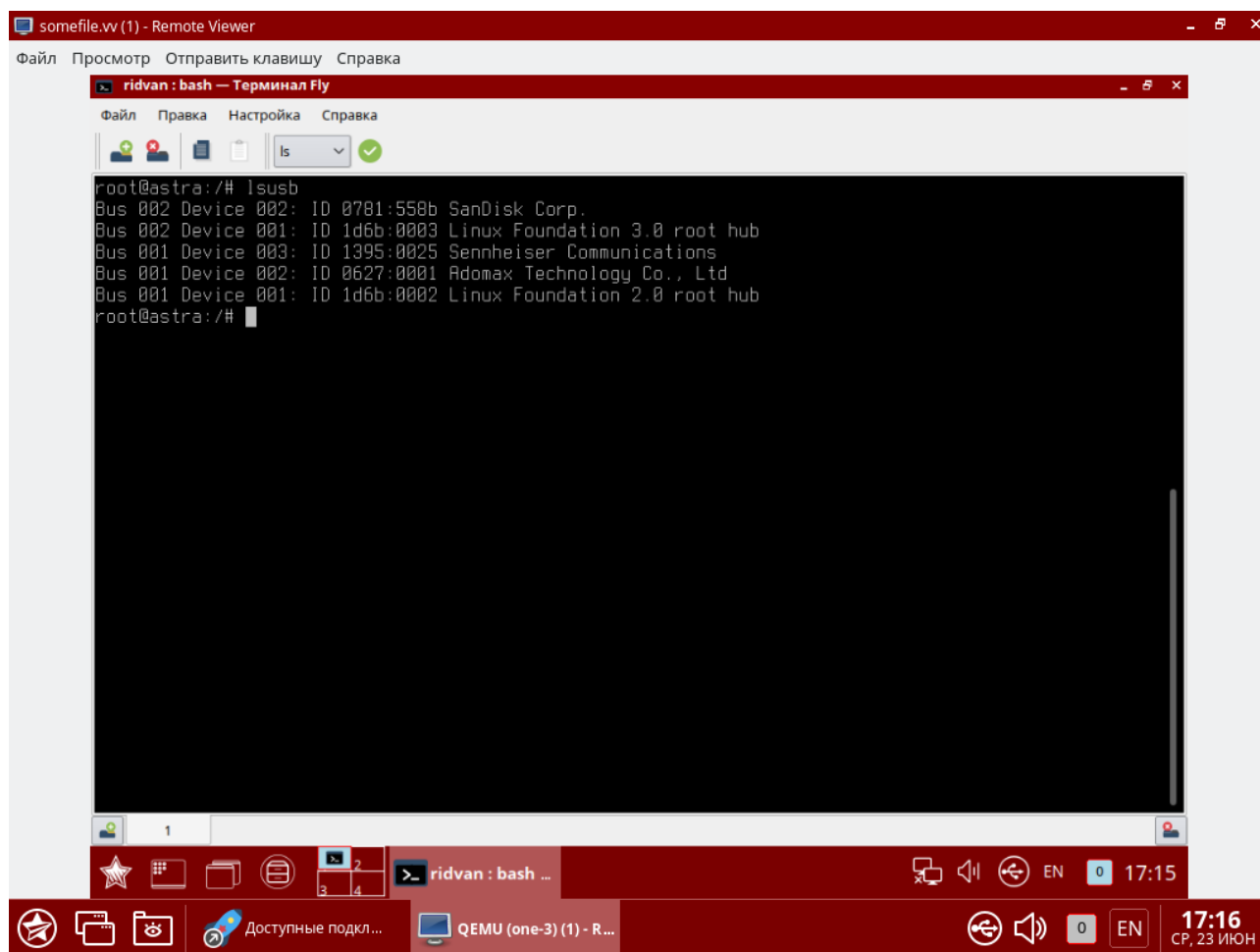


Рис. 32

4.4.2. Ретрансляция PCI

Устройства PCI серверов виртуализации можно перенаправлять на виртуальные машины.

4.4.2.1. Требования

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

4.4.2.2. Настройка сервера виртуализации

4.4.2.3. Конфигурация ядра

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

```
intel_iommu=on
```

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

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

Указанные выше параметры необходимо добавить в конфигурационный файл `/etc/default/GRUB_CMDLINE_LINUX_DEFAULT="intel_iommu=on rd.driver.pre=vfio-pci rd.driver.blacklist=nouveau"`

4.4.2.4. Загрузка драйвера `vfio` в `initrd`

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

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

```
pci_stub
vfio
vfio_iommu_type1
vfio_pci
vfio_virqfd
```

2) выполнить команду:

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

4.4.2.5. Блокировка драйверов

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

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

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

```
lspci -nn
```

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

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

4.4.2.6. Привязка устройств к `vfio`

Механизм ввода/вывода MMU разделяет устройства PCI на группы для изолирования работы памяти между устройствами и ВМ. Для добавления устройств PCI в `vfio` и назначения им группы можно использовать совместно используемые скрипты.

Пример

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

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

Необходимо сделать этот скрипт исполняемым.

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

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

Приведенный в примере выше скрипт необходимо добавить в автостарт системы.

Для этого следует выполнить следующие действия:

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

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

- 2) перезагрузить список служб командой:

```
sudo systemctl daemon-reload
```

- 3) добавить службу `vfio-bind` в автозагрузку командой:

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

4.4.2.7. Конфигурация qemu

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

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

Пример

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

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

4.4.2.8. Настройка драйвера

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

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

4.4.2.9. Настройка использования устройств PCI

Основным действием по настройке является просмотр информации о сервере виртуализации в интерфейсе командной строки или в веб-интерфейсе ПК СВ, обнаружение доступных устройств PCI и добавление желаемого устройства в шаблон. Устройства PCI можно добавлять, указывая значения параметров `vendor` (производитель), `device` (устройство) и `class` (класс). В ПК СВ виртуальная машина будет развернута только на сервере виртуализации с имеющимся устройством PCI. Если таких серверов виртуализации нет, в журнале планировщика появится сообщение об ошибке.

В интерфейсе командной строки перечень доступных устройств PCI на сервере

виртуализации (секция PCI DEVICES) можно просмотреть командой:

```
onehost show <идентификатор_сервера_виртуализации>
```

Пример

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

```
PCI DEVICES

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

где:

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

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

```
PCI = [
  VENDOR = "8086",
  DEVICE = "0a0c",
  CLASS = "0403"
]
```

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

