

Утвержден
РДЦП.10001-02-УД

ПРОГРАММНЫЙ КОМПЛЕКС «СРЕДСТВА ВИРТУАЛИЗАЦИИ «БРЕСТ»
Руководство администратора. Часть 2
РДЦП.10001-02 95 01-2
Листов 232

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

2024

Литера О₁

АННОТАЦИЯ

Настоящий документ является руководством администратора программного изделия «Программный комплекс «Средства виртуализации «Брест» (ПК СВ «Брест») РДЦП.10001-02 (далее по тексту — ПК СВ) в части применения по назначению ПК СВ с учетом особенностей операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 очередное обновление 1.7 (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.10001-02 20 01 «Программный комплекс «Средства виртуализации «Брест». Ведомость эксплуатационных документов».

Руководство администратора состоит из двух частей:

- РДЦП.10001-02 95 01-1 «Программный комплекс «Средства виртуализации «Брест». Руководство администратора. Часть 1»;
- РДЦП.10001-02 95 01-2 «Программный комплекс «Средства виртуализации «Брест». Руководство администратора. Часть 2».

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

Во второй части руководства представлен порядок 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.10001-02 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.10001-02 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	12
2. Инструменты управления ПК СВ	13
2.1. Общие сведения	13
2.2. Инструменты командной строки	13
2.3. Веб-интерфейс ПК СВ	13
3. Пользователи и группы	15
3.1. Общие сведения	15
3.2. Управление пользователями	15
3.2.1. Управление пользователями в интерфейсе командной строки	15
3.2.2. Управление пользователями в веб-интерфейсе ПК СВ	18
3.3. Управление группами	21
3.3.1. Общие сведения	22
3.3.2. Управление группами в интерфейсе командной строки	22
3.3.3. Управление группами в веб-интерфейсе ПК СВ	24
3.4. Управление VDC	27
3.4.1. Общие сведения	27
3.4.2. Управление VDC в интерфейсе командной строки	28
3.4.3. Управление VDC в веб-интерфейсе ПК СВ	30
3.5. Управление полномочиями	32
3.5.1. Общие сведения	32
3.5.2. Управление полномочиями в интерфейсе командной строки	33
3.5.2.1. Просмотр и изменение установленных полномочий для ресурса	33
3.5.2.2. Изменение установленных полномочий для ресурса	33
3.5.2.3. Установка полномочий по умолчанию	35
3.5.3. Управление полномочиями в веб-интерфейсе ПК СВ	36
3.5.3.1. Просмотр и изменение установленных полномочий	36
3.5.3.2. Установка полномочий, присваиваемых по умолчанию пользователю	37
3.5.4. Управление полномочиями в отношении экземпляра VM	37
3.6. Управление правилами ACL	38
3.6.1. Общие сведения	38
3.6.2. Структура правил ACL	39

3.6.3. Управление правилами ACL в интерфейсе командной строки	40
3.6.4. Управление правилами ACL в веб-интерфейсе ПК СВ	42
3.6.5. Использование правил ACL для реализации роли разработчика VM	43
4. Управление экземплярами VM	45
4.1. Статус и жизненный цикл виртуальной машины	45
4.2. Управление экземплярами VM в интерфейсе командной строки	50
4.2.1. Создание экземпляра VM	50
4.2.2. Отображение существующих VM	51
4.2.3. Удаление экземпляров VM	52
4.2.4. Приостановка экземпляров VM	52
4.2.5. Запуск экземпляров VM	53
4.2.6. Перезагрузка экземпляров VM	54
4.2.7. Отсрочка развертывания экземпляров VM	54
4.3. Управление экземплярами VM в веб-интерфейсе ПК СВ	54
4.3.1. Создание экземпляра VM	54
4.3.2. Отображение существующих VM	57
4.3.3. Завершение работы и приостановка экземпляров VM	58
4.3.4. Запуск экземпляра VM	58
4.3.5. Перезагрузка экземпляров VM	59
4.3.6. Отсрочка развертывания экземпляров VM	59
4.3.7. Удаление экземпляров VM	59
4.4. Настройка дискреционного и мандатного управление доступом к VM	60
4.5. Управление доступом виртуальных машин к физическому и виртуальному оборудованию	62
4.5.1. Удаленное подключение USB-устройств к VM по протоколам VNC/SPICE/RDP	62
4.5.2. Ретрансляция PCI	68
4.5.2.1. Требования	68
4.5.2.2. Настройка сервера виртуализации	68
4.5.2.3. Конфигурация ядра	68
4.5.2.4. Загрузка драйвера vfio в initrd	69
4.5.2.5. Блокировка драйверов	69
4.5.2.6. Привязка устройств к vfio	69
4.5.2.7. Конфигурация qemu	71

4.5.2.8. Настройка драйвера	71
4.5.2.9. Настройка использования устройств PCI	71
4.5.3. Горячее подключение образа диска	74
4.5.3.1. В интерфейсе командной строки	74
4.5.3.2. В веб-интерфейсе ПК СВ	74
4.5.4. Перераспределение производительности VM	76
4.5.4.1. В интерфейсе командной строки	76
4.5.4.2. В веб-интерфейсе ПК СВ	76
4.5.5. Изменение размера дисков VM	77
4.5.5.1. В интерфейсе командной строки	78
4.5.5.2. В веб-интерфейсе ПК СВ	79
4.6. Управление квотами	79
4.6.1. Общие сведения	79
4.6.2. Управление квотами в интерфейсе командной строки	80
4.6.2.1. Просмотр установленных квот	80
4.6.2.2. Установка квот	81
4.6.2.3. Изменение установленных квот	84
4.6.2.4. Установка квот для нескольких пользователей/групп	86
4.6.2.5. Установка квот по умолчанию	86
4.6.3. Управление квотами в веб-интерфейсе ПК СВ	86
4.7. Миграция VM между серверами виртуализации	88
4.7.1. Перемещение экземпляра VM в интерфейсе командной строки	89
4.7.2. Перемещение экземпляра VM в веб-интерфейсе ПК СВ	89
4.7.3. Настройка миграции работающих VM в автоматическом режиме	90
4.8. Снимки состояний VM	92
4.8.1. Управление снимками состояний в интерфейсе командной строки	92
4.8.2. Управление снимками состояний в веб-интерфейсе ПК СВ	93
4.9. Снимки дисков VM	94
4.9.1. Управление снимками дисков в интерфейсе командной строки	94
4.9.2. Управление снимками дисков в веб-интерфейсе ПК СВ	94
5. Управление серверами виртуализации и кластерами	97
5.1. Серверы виртуализации	97
5.1.1. Добавление сервера виртуализации	97

5.1.1.1. Регистрация сервера виртуализации в интерфейсе командной строки	97
5.1.1.2. Регистрация сервера виртуализации в веб-интерфейсе ПК СВ	97
5.1.2. Просмотр перечня серверов виртуализации и отображение информации о сервере виртуализации	99
5.1.2.1. В интерфейсе командной строки	99
5.1.2.2. В веб-интерфейсе ПК СВ	100
5.1.3. Жизненный цикл сервера виртуализации	101
5.1.3.1. Общие сведения	101
5.1.3.2. Управление сервером виртуализации в интерфейсе командной строки	101
5.1.3.3. Управление сервером виртуализации в веб-интерфейсе ПК СВ	102
5.1.4. Удаление сервера виртуализации	103
5.1.4.1. В интерфейсе командной строки	103
5.1.4.2. В веб-интерфейсе ПК СВ	103
5.1.5. Мониторинг сервера виртуализации	104
5.1.6. Пользовательские метки сервера виртуализации и стратегии планирования	105
5.1.7. Импорт неконтролируемых виртуальных машин	106
5.1.7.1. Импорт неконтролируемых VM в интерфейсе командной строки	106
5.1.7.2. Импорт неконтролируемых VM в веб-интерфейсе ПК СВ	107
5.2. Кластеры	107
5.2.1. Управление кластером	107
5.2.1.1. В интерфейсе командной строки	107
5.2.1.2. В веб-интерфейсе ПК СВ	108
5.2.2. Добавление серверов виртуализации к кластеру	109
5.2.2.1. В интерфейсе командной строки	109
5.2.2.2. В веб-интерфейсе ПК СВ	110
5.2.3. Добавление ресурсов к кластеру	111
5.2.4. Планирование и кластеры	112
5.2.4.1. Автоматические требования	112
5.2.4.2. Требования и ранг	112
6. Настройки виртуальных сетей	114
6.1. Виртуальные сети ПК СВ	114
6.1.1. Режимы работы сети	114
6.1.2. Параметры сети	114

6.1.2.1. Параметры физической сети	115
6.1.2.2. Диапазон адресов (AR)	116
6.1.2.3. Сетевые параметры контекстуализации	117
6.1.3. Использование сетей	117
6.1.4. Управление сетями в интерфейсе командной строки	118
6.1.4.1. Создание, удаление и просмотр параметров сети	118
6.1.4.2. Изменение параметров сети	120
6.1.4.3. Управление диапазонами адресов	120
6.1.4.4. Запрет использования адресов	122
6.1.5. Управление сетями в веб-интерфейсе ПК СВ	123
6.2. Сетевые группы безопасности	124
6.2.1. Параметры сетевой группы безопасности	125
6.2.2. Стандартная группа безопасности	125
6.2.3. Управление группами безопасности в интерфейсе командной строки	126
6.2.3.1. Добавление, удаление и просмотр списка групп безопасности	126
6.2.3.2. Просмотр и изменение правил группы безопасности	127
6.2.3.3. Применение группы безопасности	128
6.2.4. Управление группами безопасности в веб-интерфейсе ПК СВ	129
6.3. Сервис виртуальных сетевых функций (VNF)	131
6.3.1. Установка и управление VNF	131
6.3.1.1. Установка и настройка сервиса VNF	131
6.3.1.2. Подключение к виртуальному маршрутизатору	137
6.3.1.3. Журнал работы VNF (система логирования) и обработка ошибок	138
6.3.2. Функции виртуальной сети	139
6.3.2.1. Работа с параметрами контекстуализации	139
6.3.2.2. Высокая доступность (keepalived)	139
6.3.2.3. ROUTER4	141
6.3.2.4. DHCP4	141
6.3.2.5. DNS	146
6.3.2.6. NAT4	147
6.3.2.7. SDNAT4	148
6.3.2.8. LB (LoadBalancer)	149
6.3.3. VNF как виртуальный маршрутизатор	155

6.3.3.1. Подготовка VNF	155
6.3.3.2. Добавление второго и третьего сетевого интерфейса	158
6.3.3.3. Проверка конфигурации	159
6.3.3.4. Проверка работы виртуального маршрутизатора	160
6.3.3.5. Подключение интерфейса управления	160
7. Планировщик	162
7.1. Настройка планировщика	162
7.1.1. Общие параметры планировщика	162
7.1.2. Настройка стратегии размещения	164
7.1.2.1. Параметры стратегии размещения	164
7.1.2.2. Особенности ранжирования серверов виртуализации	164
7.1.2.3. Предустановленные стратегии размещения	165
7.1.2.4. Перепланирование размещения виртуальных машин	166
7.1.2.5. Ограничение ресурсов, предоставляемых сервером виртуализации	166
7.1.3. Настройка стратегии хранения	167
7.1.3.1. Параметры стратегии хранения	167
7.1.3.2. Особенности ранжирования системных хранилищ	167
7.1.3.3. Предустановленные стратегии размещения	168
7.1.3.4. Перемещение диска VM	169
7.1.3.5. Отключение хранилища	169
7.1.4. Настройка стратегии использования сетей	169
7.1.4.1. Параметры стратегии использования сетей	170
7.1.4.2. Особенности фильтрации виртуальных сетей	170
7.2. Алгоритм работы планировщика	171
8. Руководство администратора безопасности ПК СВ	173
8.1. Регистрация событий безопасности в ПК СВ	173
8.2. Настройка регистрации событий безопасности	173
8.3. Журнал событий	174
9. Магазин приложений	175
9.1. Требования	175
9.2. Установка и настройка магазина приложений	175
9.3. Добавление приложения	176
9.3.1. Создание приложения, используя образ диска	176

9.3.2. Создание приложения, используя имеющуюся VM	178
10. Управление сервисами	179
10.1. Общие сведения о сервисах в ПК СВ	179
10.2. Служба сервера OneGate	180
10.2.1. Общие сведения о службе сервера OneGate	180
10.2.2. Настройка службы сервера OneGate	180
10.2.3. Управление службой сервера OneGate	182
10.2.4. Настройка ПК СВ для использования службы сервера OneGate	182
10.2.5. Настройка шаблона VM для использования службы сервера OneGate	183
10.2.5.1. Настройка шаблона VM в интерфейсе командной строки	183
10.2.5.2. Настройка шаблона VM в веб-интерфейсе ПК СВ	183
10.2.6. Настройка VM для доступа к службе сервера OneGate	184
10.2.7. Использование клиента OneGate в ОС виртуальной машины	184
10.2.7.1. Особенности использования клиента OneGate	184
10.2.7.2. Получение служебной информации о VM	185
10.2.7.3. Получение служебной информации сервиса	185
10.2.7.4. Получение служебной информации о виртуальном маршрутизаторе	186
10.2.7.5. Получение служебной информации о виртуальной сети	186
10.2.7.6. Изменение пользовательского шаблона экземпляра VM	186
10.2.7.7. Удаление параметра из пользовательского шаблона экземпляра VM	187
10.2.7.8. Управление состоянием VM	188
10.2.7.9. Управление количеством VM в составе сервиса	188
10.2.8. Взаимодействие с API службы сервера OneGate в ОС виртуальной машины	189
10.2.8.1. Параметры доступа к API службы сервера OneGate	189
10.2.8.2. Получение служебной информации о VM	189
10.2.8.3. Получение служебной информации сервиса	190
10.2.8.4. Получение служебной информации о виртуальном маршрутизаторе	191
10.2.8.5. Получение служебной информации о виртуальной сети	192
10.2.8.6. Изменение пользовательского шаблона экземпляра VM	194
10.2.8.7. Удаление параметра из пользовательского шаблона экземпляра VM	194
10.2.8.8. Управление состоянием VM	195
10.2.8.9. Управление количеством VM в составе сервиса	196
10.3. Служба OneFlow	196

10.3.1. Общие сведения о службе OneFlow	196
10.3.2. Настройка службы OneFlow	196
10.3.3. Управление службой OneFlow	198
10.3.4. Настройка ПК СВ для использования службы OneFlow	199
10.3.4.1. Настройка веб-интерфейса ПК СВ	199
10.3.4.2. Настройка инструментов командной строки	199
10.4. Управление шаблонами сервиса	200
10.4.1. Параметры сервиса, задаваемые в шаблоне	200
10.4.1.1. Общие параметры сервиса	200
10.4.1.2. Параметры группы VM с заданной ролью	201
10.4.1.3. Параметры политики эластичности	202
10.4.1.4. Параметры политики планирования	203
10.4.2. Управление шаблонами сервиса в интерфейсе командной строки	204
10.4.2.1. Создание шаблона	204
10.4.2.2. Отображение доступных шаблонов и просмотр информации о шаблоне	205
10.4.2.3. Изменение параметров шаблона	206
10.4.2.4. Клонирование шаблона	206
10.4.2.5. Удаление шаблона	207
10.4.3. Управление шаблонами сервиса в веб-интерфейсе ПК СВ	207
10.4.3.1. Создание шаблона	207
10.4.3.2. Отображение доступных шаблонов и просмотр информации о шаблоне	209
10.4.3.3. Изменение параметров шаблона	210
10.4.3.4. Клонирование шаблона	210
10.4.3.5. Удаление шаблона	211
10.4.4. Настройка автоматического удаления сервиса	212
10.4.4.1. В интерфейсе командной строки	212
10.4.4.2. В веб-интерфейсе ПК СВ	212
10.5. Управление экземплярами сервиса	213
10.5.1. Жизненный цикл экземпляра сервиса	213
10.5.2. Управление экземплярами сервиса в интерфейсе командной строки	215
10.5.2.1. Развертывание экземпляра сервиса	215
10.5.2.2. Отображение развернутых сервисов	215
10.5.2.3. Управление состоянием сервиса	216

10.5.2.4. Добавление и удаление групп ВМ в экземпляре сервиса	216
10.5.2.5. Управление группой ВМ из состава экземпляра сервиса	217
10.5.3. Управление экземплярами сервиса в веб-интерфейсе ПК СВ	218
10.5.3.1. Развертывание экземпляра сервиса	218
10.5.3.2. Отображение развернутых сервисов	219
10.5.3.3. Управление состоянием сервиса	220
10.5.3.4. Управление группой ВМ из состава экземпляра сервиса	221
10.5.4. Особенности восстановления после сбоя	223
10.6. Автоматическое масштабирование сервиса	223
10.6.1. Особенности масштабирования сервиса	223
10.6.2. Изменение размера группы ВМ в ручном режиме	224
10.6.2.1. В интерфейсе командной строки	224
10.6.2.2. В веб-интерфейсе ПК СВ	224
10.6.3. Настройка автоматического масштабирования	225
10.6.3.1. Общие настройки автоматического масштабирования	225
10.6.3.2. Настройка политики эластичности	226
10.6.3.3. Настройка политики планирования	227
10.6.4. Просмотр установленных политик автоматического масштабирования	228
10.6.4.1. В интерфейсе командной строки	228
10.6.4.2. В веб-интерфейсе ПК СВ	229
Перечень терминов	230
Перечень сокращений	231

1. ФУНКЦИИ АДМИНИСТРАТОРА 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. 4.5);
- 5) управление квотами доступа ВМ к физическому и виртуальному оборудованию (см. 4.6);
- 6) управление перемещением экземпляров ВМ (см. 4.7);
- 7) создание снимков состояния виртуальных машин, включающих файл конфигурации ВМ, образа диска ВМ и образа памяти ВМ (см. 4.8), а также отдельное создание снимков состояния образа диска ВМ (см. 4.9);
- 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.10001-02 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.10001-02 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 VM (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.10001-02 97 01.

Примечание. Если созданный пользователь должен реализовать роль разработчика VM, 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	brest-admin	yes	brestadm	public	2 / -	4G /	0.5 / -
1	serveradmin	yes	brestadm	server_c	0 / -	0M /	0.0 / -
0	oneadmin	yes	brestadm	core	-	-	-

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

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

4. Удаление пользователя с идентификатором 3:

```
oneuser delete 3
```

5. Просмотр перечня пользователей:

```
oneuser list
```

Пример вывода после выполнения команды:

ID	NAME	ENAB	GROUP	AUTH	VMS	MEMORY	CPU
6	newuser	no	brestuse	core	0 / -	0M /	0.0 / -
5	domainuser	no	brestadm	public	0 / -	0M /	0.0 / -
4	otheradmin	no	brestadm	core	0 / -	0M /	0.0 / -
2	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» (см. рис. 1) будет представлена таблица пользователей.

ID	Название	Группа	Включено	Драйвер авторизации	VM	Память	CPU
6	newuser	brestusers	Нет	core		0 / -	0 / -
5	domainuser	brestadmins	Нет	public		0 / -	0 / -
4	otheradmin	brestadmins	Нет	core		0 / -	0 / -
2	bre-st-admin	bre-stadmins	Да	public		2 / -	0.5 / -
1	serveradmin	bre-stadmins	Да	server_cipher		0 / -	0 / -
0	oneadmin	bre-stadmins	Да	core		-	-

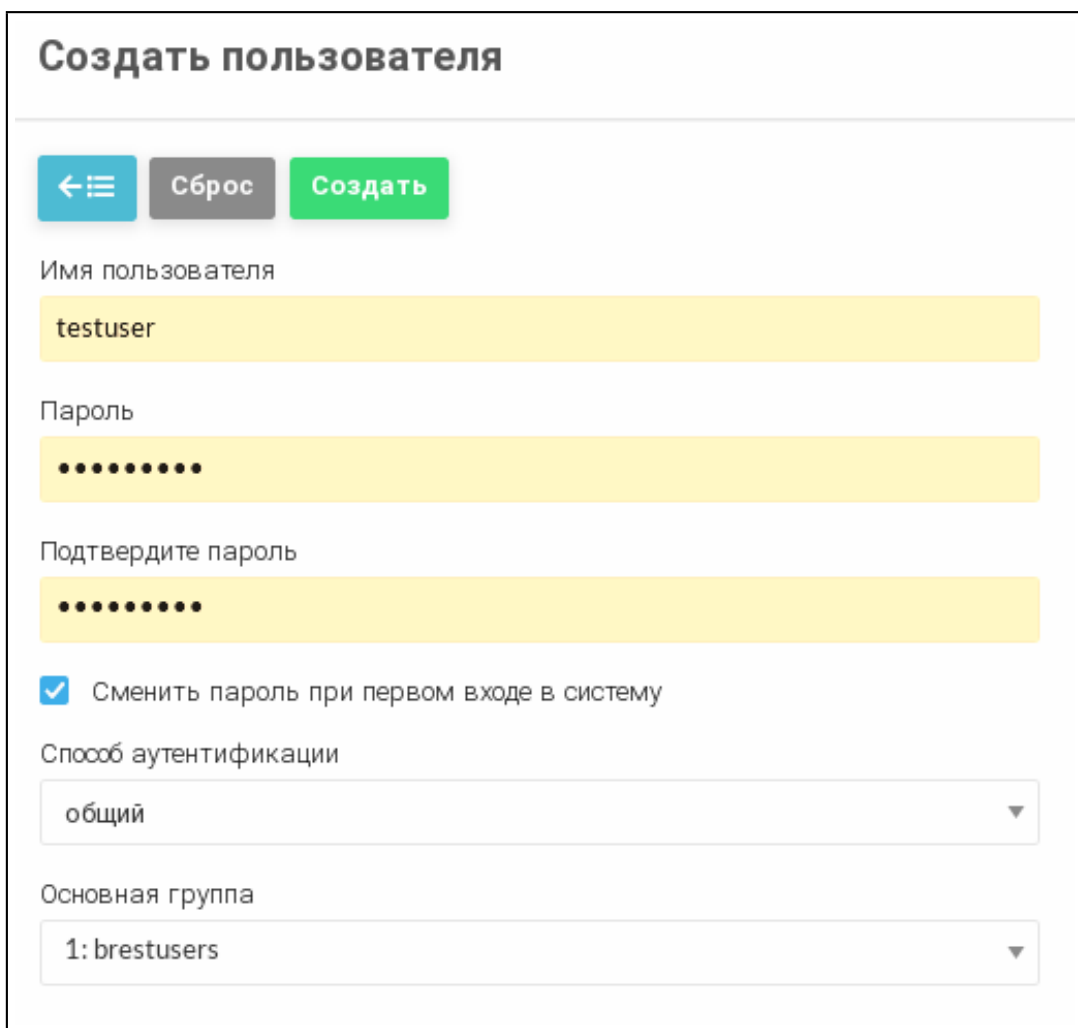
Показаны элементы списка с 1 по 6 из 6

6 всего

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 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 VM — brestusers);



Создать пользователя

← ≡ Сброс Создать

Имя пользователя
testuser

Пароль
••••••••

Подтвердите пароль
••••••••

Сменить пароль при первом входе в систему

Способ аутентификации
общий ▼

Основная группа
1: brestusers ▼

Рис. 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 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).