```
PCI = [
```

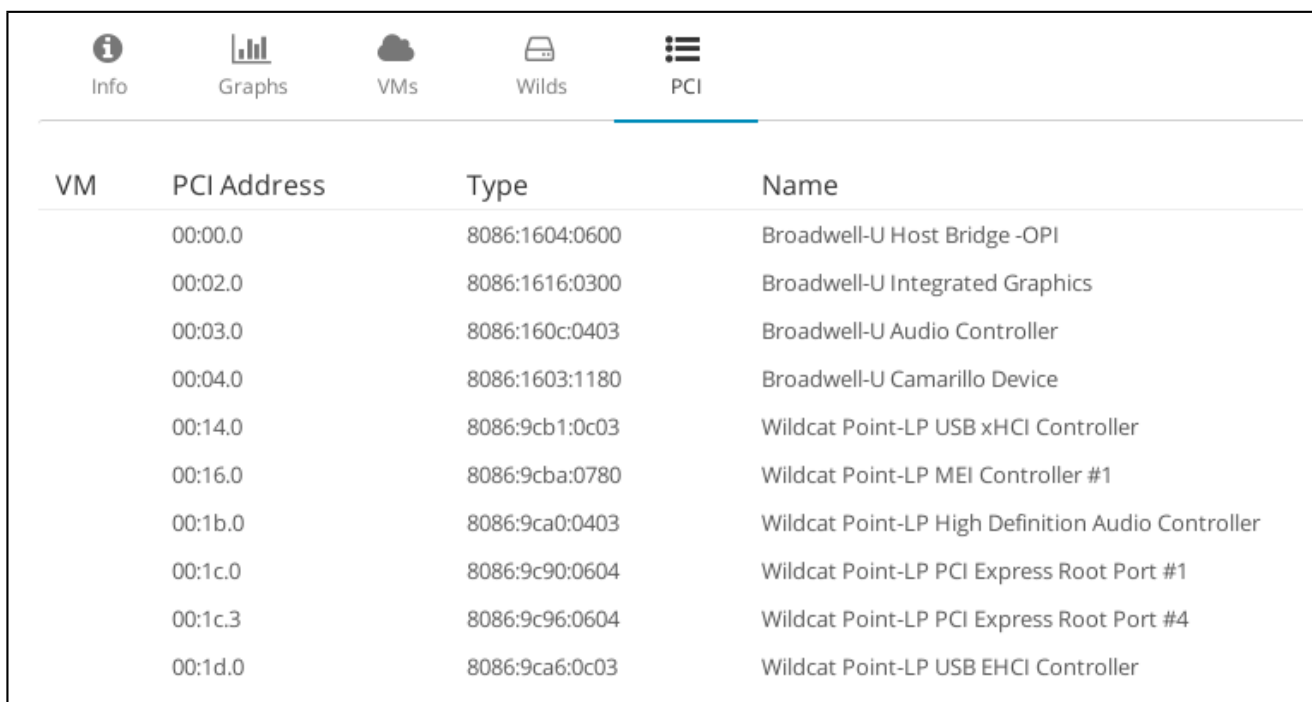
```
CLASS = "0604"
```

```
]
```

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

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

- 1) в меню слева выбрать пункт меню «Инфраструктура — Узлы»;
- 2) на открывшейся странице «Узлы» открыть вкладку «PCI» (см. рис. 33)



VM	PCI Address	Type	Name
	00:00.0	8086:1604:0600	Broadwell-U Host Bridge -OPI
	00:02.0	8086:1616:0300	Broadwell-U Integrated Graphics
	00:03.0	8086:160c:0403	Broadwell-U Audio Controller
	00:04.0	8086:1603:1180	Broadwell-U Camarillo Device
	00:14.0	8086:9cb1:0c03	Wildcat Point-LP USB xHCI Controller
	00:16.0	8086:9cba:0780	Wildcat Point-LP MEI Controller #1
	00:1b.0	8086:9ca0:0403	Wildcat Point-LP High Definition Audio Controller
	00:1c.0	8086:9c90:0604	Wildcat Point-LP PCI Express Root Port #1
	00:1c.3	8086:9c96:0604	Wildcat Point-LP PCI Express Root Port #4
	00:1d.0	8086:9ca6:0c03	Wildcat Point-LP USB EHCI Controller

Рис. 33

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

- 1) в меню слева выбрать пункт меню «Шаблоны — VM» и на открывшейся странице «Шаблоны VM» выбрать необходимый шаблон;
- 2) на открывшейся странице «Шаблон VM» нажать на кнопку **[Обновить]**;
- 3) на открывшейся странице «Изменить шаблон VM» открыть вкладку «Ввод/Вывод» (рис. 34).

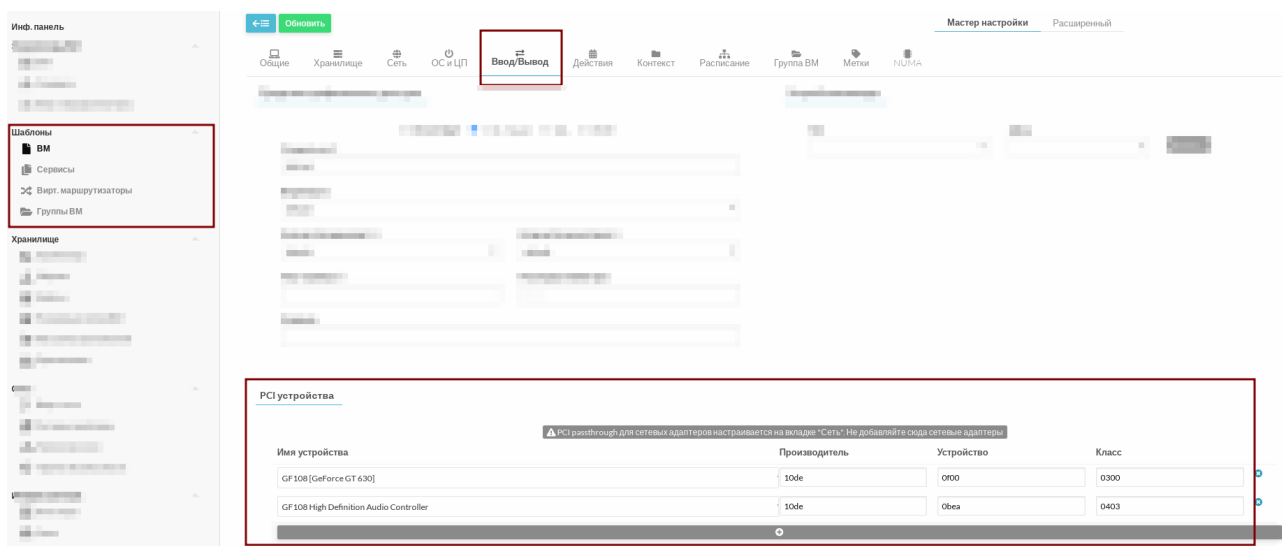


Рис. 34

4.4.3. Горячее подключение образа диска

ВНИМАНИЕ! В ПК СВ возможно подключить только те образы дисков, для эмуляции которых используется драйвер Virtio.

4.4.3.1. 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>`

4.4.3.2. 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 «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. 35);

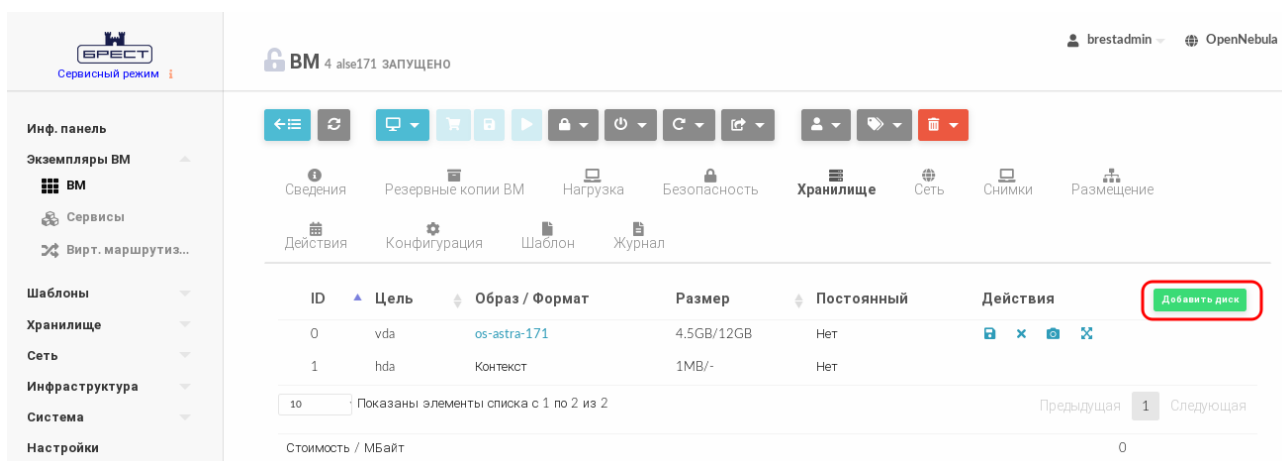


Рис. 35

4) в открывшемся окне «Присоединить диск» указать необходимый образ и нажать на кнопку **[Присоединить]** (см. рис. 36).

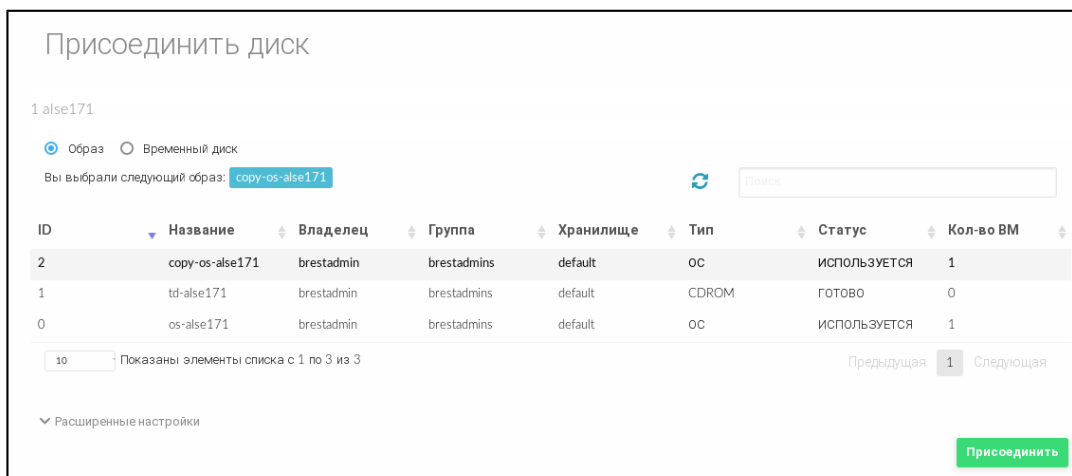


Рис. 36

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

- 1) в меню слева выбрать пункт «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. 37);

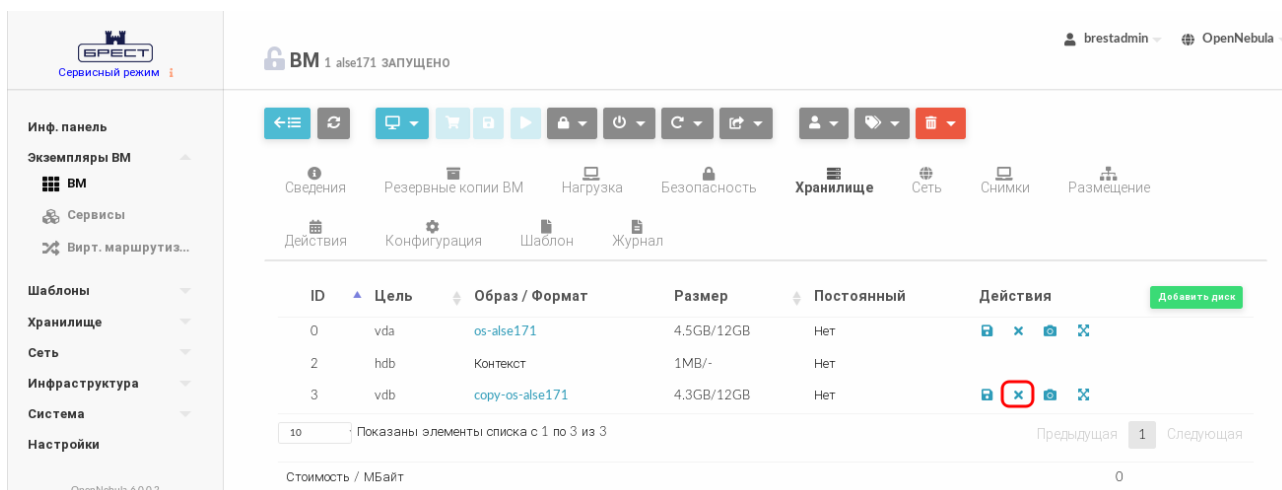


Рис. 37

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

4.4.4. Перераспределение производительности VM

В ПК СВ возможно перераспределить объем вычислительных ресурсов, выделяемых для VM в виде виртуальных ЦП и доли мощности ЦП сервера виртуализации. 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 запущенные службы вручную;
- отключить питание VM;
- перераспределить ресурсы, выделяемые для VM;
- возобновить работу VM с новой производительностью.

4.4.4.1. 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 `alse17` выделить 50% мощности ЦП сервера виртуализации и 2 виртуальных ЦП:

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

4.4.4.2. 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 «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. 38);



Рис. 38

- 4) в открывшемся окне «Изменить базовые характеристики» внести необходимые корректировки и нажать на кнопку **[Изменить]** (см. рис. 39).

Изменить базовые характеристики

1 alse171

Проводить проверку емкости ?

Память ?

3 ГБ

Физический CPU ?

0,25

Виртуальный CPU ?

1

Изменить

Рис. 39

4.4.5. 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.

4.4.5.1. 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 `alse17` и с использованием файла параметров `disk.txt`:

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

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

Пример

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

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

4.4.5.2. 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. 40)

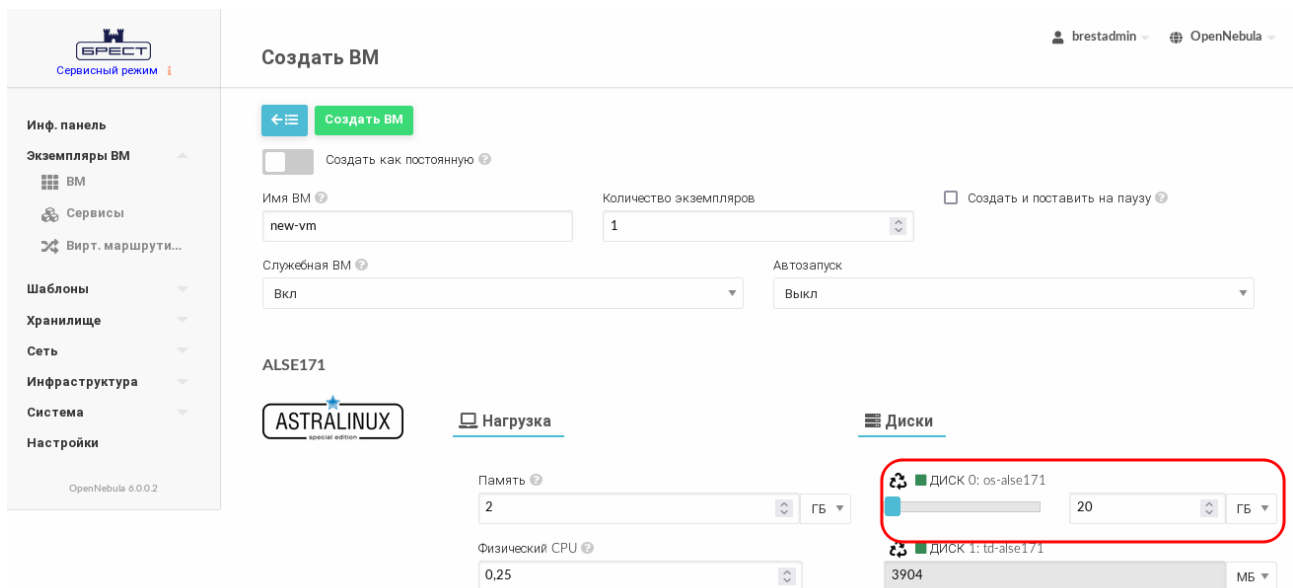


Рис. 40

4.5. Управление квотами

4.5.1. Общие сведения

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

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

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

- занимаемый объем хранилища, чтобы контролировать дисковый ресурс, выделяемой каждому пользователю/группе в каждом хранилище;
- вычислительную мощность, чтобы ограничивать оперативную память, работу центрального процессора или количества экземпляров 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 администратор ПК СВ 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.

4.5.2. Управление квотами в интерфейсе командной строки

4.5.2.1. 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.

4.5.2.2. 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 хранилища. Блок параметров DATASTORE	
ID	Идентификатор хранилища, для которого устанавливается квота
SIZE	Максимальный объем (в МБ), который допускается занимать в хранилище
IMAGE	Максимальное количество образов, которые могут быть созданы в хранилище
Квоты на вычислительную мощность. Блок параметров VM	
VMS	Максимальное количество VM, которые могут быть созданы
MEMORY	Максимальный объем оперативной памяти (в МБ), который могут запросить VM пользователя/группы
CPU	Максимальная производительность ЦП, которую могут запросить VM пользователя/группы
RUNNING VMS	Максимальное количество VM, которое может запустить пользователь/-группа
RUNNING MEMORY	Максимальный объем оперативной памяти (в МБ), выделяемый для запущенных VM пользователя/группы
RUNNING CPU	Максимальная производительность ЦП, выделяемая для запущенных VM пользователя/группы
SYSTEM_DISK_SIZE	Максимальный размер (в МБ) системных дисков, который могут запросить VM пользователя/группы
Квоты на сеть. Блок параметров NETWORK	

Окончание таблицы 5

Параметр	Описание
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

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

Существует два специальных ограничения для каждой квоты:

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

Примеры:

1. Содержание файла шаблона quota.txt:

```

DATASTORE=[
  ID="1",
  IMAGES="-2",
  SIZE="20480"
]
VM=[
  CPU="5",
  MEMORY="2048",
  VMS="4",
  SYSTEM_DISK_SIZE="-1"
]
NETWORK=[
  ID="1",
  LEASES="4"
]
IMAGE=[
  ID="1",
  RVMS="3"
]
IMAGE=[
  ID="2",

```

```
RVMS="-2"
```

```
]
```

В представленном примере:

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

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

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

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

```
oneuser show 5
```

Пример вывода после выполнения команды:

```
USER 5 INFORMATION
```

```
ID                : 5
NAME              : simpleuser
GROUP             : another-group
SECONDARY GROUPS : 1,102
PASSWORD         : simpleuser
AUTH_DRIVER      : public
ENABLED          : Yes
```

```
...
```

```
VMS USAGE & QUOTAS
```

VMS	MEMORY	CPU	SYSTEM_DISK_SIZE
0/4	0M/2G	0.00/5.00	0M/-

```
VMS USAGE & QUOTAS - RUNNING
```

RUNNING VMS	RUNNING MEMORY	RUNNING CPU
0/-	0M/-	0.00/-

```
DATASTORE USAGE & QUOTAS
```

ID	IMAGES	SIZE
1	0/-	0M/20G

NETWORK USAGE & QUOTAS

```
ID    LEASES
1     0/4
```

IMAGE USAGE & QUOTAS

```
ID    RUNNING VMS
1     0/3
2     0/-
```

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

4.5.2.3. 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" ]

```

4.5.2.4. 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 — «..»).

4.5.2.5. 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.

4.5.3. Управление квотами в веб-интерфейсе ПК СВ

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

- 1) в меню слева выбрать пункт «Система — Пользователи»;
- 2) на открывшейся странице «Пользователи» выбрать необходимого пользователя;
- 3) на открывшейся странице пользователя открыть вкладку «Квоты» (см. рис. 41):

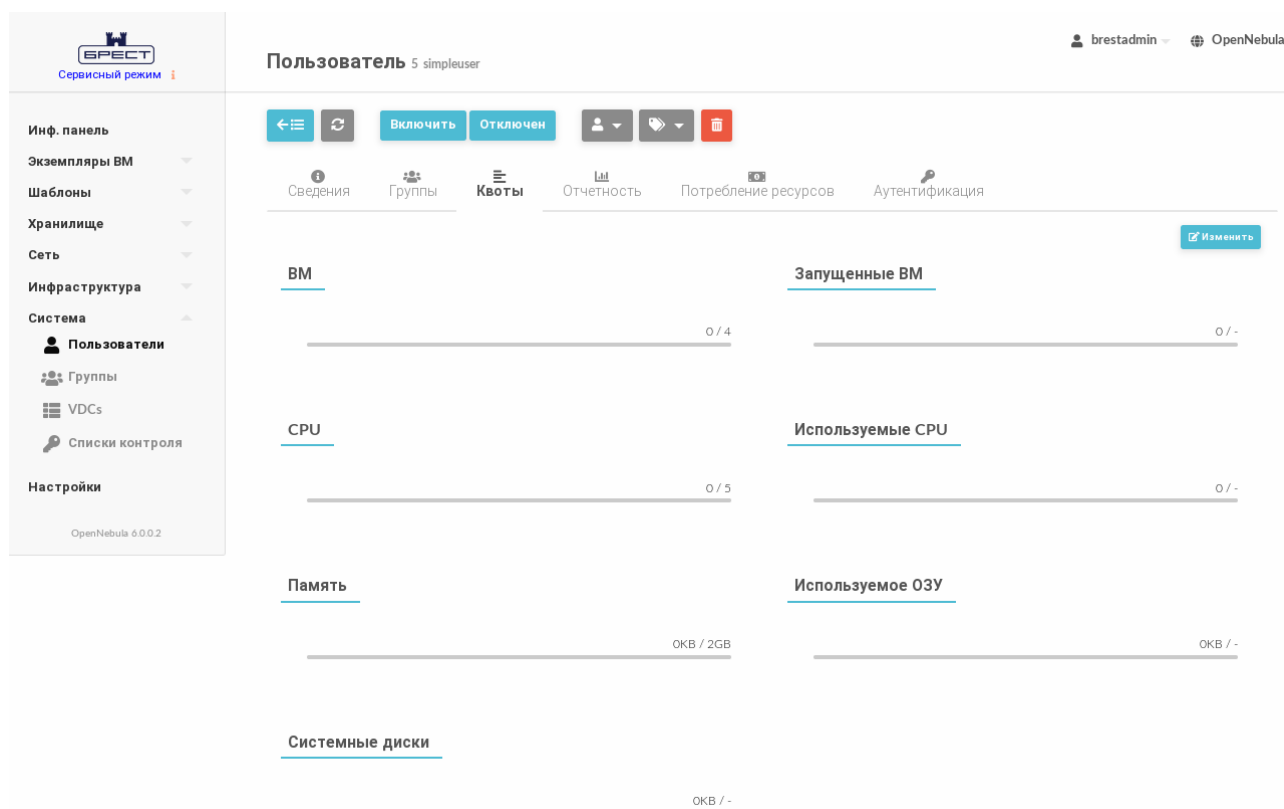


Рис. 41

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

- 1) в меню слева выбрать пункт «Система — Пользователи»;
- 2) на открывшейся странице «Пользователи» выбрать необходимого пользователя;
- 3) на открывшейся странице пользователя открыть вкладку «Квоты» и нажать на кнопку **[Изменить]**;
- 4) на открывшейся странице установить необходимые значения квот и нажать на кнопку **[Применить]**. Для отмены внесенных изменений нажать на кнопку **[Отменить]** (см. рис. 42):

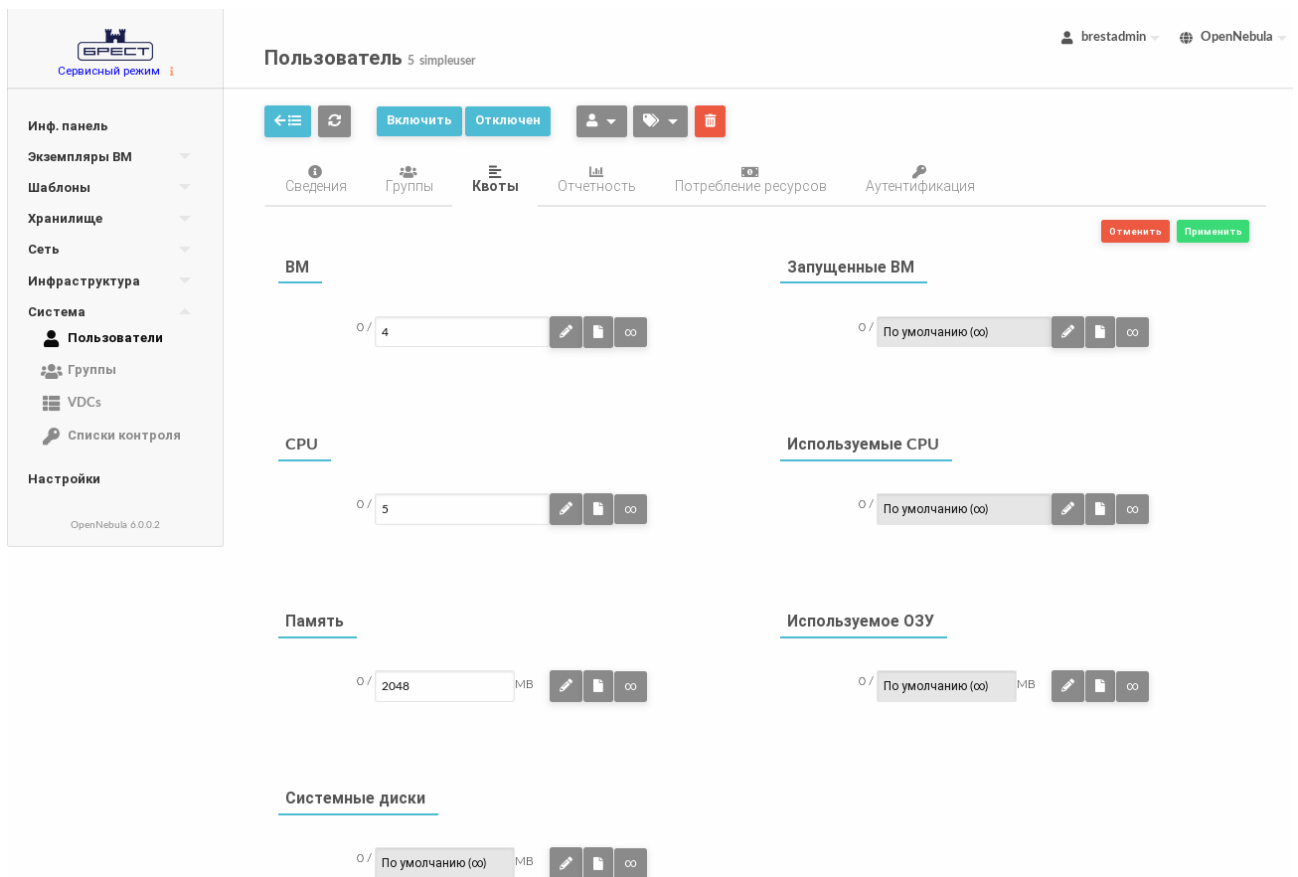


Рис. 42

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

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

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

4.6. Миграция VM между серверами виртуализации

В ПК СВ поддерживается возможность миграции (перемещения) виртуальных машин с одного компьютера, выполняющего функцию сервера виртуализации, на другой. При этом миграция VM возможна как с остановкой, так и без остановки ее работы (при использовании общего хранилища образов).

Управление перемещением виртуальных машин между серверами виртуализации осуществляется администратором ПК СВ.

4.6.1. Перемещение экземпляра VM в интерфейсе командной строки

Для перемещения виртуальных машин используется команда:

```
onevm migrate <идентификатор_VM> <идентификатор_сервера_виртуализации>
```

Если необходимо выполнить миграцию VM без остановки ее работы, то дополнительно необходимо указать следующий аргумент команды: «--live».

Пример

Пример команды для перемещения без остановки работы VM с идентификатором 20 на сервер виртуализации с идентификатором 3:

```
onevm migrate 20 3 --live
```

4.6.2. Перемещение экземпляра VM в веб-интерфейсе ПК СВ

Для перемещения виртуальных машин 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. 43);

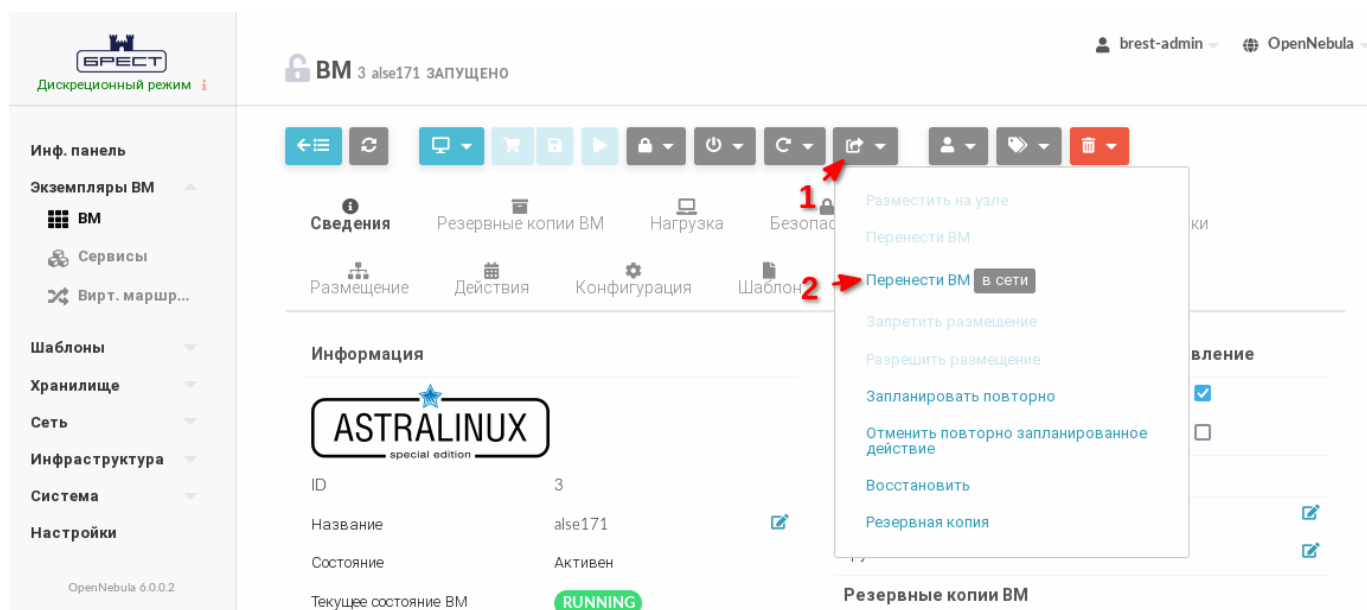


Рис. 43

2) в открывшемся окне «Мигрировать виртуальную машину» следует выполнить следующие шаги:

а) в секции «Выберите Узел» выбрать узел, на который необходимо переместить VM (см. рис. 44),

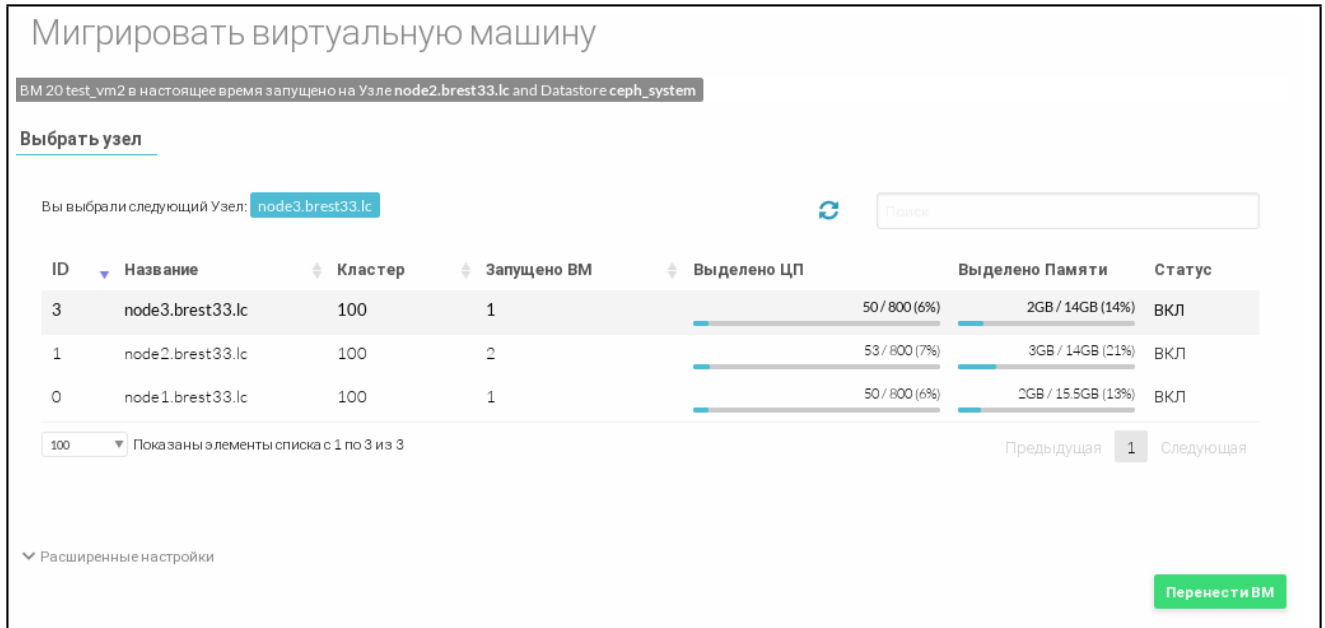


Рис. 44

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

3) в веб-интерфейсе в меню слева выбрать пункт «Экземпляры VM — VM» и дождаться пока в поле «Статус» для перемещаемой VM значение Миграция не изменится на ЗАПУЩЕНО. (см. рис. 45);



Рис. 45

4.7. 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).

4.7.1. 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>
```

4.7.2. 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 «Экземпляры VM — VM»;
- 2) на открывшейся странице «VM» выбрать необходимую виртуальную машину;
- 3) на странице виртуальной машины открыть вкладку «Снимки» (см. рис. 46).

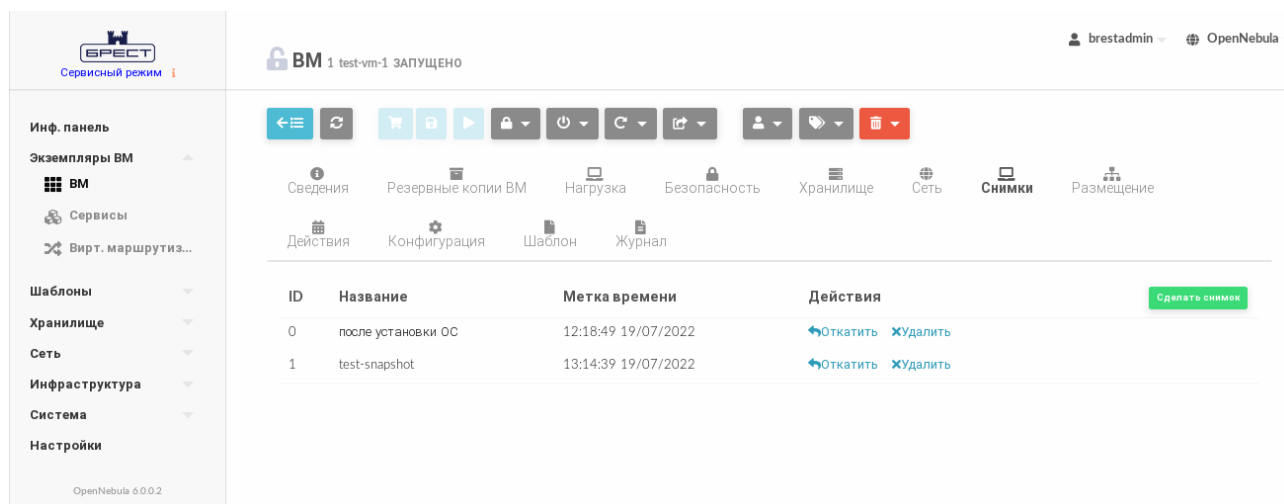


Рис. 46

На странице виртуальной машины во вкладке «Снимки»:

- для создания снимка состояния VM необходимо нажать на кнопку **[Сделать снимок]**;
- 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.

4.8. 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 качестве 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.

4.8.1. 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_ВМ> \  
<идентификатор_диска_ВМ> <идентификатор_снимка>
```

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

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

Для удаления снимка необходимо выполнить команду:

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

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

4.8.2. Управление снимками дисков в веб-интерфейсе ПК СВ

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

- 1) в меню слева выбрать пункт «Экземпляры ВМ — ВМ»;
- 2) на открывшейся странице «ВМ» выбрать необходимую виртуальную машину;
- 3) на странице виртуальной машины открыть вкладку «Хранилище» и в строке необходимого диска нажать на кнопку **[Snapshot]** (см. рис. 47);

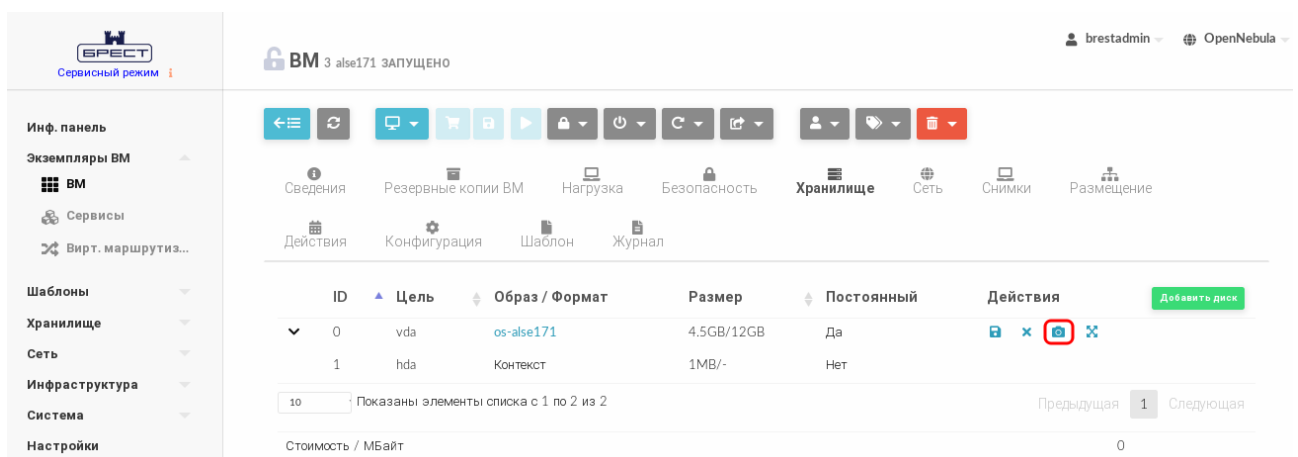


Рис. 47

- 4) в открывшемся окне «Снимок диска» задать наименование снимка и нажать на кнопку **[Сделать снимок]** (см. рис. 48).