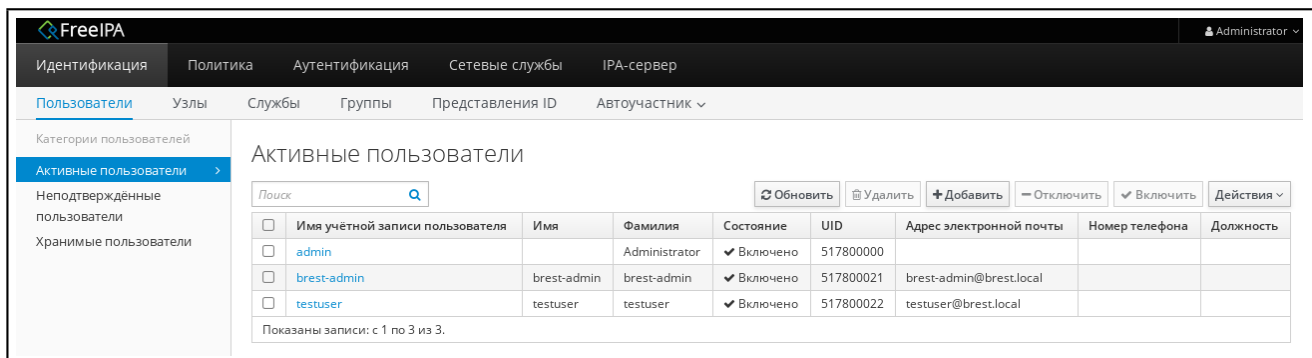


Рис. 3

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.10001-02 97 01.

Примечание. Если созданный пользователь должен реализовать роль разработчика VM, 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).

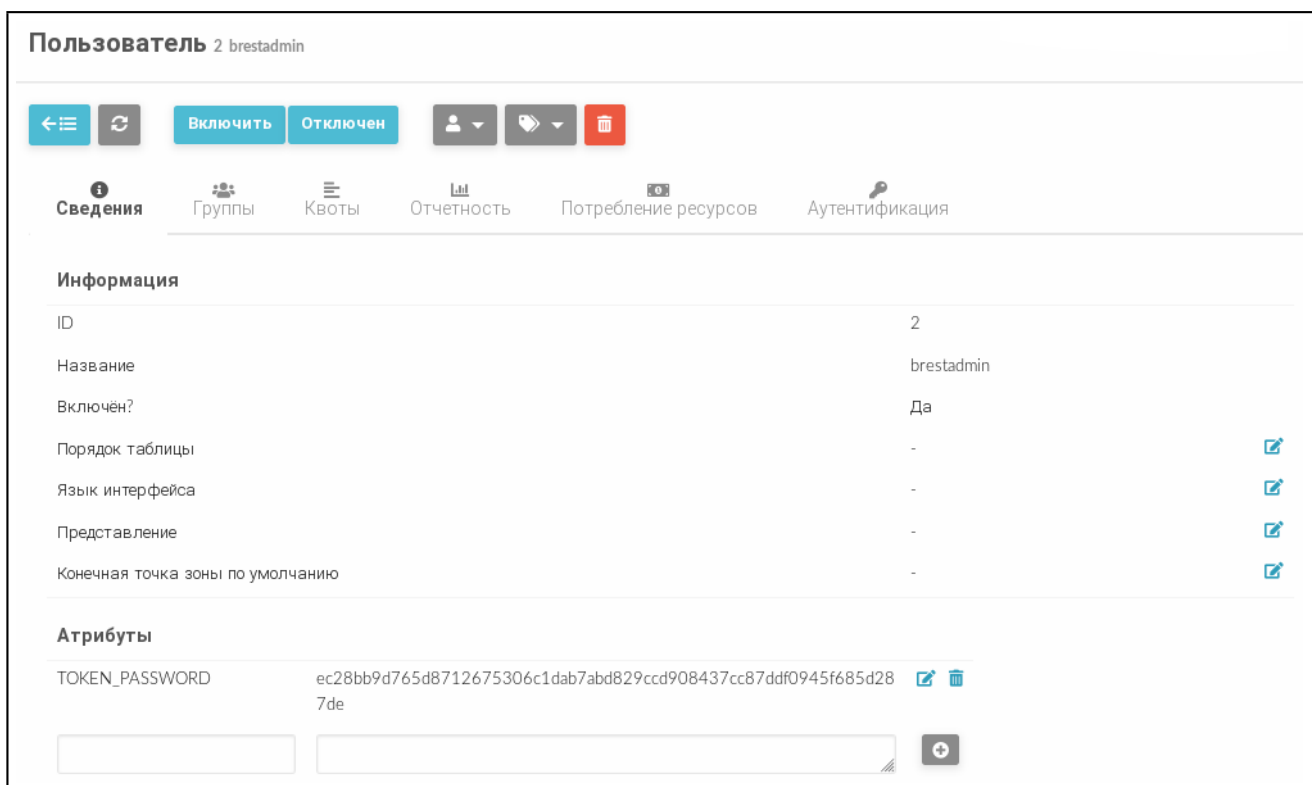


Рис. 4

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.10001-02 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 пользователей. 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 (`brestartusers`). 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 `brestartadmins` 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	brestusers	0	0 / -	0M / -	0.0 / -
0	brestadmins	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 `brestadmins`), необходимо выполнить команду:

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

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

группы brestusers.

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

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

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

3.3.3. Управление группами в веб-интерфейсе ПК СВ

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

Показаны элементы списка с 1 по 5 из 5

5 ВСЕГО

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 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 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).

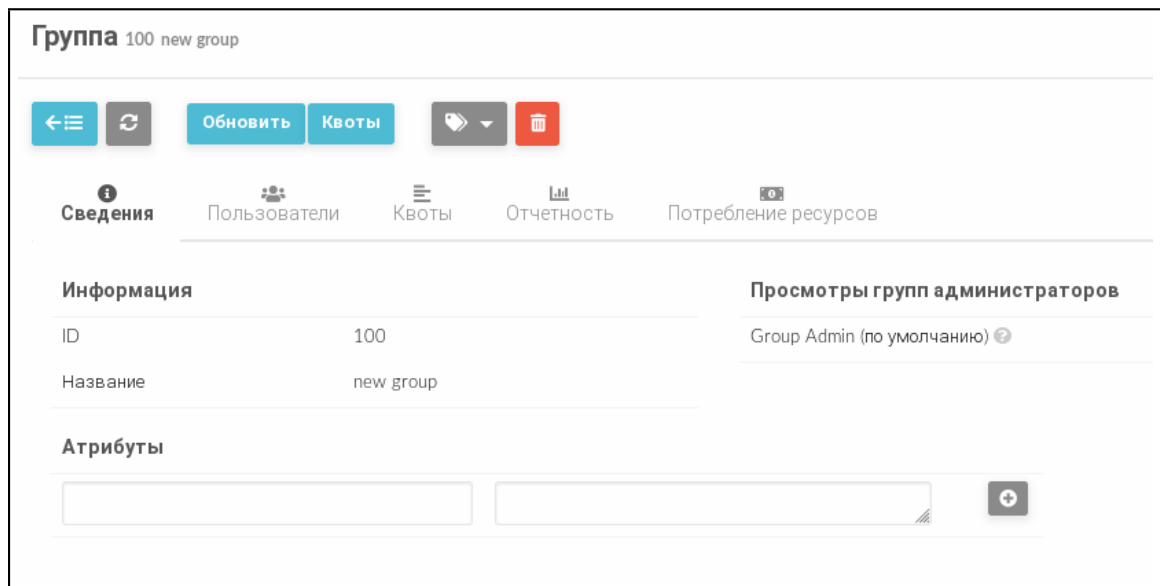


Рис. 7

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 кнопку **[Изменить]** (см. рис. 8);

Пользователь 4 new_group_Admin

← ≡ ↻ Включить Отключен 👤 👤 🗑️

Сведения Группы Квоты Отчетность Потребление ресурсов Аутентификация

Изменить

Основная группа

brestusers

Дополнительная группа

🔄 Поиск

ID	Название	Пользователи	VM	Память	CPU
1	brestusers	1		0 / -	ОКВ / -

10 Показаны элементы списка с 1 по 1 из 1

Предыдущая 1 Следующая

Рис. 8

- 3) на странице «Пользователь» во вкладке «Группы» (см. рис. 9):
- в секции «Основная группа» в выпадающем списке выбрать одну из групп;
 - в секции «Дополнительная группа» в таблице выбрать необходимые группы (если необходимо исключить пользователя из группы — снять выделение);
 - нажать кнопку **[Применить изменения]**.

Пользователь 4 new_group_Admin

Включить Отключен

Сведения Группы Квоты Отчетность Потребление ресурсов Аутентификация

Основная группа

1: brestusers

Дополнительная группа

Вы выбрали следующие группы: brestusers new group

ID	Название	Пользователи	VM	Память	CPU
102	another-group	0		0 / -	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

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 предва-

нительно 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
----	------	--------	----------	-------	-------	------------

РДЦП.10001-02 95 01-2

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 (см. рис. 10).

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 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 во вкладке «Ресурсы» в секции «Кластеры» выделить этот кластер (см. рис. 11)

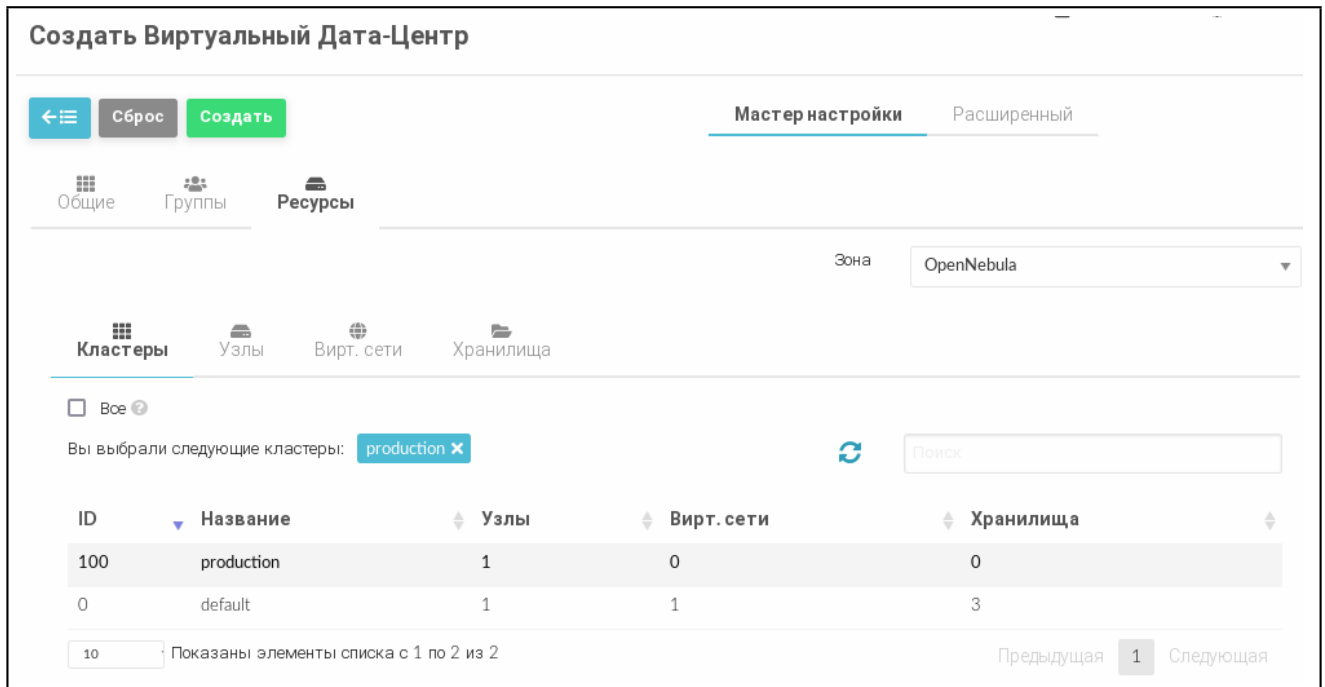


Рис. 11

3) на странице **Создать Virtual Data Center** нажать кнопку **[Создать]**;

После этого на открывшейся странице «Virtual Data Centers» появится запись о созданном VDC.

Для просмотра информации о конкретном VDC на странице «Virtual Data Centers» необходимо выбрать соответствующую строку. После этого откроется страница «Virtual Data Center» (вкладка «Сведения» — см. рис. 12).

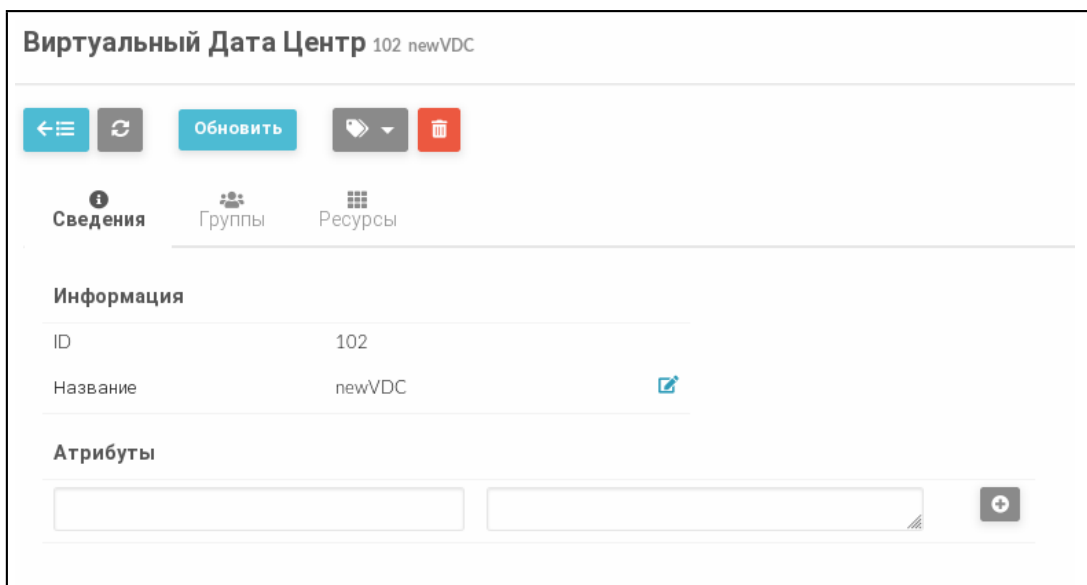


Рис. 12

Чтобы изменить наименование, состав групп или скорректировать перечень физи-

ческих 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 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 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 ресурсов:

- 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).

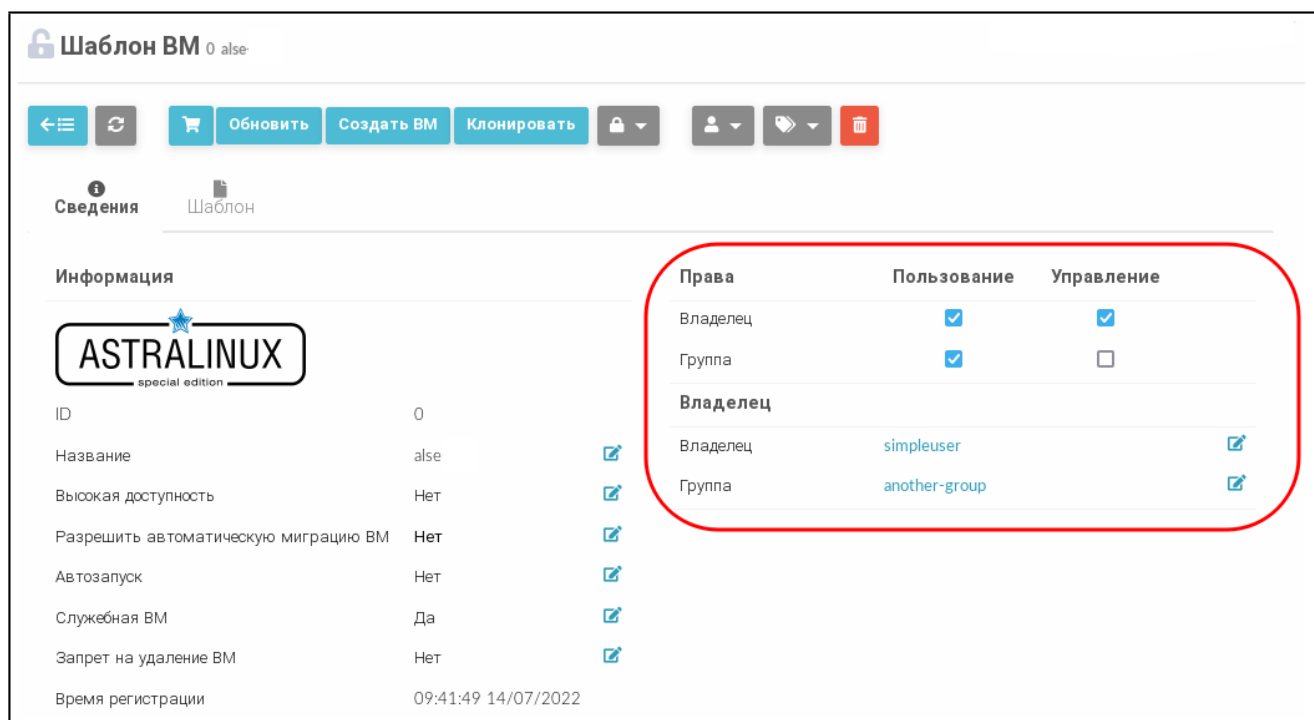


Рис. 13

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 кнопку [+].

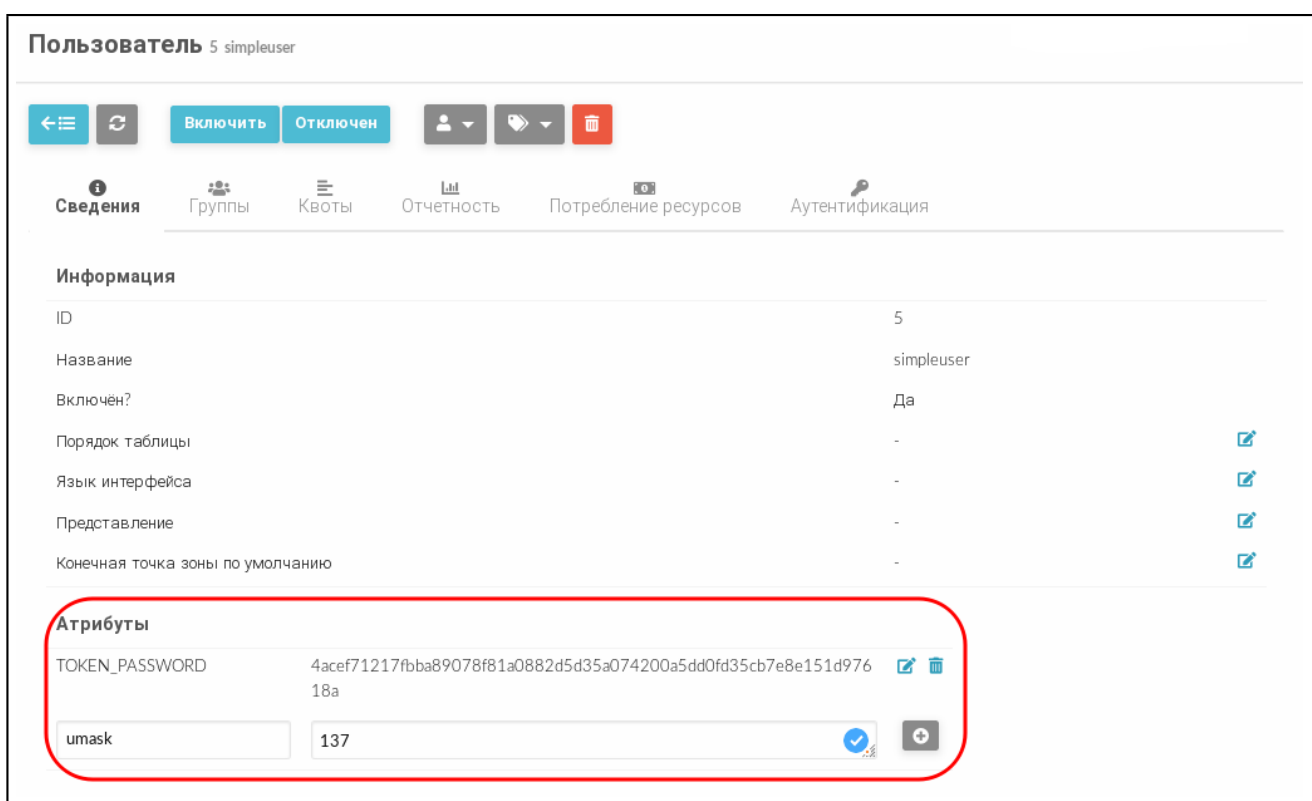


Рис. 14

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 ВМ 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 ВМ 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.10001-02 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 развора-

чивать 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	OPR_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).

ID	Применено к	Затрагиваемые ресурсы	№ ресурса / Принадлежит	Разрешенные действия	Зона
0	Группа brestusers	ВМ, Образы, Шаблоны ВМ, Документы, Группы безопасности, Группы ВМ	Все	create	Все
1	Все	Зоны	Все	use	Все
2	Все	Магазин приложений, Приложения из магазина приложений	Все	use	Все
3	Группа brestusers	Узлы	Все	manage	OpenNebula
4	Группа brestusers	Вирт. сети	Все	use	OpenNebula
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 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

← Сброс Создать

Область применения

Зоны, в которых будет действовать правило
Все

Все
 Пользователь
 Группа

Группа:
100: new group

Затрагиваемые ресурсы

<input type="checkbox"/> Узлы	<input type="checkbox"/> Кластеры	<input type="checkbox"/> Хранилища	<input type="checkbox"/> VM
<input type="checkbox"/> Вирт. сети	<input checked="" type="checkbox"/> Образы	<input type="checkbox"/> Шаблоны	<input type="checkbox"/> Пользователи
<input type="checkbox"/> Группы	<input type="checkbox"/> Документы	<input type="checkbox"/> Зоны	<input type="checkbox"/> Группы безопасности
<input type="checkbox"/> VDCs	<input type="checkbox"/> Вирт. маршрутизаторы	<input type="checkbox"/> Магазины приложений	<input type="checkbox"/>
<input type="checkbox"/> Группа VM			Приложения из магазина приложений

Подмножество ресурсов

Все
 ID
 Группа
 Кластер

Группа:
102: another-group

Рис. 16

3) на странице «Создать правило контроля» в поле «Строка, задающая правило» проверить корректность сформированного правила и нажать 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 кнопку **[Удалить]**;
- 3) в открывшемся окне «Удалить» нажать кнопку **[OK]**.