Снимок диска

3 alse171

№ диска
0

Название
настройка сети

Сделать снимок

Рис. 48

На странице виртуальной машины во вкладке «Хранилище» (после остановки VM) — см. рис. 49:

- 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]**.

Инф. панель
Сервисный режим

VM 3 alse171 STOPPED

Сведения Резервные копии VM Нагрузка Безопасность Хранилище Сеть Снимки Размещение

Действия Конфигурация Шаблон Журнал

ID	Цель	Образ / Формат	Размер	Постоянный	Действия
0	vda	os-alse171	4.5GB/12GB	Да	Добавить диск

Сохранить как Переименовать Откатить Удалить

<input type="checkbox"/>	0	15:56:48 19/07/2022	-/12GB	после установки ОС
<input checked="" type="checkbox"/>	1	16:24:31 19/07/2022	-/12GB	настройка сети
<input type="checkbox"/>	2	16:28:02 19/07/2022	-/12GB	сетевое имя

Рис. 49

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. УПРАВЛЕНИЕ СЕРВЕРАМИ ВИРТУАЛИЗАЦИИ И КЛАСТЕРАМИ

Установка и инициализация службы сервера виртуализации производятся в соответствии с документом РДЦП.10001-07 95 01-1 «Программный комплекс «Средства виртуализации «Брест». Руководство администратора. Часть 1».

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

Кластеры (Clusters) представляют собой группы серверов виртуализации с общими хранилищами и сетями. Более подробная информация о кластерах приведена в 5.2.

5.1. Серверы виртуализации

5.1.1. Добавление сервера виртуализации

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

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

В 5.1.1.1 — 5.1.1.2 описан процесс регистрации сервера виртуализации в сервисном режиме функционирования ПК СВ.

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

5.1.1.1. Регистрация сервера виртуализации в интерфейсе командной строки

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

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

Процесс регистрации сервера виртуализации занимает от 20 до 60 секунд.

Пример

Регистрация сервера виртуализации с гипервизором KVM:

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

Пример вывода после выполнения команды:

```
ID: 1
```

5.1.1.2. Регистрация сервера виртуализации в веб-интерфейсе ПК СВ

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

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

- 2) на открывшейся странице Создать узел (см. рис. 50):
- а) в поле «Тип» указать тип драйвера виртуализации,
 - б) в поле «Имя хоста» ввести сетевое имя сервера виртуализации,
 - в) в поле «Логин администратора» ввести имя локального администратора компьютера, выполняющем функцию сервера виртуализации,
 - г) в поле «Пароль администратора» ввести пароль локального администратора компьютера, выполняющем функцию сервера виртуализации,
 - д) нажать на кнопку **[Создать]**;

The screenshot shows the 'Создать узел' (Create Node) page in the OpenNebula web interface. The page has a sidebar on the left with navigation options: 'Инф. панель', 'Экземпляры VM', 'Шаблоны', 'Хранилище', 'Сеть', 'Инфраструктура' (with sub-items: 'Кластеры', 'Узлы', 'Зоны'), 'Система', and 'Настройки'. The main content area is titled 'Создать узел' and contains a form with the following fields and controls:

- Buttons: '<=>', 'Сброс', and 'Создать'.
- 'Тип' (Type): A dropdown menu with 'KVM' selected.
- 'Кластер' (Cluster): A dropdown menu with '0: default' selected.
- 'Имя хоста' (Host Name): A text input field.
- 'SSH ключ уже проброшен' (SSH key already scanned): A checkbox that is currently unchecked.
- 'Логин администратора' (Admin Username): A text input field.
- 'Пароль администратора' (Admin Password): A text input field.

The bottom left corner of the interface shows 'OpenNebula 6.0.0.2'.

Рис. 50

- 3) на открывшейся странице «Узлы» появится запись о зарегистрированном сервере виртуализации. Необходимо дождаться пока в столбце Статус для этого сервера виртуализации значение Инициализация не изменится на ВКЛ. Процесс регистрации сервера виртуализации занимает от 20 до 60 секунд. Для обновления отображаемого статуса можно воспользоваться кнопкой **[Обновить]** (см. рис. 51).

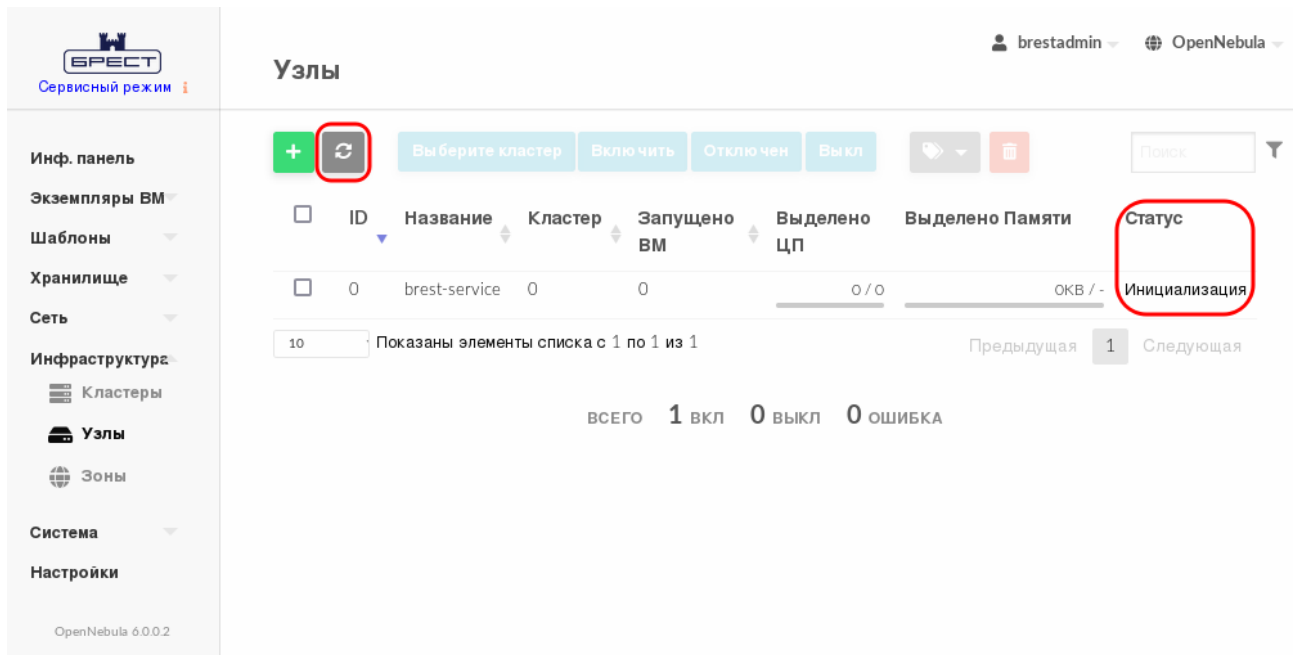


Рис. 51

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

5.1.2.1. В интерфейсе командной строки

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

```
onehost show <идентификатор_сервера_виртуализации>
```

Информация о сервере виртуализации включает:

- общую информацию с указанием его названия и драйверов, которые используются для взаимодействия с ним;
- информацию о производительности (совместно используемые ресурсы сервера виртуализации) для центрального процессора (ЦП) и оперативной памяти;
- информацию о подключенном хранилище;
- информацию мониторинга (см. 5.1.5).

Пример

Отображение информации о сервере виртуализации с идентификатором 1:

```
onehost show 1
```

Пример вывода после выполнения команды:

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

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

HOST SHARES

```
RUNNING VMS : 0
```

MEMORY

```
TOTAL : 3.8G
```

```
TOTAL +/- RESERVED : 3.8G
```

```
USED (REAL) : 230.8M
```

```
USED (ALLOCATED) : 0K
```

CPU

```
TOTAL : 400
```

```
TOTAL +/- RESERVED : 400
```

```
USED (REAL) : 28
```

```
USED (ALLOCATED) : 0
```

MONITORING INFORMATION

```
ARCH="x86_64"
```

```
CLUSTER_ID="0"
```

```
CPUSPEED="2304"
```

```
HOSTNAME="host01"
```

```
HYPERVISOR="kvm"
```

```
IM_MAD="kvm"
```

```
...
```

```
VM_MAD="kvm"
```

```
...
```

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

Пример вывода после выполнения команды:

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

5.1.2.2. В веб-интерфейсе ПК СВ

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

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

страница с информацией о сервере виртуализации (вкладка «Сведения» — см. рис. 52).

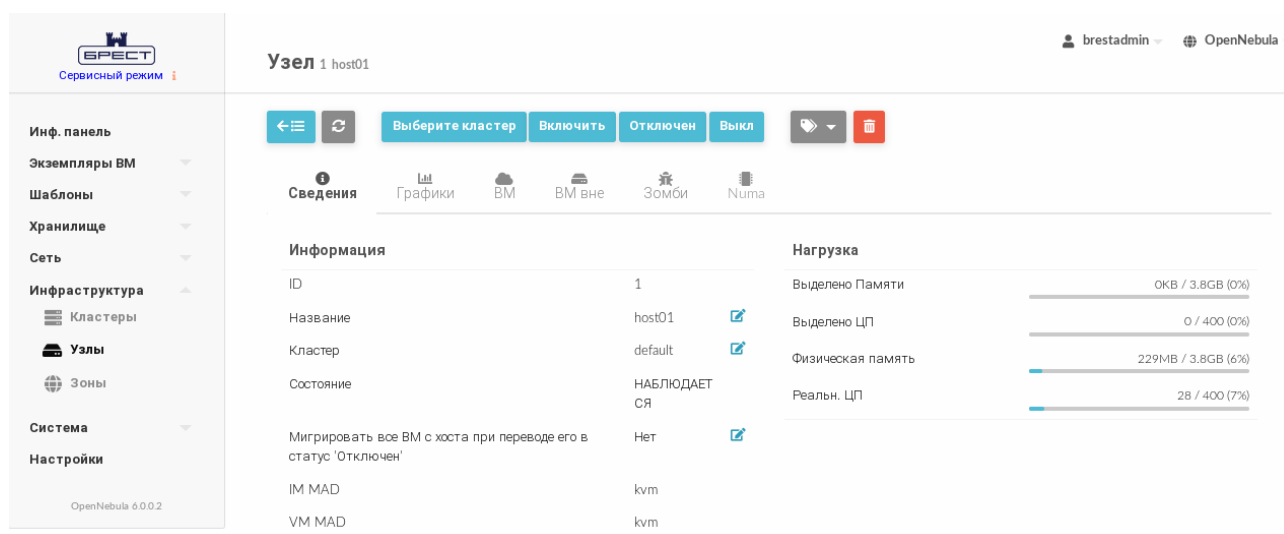


Рис. 52

5.1.3. Жизненный цикл сервера виртуализации

5.1.3.1. Общие сведения

Для управления жизненным циклом сервера виртуализации его можно переключать в различные состояния: включен (on), выключен (dsbl), отключен от сети (off) и др. Состояния описаны в таблице 6:

Таблица 6

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

5.1.3.2. Управление сервером виртуализации в интерфейсе командной строки

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

1) для отключения сервера виртуализации необходимо использовать команду:

```
onehost disable <идентификатор_сервера_виртуализации>
```

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

```
onehost enable <идентификатор_сервера_виртуализации>
```

3) для полного отключения сервера виртуализации необходимо использовать команду:

```
onehost offline <идентификатор_сервера_виртуализации>
```

Примеры:

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

```
onehost disable 1
```

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

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

2. Включение сервера виртуализации с идентификатором 1

```
onehost enable 1
```

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

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

3. Полное отключение сервера виртуализации с идентификатором 1

```
onehost offline 1
```

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

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

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

```
onehost flush <наименование_сервера_виртуализации>
```

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

5.1.3.3. Управление сервером виртуализации в веб-интерфейсе ПК СВ

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

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

После этого откроется страница с информацией о сервере виртуализации. Для изменения состояния сервера виртуализации можно воспользоваться кнопками (см. рис. 52):

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

5.1.4. Удаление сервера виртуализации

5.1.4.1. В интерфейсе командной строки

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

```
onehost delete <сетевое_имя_сервера_виртуализации>
```

или команду:

```
onehost delete <идентификатор_сервера_виртуализации>
```

Пример

Удаление сервера виртуализации node01:

```
onehost delete node1
```

5.1.4.2. В веб-интерфейсе ПК СВ

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

- 1) в меню слева выбрать пункт меню «Инфраструктура — Узлы»;
- 2) на открывшейся странице «Узлы» выделить необходимый сервер виртуализации и нажать на кнопку **[Удалить]** (см. рис. 53).