3.6.5. Использование правил ACL для реализации роли разработчика VM

Для реализации роли разработчика VM 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 VM. 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 ВМ сигнал ACPI для завершения работы и ожидает его выполнения. Если за время ожидания ВМ не будет удалена, система будет считать, что ОС виртуальной машины проигнорировала сигнал ACPI, и статус ВМ будет изменен на RUNNING, вместо UNDEPLOYED
EPILOG_UNDEPLOY	epil	Система очищает сервер виртуализации, который использовался для запуска ВМ, кроме того, образы постоянных дисков перемещаются обратно в хранилище образов
PROLOG_UNDEPLOY	prol	Передача файлов после возобновления действия (связан с статусом UNDEPLOY)
BOOT_UNDEPLOY	boot	Система ожидает, пока сервер виртуализации создаст ВМ (связан с статусом UNDEPLOY)
HOTPLUG_PROLOG_POWEROFF	hotp	Передача файлов для подключения к диску при отключении питания
HOTPLUG_EPILOG_POWEROFF	hotp	Передача файлов при отсоединении диска от источника питания
BOOT_MIGRATE	boot	Система ожидает, пока сервер виртуализации создаст ВМ (в результате «холодной» миграции)
BOOT_FAILURE	fail	Сбой при переводе в состояние BOOT
BOOT_MIGRATE_FAILURE	fail	Сбой при переводе в состояние BOOT_MIGRATE
PROLOG_MIGRATE_FAILURE	fail	Сбой при переводе в состояние PROLOG_MIGRATE
PROLOG_FAILURE	fail	Сбой при переводе в состояние PROLOG
EPILOG_FAILURE	fail	Сбой при переводе в состояние EPILOG

Продолжение таблицы 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. 4.2.2) или в веб-интерфейсе ПК СВ на странице ВМ во вкладке «Сведения» (см. 4.3.2).

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. Создание экземпляра ВМ

Для создания экземпляра ВМ предварительно необходимо подготовить шаблон ВМ. Порядок управления шаблонами виртуальной машины приведен в документе РДЦП.10001-02 93 01 «Программный комплекс «Средства виртуализации «Брест». Руководство пользователя».

Для развертывания ВМ из шаблона можно воспользоваться командой:

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

где <файл_параметров> — файл в котором перечислены параметры ВМ, заменяющие

значения, которые были определены в шаблоне. Кроме того, возможно вместо файла параметров в команде в качестве аргумента указывать новые значения параметров.

Примеры:

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

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

Пример вывода после выполнения команды:

```
VM ID: 1
```

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

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

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

<наименование_шаблона>-<идентификатор_VM>

Пример

Развертывание двух VM из шаблона с идентификатором 0:

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

4.2.2. Отображение существующих VM

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

Пример вывода после выполнения команды:

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

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

Для просмотра полной информации о VM необходимо использовать команду:

```
onevm show <идентификатор_VM>
```

Пример вывода после выполнения команды `onevm show 1`:

```
VIRTUAL MACHINE 1 INFORMATION
```

```
ID                : 1
NAME              : test-vm-1
USER              : brestadmin1
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               : ---
```

4.2.3. 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.

4.2.4. 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 вы-

деленные 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.

4.2.5. Запуск экземпляров VM

Чтобы возобновить работу VM при успешной остановке или приостановке их работы, а также запустить VM, развертывание которых было отменено или электропитание которых было отключено, необходимо выполнить команду:

```
onevm resume <идентификатор_VM>
```

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

4.2.6. Перезагрузка экземпляров VM

Для перезагрузки VM используются следующие команды:

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

4.2.7. Отсрочка развертывания экземпляров VM

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

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

4.3. Управление экземплярами VM в веб-интерфейсе ПК СВ

4.3.1. Создание экземпляра VM

Для создания экземпляра VM предварительно необходимо подготовить шаблон VM. Порядок управления шаблонами виртуальной машины приведен в документе РДЦП.10001-02 93 01 «Программный комплекс «Средства виртуализации «Брест». Руководство пользователя».

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

- 1) в меню слева выбрать пункт «Шаблоны — VM»;
- 2) на открывшейся странице «Шаблоны VM» выбрать необходимый шаблон;
- 3) на открывшейся странице «Шаблон VM» нажать кнопку **[Создать VM]** (см. рис. 17);

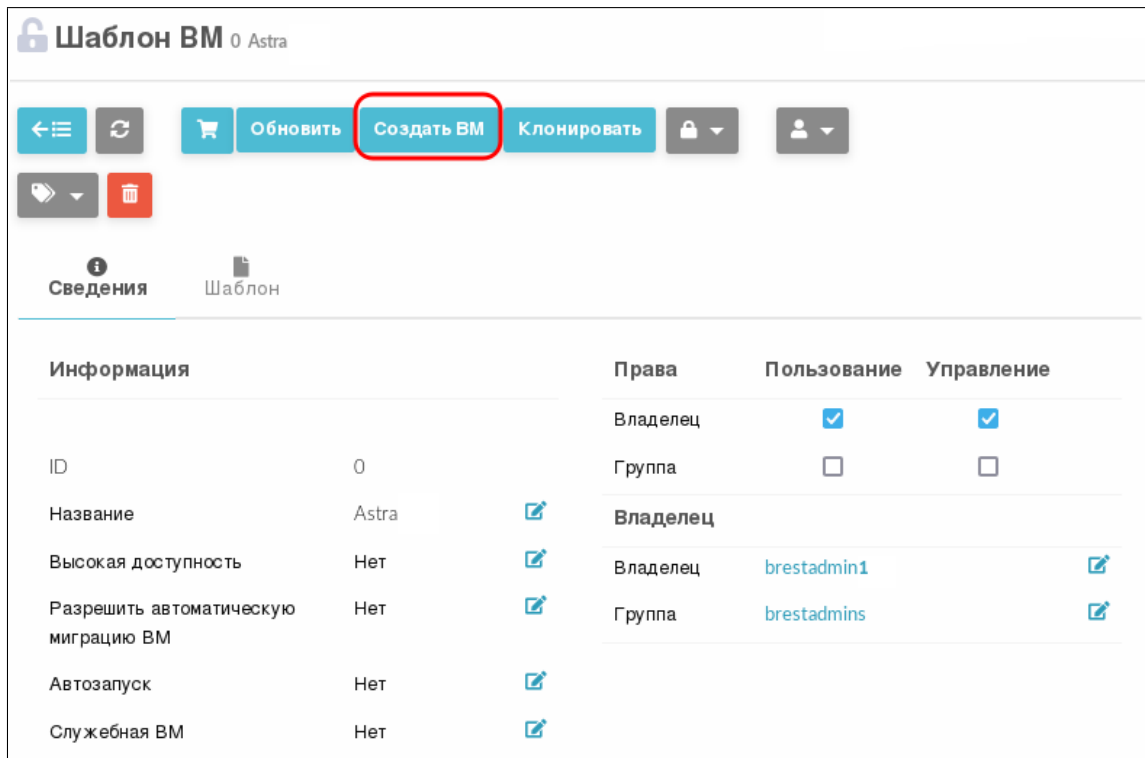


Рис. 17

4) на открывшейся странице «Создать VM» в поле «Имя VM» задать наименование и количество экземпляров VM и нажать кнопку **[Создать VM]** (см. рис. 18);

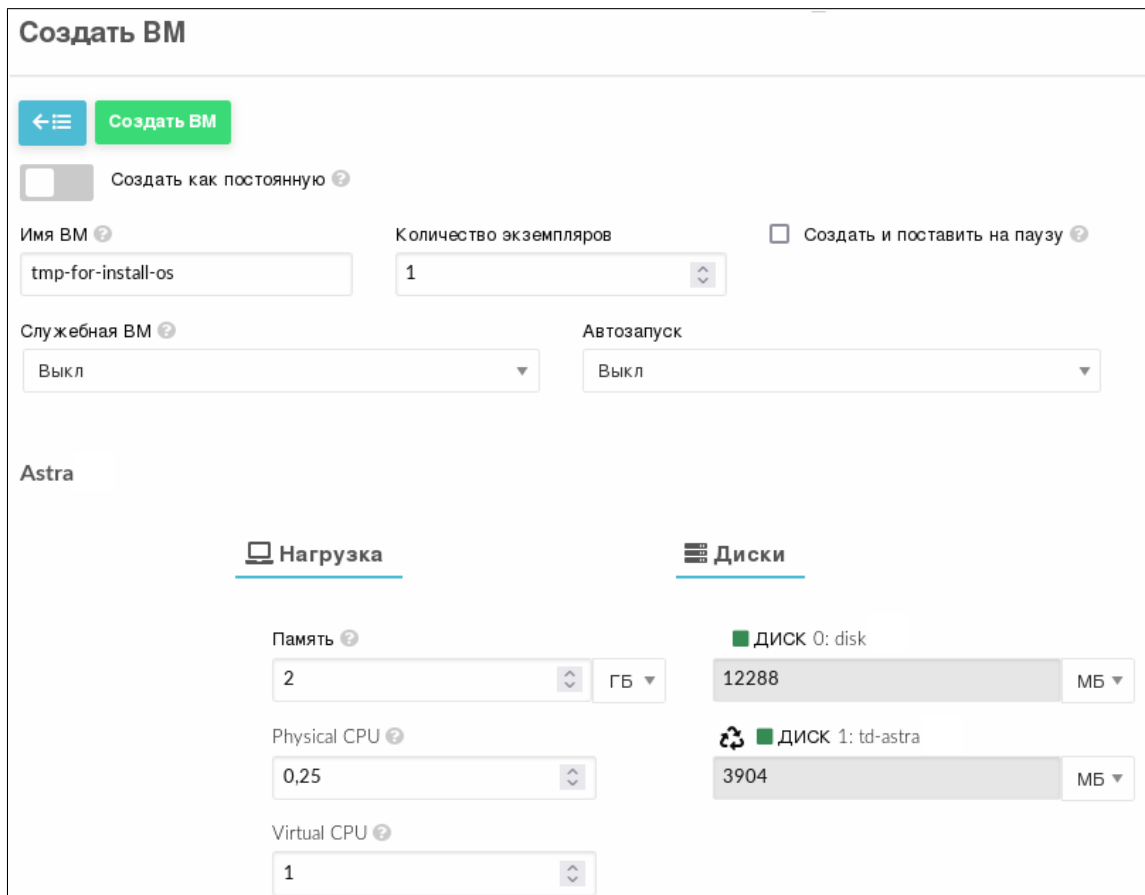


Рис. 18

5) в веб-интерфейсе в меню слева выбрать пункт «Экземпляры VM – VM» и дождаться пока в поле «Статус» для созданной на предыдущем шаге VM значение Инициализация не изменится на **ВЫКЛЮЧЕНО** (промежуточные значения: Ожидание и Пролог). Для обновления значения статуса можно воспользоваться кнопкой **[Обновить]** (см. рис. 19).

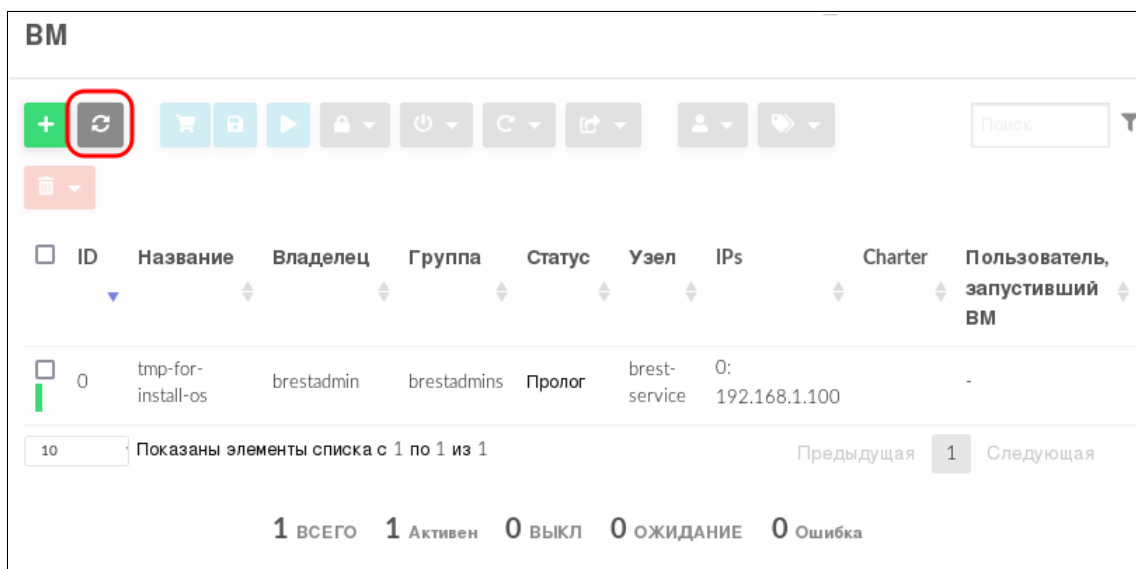


Рис. 19

Кроме того, создать экземпляр VM можно непосредственно на странице перечня виртуальных машин, для этого необходимо выполнить следующие действия:

- 1) в веб-интерфейсе ПК СВ необходимо в меню слева выбрать пункт «Экземпляры VM – VM»;
- 2) на открывшейся странице «VM» нажать кнопку **[+]**;
- 3) на открывшейся странице «Укажите параметры виртуальной машины» (см. рис. 20) выбрать шаблон VM;

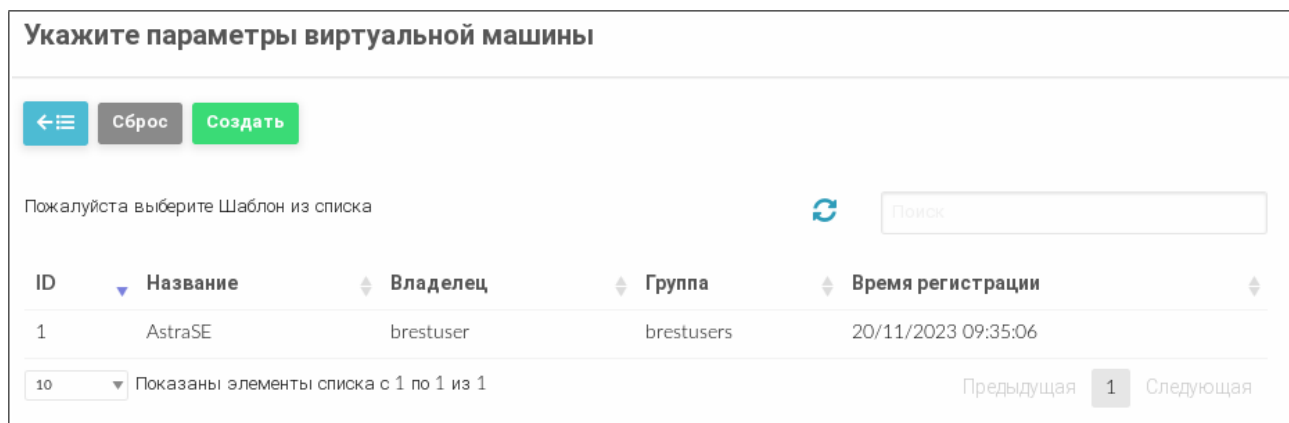


Рис. 20

4) на странице «Укажите параметры виртуальной машины» в поле «Имя VM» задать наименование и количество экземпляров VM и нажать кнопку **[Создать]**.

4.3.2. Отображение существующих VM

Для отображения существующих VM в веб-интерфейсе ПК СВ необходимо в меню слева выбрать пункт «Экземпляры VM — VM». На открывшейся странице «VM» будет отображена таблица экземпляров VM (см. рис. 21)

ID	Название	Владелец	Группа	Статус	Узел	IPs	Charter	Пользователь, запустивший VM	MAC	Подключение
1	test-vm-1	oneadmin	brestadmins	ВЫКЛЮЧЕНО	172.16.1.210	0: 172.16.1.100	-	-	-	-

Показаны элементы списка с 1 по 1 из 1

1 ВСЕГО 0 Активен 1 ВЫКЛ 0 ОЖИДАНИЕ 0 Ошибка

Рис. 21

Для просмотра полной информации о VM необходимо на странице «VM» выбрать необходимую VM. После этого откроется страница виртуальной машины (вкладка «Сведения») (см. рис. 22).

Информация		Права	Пользование	Управление
ID	1	Владелец	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Название	test-vm-1	Группа	<input type="checkbox"/>	<input type="checkbox"/>
Состояние	ВЫКЛЮЧЕНО	Владелец		
Текущее состояние VM	LCM_INIT	Владелец	oneadmin	✎
Узел	172.16.1.210	Группа	brestadmins	✎
Высокая доступность	Нет			✎
Разрешить автоматическую миграцию VM	Нет			✎
Автозапуск	Нет			✎
Служебная VM	Да			✎
Запрет на удаление VM	Нет			✎
IP-адрес	0: 172.16.1.100			
Время запуска	19:05:39 18/07/2022			

Рис. 22

4.3.3. Завершение работы и приостановка экземпляров ВМ

Для завершения работы экземпляра ВМ или его приостановки в веб-интерфейсе ПК СВ используется кнопка **[Управление питанием]**, после нажатия на которую откроется меню действий (см. рис. 23):

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

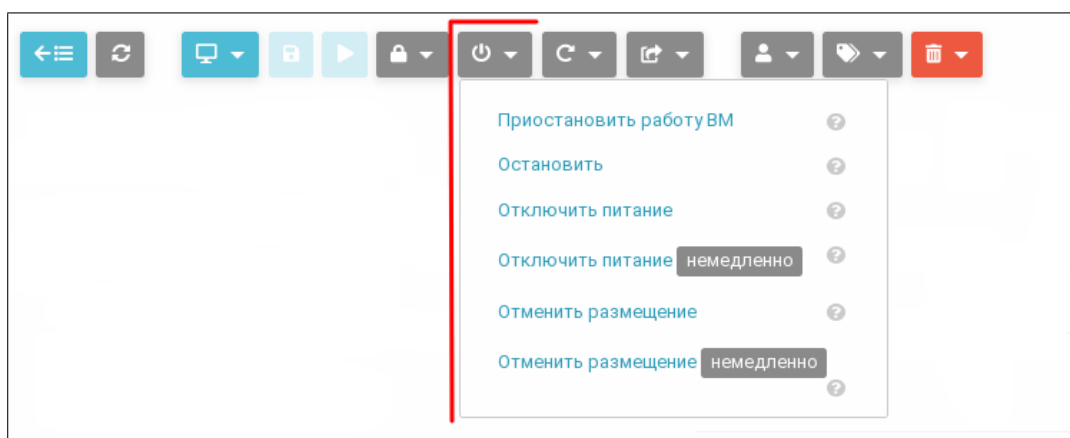


Рис. 23

4.3.4. Запуск экземпляра ВМ

Чтобы возобновить работу ВМ после успешной остановки или приостановки ее работы, а также запустить ВМ, развертывание которой было отменено или электропитание

которых было отключено, необходимо нажать кнопку **[Запустить]** (см. рис. 24):



Рис. 24

4.3.5. Перезагрузка экземпляров ВМ

Для перезагрузки ВМ в веб-интерфейсе ПК СВ используется кнопка **[Перезагрузка]**, после нажатия на которую откроется меню действий (см. рис. 25):

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



Рис. 25

4.3.6. 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. 26):

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

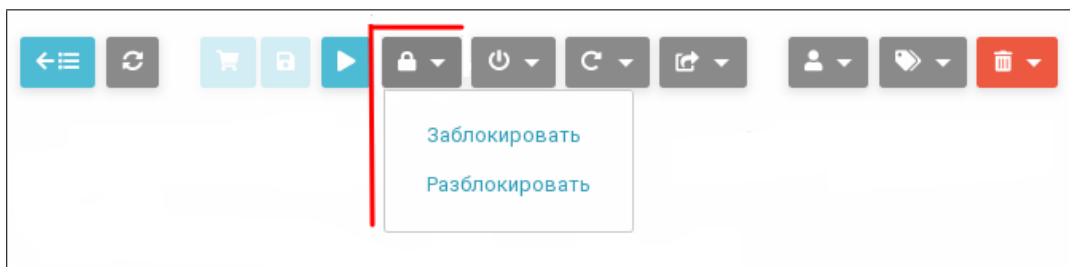


Рис. 26

4.3.7. Удаление экземпляров ВМ

Для удаления экземпляров ВМ в веб-интерфейсе ПК СВ используется кнопка **[Уничтожить]**, после нажатия на которую откроется меню действий (см. рис. 27):

- Уничтожить — корректно завершить работу и удалить ВМ, отправляя сигнал ACPI. Если по истечении определенного времени после выполнения команды ВМ все еще

работает, т.е. ОС виртуальной машины игнорирует сигналы ACPI, служба сервера управления снова присвоит VM статус RUNNING;

- Уничтожить (немедленно) — удалить VM незамедлительно. Следует использовать данную команду, если VM не поддерживает ACPI.



Рис. 27

4.4. Настройка дискреционного и мандатного управление доступом к VM

Дискреционное и мандатное управление доступом, а также управление режимом запрета модификации образов дисков виртуальных машин осуществляются СЗИ из состава ОС СН.

ВНИМАНИЕ! Дискреционное и мандатное управление доступом к VM обеспечивается только в дискреционном режиме функционирования ПК СВ. В таком режиме VM запускаются от имени доменного пользователя, авторизовавшегося в ПК СВ.

В ПК СВ различаются два типа дискреционного доступа к виртуальной машине:

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

Примечание. При установке ПК СВ максимальный уровень целостности компонентов ОС (как и компонентов ПК СВ) повышается до 127. Целостность VM по умолчанию равна 63, ее можно изменить в конфигурационном файле `/etc/libvirt/libvirtd.conf` (параметр `ilev_vm`).

Для настройки мандатного управления доступом к VM требуется указать тип модели `parsec`:

- «Динамический» — уровень доступа к VM назначается согласно классификационной метке пользователя;
- «Статический» — заданный уровень доступа в соответствии с классификационной меткой вида «X:0:0xY», где:
 - «X» — иерархический уровень конфиденциальности;
 - «0» — неиерархический уровень целостности (игнорируется);
 - «0xY» — неиерархическая категория конфиденциальности.

Примечания:

1. По умолчанию в ПК СВ используется динамический тип модели `parsec`, т.е. при запуске ВМ приобретает метки безопасности, включающие идентификатор запустившего ее пользователя и его мандатные атрибуты. После этого при доступе к данной ВМ применяются дискреционное и мандатное управление доступом.
2. Использование статического типа модели `parsec` позволяет определить доступ к ВМ в случае наличия нескольких уровней и категорий ограничения доступа у пользователя или скорректировать доступ исходя из потребностей на объекте эксплуатации.
3. В случае использования ОС СН в качестве гостевой операционной системы виртуальная машина не должна запускаться в мандатном контексте. Вместо этого необходимо выполнять удаленный вход с требуемым мандатным уровнем доступа средствами ОС СН.
4. При запуске ВМ в ненулевом мандатном контексте рекомендуется использовать режим только на чтение.

Для настройки дискреционного и мандатного управления доступом к ВМ необходимо выполнить следующие действия:

- 1) в веб-интерфейсе ПК СВ в меню слева выбрать пункт «Экземпляры ВМ — ВМ»;
- 2) на открывшейся странице «ВМ» из списка выбрать ВМ, для которой необходимо настроить доступ;
- 3) на странице ВМ во вкладке «Безопасность» (см. рис. 28):
 - а) в секции «Модель PARSEC» в выпадающем списке «Тип» выбрать тип модели `parsec`. При выборе статической модели в поле «Метка» необходимо также задать классификационную метку;
 - б) в секции «Дискреционный контроль доступа»:
 - в выпадающем списке «Тип» выбрать тип субъекта (Пользователь или Группа), в отношении которого будет применяться правило доступа;
 - в выпадающем списке «Субъект» выбрать учетную запись субъекта, в отношении которого будет применяться правило доступа;
 - в выпадающем списке «Права доступа» выбрать тип дискреционного доступа (Использование или Управление);
 - если необходимо добавить правило доступа, то следует нажать кнопку **[Добавить]**;
 - если необходимо удалить правило доступа, то следует нажать кнопку **[Удалить]**;
- 4) нажать кнопку **[Сохранить]**.

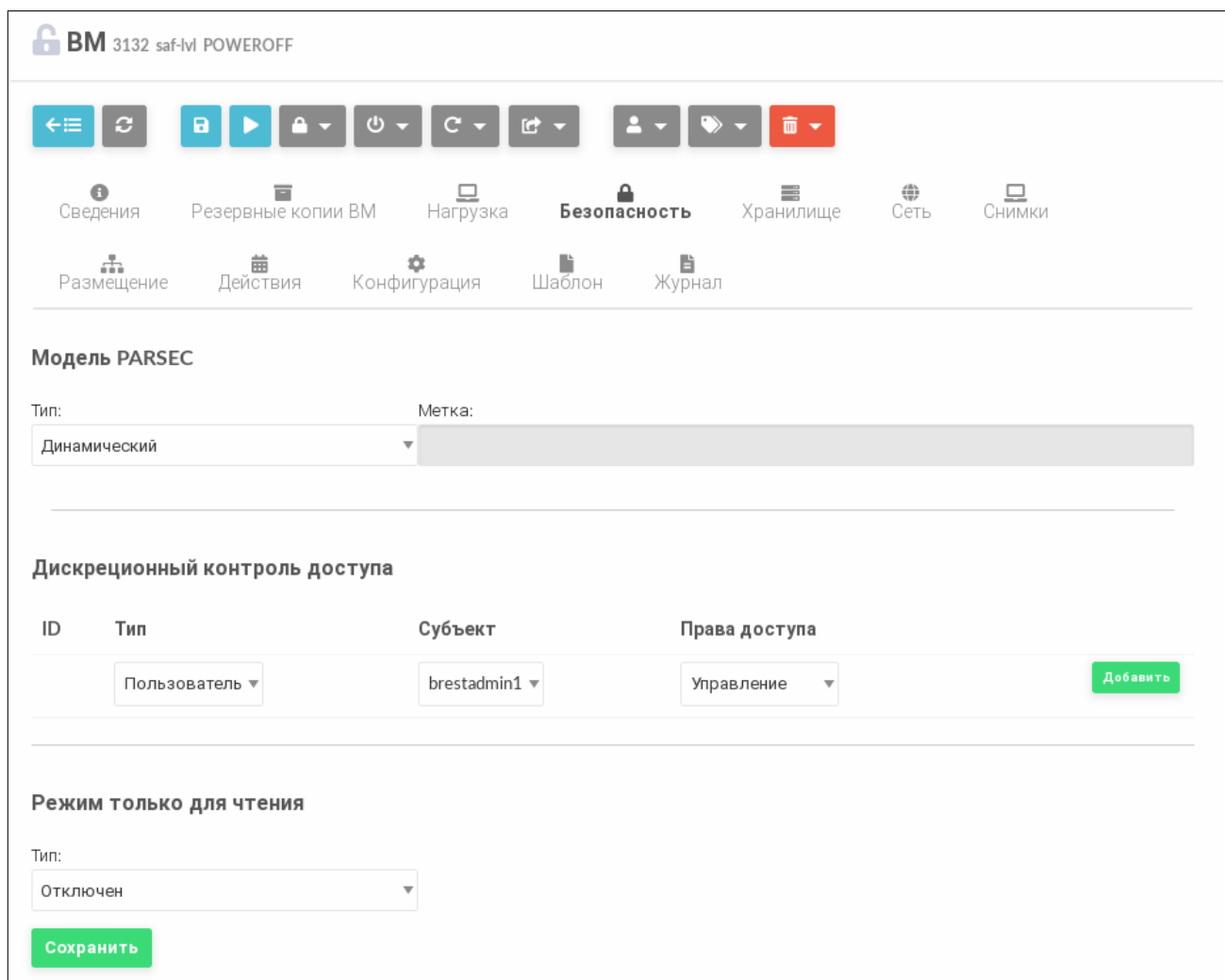


Рис. 28

ВНИМАНИЕ! Настройка доступа возможно только для выключенной VM.

4.5. Управление доступом виртуальных машин к физическому и виртуальному оборудованию

4.5.1. 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.

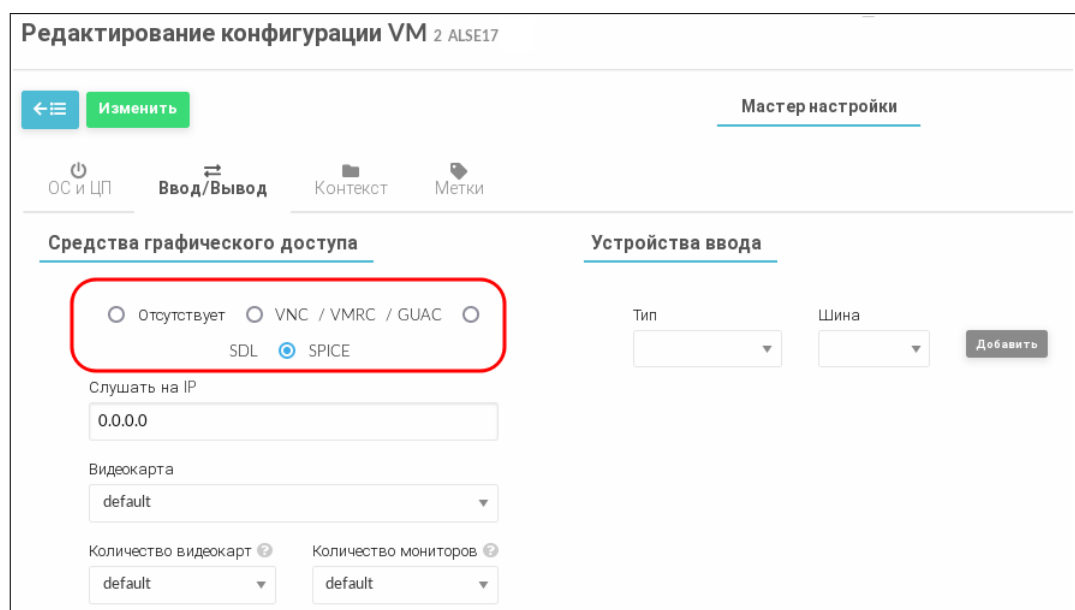
Для того чтобы обеспечить возможность перенаправить подключенные USB-устройства на VM, необходимо выполнить следующие действия:

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 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. 29),



Редактирование конфигурации VM 2 ALSE17

Изменить Мастер настройки

ОС и ЦП Ввод/Вывод Контекст Метки

Средства графического доступа Устройства ввода

Отсутствует VNC / VMRC / GUAC SPICE SDL

Слушать на IP: 0.0.0.0

Видеокарта: default

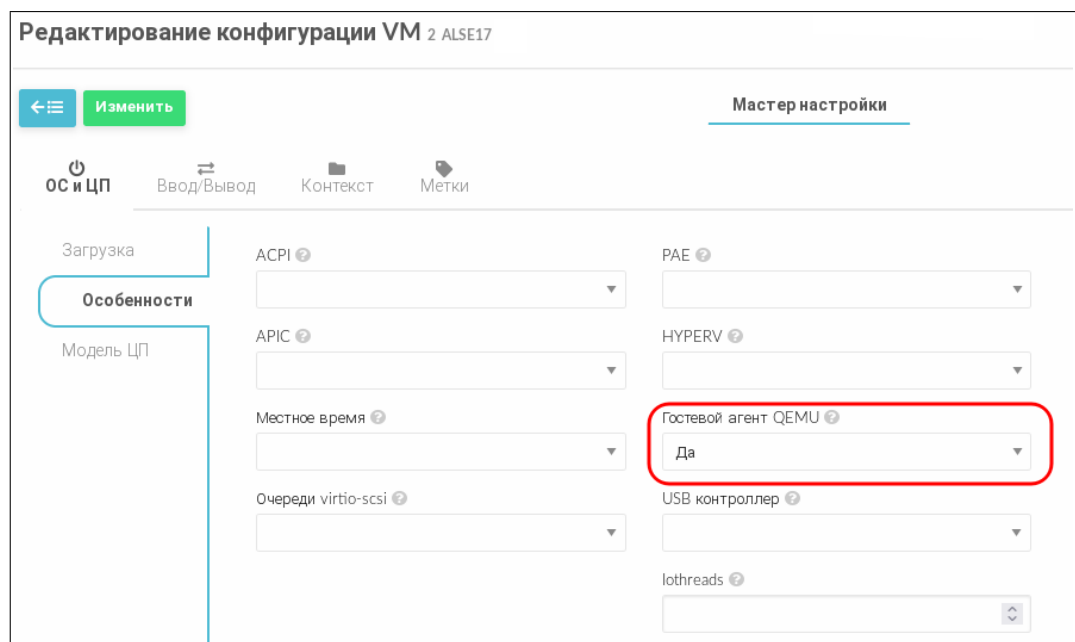
Количество видеокарт: default

Количество мониторов: default

Тип Шина Добавить

Рис. 29

- при выборе RDP — во вкладке «ОС и ЦП» в секции «Особенности» в выпадающем списке «Гостевой агент Qemu» выбрать «Да» (см. рис. 30),



Редактирование конфигурации VM 2 ALSE17

Изменить Мастер настройки

ОС и ЦП Ввод/Вывод Контекст Метки

Загрузка Особенности Модель ЦП

АСПИ PAE

APIC HYPERV

Местное время **Гостевой агент QEMU**

Очереди virtio-scsi USB контроллер

lothreads

Рис. 30

- 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. 30),

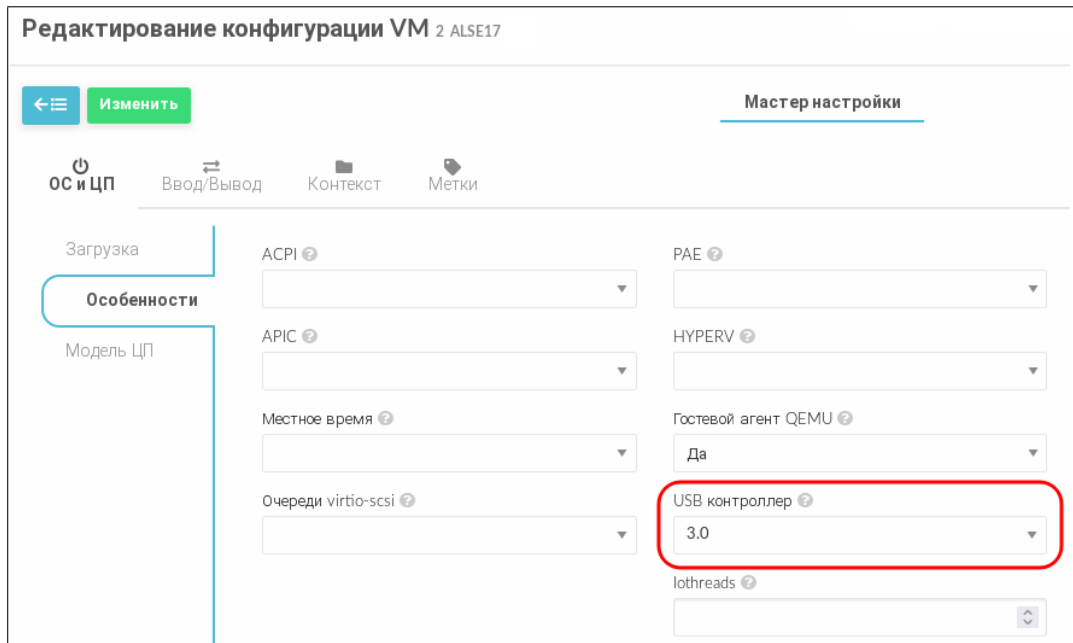


Рис. 31

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

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

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

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

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

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

Для того чтобы перенаправить подключенное USB-устройство на 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. 32).

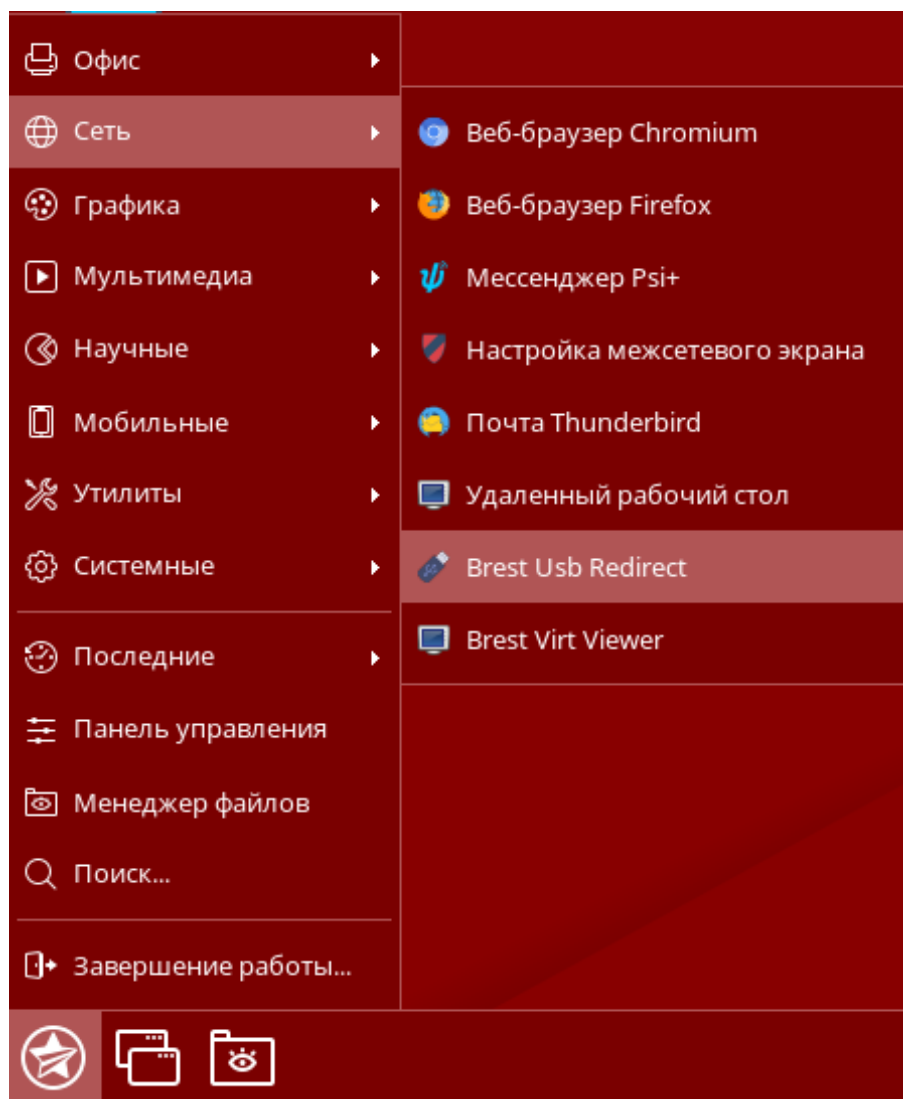
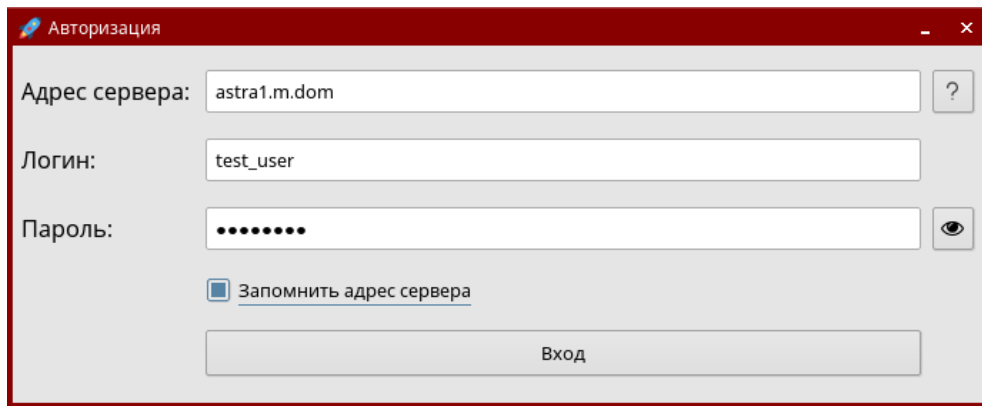


Рис. 32

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. 33) 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

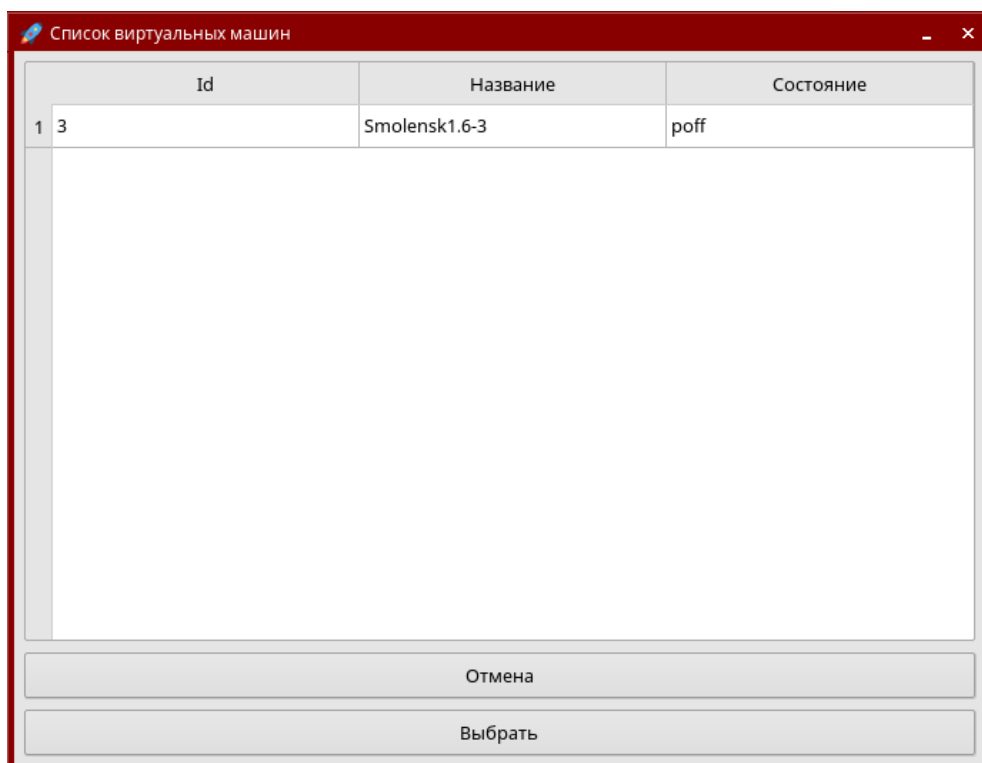
Пароль:

Запомнить адрес сервера

Вход

Рис. 33

3) в открывшемся окне «Список виртуальных машин» (см. рис. 34) указать виртуальную машину, на которую необходимо перенаправить USB-устройство.



Id	Название	Состояние
1 3	Smolensk1.6-3	poff

Отмена

Выбрать

Рис. 34

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. 35) выбрать одно или несколько USB-устройств, которые необходимо перенаправить;

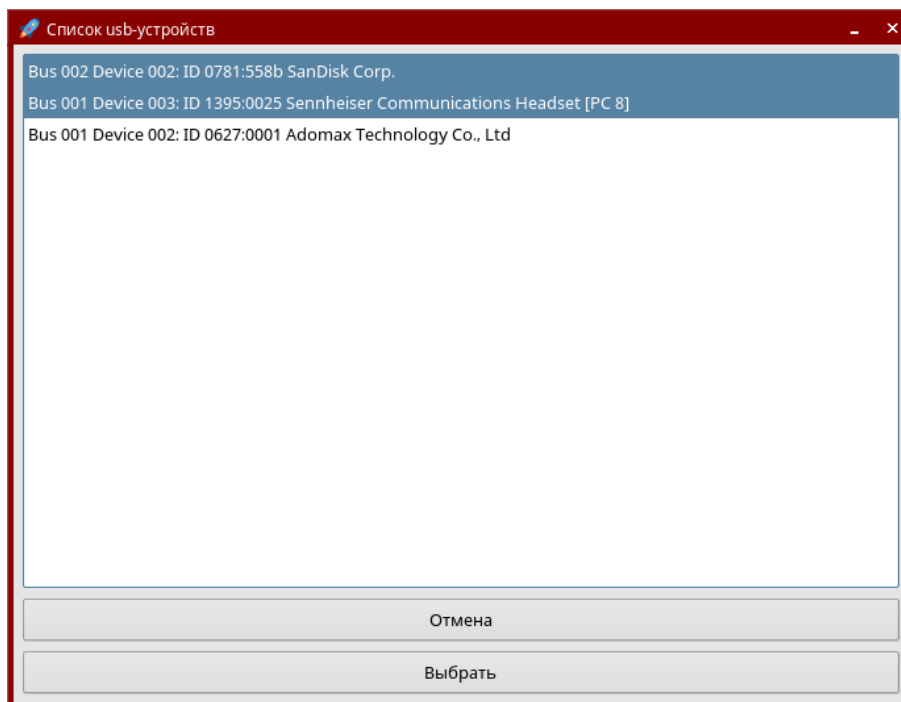


Рис. 35

5) в открывшемся окне «Доступные подключения» (см. рис. 36) выбрать протокол подключения;

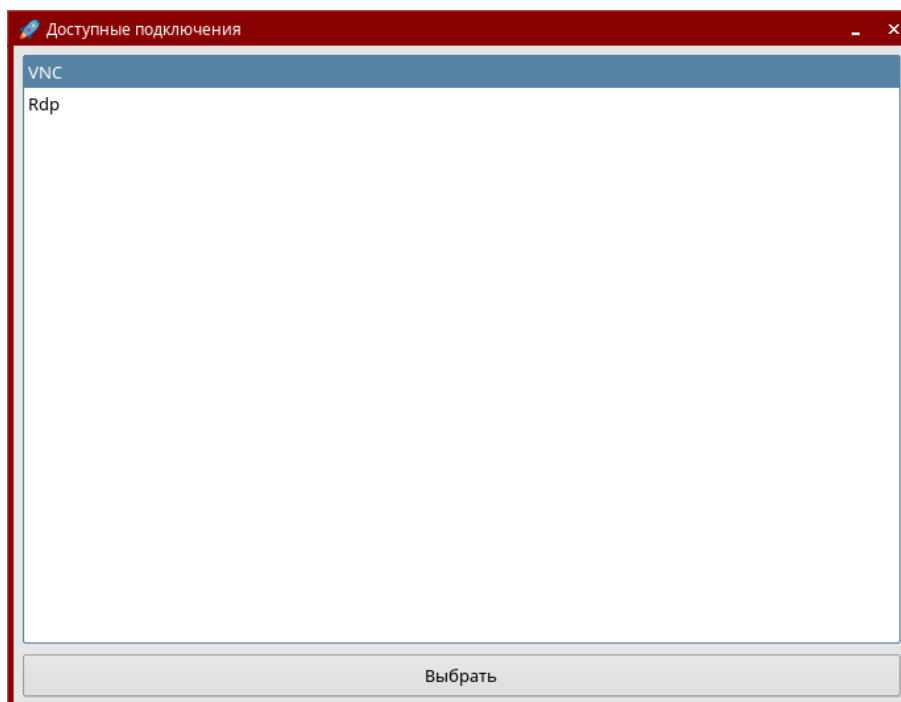


Рис. 36

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. 37).