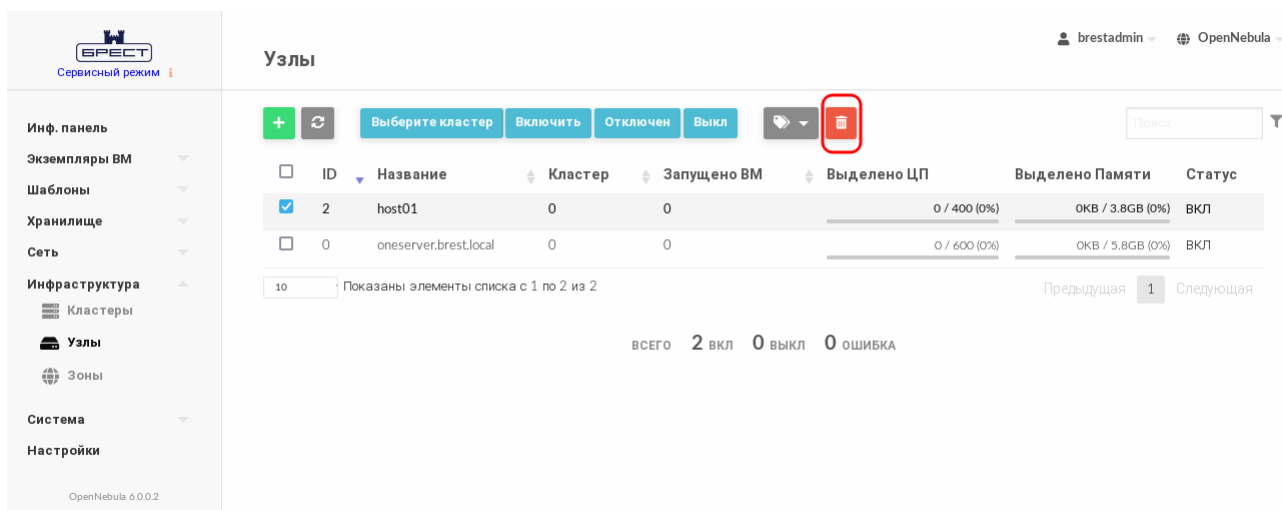


Рис. 53

3) в открывшемся окне нажать на кнопку **[OK]** (см. рис. 54).

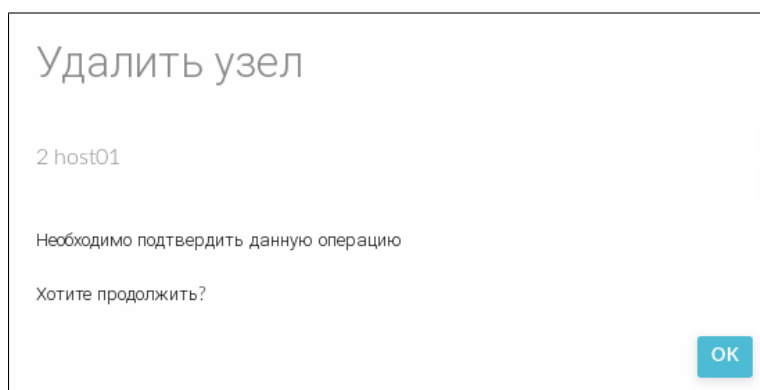


Рис. 54

5.1.5. Мониторинг сервера виртуализации

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

Примечание. Функционирование системы мониторинга ПК СВ описано в документе РДЦП.10001-07 95 01-1.

Информация мониторинга, собранная в ходе выполнения тестов, содержит значения параметров, приведенных в таблице 7.

Таблица 7

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

Продолжение таблицы 7

Параметр	Описание
CPUSPEED	Частота ЦП в МГц
HOSTNAME	Сетевое имя сервера виртуализации (в соответствии с ответом на команду <code>hostname</code>)
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 <code>CPU TOTAL</code> в секции <code>HOST SHARE</code> после выполнения команды <code>onehost show</code> (см. 5.1.2.1)
MAX_MEM	Максимальное количество памяти, которое может использоваться для VM. Кроме того, это значение отображается в виде параметра <code>MEMORY TOTAL</code> в секции <code>HOST SHARE</code> после выполнения команды <code>onehost show</code> (см. 5.1.2.1)
MAX_DISK	Общий объем пространства хранилища в МБ
USED_CPU	Процент используемой мощности ЦП, умноженной на количество ядер. Кроме того, это значение отображается как <code>CPU USED</code> в секции <code>HOST SHARE</code> после выполнения команды <code>onehost show</code> (см. 5.1.2.1)
USED_MEM	Используемая память, в килобайтах. Кроме того, это значение отображается в виде параметра <code>MEMORY USED (REAL)</code> в секции <code>HOST SHARE</code> после выполнения команды <code>onehost show</code> (см. 5.1.2.1)
USED_DISK	Используемый объем пространства хранилища в МБ
FREE_CPU	Процент неиспользуемой мощности ЦП, умноженной на количество ядер. Например, если в 4-ядерной машине не используются 50% мощности ЦП, значение данного параметра составит 200
FREE_MEM	Память, доступная для VM на данный момент, в КБ
FREE_DISK	Объем свободного пространства хранилища в МБ
CPU_USAGE	Общая мощность ЦП, распределенная среди VM, запущенных на данном сервере виртуализации в соответствии с запросом, который указан в параметре <code>CPU</code> в каждом шаблоне VM. Кроме того, это значение отображается в виде параметра <code>CPU USED (ALLOCATED)</code> в секции <code>HOST SHARE</code> после выполнения команды <code>onehost show</code> (см. 5.1.2.1)
MEM_USAGE	Общая память, распределенная среди VM, запущенных на данном сервере виртуализации в соответствии с запросом, который указан в параметре <code>MEMORY</code> в каждом шаблоне VM. Кроме того, это значение отображается в виде параметра <code>MEMORY USED (ALLOCATED)</code> в секции <code>HOST SHARE</code> после выполнения команды <code>onehost show</code> (см. 5.1.2.1)
DISK_USAGE	Общий размер образов диска для VM, запущенных на сервере виртуализации, рассчитанный с применением параметра <code>SIZE</code> каждого образа с учетом характеристик хранилища
NETRX	Объем входящего сетевого трафика
NETTX	Объем исходящего сетевого трафика
WILD	Перечень VM, разделенных запятой, работающих на сервере виртуализации и которые не были запущены службами ПК СВ и не контролируются в данный момент

Окончание таблицы 7

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

5.1.6. Пользовательские метки сервера виртуализации и стратегии планирования

Кроме значений параметров, получаемых в ходе выполнения тестов системы мониторинга (см. таблицу 7), можно получать значения пользовательских меток сервера виртуализации. Администратор может добавлять пользовательские метки путем создания дополнительного теста для сервера виртуализации, либо обновляя информацию о сервере виртуализации через команду `onehost update`. Например, чтобы пометить сервер виртуализации как «боевой» (`production`), нужно добавить пользовательскую метку `TYPE` командой:

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

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

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

Использование данной метки в шаблоне ограничит развертывание VM только серверами виртуализации с меткой `TYPE=production`. Для определения требований планирования можно использовать любой признак, указанный при выполнении команды `onehost show`. Более подробная информация о планировании приведена в разделе 7.

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

5.1.7. Импорт неконтролируемых виртуальных машин

Система мониторинга в ПК СВ сообщает обо всех найденных в гипервизоре виртуальных машинах, в том числе не запущенных посредством ПК СВ (параметр `WILD` — см. 5.1.5). Такие виртуальные машины называются неконтролируемыми и могут быть импортированы для управления через ПК СВ. Это относится ко всем поддерживаемым гипервизорам, в том числе гибридным.

После импорта виртуальной машины ее состояние, включая создание снимков

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

5.1.7.1. Импорт неконтролируемых ВМ в интерфейсе командной строки

Для обнаружения неконтролируемых виртуальных машин используется команда:
`onehost show <идентификатор_сервера_виртуализации>`

Пример

Пример вывода после выполнения команды `onehost show 3`:

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

Для импорта неконтролируемых виртуальных машин используется команда:
`onehost importvm <идентификатор_сервера_виртуализации> <наименование_ВМ>`

5.1.7.2. Импорт неконтролируемых ВМ в веб-интерфейсе ПК СВ

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

- 1) в меню слева выбрать пункт меню «Инфраструктура — Узлы»;
- 2) на открывшейся странице «Узлы» выбрать необходимый сервер виртуализации;
- 3) на открывшейся странице сервера виртуализации открыть вкладку «ВМ вне» (см. рис. 55).

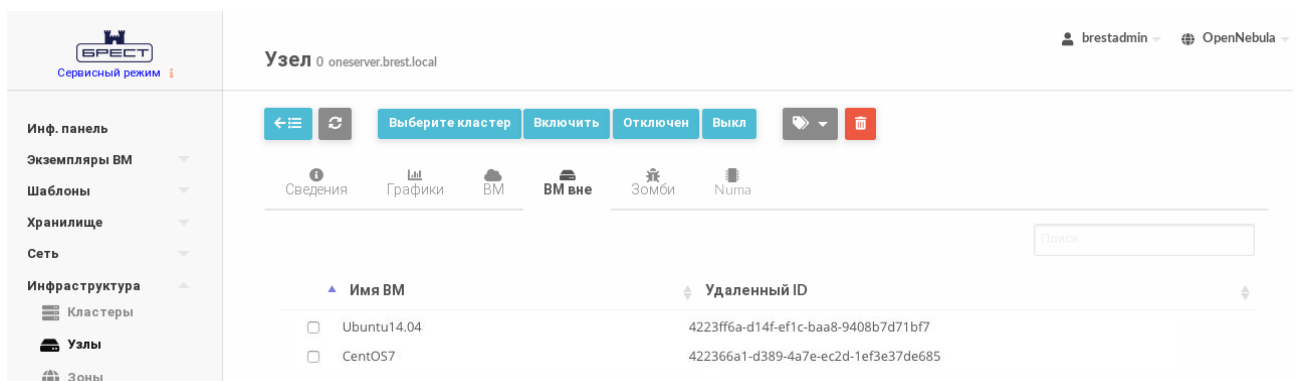


Рис. 55

5.2. Кластеры

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

5.2.1. Управление кластером

5.2.1.1. 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

5.2.1.2. 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. 56).

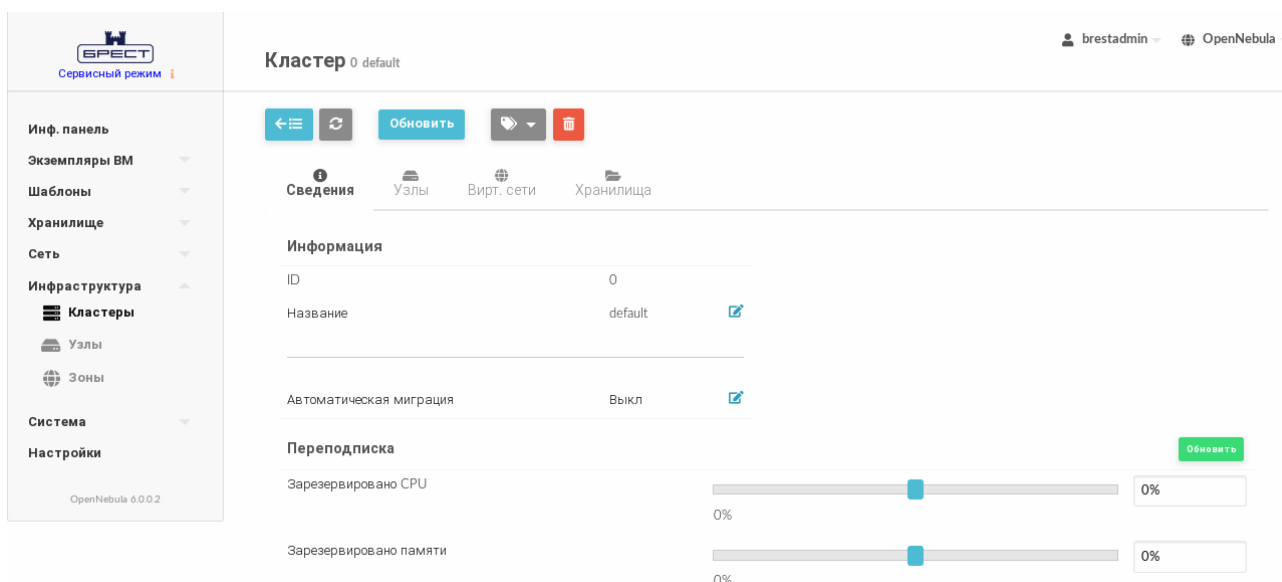


Рис. 56

5.2.2. Добавление серверов виртуализации к кластеру

5.2.2.1. В интерфейсе командной строки

Серверы виртуализации можно регистрировать непосредственно в кластере с помощью команды `onehost create` (см. 5.1.1.1), указав в команде аргумент `--cluster <идентификатор/наименование_кластера>`.

Чтобы добавить сервер виртуализации в кластер необходимо выполнить команду:

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

Одновременно сервер виртуализации может находиться только в одном кластере.

Для исключения сервера виртуализации из кластера используется команда:

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

<идентификатор/наименование_сервера_виртуализации>

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

Примеры:

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

```
onecluster addhost production host01
```

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

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

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

```
onecluster show production
```

Пример вывода после выполнения команды:

```
CLUSTER 100 INFORMATION
```

```
ID : 100
```

```
NAME : production
```

```
CLUSTER RESOURCES
```

```
TOTAL CPUs: 4
```

```
OCCUPIED CPUs: 0
```

```
AVAILABLE CPUs: 4
```

```
TOTAL RAM: 3
```

```
OCCUPIED RAM: 0
```

```
AVAILABLE RAM: 3
```

```
CLUSTER TEMPLATE
```

```
RESERVED_CPU=""
```

```
RESERVED_MEM=""
```

```
HOSTS
```

```
1
```

```
VNETS
```

DATASTORES

5.2.2.2. В веб-интерфейсе ПК СВ

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

- 1) в меню слева выбрать пункт меню «Инфраструктура — Узлы»;
- 2) на открывшейся странице «Узлы» выделить необходимый сервер виртуализации и нажать на кнопку **[Выберите кластер]**;
- 3) в открывшемся окне выбрать необходимый кластер и нажать на кнопку **[ОК]** (см. рис. 57).



Рис. 57

5.2.3. Добавление ресурсов к кластеру

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

Для добавления/удаления сети используется команда:

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

Для добавления/удаления хранилища используется команда:

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

Примеры:

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

```
onecluster addvnet production priv-ovswitch
```

```
onecluster adddatastore production iscsi
```

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

```
onecluster show production
```

Пример вывода после выполнения команды:

```
CLUSTER 100 INFORMATION
```

```
ID                : 100
```

```
NAME              : production
```

```
CLUSTER RESOURCES
```

```
TOTAL CPUS: 4
```

```
OCCUPIED CPUS: 0
```

```
AVAILABLE CPUS: 4
```

```
TOTAL RAM: 3
```

```
OCCUPIED RAM: 0
```

```
AVAILABLE RAM: 3
```

```
CLUSTER TEMPLATE
```

```
RESERVED_CPU=""
```

```
RESERVED_MEM=""
```

```
HOSTS
```

```
VNETS
```

```
1
```

```
DATASTORES
```

```
100
```

5.2.4. Планирование и кластеры

5.2.4.1. Автоматические требования

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

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

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

```
onetemplate instantiate 0
```

```
[TemplateInstantiate] Error allocating a new virtual machine. Incompatible /  
cluster IDs.
```

```
DISK [0]: IMAGE [0] from DATASTORE [1] requires CLUSTER [101]
```

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

5.2.4.2. Требования и ранг

Параметры размещения SCHED_REQUIREMENTS и SCHED_RANK, используемые в планировщике (см. раздел 7) могут использовать параметры из шаблона кластера.

Пример

Просмотр информации о серверах виртуализации. Пример вывода после выполнения команды `onehost list`:

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

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

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

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

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

Для приведенного выше примера можно использовать следующие выражения:

```
SCHED_REQUIREMENTS="QOS=GOLD"
```

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

6. НАСТРОЙКИ ВИРТУАЛЬНЫХ СЕТЕЙ

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

6.1. Виртуальные сети ПК СВ

6.1.1. Режимы работы сети

ПК СВ поддерживает работу виртуальных сетей в четырех сетевых режимах:

- 1) режим Сетевой мост (Bridged) — ВМ напрямую соединяется с существующим мостом на сервере виртуализации. Данный режим может быть настроен на использование сетевых групп безопасности и изоляции сети;
- 2) режим VLAN — для каждой сети создается мост, к которому подключается VLAN-тегированный сетевой интерфейс (VLAN-тегирование стандарта IEEE802.1Q);
- 3) режим VXLAN — для каждой сети создается мост, к которому подключается VXLAN-тегированный сетевой интерфейс. Используемый протокол VXLAN основан на UDP-инкапсуляции и групповой адресации IP;
- 4) режим Open vSwitch — аналогичен режиму VLAN, но использует программный коммутатор Open vSwitch (OVS) вместо сетевого моста. Сетевые группы безопасности данным режимом не поддерживаются.

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

6.1.2. Параметры сети

Параметры сети объединяются в три группы:

- 1) параметры физической сети, которая будет ее поддерживать, включая сетевой драйвер;
- 2) доступное адресное пространство. Адресами, связанными с виртуальной сетью, могут быть IPv4, IPv6, IPv4-IPv6 с двумя стеками или Ethernet;
- 3) параметры контекстуализации (сетевые настройки виртуальных машин, которые

могут включать, например, маски сети, сервера DNS или шлюзы).

6.1.2.1. Параметры физической сети

В группу параметров физической сети входят следующие параметры, приведенные в таблице 8.

Таблица 8

Параметр	Применимость	Обязательный	Описание
NAME	Для всех режимов	Да	Наименование сети
VN_MAD	Для всех режимов	Да	Драйвер виртуальной сети, может принимать следующие значения: - bridge — для режима «сетевой мост без фильтрации» (Bridged); - fw — для режима «сетевой мост с группами безопасности» (Bridged with Security Groups); - ebttables — для режима «сетевой мост с правилами ebttables» (Bridged with ebttables isolation); - 802.1Q — для режима VLAN; - vxlan — для режима VXLAN; - ovswitch — для режима Open vSwitch.
BRIDGE	Для всех режимов	Обязательный для режимов: - bridge - fw - ebttables - ovswitch	Имя сетевого моста на серверах виртуализации
VLAN_ID	Для режимов: - 802.1Q - vxlan - ovswitch	Обязательный для режима 802.1Q	Идентификационный номер сети VLAN. Будет сгенерирован, если не указан и для параметра AUTOMATIC_VLAN_ID установлено значение YES
AUTOMATIC_VLAN_ID	Для режимов: - 802.1Q - vxlan - ovswitch	Обязательный для режима 802.1Q	Игнорируется, если параметр VLAN_ID определен. Следует установить значение YES, если необходимо в автоматическом режиме генерировать идентификационный номер сети VLAN
PHYDEV	Для режимов: - 802.1Q - vxlan	Да	Имя физического сетевого устройства, которое будет подключено к сетевому мосту

Окончание таблицы 8

Параметр	Применимость	Обязательный	Описание
MTU	Для режимов: - 802.1Q - vxlan - ovswitch	Нет	Максимальный размер в байтах пакета данных (MTU), устанавливаемый для тегированного интерфейса и моста

Кроме того, для каждого сетевого интерфейса ВМ, подключаемого к виртуальной сети, можно настроить параметры оптимизации сетевого трафика (QoS). Применяются для ограничения средней и пиковой пропускной способности входящего и исходящего трафика, а также объема пакетных данных, которые могут передаваться на максимальной скорости. Перечень параметров приведен в таблице 9.

Таблица 9

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

6.1.2.2. Адресное пространство (AR)

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

- IP4 — для определения адресов IPv4 (бесклассовый);
- IP6 — для определения адресов IPv6 (уникальные глобальные и локальные адреса);
- IP6_STATIC — для определения адресов IPv6 (no-SLAAC);
- IP4_6 — с двумя стеками, каждый сетевой интерфейс в сети получит адрес IPv4 и адрес IPv6;
- ETHER — для ВМ формируются только MAC-адреса. Данный AR следует использовать, когда IP-адреса предоставляются внешним сервисом, например, сервером DHCP.

6.1.2.3. Сетевые параметры контекстуализации

В шаблоне виртуальной сети можно задать сетевые настройки виртуальных машин, которые будут применены в ОС виртуальной машины. Перечень параметров, значения которых можно задать для сетевого интерфейса VM, приведен в таблице 10.

Таблица 10

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

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

6.1.3. Использование сетей

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

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

Примеры:

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

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

2. При использовании идентификатора сети добавить в шаблон строку:

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

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

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

6.1.4. Управление сетями в интерфейсе командной строки

Для управления сетями используется инструмент командной строки `onevnet`.

6.1.4.1. Добавление, удаление и просмотр параметров сети

Для создания сети используется команда:

```
onevnet create <файл-шаблон>
```

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

Примеры:

1. Содержание файла шаблона `priv.net`:

```
NAME      = "Private"
VN_MAD    = "bridge"
AR=[
  TYPE = "IP4",
  IP   = "10.0.0.150",
  SIZE = "51"
]
DNS       = "10.0.0.23"
GATEWAY   = "10.0.0.1"
DESCRIPTION = "Частная сеть для VM с доступом к сети Интернет"
```

В представленном примере описана сеть, работающая в режиме «сетевой мост» без фильтрации. Сеть предоставит IP-адреса в диапазоне от 10.0.0.150 до 10.0.0.200.

Виртуальные машины в сети 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 сети с использованием файла шаблона `priv.net`:

```
onevnet create priv.net
```

Пример вывода после выполнения команды:

```
ID: 1
```

Для удаления сети используется команда:

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

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

Для отображения имеющихся сетей используется команда `onevnet list`.

Для получения подробной информации о конкретной сети используется команда:

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

Пример

Пример вывода после выполнения команды `onevnet show 1`:

```
VIRTUAL NETWORK 1 INFORMATION
```

```
ID : 1
```

```
NAME : Private
```

```
USER : oneadmin
```

```
GROUP : brestadmins
```

```
LOCK : None
```

```
CLUSTERS : 0
```

```
BRIDGE : onebr1
```

```
VN_MAD : bridge
```

```
AUTOMATIC VLAN ID : NO
```

```
AUTOMATIC OUTER VLAN ID : NO
```

```
USED LEASES : 0
```

```
PERMISSIONS
```

```
OWNER : um-
```

```
GROUP : ---
```

```
OTHER : ---
```

```
VIRTUAL NETWORK TEMPLATE
```

```
BRIDGE="onebr1"
```

```
BRIDGE_TYPE="linux"
```

```
DESCRIPTION="Частная сеть для VM с доступом к сети Интернет"
```

```
DNS="10.0.0.23"
GATEWAY="10.0.0.1"
PHYDEV=""
SECURITY_GROUPS="0"
VN_MAD="bridge"
```

6.1.4.2. Изменение параметров сети

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

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

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

Кроме того, можно изменить название сети при помощи команды:

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

6.1.4.3. Управление диапазонами адресов

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

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

Примеры:

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

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

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

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

```
AR 1
```

```

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

```

Для удаления AR необходимо использовать команду:

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

Примеры:

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

```
onevnet rmar Private 0
```

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

```

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

```

Для изменения значений параметров AR необходимо использовать команду:

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

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

Возможно изменить значения следующих параметров AR:

- префикс IPv6 — GLOBAL_PREFIX и ULA_PREFIX;
- любой пользовательский параметр, значение которого может отменять стандартные значения параметров сети.

6.1.4.4. Резервирование адресов

Адресам можно временно присвоить метку `hold` (зарезервировано). Они будут являться частью сети, но не будут выделяться для 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 сети с наименованием «Private»

```
onevnet hold Private 10.0.0.120
```

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

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

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

...

ADDRESS RANGE POOL

AR 1

SIZE : 20

LEASES : 1

RANGE	FIRST	LAST
MAC	02:00:0a:00:00:c8	02:00:0a:00:00:db
IP	10.0.0.200	10.0.0.219

AR 2

SIZE : 51

LEASES : 1

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

LEASES

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

Для разблокировки адреса используется команда:

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

6.1.5. Управление сетями в веб-интерфейсе ПК СВ

Для отображения перечня всех сетей в веб-интерфейсе ПК СВ необходимо в меню слева выбрать пункт меню «Система — Вирт.сети». На открывшейся странице «Вирт. сети» будет представлена таблица сетей (см. рис. 58).

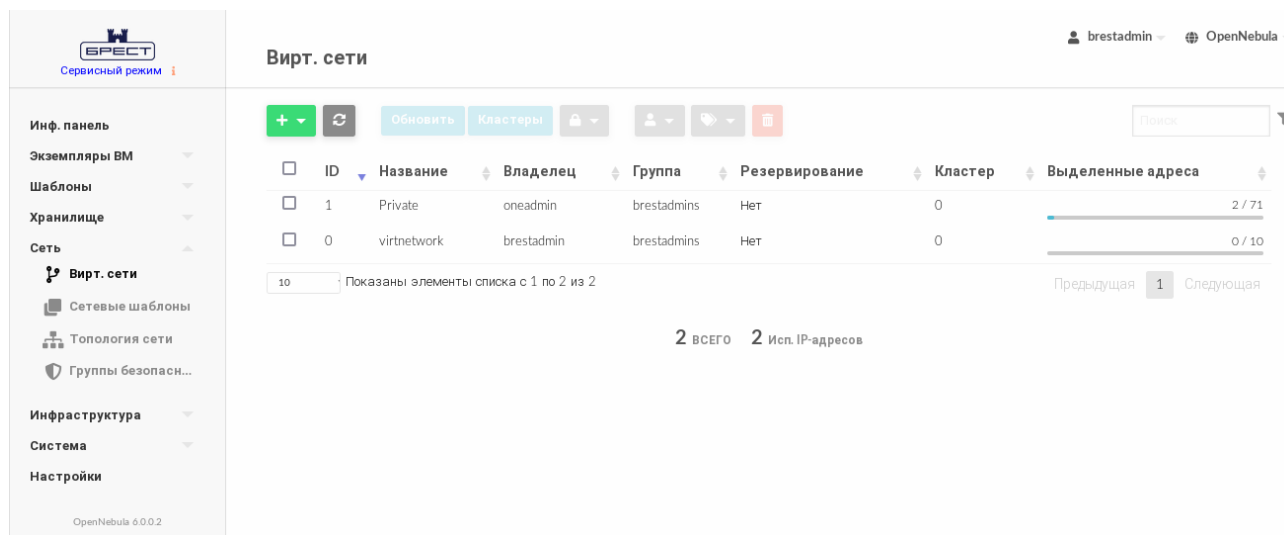


Рис. 58

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

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

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

Для просмотра информации о конкретной сети на странице «Вирт.сети» необходимо выбрать соответствующую строку. После этого откроется страница сети (вкладка «Сведения» — см. рис. 59).

Информация	Права	Пользование	Управление	Администрирование
ID	Владелец	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1	Группа	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Private	Все остальные	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN ID	Владелец			
--	Владелец	oneadmin		
AUTO VLAN ID	Группа	brestadmins		
Нет				
OUTER VLAN ID				
--				
AUTO OUTER VLAN ID				
Нет				

Рис. 59

Чтобы изменить параметры сети (в том числе, наименование), в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

- 1) в меню слева выбрать пункт меню «Сеть — Вирт.сети» и на открывшейся странице «Вирт.сети» выбрать необходимую сеть;
- 2) на открывшейся странице сети нажать на кнопку **[Обновить]**;
- 3) на открывшейся странице «Изменить виртуальную сеть»:
 - а) во вкладке «Общие» скорректировать наименование сети;
 - б) во вкладке «Конфигурация» скорректировать режим работы сети;
 - в) во вкладке «Адреса» скорректировать диапазоны адресов (AR)
 - г) нажать на кнопку **[Обновить]**.

Чтобы зарезервировать адрес, в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

- 1) в меню слева выбрать пункт меню «Сеть — Вирт.сети» и на открывшейся странице «Вирт.сети» выбрать необходимую сеть;
- 2) на открывшейся странице сети нажать на кнопку **[+]**, а затем в открывшемся меню выбрать пункт «Зарезервировано»;
- 3) на открывшейся странице «Резервирование из Виртуальной сети» указать адрес/адреса, которые необходимо зарезервировать и нажать на кнопку **[Зарезервировано]** (см. рис. 60).

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. 60

6.2. Сетевые группы безопасности

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

Подробная информация о функции безопасности по управлению сетевыми потоками приведена в документе РДЦП.10001-07 97 01.

ВНИМАНИЕ! Сетевые группы безопасности не поддерживаются для сетей OpenvSwitch.

6.2.1. Параметры сетевой группы безопасности

Сетевая группа безопасности состоит из нескольких правил. Каждое правило определяется параметрами, приведенными в таблице 11.