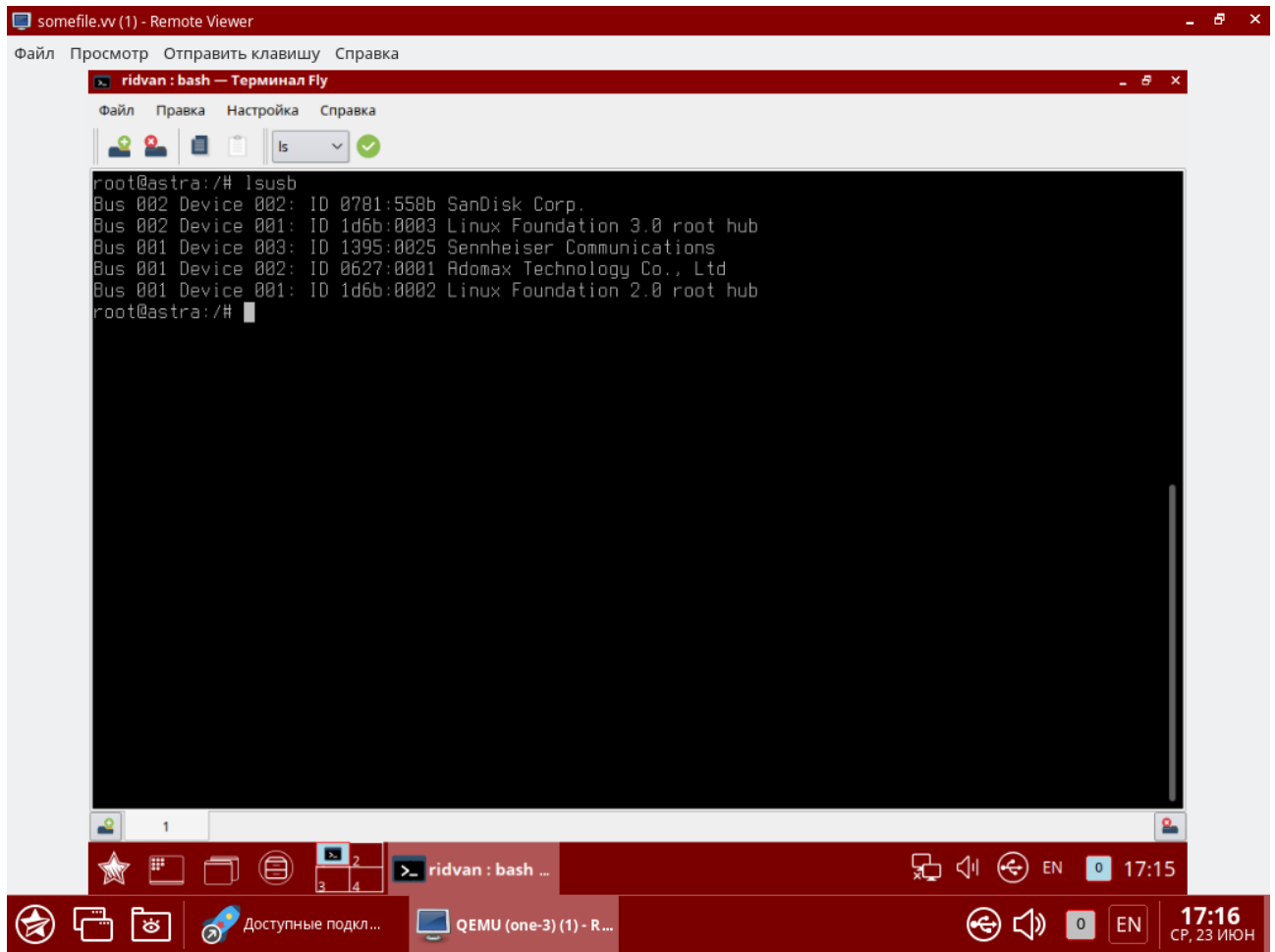


Рис. 37

4.5.2. Ретрансляция PCI

Устройства PCI серверов виртуализации можно перенаправлять на виртуальные машины.

4.5.2.1. 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.

4.5.2.2. Настройка сервера виртуализации

4.5.2.3. 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 блокировать драйверы для выбранных карт. Например, для графической платы nvidia можно применять следующие параметры:

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

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

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

4.5.2.4. 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
```

4.5.2.5. 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 lbm-nouveau
options nouveau modeset=0
alias nouveau off
alias lbm-nouveau off
```

Наряду с этой конфигурацией драйвер vfio должен быть загружен с передачей идентификатора карт PCI, которые предполагается подключить к VM. 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
```

4.5.2.6. Привязка устройств к vfio

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

им группы можно использовать совместно используемые скрипты.

Пример

Скрипт привязывает карту к vfio, прописывается в файле

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

Необходимо сделать этот скрипт исполняемым.

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

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

Приведенный в примере выше скрипт необходимо добавить в автостарт системы.

Для этого следует выполнить следующие действия:

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

```
[Unit]
Description=Binds devices to vfio-pci
After=syslog.target

[Service]
EnvironmentFile=-/etc/default/vfio-bind
Type=oneshot
RemainAfterExit=yes
ExecStart=-/usr/local/bin/vfio-bind $DEVICES

[Install]
WantedBy=multi-user.target
```

2) перезагрузить список служб командой:

```
sudo systemctl daemon-reload
```

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

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

4.5.2.7. 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"
]
```

4.5.2.8. 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
```

4.5.2.9. 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

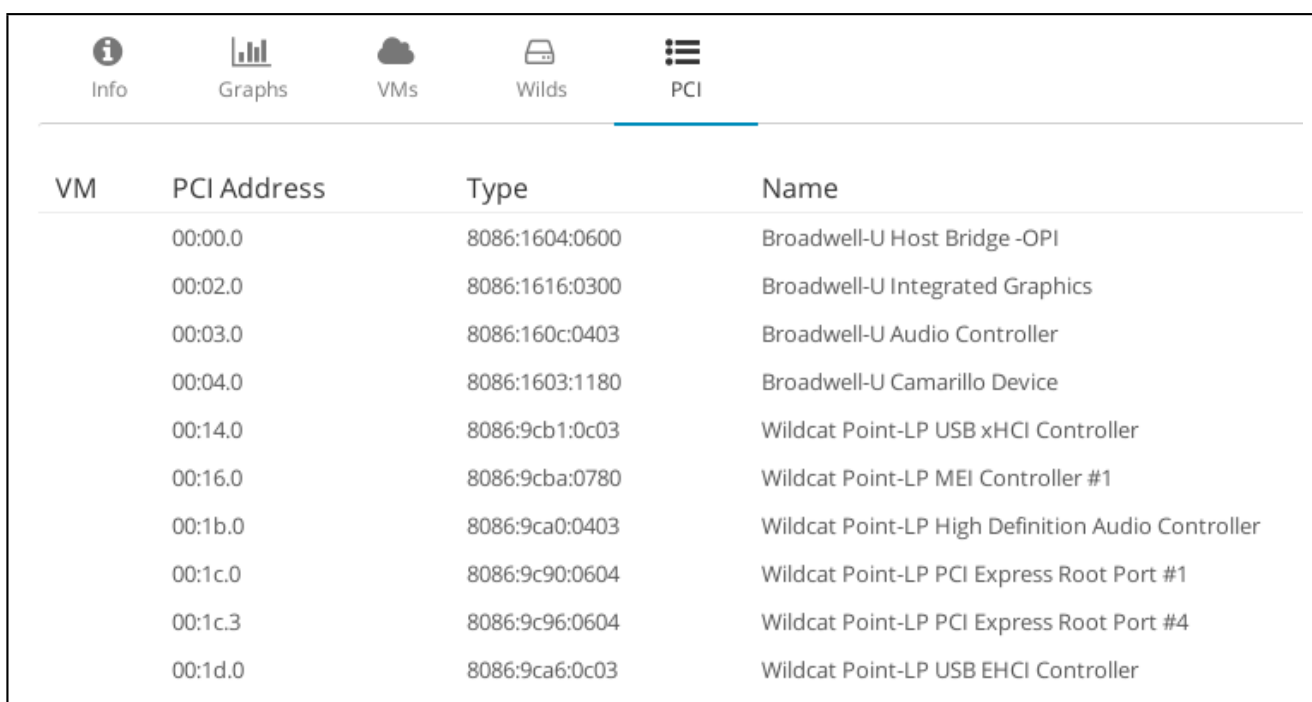
получения любых портов PCI Express Root Ports в шаблон VM можно добавить:

```
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. 38)



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. 38

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 кнопку **[Обновить]**;
- 3) на открывшейся странице «Изменить шаблон VM» открыть вкладку «Ввод/Вывод» (рис. 39).

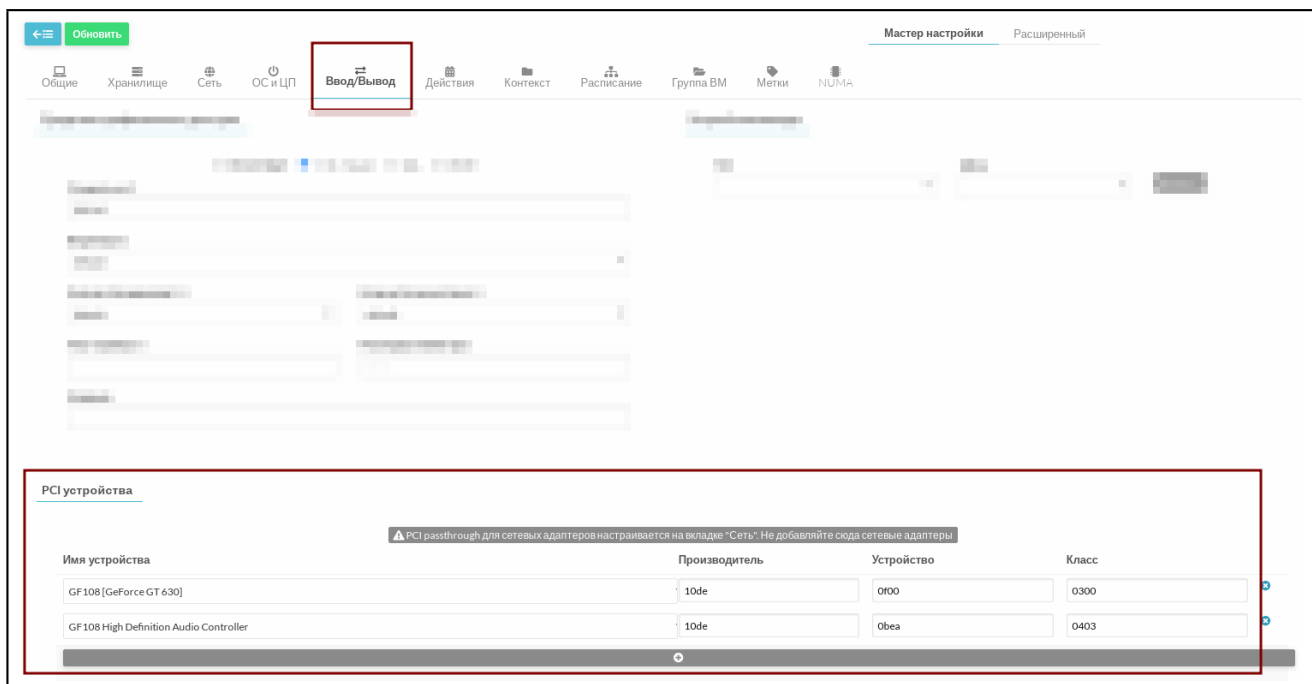


Рис. 39

4.5.3. Горячее подключение образа диска

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

4.5.3.1. 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>
```

4.5.3.2. 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 кнопку **[Добавить диск]** (см. рис. 40);

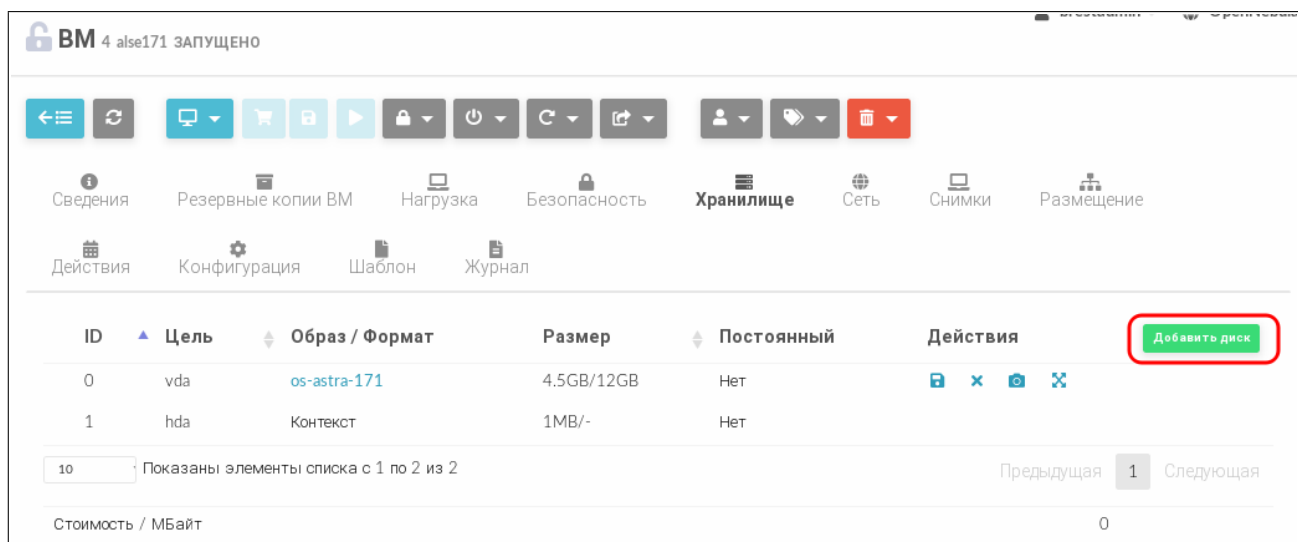


Рис. 40

4) в открывшемся окне «Присоединить диск» указать необходимый образ и нажать кнопку **[Присоединить]** (см. рис. 41).

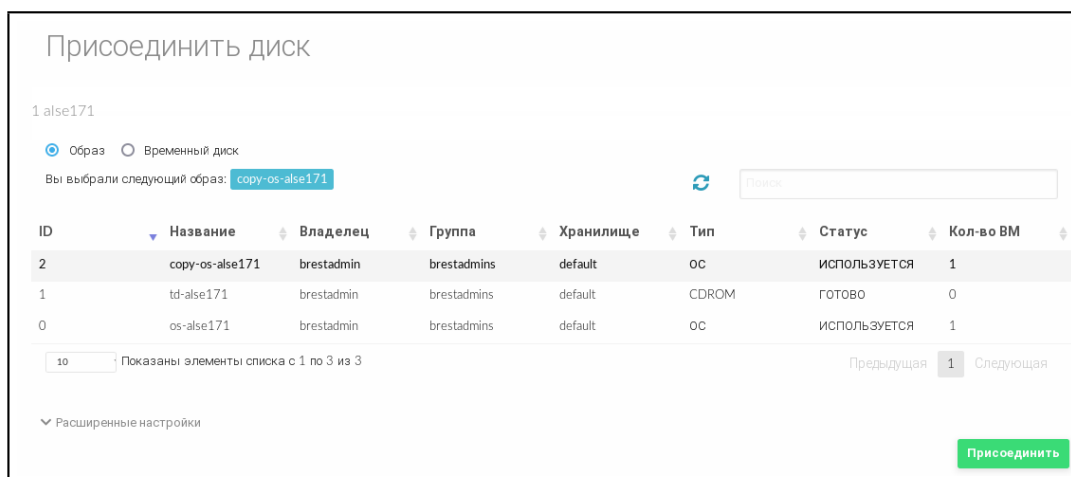


Рис. 41

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 кнопку **[Detach]** (см. рис. 42);

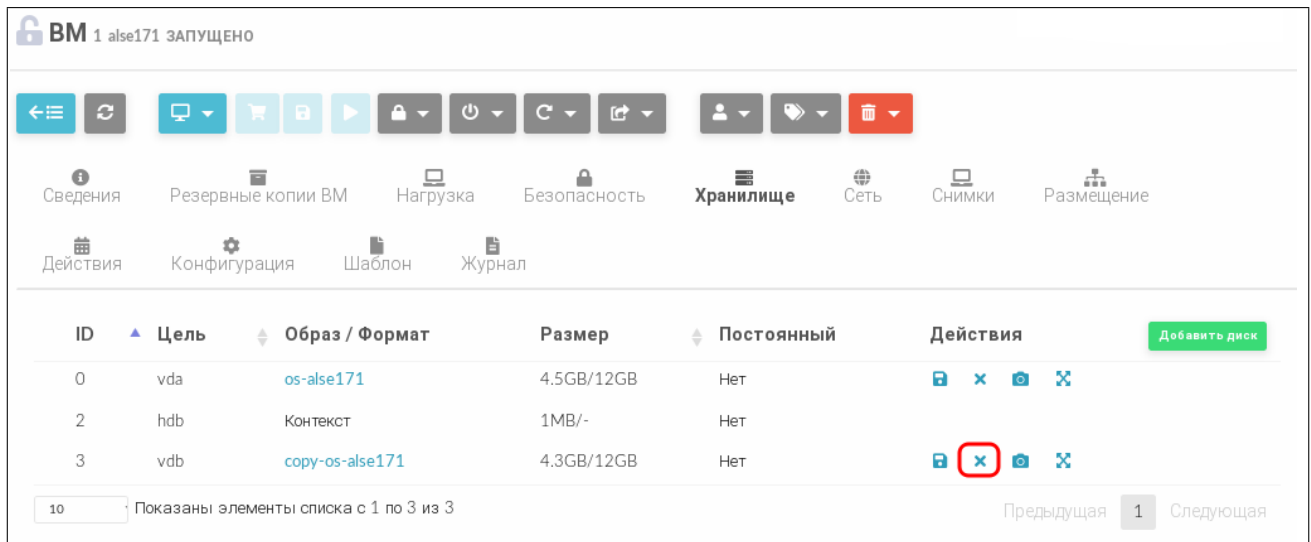


Рис. 42

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

4.5.4. Перераспределение производительности ВМ

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

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

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

4.5.4.1. В интерфейсе командной строки

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

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

Пример

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

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

4.5.4.2. В веб-интерфейсе ПК СВ

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

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

- 2) на открывшейся странице «VM» выбрать необходимую виртуальную машину;
- 3) на странице виртуальной машины открыть вкладку «Нагрузка» и нажать кнопку **[Изменить]** (см. рис. 43);

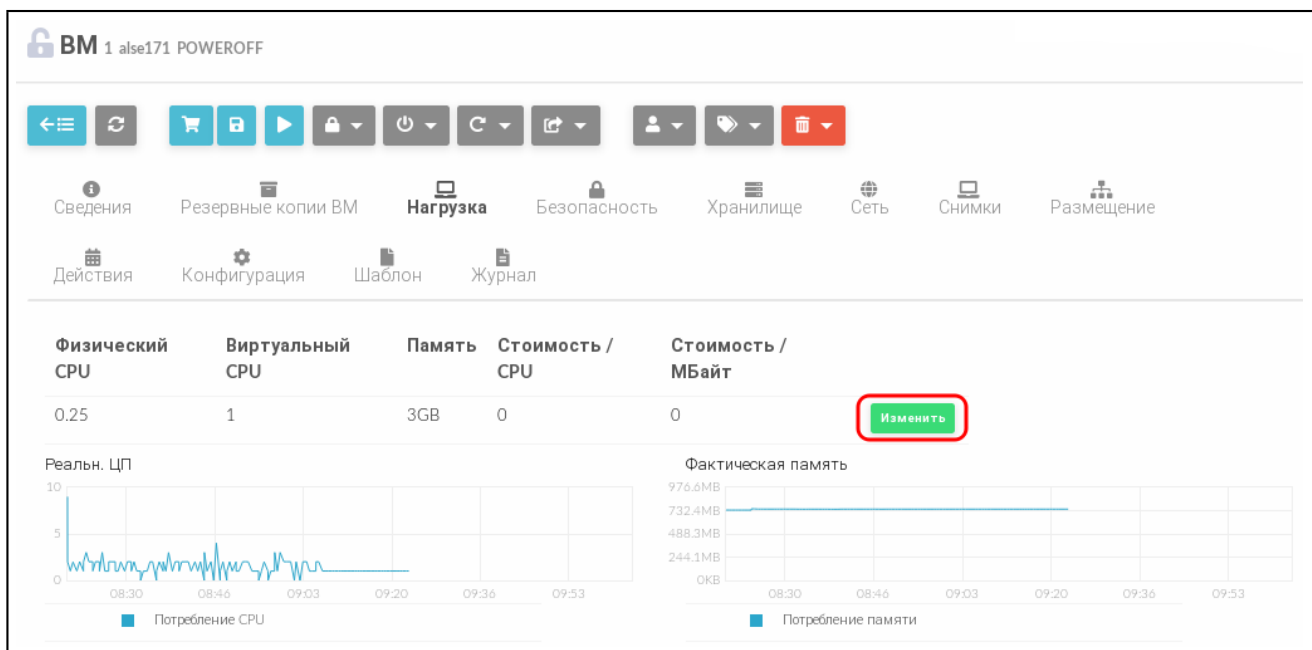


Рис. 43

- 4) в открывшемся окне «Изменить базовые характеристики» внести необходимые корректировки и нажать кнопку **[Изменить]** (см. рис. 44).

Изменить базовые характеристики

1 alse171

Проводить проверку емкости ?

Память ?

3 ГБ

Физический CPU ?

0,25

Виртуальный CPU ?

1

Изменить

Рис. 44

4.5.5. 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 ВМ. Для того чтобы в ОС виртуальной машины в автоматическом режиме были применены изменения локальной файловой системы, необходимо использовать пакеты контекстуализации.

4.5.5.1. В интерфейсе командной строки

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

Примеры:

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

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

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

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

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

Пример вывода после выполнения команды:

```
VM ID: 3
```

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

```
VIRTUAL MACHINE 3 INFORMATION
ID                : 3
NAME              : alse17-3
USER              : oneadmin
GROUP             : brestadmins
STATE             : PENDING
LCM_STATE         : LCM_INIT
LOCK              : None
RESCHED           : No
START TIME        : 07/20 10:56:01
END TIME          : -
DEPLOY ID         : -
...
VM DISKS
```

ID	DATSTORE	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:

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

4.5.5.2. 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. 45)

The screenshot shows the 'Создать VM' (Create VM) interface. It includes fields for VM name ('new-vm'), number of instances (1), and service VM status (Вкл). The 'ALSE171' section shows the 'ASTRALINUX' logo and 'Нагрузка' (Load) settings: Memory (2 GB) and Physical CPU (0,25). The 'Диски' (Disks) section is highlighted with a red box, showing two disks: 'DISK 0: os-alse17' with a volume of 20 GB, and 'DISK 1: td-alse17' with a volume of 3904 MB.

Рис. 45

4.6. Управление квотами

4.6.1. 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.

4.6.2. Управление квотами в интерфейсе командной строки

4.6.2.1. 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.

4.6.2.2. 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

Окончание таблицы 5

Параметр	Описание
SIZE	Максимальный объем (в МБ), который допускается занимать в хранилище
IMAGE	Максимальное количество образов, которые могут быть созданы в хранилище
Квоты на вычислительную мощность. Блок параметров VM	
VMS	Максимальное количество 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	
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.

4.6.2.3. 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" ]
```

4.6.2.4. 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 — «..»).

4.6.2.5. 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.

4.6.3. 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. 46):

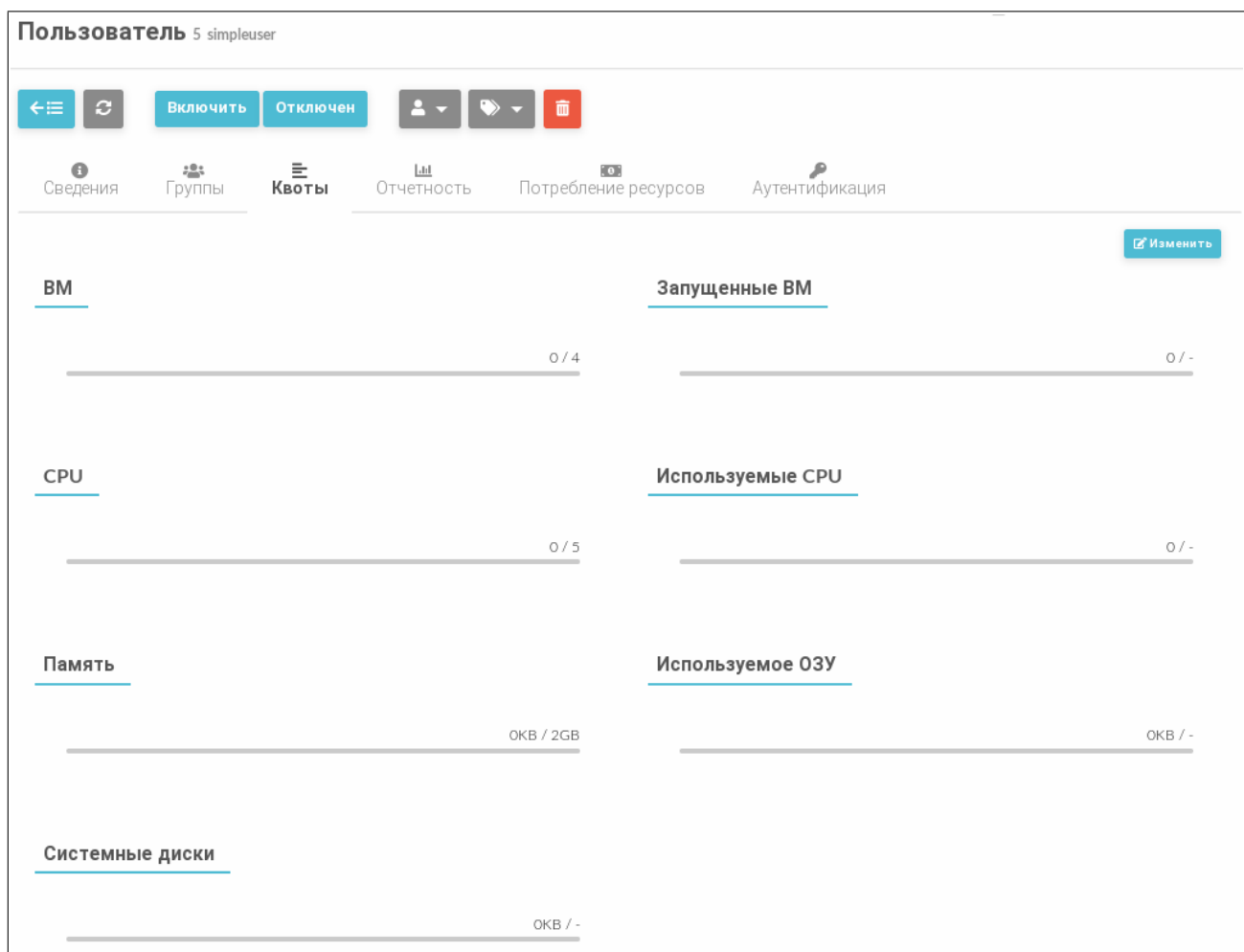


Рис. 46

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 кнопку **[Изменить]**;
- 4) на открывшейся странице установить необходимые значения квот и нажать кнопку **[Применить]**. Для отмены внесенных изменений нажать кнопку **[Отменить]** (см. рис. 47):

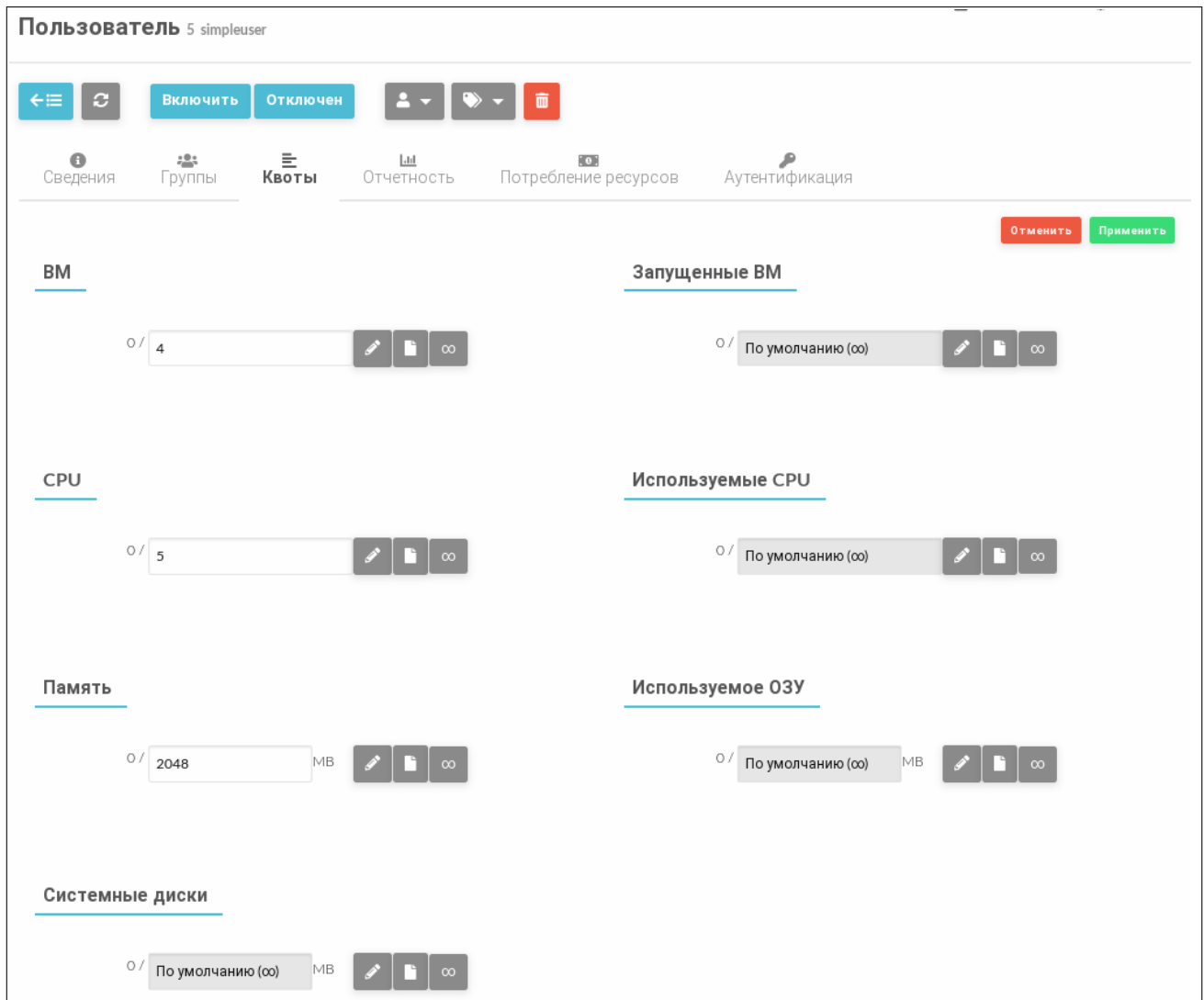


Рис. 47

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.

4.7. Миграция VM между серверами виртуализации

В ПК СВ поддерживается возможность миграции (перемещения) виртуальных машин с одного компьютера, выполняющего функцию сервера виртуализации, на другой в рамках одного кластера. Кластер представляет собой группу серверов виртуализации. В зависимости от настроек кластеры могут иметь общие хранилища и сети (подробнее — см. 5.2). 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.

4.7.1. Перемещение экземпляра ВМ в интерфейсе командной строки

Для перемещения виртуальных машин используется команда:

```
onevm migrate <идентификатор_ВМ> <идентификатор_сервера_виртуализации>
```

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

Пример

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

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

4.7.2. Перемещение экземпляра ВМ в веб-интерфейсе ПК СВ

Для перемещения виртуальных машин в веб-интерфейсе ПК СВ необходимо:

1) на странице ВМ нажать кнопку управления размещением и в открывшемся меню выбрать пункт «Перенести ВМ» (см. рис. 48);

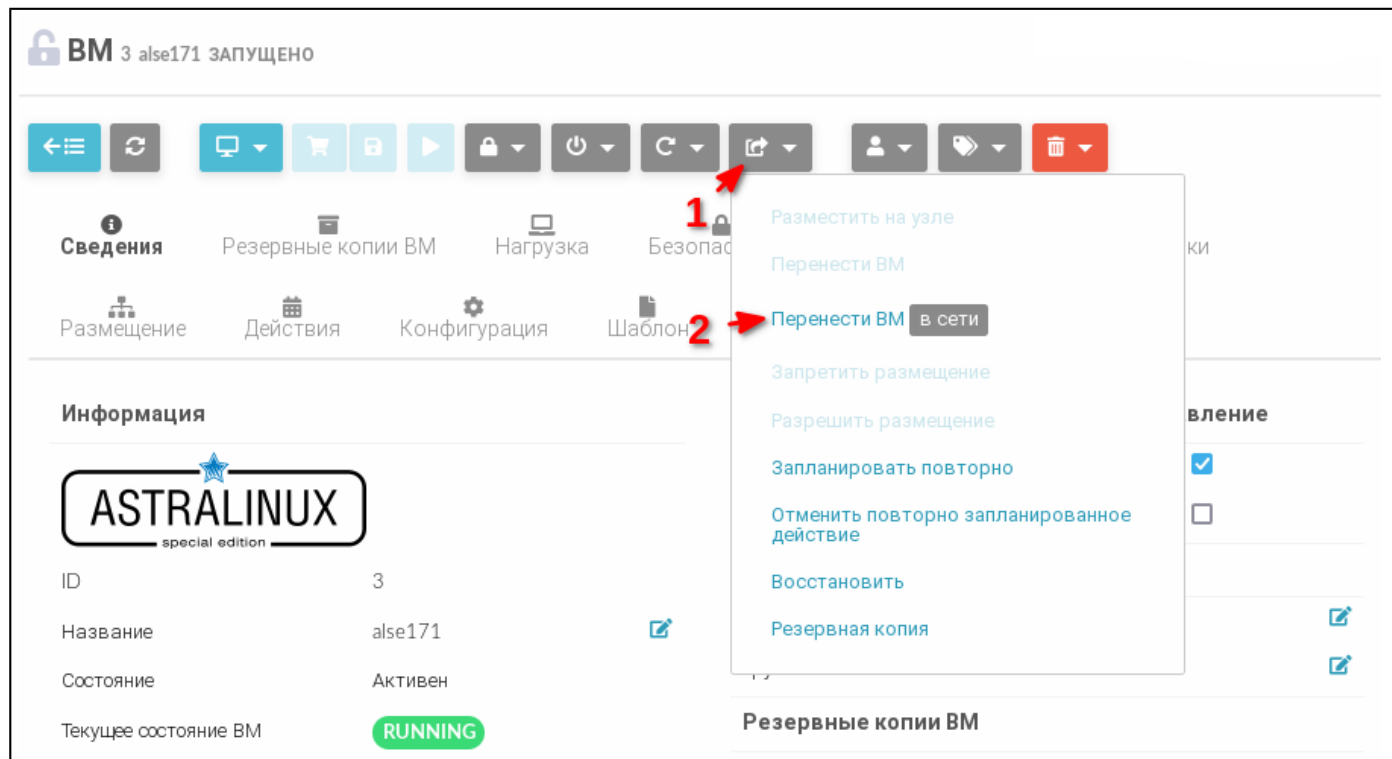


Рис. 48

2) в открывшемся окне «Мигрировать виртуальную машину» (см. рис. 49) выполнить следующие шаги:

- а) в секции «Выберите Узел» выбрать узел, на который необходимо переместить ВМ;
- б) нажать кнопку **[Перенести ВМ]**;

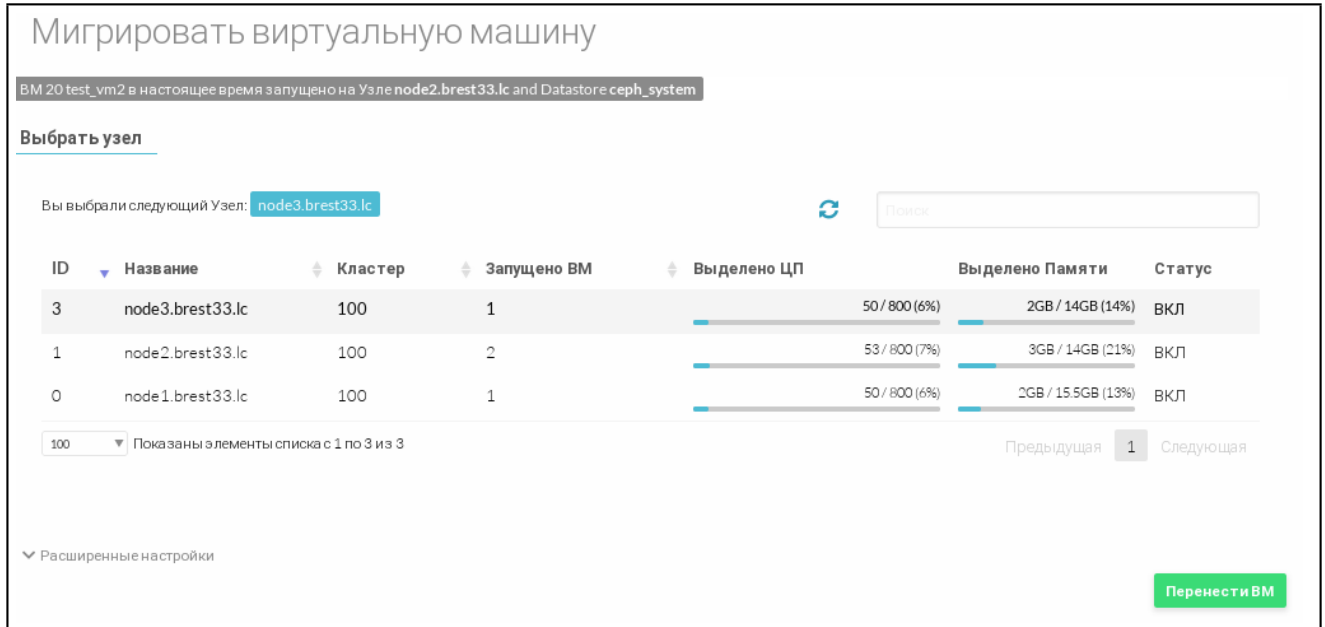


Рис. 49

- 3) в веб-интерфейсе в меню слева выбрать пункт «Экземпляры ВМ — ВМ» и дождаться пока в поле «Статус» для перемещаемой ВМ значение Миграция не изменится на ЗАПУЩЕНО. (см. рис. 50);



Рис. 50

4.7.3. Настройка миграции работающих ВМ в автоматическом режиме

В ПК СВ можно настроить автоматическую миграцию ВМ между серверами виртуализации, объединенными в единый кластер, в случае, если загрузка ЦП сервера виртуализации превышает заданное пороговое значение. В качестве порогового значения берется средняя загрузка ЦП, подсчитанная за расчетное время. При этом в автоматическом режиме будут

перемещены те ВМ, которую не генерируют эту нагрузку, т.е. мигрируют ВМ с наименьшим показателем нагрузки по ЦП, освобождая мощности сервера виртуализации.

Для настройки автоматической миграции работающих ВМ между серверами виртуализации, объединенными в единый кластер, необходимо:

- 1) подключиться к веб-интерфейсу от имени администратора ПК СВ;
- 2) в веб-интерфейсе ПК СВ в меню слева выбрать пункт «Инфраструктура — Кластеры»;
- 3) настроить условия срабатывания автоматического перемещения ВМ (см. рис. 51):
 - а) в раскрывающемся списке «Автоматическая миграция» выбрать значение Да;
 - б) в раскрывающемся списке «Средняя загрузка процессора» выбрать пороговое значение;
 - в) в раскрывающемся списке «Время расчета среднего значения загрузки» выбрать интервал времени, на протяжении которого будет вычисляться средняя загрузка процессора;

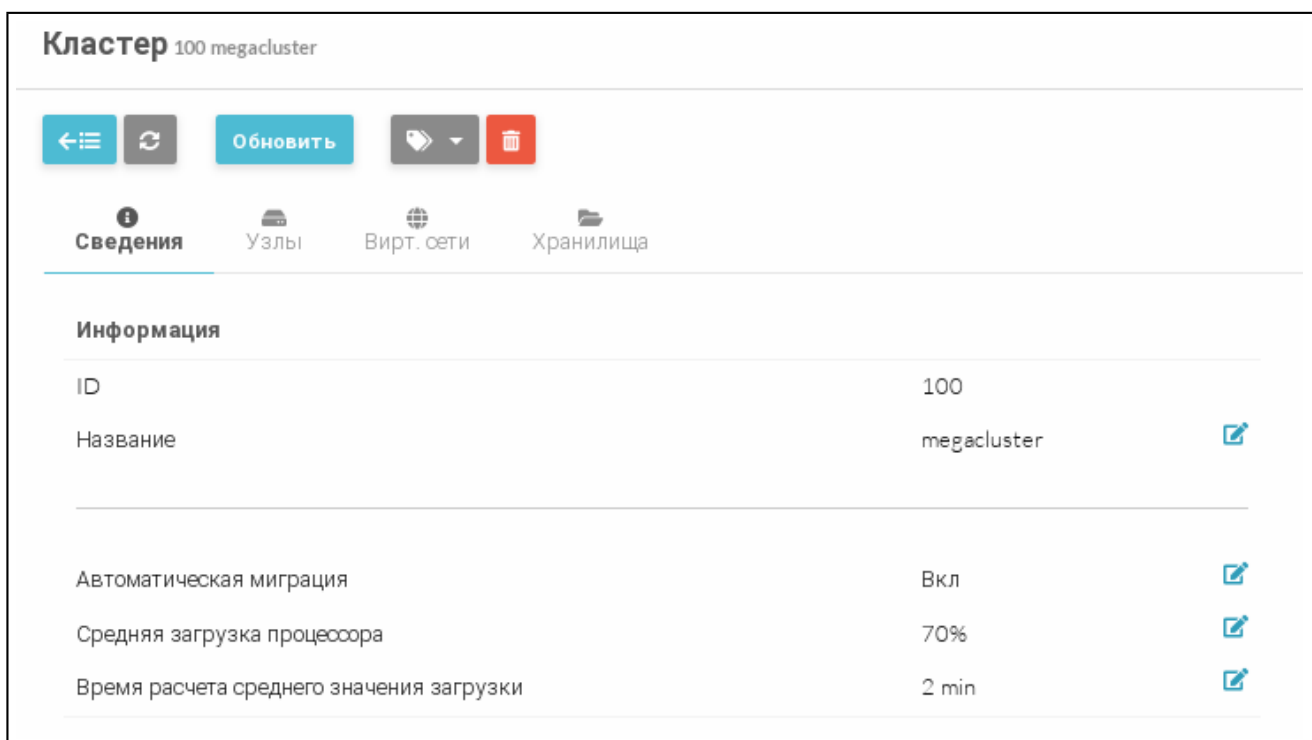


Рис. 51

- 4) в веб-интерфейсе ПК СВ в меню слева выбрать пункт «Экземпляры ВМ — ВМ»;
- 5) на открывшейся странице «ВМ» выбрать ВМ;
- 6) на странице выбранной ВМ во вкладке «Сведения» для параметра «Разрешить автоматическую миграцию ВМ» установить значение Да (см. рис. 52);

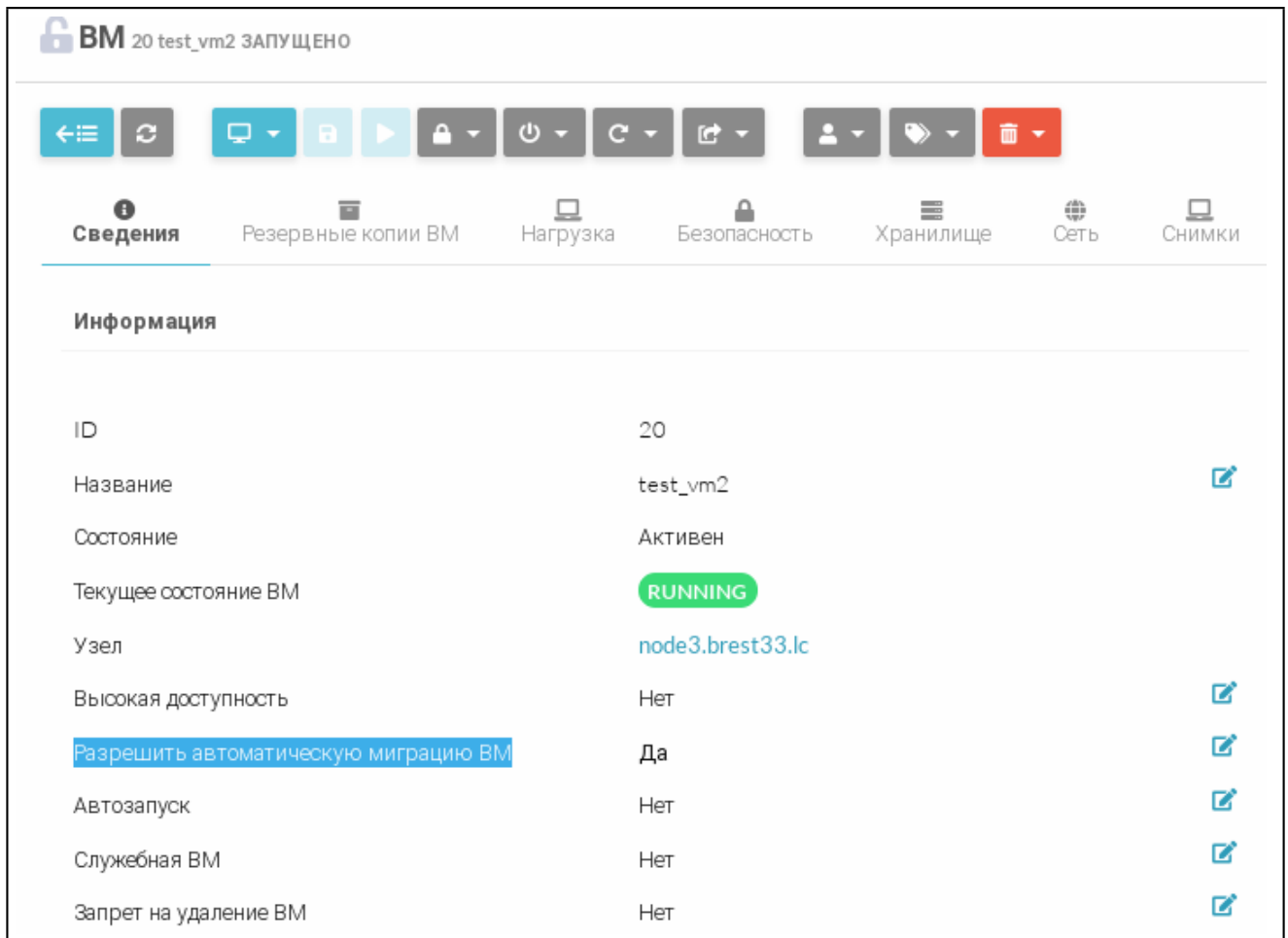


Рис. 52

Примечание. Кроме того, установить значение для параметра «Разрешить автоматическую миграцию VM» можно в шаблоне VM. Тогда все VM, создаваемые из шаблона, будут настроены на автоматическую миграцию.