Таблица 11

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 11

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 сети. Используется, если правило применяется только для определенной сети.	Идентификатор существующей сети

6.2.2. Стандартная группа безопасности

По умолчанию применяется стандартная группа безопасности (с наименованием `default` и идентификатором 0). Данная группа разрешает весь входящий (INBOUND) и исходящий трафик (OUTBOUND). Если нужно ограничить соединения, необходимо изменить стандартную группу безопасности. Стандартную группу безопасности следует рассматривать как абсолютный минимум для всех 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 сети при их создании, но впоследствии ее можно удалить, обновив свойства сети.

6.2.3. Управление группами безопасности в интерфейсе командной строки

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

6.2.3.1. Добавление, удаление и просмотр списка групп безопасности

Для создания группы безопасности используется команда:

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

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

Примеры:

1. Содержание файла шаблона `sg.txt`:

```

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

```

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

```
onesecgroup create sg.txt
```

Пример вывода после выполнения команды:

```
ID: 100
```

Для просмотра имеющихся групп безопасности, необходимо выполнить команду:

```
onesecgroup list
```

Пример вывода после выполнения команды:

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

Для удаления группы безопасности используется команда:

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

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

6.2.3.2. Просмотр и изменение правил группы безопасности

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

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

Пример вывода после выполнения команды:

```
SECURITY GROUP 100 INFORMATION
```

```

ID           : 100
NAME         : test
USER        : oneadmin
GROUP       : brestadmins
PERMISSIONS
OWNER       : um-
GROUP      : ---
OTHER      : ---

```

VIRTUAL MACHINES

```

UPDATED      :
OUTDATED    :
ERROR       :

```

RULES

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

Для изменения правил необходимо использовать команду:

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

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

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

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

6.2.3.3. Применение группы безопасности

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

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

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

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

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

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

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

Пример

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

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

6.2.4. Управление группами безопасности в веб-интерфейсе ПК СВ

Для отображения перечня всех групп безопасности в веб-интерфейсе ПК СВ необходимо в меню слева выбрать пункт меню «Система — Группы безопасности». На открывшейся странице «Группы безопасности» будет представлена таблица имеющихся групп безопасности (см. рис. 61).

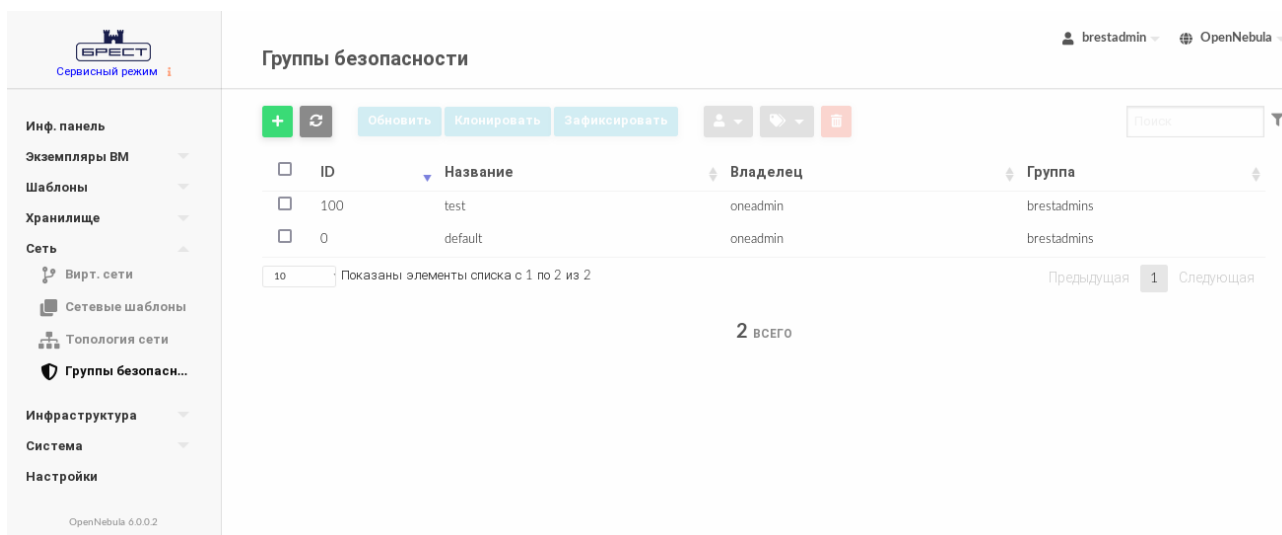


Рис. 61

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. 62).

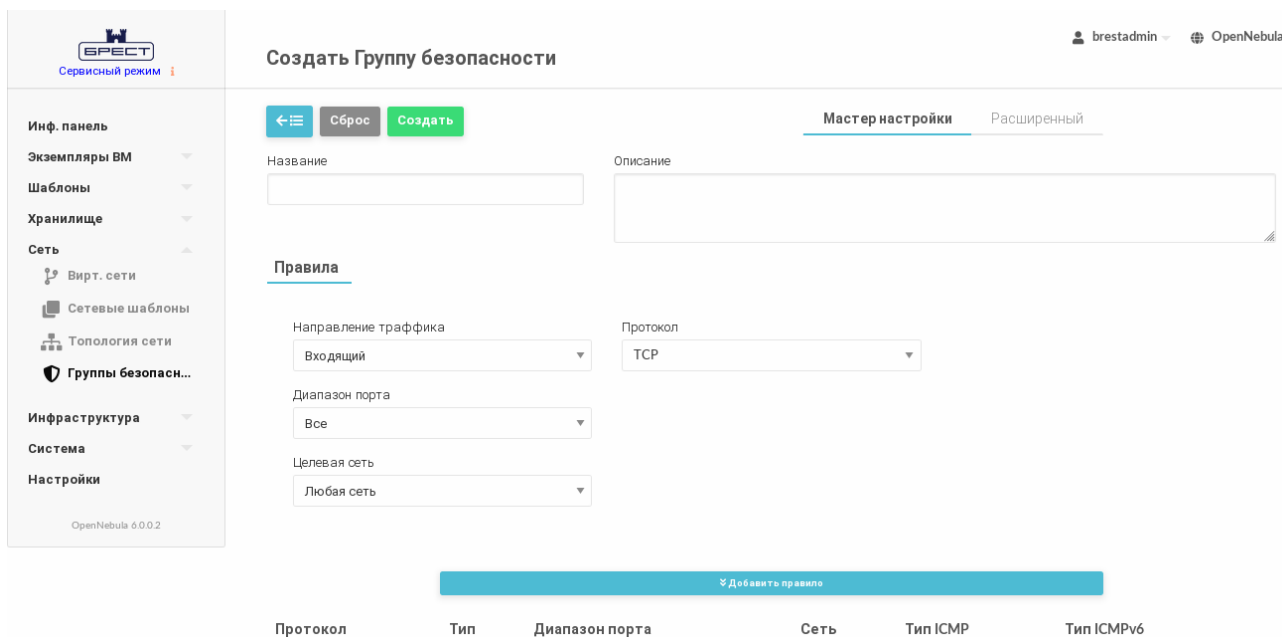


Рис. 62

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

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

пы безопасности» необходимо выбрать соответствующую строку. После этого откроется страница группы безопасности (вкладка «Сведения» — см. рис. 63).

Группа безопасности 100 test

Информация

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

Владелец

Владелец	oneadmin	✎
Группа	brestadmins	✎

Правила

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

Атрибуты

Рис. 63

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

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

7. ПЛАНИРОВЩИК

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

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

Действия по настройке планировщика осуществляются администратором ПК СВ.

7.1. Настройка планировщика

7.1.1. Общие параметры планировщика

Действия планировщика настраиваются с целью адаптации под определенную инфраструктуру. Значения параметров планировщика определяются в конфигурационном файле `/etc/one/sched.conf`. Для настройки действий планировщика используются параметры, приведенные в таблице 12.

Таблица 12

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

Окончание таблицы 12

Параметр	Описание
COLD_MIGRATE_MODE	Режим выключения VM перед перемещением, может принимать следующие значения: «0» — режим <code>save</code> , выключение с сохранением состояния VM (установлено по умолчанию); «1» — режим <code>poweroff</code> , корректное выключение VM без сохранения состояния; «2» — режим <code>poweroff-hard</code> , принудительное выключение VM без сохранения состояния
DEFAULT_SCHED	Блок параметров стратегии размещения (подробнее — см. 7.1.2)
DEFAULT_DS_SCHED	Блок параметров стратегии хранения (подробнее — см. 7.1.3)
DEFAULT_NIC_SCHED	Блок параметров стратегии использования сетей (подробнее — см. 7.1.4)
LOG	Блок параметров для настройки регистрации событий планировщика. Содержит следующие параметры: 1) <code>SYSTEM</code> — тип системы регистрации, возможные значения: - <code>file</code> — регистрация в файл <code>/var/log/one/sched.log</code> (установлено по умолчанию), - <code>syslog</code> — регистрация в системный журнал, - <code>std</code> — регистрация в стандартный поток ошибок; 2) <code>DEBUG_LEVEL</code> — уровень протоколирования, возможные значения: - «0» — регистрировать сообщения об ошибках, - «1» — регистрировать предупреждения, - «2» — регистрировать информационные сообщения, - «3» — регистрировать общие отладочные сообщения (установлено по умолчанию), - «4» — регистрировать отладочные сообщения, включая дату и время каждой итерации перемещения, - «5» — регистрировать подробные отладочные сообщения

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

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

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

Конфигурацию стратегий планирования можно настроить в двух местах:

- для каждой VM в соответствии с определением параметров `SCHED_RANK` и `SCHED_DS_RANK` в шаблоне VM;
- для всех виртуальных машин в целом — в файле `/etc/one/sched.conf` (требуется перезапуск службы `opennebula-scheduler`).

7.1.2. Настройка стратегии размещения

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

7.1.2.1. Параметры стратегии размещения

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

- `RANK` — арифметическое выражение для ранжирования подходящих серверов виртуализации в зависимости от их производительности (используется при настройке пользовательской стратегии размещения);
- `POLICY` — номер используемой стратегии размещения (см. таблицу 13).

Таблица 13

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

7.1.2.2. Особенности ранжирования серверов виртуализации

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

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

- «+» — сложение;

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

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

Арифметическое выражение может состоять только из одного параметра.

Пример

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

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

Пример

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

7.1.2.3. Предустановленные стратегии размещения

Стратегия вида «Уплотнение»:

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

Этой стратегии соответствует следующее арифметическое выражение для ранжирования серверов виртуализации:

RANK=RUNNING_VMS

Стратегия вида «Распределение»:

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

Этой стратегии соответствует следующее арифметическое выражение для ранжирования серверов виртуализации:

RANK="- RUNNING_VMS"

Стратегия вида «С учетом нагрузки»:

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

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

Этой стратегии соответствует следующее арифметическое выражение для ранжирования серверов виртуализации:

```
RANK=FREE_CPU
```

Стратегия вида «Фиксированная»:

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

Этой стратегии соответствует следующее арифметическое выражение для ранжирования серверов виртуализации:

```
RANK=PRIORITY
```

7.1.2.4. Перепланирование размещения виртуальных машин

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

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

7.1.2.5. Ограничение ресурсов, предоставляемых сервером виртуализации

Перед назначением ВМ на сервер виртуализации проверяется его доступная вычислительная мощность, чтобы убедиться, что имеющихся ресурсов сервера виртуализации достаточно для развертывания ВМ. Данные о вычислительной мощности передаются агентами мониторинга (см. 5.1.5). Данный алгоритм можно изменить, зарезервировав определенное количество вычислительной мощности (`MEMORY` и `CPU`). Для резервирования доступны следующие методы:

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

В частности, возможно резервирование следующих параметров вычислительной мощности:

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

- RESERVED_MEM в КБ. Будет вычитаться из TOTAL MEM.

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

7.1.3. Настройка стратегии хранения

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

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

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

7.1.3.1. Параметры стратегии хранения

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

- RANK — арифметическое выражение для ранжирования подходящих хранилищ в зависимости от их параметров (используется при настройке пользовательской стратегии хранения);
- POLICY — номер используемой стратегии хранения (см. таблицу 14).

Таблица 14

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

7.1.3.2. Особенности ранжирования системных хранилищ

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

Ранг системного хранилища вычисляется в соответствии с арифметическим выра-

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

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

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

Арифметическое выражение может состоять только из одного параметра.

Пример

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

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

Пример

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

7.1.3.3. Предустановленные стратегии размещения

Стратегия вида «Уплотнение»:

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

Этой стратегии соответствует следующее арифметическое выражение для ранжирования системных хранилищ:

RANK="- FREE_MB"

Стратегия вида «Распределение»:

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

Этой стратегии соответствует следующее арифметическое выражение для ранжирования

системных хранилищ:

RANK=FREE_MB

Стратегия вида «Фиксированная»:

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

Этой стратегии соответствует следующее арифметическое выражение для ранжирования системных хранилищ:

RANK=PRIORITY

7.1.3.4. Перемещение диска VM

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

7.1.3.5. Отключение хранилища

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

Пример

Отключение системного хранилища:

```
onedatastore disable system -v
```

Пример вывода после выполнения команды:

```
DATASTORE 0: disabled
```

Просмотр информации о системном хранилище. Пример вывода после выполнения команды

```
onedatastore show system:
```

```
DATASTORE 0 INFORMATION
```

```
ID:0
```

```
:system
```

```
...
```

```
:DISABLED
```

7.1.4. Настройка стратегии использования сетей

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

7.1.4.1. Параметры стратегии использования сетей

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

- `RANK` — логическое (булево) выражение для фильтрации доступных виртуальных сетей (используется при настройке пользовательской стратегии размещения);
- `POLICY` — номер используемой стратегии размещения (см. таблицу 15).

Таблица 15

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

7.1.4.2. Особенности фильтрации виртуальных сетей

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

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

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

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

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

7.2. Алгоритм работы планировщика

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

Алгоритм установления соответствия работает следующим образом:

- 1) виртуальные машины, для размещения диска которых требуется больше дискового пространства, чем доступно на данный момент, отфильтровываются и остаются в состоянии ожидания (pending);
- 2) серверы виртуализации, которые не соответствуют требованиям (задаются параметром SCHED_REQUIREMENTS в шаблоне ВМ) или не имеют достаточной вычислительной мощности (свободных ЦП и оперативной памяти) для запуска ВМ, отфильтровываются;
- 3) системные хранилища, которые не соответствуют требованиям (задаются параметром SCHED_DS_REQUIREMENTS в шаблоне ВМ) или не имеют достаточного дискового ресурса, отфильтровываются;
- 4) виртуальные сети, которые не соответствуют требованиям (задаются параметром SCHED_REQUIREMENTS в блоке параметров NIC шаблона ВМ) или не имеют достаточного количества свободных (арендованных) адресов, отфильтровываются;
- 5) производится финальная фильтрация и ранжирование серверов виртуализации, системных хранилищ и виртуальных сетей в соответствии со значениями параметров, указанных в следующих источниках (по убыванию приоритета):
 - в шаблоне ВМ (используются параметры SCHED_RANK и SCHED_DS_RANK);
 - для всех виртуальных машин в целом — в файле /etc/one/sched.conf (используются блоки параметров DEFAULT_SCHED, DEFAULT_DS_SCHED и DEFAULT_NIC_SCHED).
- 6) при развертывании ВМ в первую очередь используются ресурсы с более высоким рангом.