4.8. 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).

4.8.1. 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 — «..»)

Пример

1) создать снимок состояния VM с идентификатором 1:

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

2) просмотреть информации о VM с идентификатором 1:

```
onevm show 1
```

Пример вывода после выполнения команды:

```
VIRTUAL MACHINE 1
```

```
...
```

```
SNAPSHOTS
```

```
ID TIME NAME HYPERVERSOR_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>
```

4.8.2. 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. 53).

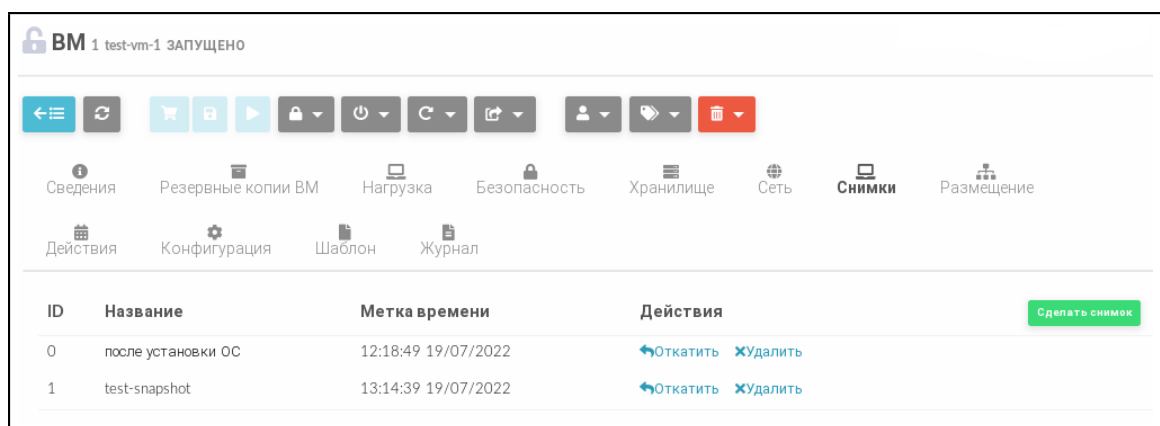


Рис. 53

На странице виртуальной машины во вкладке «Снимки»:

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

4.9. 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.

4.9.1. Управление снимками дисков в интерфейсе командной строки

Для создания снимка состояния диска необходимо выполнить команду:

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

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

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

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

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

Для удаления снимка необходимо выполнить команду:

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

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

4.9.2. Управление снимками дисков в веб-интерфейсе ПК СВ

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

- 1) в меню слева выбрать пункт «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 кнопку **[Snapshot]** (см. рис. 54);

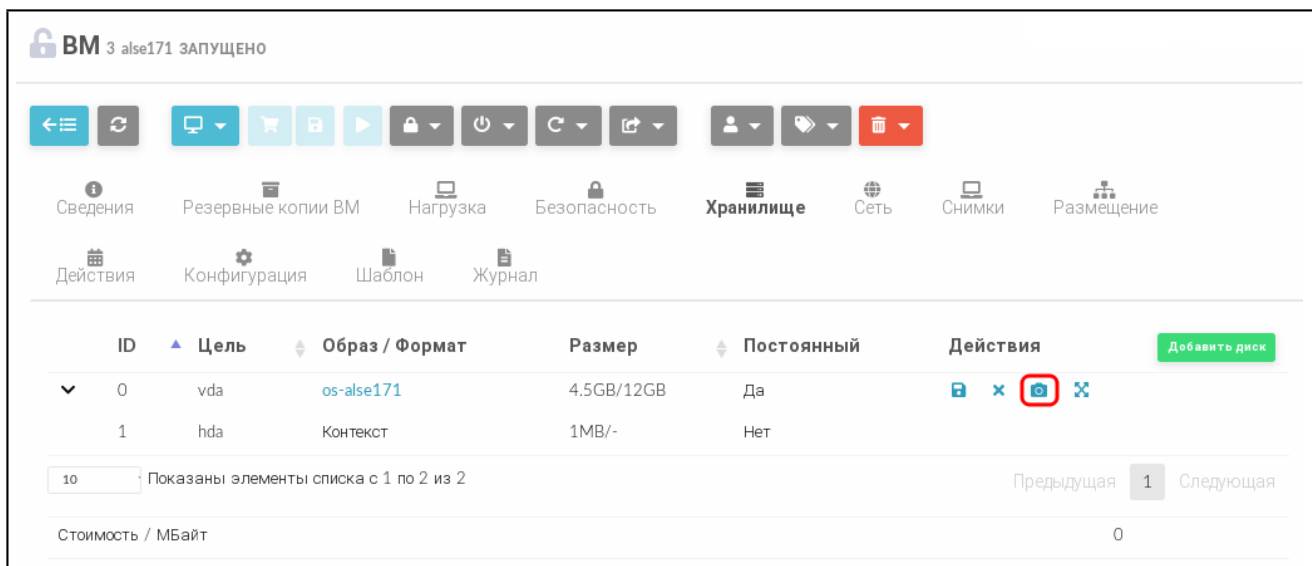


Рис. 54

4) в открывшемся окне «Снимок диска» задать наименование снимка и нажать кнопку **[Сделать снимок]** (см. рис. 55).

Снимок диска

3 alse171

№ диска
0

Название
настройка сети

Сделать снимок

Рис. 55

Управление состоянием диска VM осуществляется на странице виртуальной машины во вкладке «Хранилище» (после остановки VM) — см. рис. 56:

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

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. 56

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

5. УПРАВЛЕНИЕ СЕРВЕРАМИ ВИРТУАЛИЗАЦИИ И КЛАСТЕРАМИ

Установка и инициализация службы сервера виртуализации производятся в соответствии с документом РДЦП.10001-02 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 кнопку **[+]**;

- 2) на открывшейся странице Создать узел (см. рис. 57):
- в поле «Тип» указать тип драйвера виртуализации,
 - в поле «Имя хоста» ввести сетевое имя сервера виртуализации,
 - в поле «Логин администратора» ввести имя локального администратора компьютера, выполняющем функцию сервера виртуализации,
 - в поле «Пароль администратора» ввести пароль локального администратора компьютера, выполняющем функцию сервера виртуализации,
 - нажать кнопку **[Создать]**;

Рис. 57

- 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. 58).

ID	Название	Кластер	Запущено VM	Выделено ЦП	Выделено Памяти	Статус
0	breast-service	0	0	0/0	ОКВ / -	Инициализация

Показаны элементы списка с 1 по 1 из 1

ВСЕГО 1 ВКЛ 0 ВЫКЛ 0 ОШИБКА

Рис. 58

5.1.2. Просмотр перечня серверов виртуализации и отображение информации о сервере виртуализации

5.1.2.1. В интерфейсе командной строки

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

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"
...

```

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` (см. 5.1.2.1).

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. 59).

Информация		Нагрузка	
ID	1	Выделено Памяти	0KB / 3.8GB (0%)
Название	host01	Выделено ЦП	0 / 400 (0%)
Кластер	default	Физическая память	229MB / 3.8GB (6%)
Состояние	НАБЛЮДАЕТ СЯ	Реальн. ЦП	28 / 400 (7%)
Мигрировать все VM с хоста при переводе его в статус 'Отключен'	Нет		
IM MAD	kvm		
VM MAD	kvm		

Рис. 59

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 ВМ		Значение
		Вручную	Планир.	
Включен (on)	Да	Да	Да	Сервер виртуализации находится в полностью рабочем состоянии
Обновление (update)	Да	Да	Да	Обновление информации о состоянии сервера виртуализации в системе мониторинга
Отключен (dsbl)	Да	Да	Нет	Отключен, например, для проведения техобслуживания
Отключен от сети (off)	Нет	Нет	Нет	Сервер виртуализации полностью отключен от сети
Ошибка (err)	Да	Да	Нет	При обновлении информации о состоянии сервера виртуализации выявлена ошибка. Можно использовать команду <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 ВМ, работающих на сервере виртуализации. Для того чтобы выполнить автоматическую миграцию ВМ на другие серверы виртуализации, обладающие достаточным вычислительным ресурсом, необходимо выполнить команду

```
onehost flush <наименование_сервера_виртуализации>
```

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

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. 59):

- **[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 кнопку **[Удалить]** (см. рис. 60).

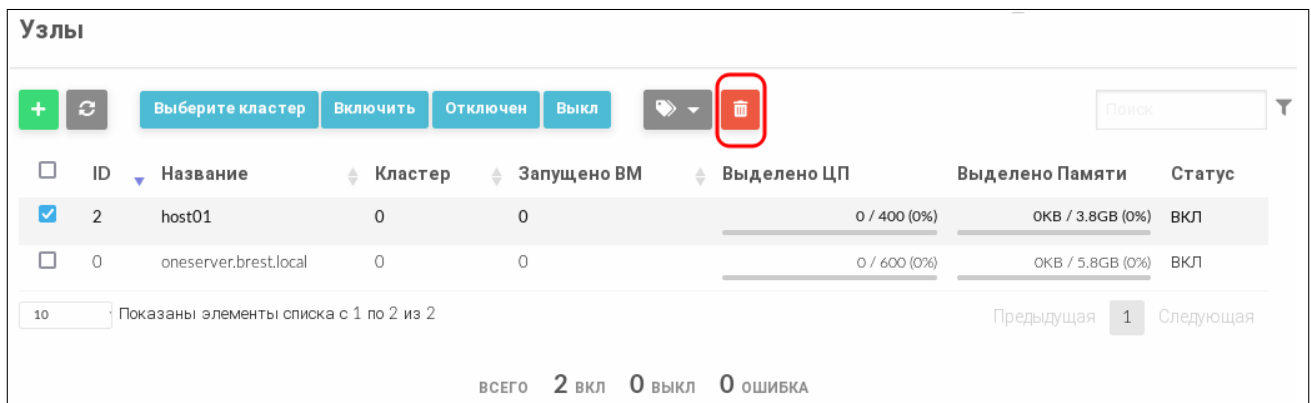


Рис. 60

- 3) в открывшемся окне «Удалить узел» нажать кнопку **[ОК]** (см. рис. 61).

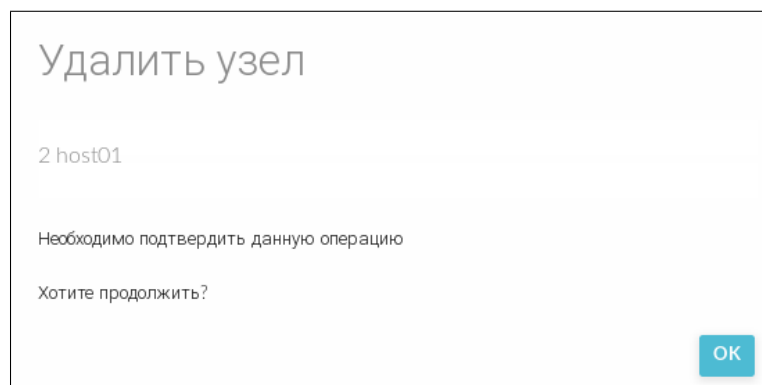


Рис. 61

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 `onemonditor` на сервере управления.

Примечание. Функционирование системы мониторинга ПК СВ описано в документе РДЦП.10001-02 95 01-1.

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

Таблица 7

Параметр	Описание
<code>HYPERVISOR</code>	Название гипервизора сервера виртуализации, применяется для выбора серверов виртуализации с определенной технологией
<code>ARCH</code>	Архитектура ЦП сервера виртуализации, например, <code>x86_64</code>
<code>MODELNAME</code>	Название модели ЦП сервера виртуализации, например, <code>Intel(R) Core(TM) i7-2620M CPU @ 2.70GHz</code>
<code>CPUSPEED</code>	Частота ЦП в МГц
<code>HOSTNAME</code>	Сетевое имя сервера виртуализации (в соответствии с ответом на команду <code>hostname</code>)
<code>VERSION</code>	Версия тестовых программ. Используются для контроля локальных изменений и обновления
<code>MAX_CPU</code>	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)
<code>MAX_MEM</code>	Максимальное количество памяти, которое может использоваться для ВМ. 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)
<code>MAX_DISK</code>	Общий объем пространства хранилища в МБ
<code>USED_CPU</code>	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)
<code>USED_MEM</code>	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)
<code>USED_DISK</code>	Используемый объем пространства хранилища в МБ
<code>FREE_CPU</code>	Процент неиспользуемой мощности ЦП, умноженной на количество ядер. Например, если в 4-ядерной машине не используются 50% мощности ЦП, значение данного параметра составит 200
<code>FREE_MEM</code>	Память, доступная для ВМ на данный момент, в КБ
<code>FREE_DISK</code>	Объем свободного пространства хранилища в МБ

Окончание таблицы 7

Параметр	Описание
CPU_USAGE	Общая мощность ЦП, распределенная среди ВМ, запущенных на данном сервере виртуализации в соответствии с запросом, который указан в параметре CPU в каждом шаблоне ВМ. Кроме того, это значение отображается в виде параметра CPU USED (ALLOCATED) в секции HOST SHARE после выполнения команды <code>onehost show</code> (см. 5.1.2.1)
MEM_USAGE	Общая память, распределенная среди ВМ, запущенных на данном сервере виртуализации в соответствии с запросом, который указан в параметре MEMORY в каждом шаблоне ВМ. Кроме того, это значение отображается в виде параметра MEMORY USED (ALLOCATED) в секции HOST SHARE после выполнения команды <code>onehost show</code> (см. 5.1.2.1)
DISK_USAGE	Общий размер образов диска для ВМ, запущенных на сервере виртуализации, рассчитанный с применением параметра SIZE каждого образа с учетом характеристик хранилища
NETRX	Объем входящего сетевого трафика
NETTX	Объем исходящего сетевого трафика
WILD	Перечень ВМ, разделенных запятой, работающих на сервере виртуализации и которые не были запущены службами ПК СВ и не контролируются в данный момент
ZOMBIES	Перечень ВМ, 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 (ВМ):

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

Использование данной метки в шаблоне ограничит развертывание ВМ 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. 62).

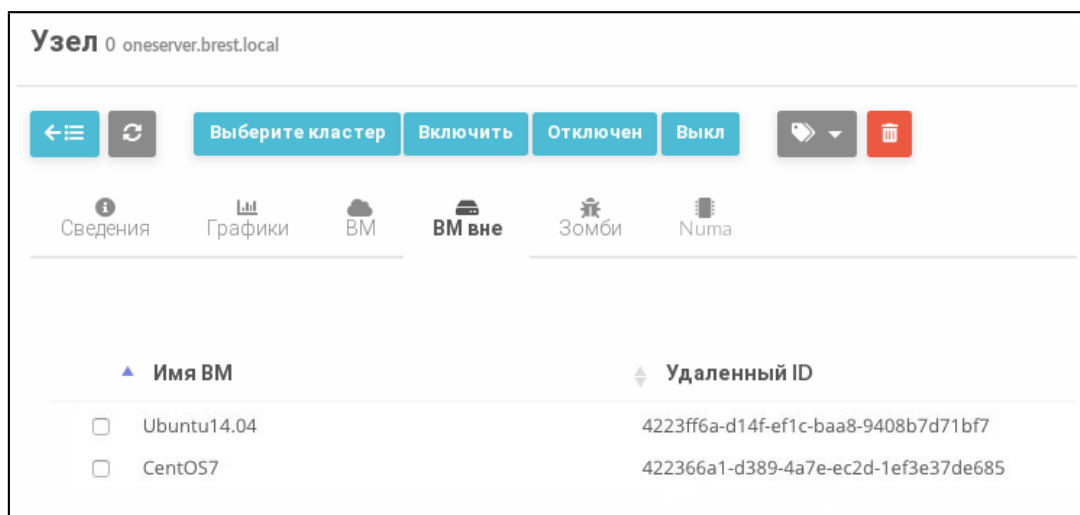


Рис. 62

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. 63).

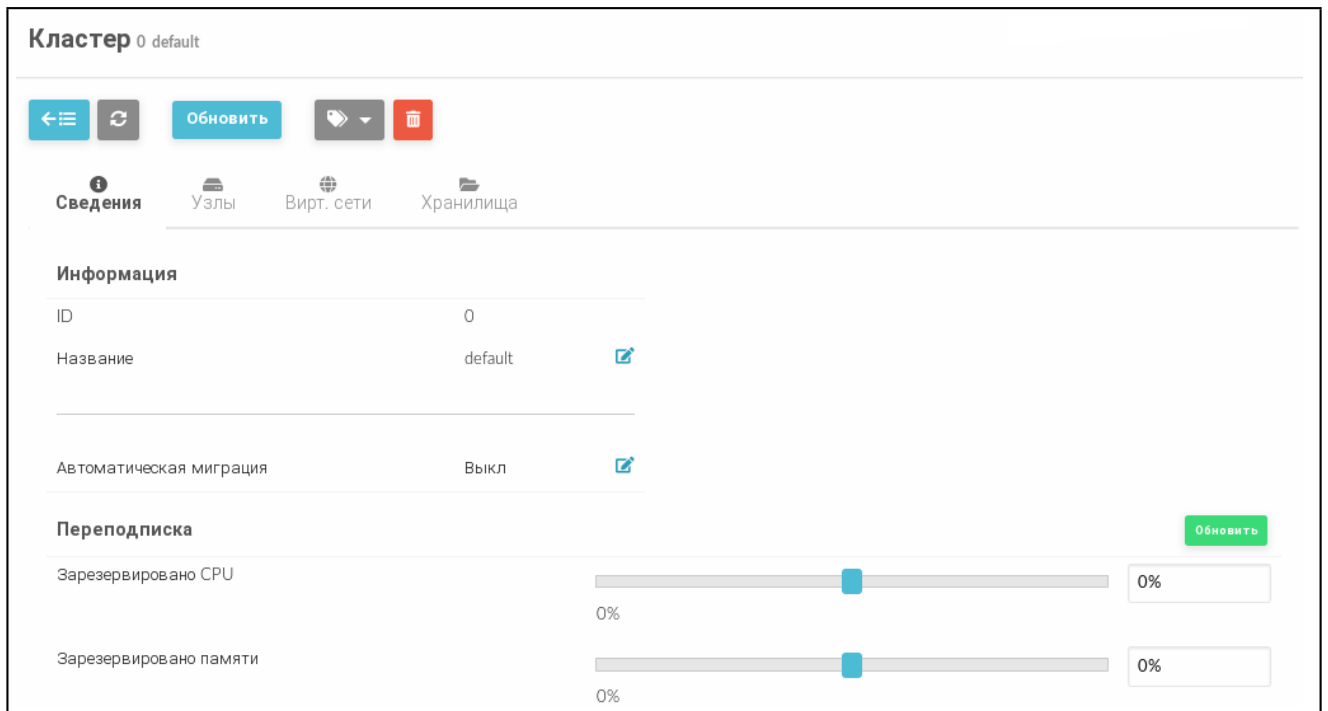


Рис. 63

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 кнопку **[Выберите кластер]**;
- 3) в открывшемся окне выбрать необходимый кластер и нажать кнопку **[ОК]** (см. рис. 64).



Рис. 64

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. Диапазон адресов (AR)

IP-адреса, доступные внутри сети, определяются одним и более диапазоном адресов (Address Ranges — 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

Подключить VM к сети 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. Создание, 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 (AR) 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

```

ВНИМАНИЕ! Если в удаляемом диапазоне адресов для какого-либо IP-адреса был установлен запрет на использование (командой `onevnet hold`), то перед удалением диапазона адресов необходимо разблокировать этот IP-адрес командой `onevnet release`.

ВНИМАНИЕ! Если в удаляемом диапазоне адресов какие-либо адреса были зарезервированы (командой `onevnet reserve`), то перед удалением диапазона адресов необходимо снять резервирование этих адресов командой `onevnet free`.

Примечание. Команда `onevnet reserve` применяется для создания пользовательской сети путем резервирования адресов. Порядок использования пользовательских сетей приведен в документе РДЦП.10001-02 93 01 «Программный комплекс «Средства виртуализации «Брест». Руководство пользователя».

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, подготов-

ленный 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. Запрет использования адресов

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

Для установки запрета на использования адреса применяется 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>.

Пример

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
```

РДЦП.10001-02 95 01-2

```
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 IP-адреса используется команда:

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

ВНИМАНИЕ! Не допускается использование команды `onevnet free` для разблокировки IP-адреса.

Команда `onevnet free` применяется для снятия резервирования IP-адресов в пользовательской сети. Порядок использования пользовательских сетей приведен в документе РДЦП.10001-02 93 01 «Программный комплекс «Средства виртуализации «Брест». Руководство пользователя».

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. 65).

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

Показаны элементы списка с 1 по 2 из 2

2 ВСЕГО 2 Исп. IP-адресов

Рис. 65

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 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 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. 66).

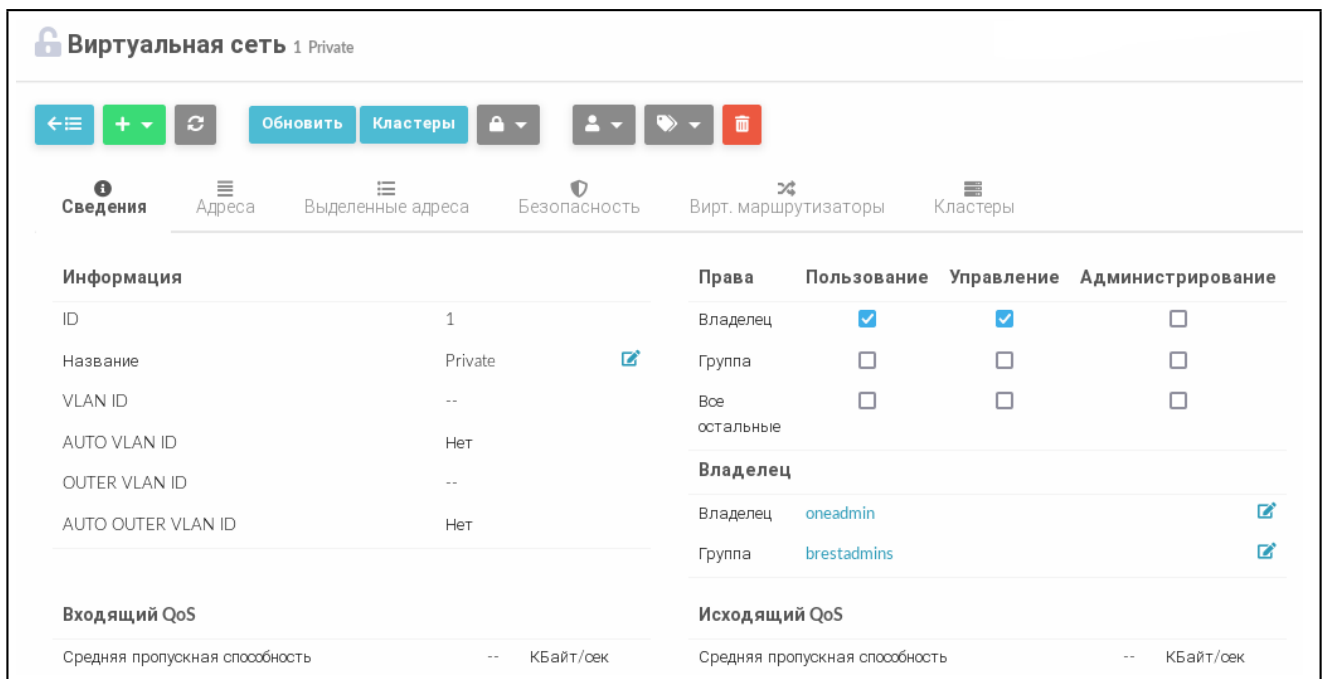


Рис. 66

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 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 кнопку **[Обновить]**.