8. РУКОВОДСТВО АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ПК СВ

Данный раздел предназначен для пользователей, для которых назначена роль в ПК СВ - администратор безопасности.

8.1. Регистрация событий безопасности в ПК СВ

В ПК СВ регистрация событий безопасности выполняется с учетом требований ГОСТ Р 59548-2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации».

Регистрация событий безопасности реализуется использованием службы `auditd` и подсистемы регистрации событий из состава ОС СН. Служба `auditd` выполняет регистрацию событий объектов файловой системы (аудит файлов) и пользователей (аудит процессов) согласно заданным правилам. Регистрация событий осуществляется в журнал аудита.

Описание настройки параметров регистрации событий безопасности приведено в документе РУСБ.10015-37 97 01-1.

8.2. Настройка регистрации событий безопасности

Для настройки регистрации событий безопасности используется программа `fly-admin-events` из состава ОС СН, с помощью которой доступно выполнять регистрацию событий запуска и остановки службы `auditd`, регистрацию событий добавления и удаления правил `auditd`, регистрацию действий с журналом аудита. Дополнительно утилита позволяет добавлять правила аудита. Порядок использования программы `fly-admin-events` приведен в электронной справке.

Кроме того, для управления правилами аудита используются следующие инструменты командной строки из состава ОС СН:

- `getfaud` — служит для получения списков правил регистрации событий над файловыми объектами;
- `setfaud` — устанавливает на файлы списки правил регистрации событий;
- `useraud` — позволяет просматривать и изменять правила регистрации событий для пользователей;
- `psaud` — позволяет изменить или считать правила регистрации событий заданного процесса;
- `ausearch` — предназначен для просмотра файлов журнала регистрации событий ядра, а также событий пользователя.

Описание представленных выше инструментов командной строки приведено в документе РУСБ.10015-37 97 01-1.

8.3. Журнал событий

Служба `syslog-ng` выполняет регистрацию событий в журнал `/parsec/log/astra/events`. В журнале событий регистрируются попытки запуска неподписанных файлов, успешная и неуспешная авторизация, данные о пользовательских сессиях и другие события безопасности, регистрация которых настроена (см. 8.2).

Для просмотра журнала событий может использоваться:

- программа `fly-event-viewer` («Журнал системных событий»), описание программы приведено в электронной справке;
- инструмент командной строки `astra-event-viewer`, порядок использования инструмента приведен на странице помощи, вызываемой командой:

```
astra-event-viewer -h
```

Действия с журналом событий (удаление, переименование, перемещение, ротация файла журнала событий) регистрируются подсистемой регистрации событий и указываются первой записью в журнале событий:

- удаление журнала событий регистрируется событием «Журнал событий удален»;
- переименование или перемещение журнала событий регистрируется событием «Журнал событий переименован или перемещен»;
- ротация журнала событий регистрируется событием «Журнал событий ротирован»;
- действия с журналом событий недоверенными процессами (всеми процессами, кроме процессов `syslog-ng` и `logrotate`) регистрируются событием «Журнал событий изменен недоверенным процессом».

Кроме того, программа `fly-event-viewer` позволяет выполнить выгрузку (экспорт) данных из журнала событий безопасности в файл формата CSV или JSON. Порядок действий описан в электронной справке.

9. МАГАЗИН ПРИЛОЖЕНИЙ

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

Создание и управление магазином приложений осуществляются администратором ПК СВ.

9.1. Требования

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

9.2. Установка и настройка магазина приложений

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

```
sudo apt install breast-marketplace
```

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

Примечание. Алгоритм Raft описан в документе РДЦП.10001-07 95 01-1.

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

```
sudo breast-marketplace-configure
```

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

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

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

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

По окончании работы мастера настройки в веб-интерфейсе ПК СВ появится информация о добавленном магазине приложений (см. рис. 64).

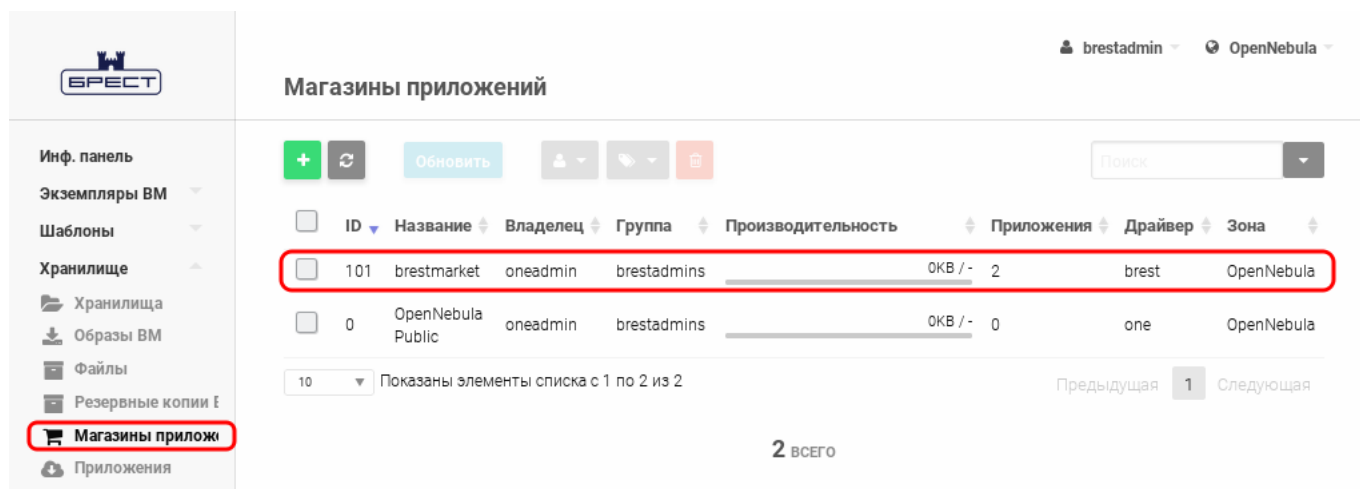


Рис. 64

9.3. Добавление приложения

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

9.3.1. Создание приложения, используя образ диска

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

- 1) в меню слева выбрать пункт «Хранилище — Приложения» и на открывшейся странице «Приложения» нажать на кнопку **[+]** (см. рис. 65);

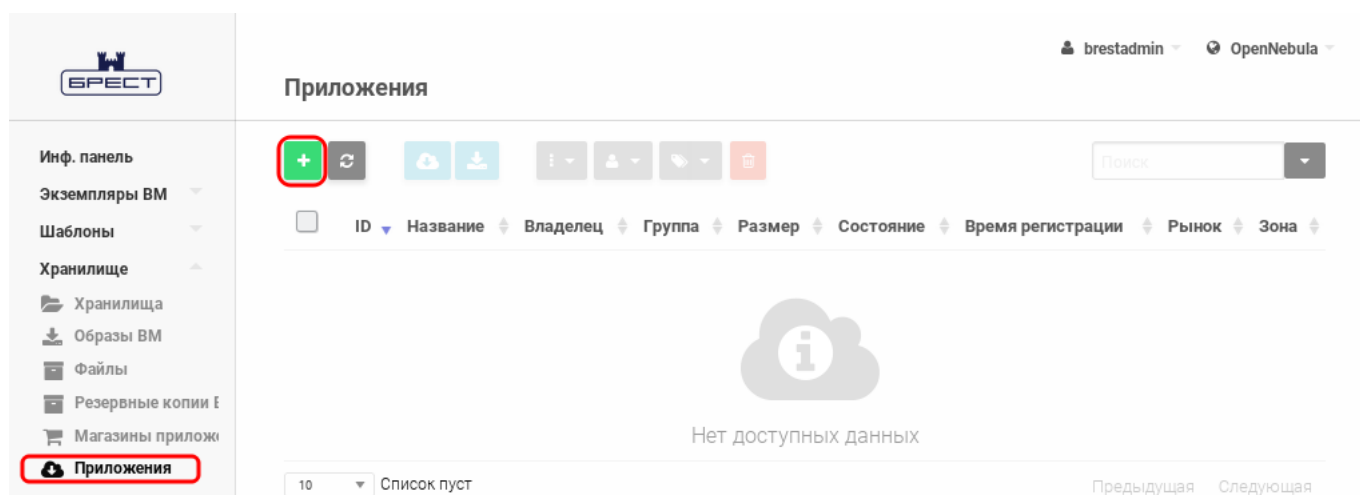


Рис. 65

- 2) на открывшейся странице «Создать приложение в магазине приложений» (см. рис. 66) 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

Инф. панель | Экземпляры VM | Шаблоны | Хранилище | Хранилища | Образы VM | Файлы | Резервные копии | Магазины прилож | **Приложения** | Сеть | Инфраструктура | Система | Настройки

OpenNebula 5.4.6 by OpenNebula Systems

бrestadmin | OpenNebula

Включить/Выключить **Создать** | Мастер настройки | Расширенный

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. 66

Созданное приложение будет отображено в веб-интерфейсе ПК СВ на странице «Приложения» (см. рис. 67).

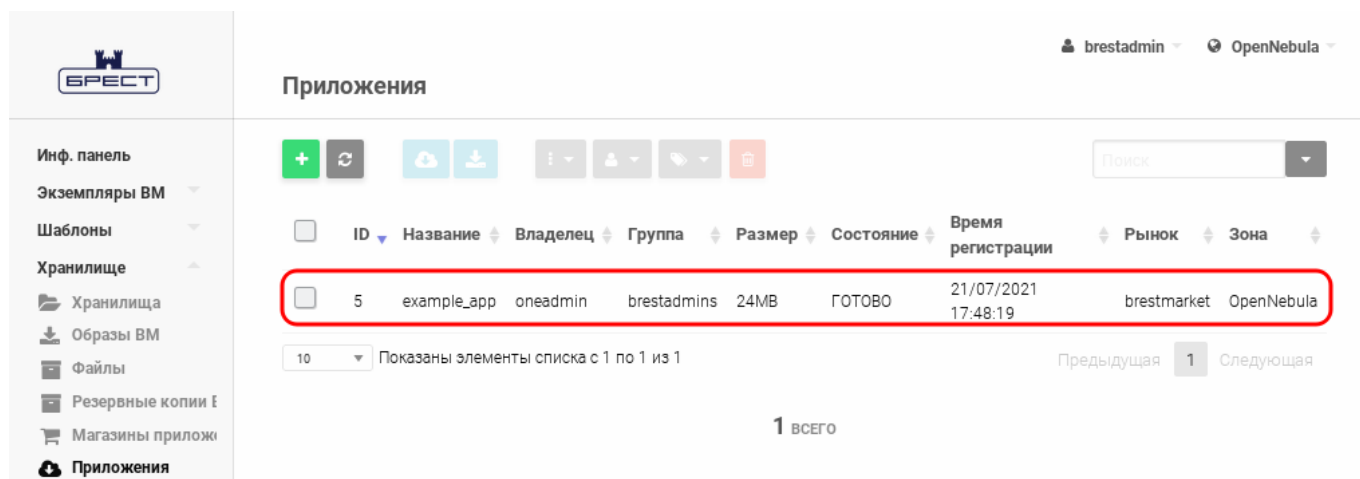


Рис. 67

Примечание. После создания и завершения загрузки приложения в магазин приложений оно исчезнет из веб-интерфейса и в течении одной минуты появится.

9.3.2. Создание приложения, используя имеющуюся VM

Для того чтобы создать приложение, используя имеющуюся VM, и добавить его в магазин приложений, необходимо на сервере управления 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. 68).

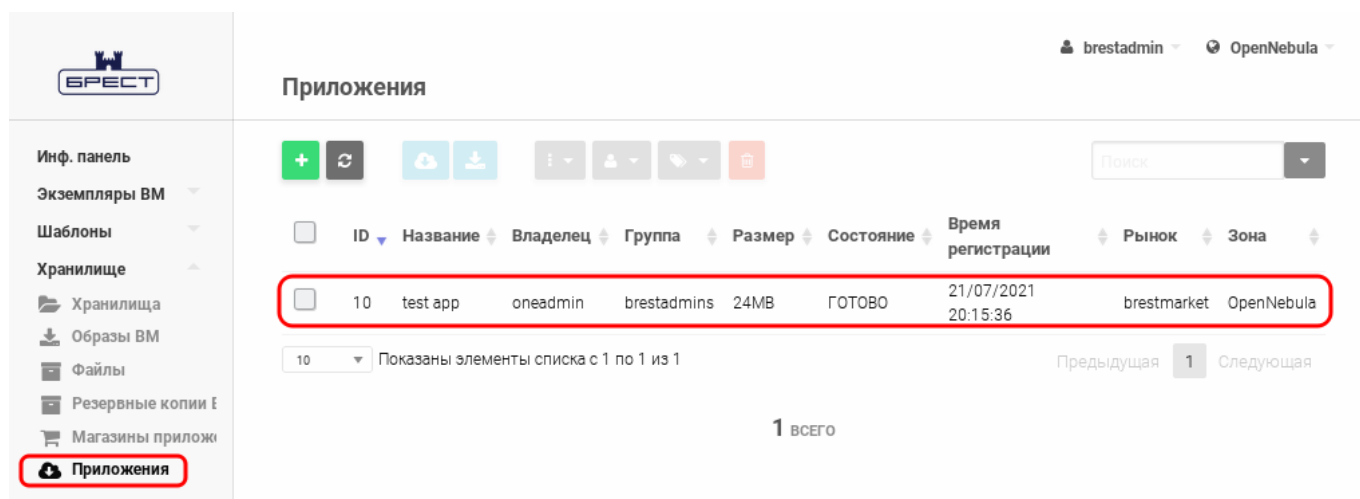


Рис. 68

ПЕРЕЧЕНЬ ТЕРМИНОВ

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

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

Примечание. Описание ролей пользователей представлено в документе РДЦП.10001-07 97 01 «Программный комплекс «Средства виртуализации «Брест». Руководство по КСЗ».

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

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

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

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)