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.10001-02 97 01.

ВНИМАНИЕ! Сетевые группы безопасности не поддерживаются для сетей OpenvSwitch.

Правила сетевых групп безопасности не применяются для трафика, исходящего от узла виртуализации, на котором запущена ВМ с настроенными группами безопасности. Правила всегда применяются для внешнего трафика по отношению к ВМ и узлу виртуализации.

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
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 ВМ. Например, может быть целесообразно установить TCP-порт 22 как входящий для SSH, а порт 80 и порт 443 — как исходящий, чтобы иметь возможность устанавливать пакеты.

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

6.2.3. Управление группами безопасности в интерфейсе командной строки

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

6.2.3.1. Добавление, удаление и просмотр списка групп безопасности

Для создания группы безопасности используется команда:

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

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

Примеры:

1. Содержание файла шаблона `sg.txt`:

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

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

```
onesecgroup create sg.txt
```

Пример вывода после выполнения команды:

```
ID: 100
```

Для просмотра имеющихся групп безопасности, необходимо выполнить команду:

```
onesecgroup list
```

Пример вывода после выполнения команды:

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

Для удаления группы безопасности используется команда:

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

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

6.2.3.2. Просмотр и изменение правил группы безопасности

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

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

Пример вывода после выполнения команды:

```
SECURITY GROUP 100 INFORMATION
```

```
ID           : 100
```

```
NAME         : test
```

```
USER         : oneadmin
```

```
GROUP        : brestadmins
```

```
PERMISSIONS
```

```
OWNER        : um-
```

```
GROUP        : ---
```

```
OTHER        : ---
```

```
VIRTUAL MACHINES
```

```
UPDATED      :
```

```
OUTDATED     :
```

```
ERROR        :
```

```
RULES
```

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

Для изменения правил необходимо использовать команду:

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

где <файл-шаблон> — файл шаблона для изменения правил. Если файл шаблона не указан,

то после ввода команды откроется текстовый редактор Vim для формирования временного шаблона. После сохранения внесенных данных и закрытия редактора, подготовленный шаблон будет применен для изменения правил, а временный файл шаблона будет удален.

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

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

6.2.3.3. Применение группы безопасности

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

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

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

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

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

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

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

Пример

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

ВНИМАНИЕ! Если AR или NIC шаблона определяют группы безопасности с помощью параметра SECURITY_GROUPS, то указанные идентификаторы не будут перезаписывать

идентификаторы, определенные в сети. Все идентификаторы групп безопасности объединяются и применяются в отношении экземпляра ВМ.

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

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

6.2.4. Управление группами безопасности в веб-интерфейсе ПК СВ

Для отображения перечня всех групп безопасности в веб-интерфейсе ПК СВ необходимо в меню слева выбрать пункт меню «Система — Группы безопасности». На открывшейся странице «Группы безопасности» будет представлена таблица имеющихся групп безопасности (см. рис. 67).

ID	Название	Владелец	Группа
100	test	oneadmin	brestadmins
0	default	oneadmin	brestadmins

Рис. 67

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 кнопку **[+]**;
- 2) на открывшейся странице «Создать Группу безопасности» (см. рис. 68):
 - а) в поле «Название» задать наименование группы безопасности;
 - б) в секции «Правила» задать правила фильтрации трафика;
 - в) нажать кнопку **[Создать]**.

Создать Группу безопасности

← Сброс Создать
Мастер настройки | Расширенный

Название:
 Описание:

Правила

Направление трафика:
 Протокол:

Диапазон порта:

Целевая сеть:

Рис. 68

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

Для просмотра информации о конкретной группе безопасности на странице «Группы безопасности» необходимо выбрать соответствующую строку. После этого откроется страница группы безопасности (вкладка «Сведения» — см. рис. 69).

Группа безопасности 100 test

← ↻ Обновить Клонировать Зафиксировать

👤 🔍 🗑️

📄 📄

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

Рис. 69

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 кнопку **[Обновить]**;
- 3) на открывшейся странице «Обновить Группу безопасности» скорректировать правила фильтрации трафика и нажать кнопку **[Обновить]**.

6.3. Сервис виртуальных сетевых функций (VNF)

Сервис виртуальных сетевых функций (VNF) предоставляется в виде пакета `breast-vnf`, предназначенного для установки в Astra Linux MG.

Параметры подготовленного шаблона виртуальной машины определяют подключенный образ как «виртуальный маршрутизатор», что позволяет использовать функции GUI при работе с сервисом VNF.

VNF позволяет реализовывать и управлять рядом сетевых функций и использоваться как виртуальный маршрутизатор.

6.3.1. Установка и управление VNF

6.3.1.1. Установка и настройка сервиса VNF

Для подготовки образа VM для сервиса VNF необходимо:

- 1) для начала работы с сервисом необходимо получить образ Astra Linux MG (.qcow2) из хранилища <https://dl.astralinux.ru/ui/native/mg-generic/alse/qemu/> (для клиентов с лицензией на ALSE). Для образа VNF оптимально использовать base-образ без GUI (например, `alse-vanilla-1.7.4uu1-qemu-base-mg11.3.0.qcow2`);
- 2) в веб-интерфейсе ПК СВ перейти в раздел «Хранилище — Образы» и создать новый постоянный образ из образа Astra Linux MG с именем `service-vnf-alse`;
- 3) в разделе «Шаблоны — VM» создать временный шаблон VM для подготовки сервиса VNF:

- на странице «Создать шаблон VM» во вкладке «Общие» указать название шаблона и объем оперативной памяти 8 Гб, остальные параметры задать по своему усмотрению (см. рис. 70):

Создать шаблон VM

← Сброс Создать

Мастер настройки Расширенный

Общие Хранилище Сеть ОС и ЦП Ввод/Вывод Действия Контекст Расписание Группа VM
Метки NUMA

Название: Гипервизор / KVM vCenter LXC Firecracker

Описание: Логотип:

Память: ГБ Включить горячее изменение размера? Модификация ОЗУ:

Cost Стоимость / МЕСЯЦ

Рис. 70

- на вкладке «Хранилище» выбрать образ `service-vnf-alse` (см. рис. 71):

Создать шаблон VM

← Сброс Создать

Мастер настройки Расширенный

Общие **Хранилище** Сеть ОС и ЦП Ввод/Вывод Действия Контекст Расписание Группа VM
Метки NUMA

Диско

Образ Временный диск

Вы выбрали следующий образ:

ID	Название	Владелец	Группа	Хранилище	Тип	Статус	Кол-во VM
2	service-...	brester	brestad...	default	ОС	ГОТОВО	0

Показаны элементы списка с 1 по 1 из 1

Расширенные настройки

Рис. 71

- после завершения настройки шаблона нажать кнопку [Создать];

4) создать экземпляр VM из временного шаблона. Запустить VM, подключиться к консоли и настроить доступ к сетевому или локальному репозиторию ПК СВ версии 3.3.1;

Примечание. При использовании сетевого репозитория потребуется создать временную виртуальную сеть.

5) в созданной VM установить пакет сервиса VNF командой:

```
sudo apt-get install -t brest brest-vnf
```

6) скопировать содержимое файла

`/usr/share/doc/brest-vnf/brest-vnf-template` в буфер обмена сервера виртуализации или сам файл на сервер виртуализации;

7) отключить VM и удалить временную VM и шаблон. Перейти в раздел «Хранилище — Образы» и сменить тип образа `service-vnf-alse` на непостоянный (открыть страницу образа и во вкладке «Сведения» в выпадающем списке «Постоянный» выбрать «Нет»).

Примечание. Перед созданием маршрутизатора с функцией SDNAT4 или LB (LoadBalancer) необходимо настроить ПК СВ для использования службы сервера OneGate.

Все сетевые функции отключены по умолчанию, кроме высокой доступности (Keepalived), которая требует задания плавающего IP-адреса (необходимо установить флаг и ввести принудительный IPv4 адрес).

Для создания виртуального маршрутизатора необходимо:

1) в веб-интерфейсе ПК СВ в разделе «Шаблоны — Вирт. маршрутизаторы» создать новый шаблон. На странице «Шаблоны VM» виртуального маршрутизатора перейти во вкладку «Расширенный» и вставить содержимое файла `/usr/share/doc/brest-vnf/brest-vnf-template`. При необходимости — изменить параметры выделенных ресурсов (см. рис. 72):

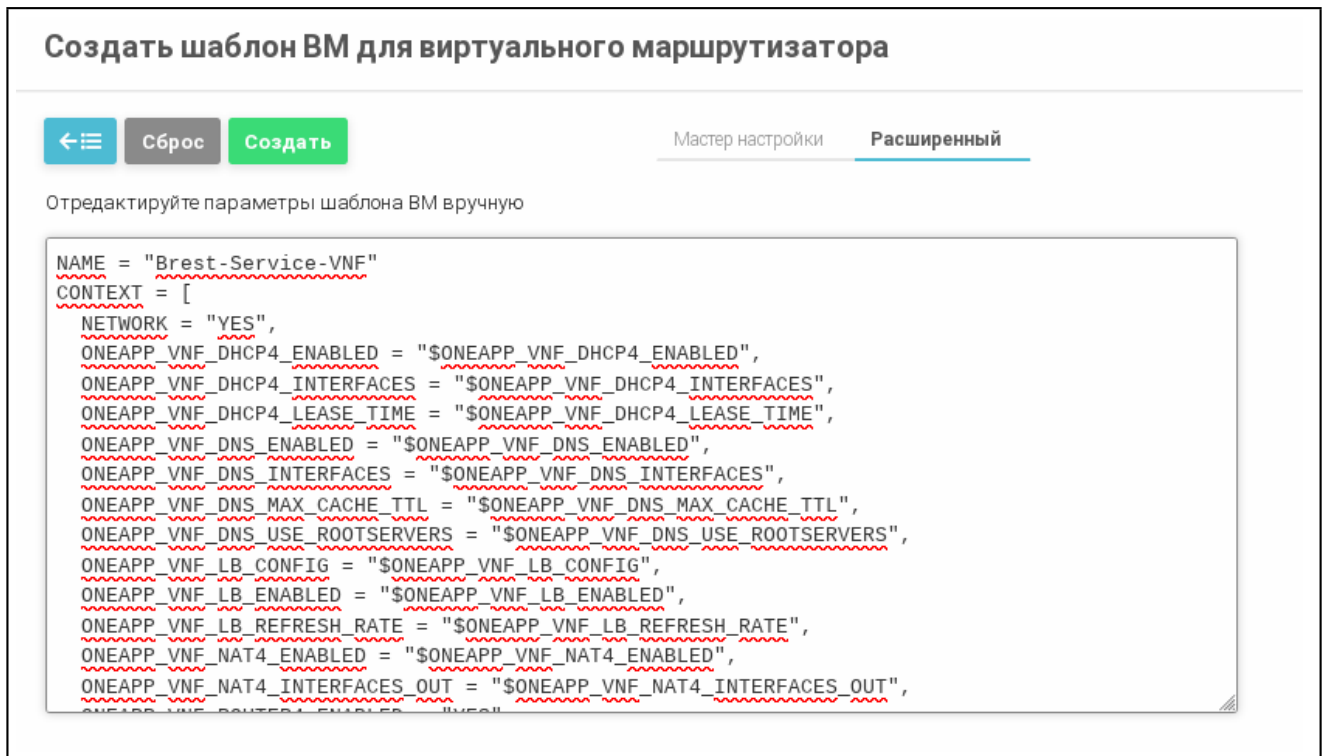


Рис. 72

Нажать кнопку [Создать].

2) перейти в раздел «Экземпляры VM — Вирт. маршрутизаторы» и создать новый маршрутизатор из созданного шаблона Brest-Service-VNF:

- на странице «Создать виртуальный маршрутизатор» указать название виртуального маршрутизатора: (см. рис. 73):

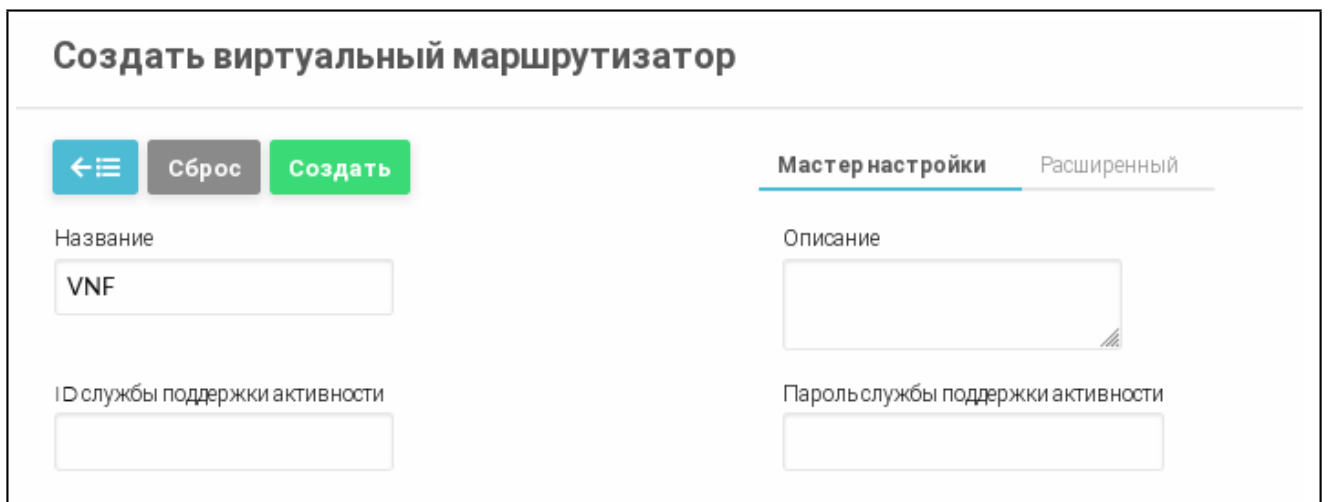


Рис. 73

- в блоке «Сеть» нажать кнопку [+Сетевой интерфейс] и подключить необходимые сетевые интерфейсы и группы безопасности: (см. рис. 74):

ID Название Владелец Группа Резервирование Кластер Выделенные адреса
 0 virtnetwork brestuser brestadmins Нет 0 0/2

10 Показаны элементы списка с 1 по 1 из 1

 Предыдущая 1 Следующая

Принудительный IPv4:
 Принудительный IPv6:

Плавающий IP
 Интерфейс управления

Группы безопасности

Пожалуйста выберите не менее одной группы безопасности из списка

ID	Название	Владелец	Группа
0	default	oneadmin	brestadmins

10 Показаны элементы списка с 1 по 1 из 1

 Предыдущая 1 Следующая

Рис. 74

Примечание. Для настройки высокой доступности (Keepalived) необходимо установить флаг «Плавающий IP» и указать IP-адрес.

- в блоке «Шаблон» выбрать шаблон Brest-Service-VNF и задать количество экземпляров VM (для обеспечения высокой доступности необходимо указать минимум 2 VM) (см. рис. 75):

Шаблон

Вы выбрали следующий Шаблон: Brest-Service-VNF

ID	Название	Владелец	Группа	Время регистрации
3	Brest-Service-VNF	brestuser	brestadmins	20/05/2024 10:59:24

10 Показаны элементы списка с 1 по 1 из 1

 Предыдущая 1 Следующая

Имя виртуальной машины:

Количество экземпляров VM:

Создать и поставить на паузу

Рис. 75

- в блоке «Пользовательские атрибуты» включить необходимые сетевые функции (DHCPv4, DNS, NAT и т.д.) (см. рис. 76):

Пользовательские атрибуты

DNCR4 - Включить / Enable
 ДА НЕТ

DNCR4 - Список прослушиваемых интерфейсов / Listening Interfaces

DNS - Включить сервер / Enable DNS Server
 ДА НЕТ

DNS - Список прослушиваемых интерфейсов / Listening Interfaces

NAT - Включить / Enable

Рис. 76

- после завершения настройки маршрутизатора нажать кнопку [Создать].
 Перейти в раздел «Экземпляры VM — VM» и дождаться запуска виртуальных машин;

3) в разделе «Сеть — Топология сети» отобразится созданный виртуальный маршрутизатор, а при наведении курсора отобразятся названия VM, объединенных в виртуальный маршрутизатор протоколом VRRP (см. рис. 77):

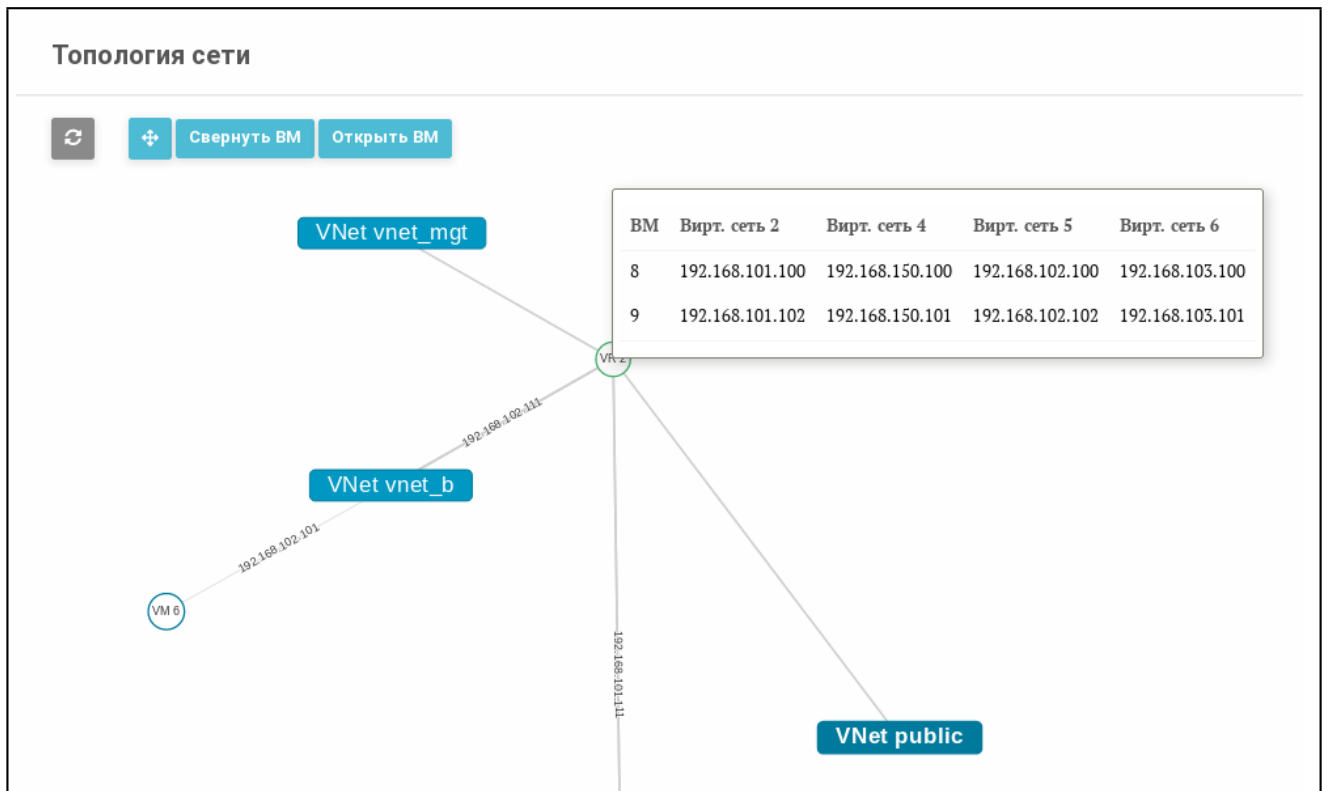


Рис. 77

6.3.1.2. Подключение к виртуальному маршрутизатору

При начальной настройке доступ к виртуальному маршрутизатору может осуществляться с использованием SSH с сервера виртуализации, либо через публичную виртуальную сеть.

После введения маршрутизатора в работу предполагается, что дальнейший доступ возможен только через сетевой интерфейс управления (management interface), который задается при создании экземпляра маршрутизатора (флаг «Интерфейс управления»). На интерфейсе управления не будут запущены никакие сетевые функции, кроме сервера SSH (см. рис. 78):

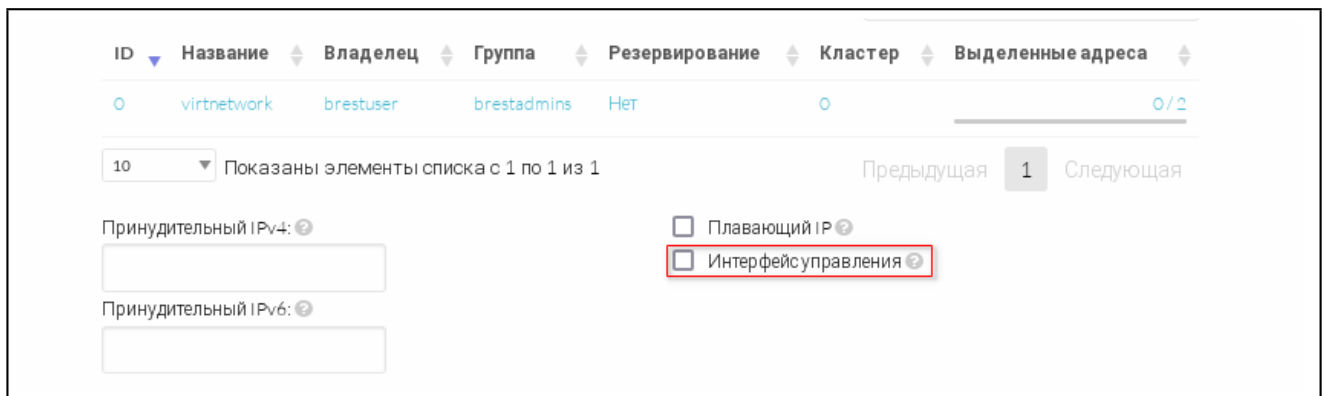


Рис. 78

Примечание. Для входа в VM необходимо воспользоваться логином и паролем: astra / astra.

При подключении к виртуальному маршрутизатору выводится статус сервиса VNF:

```
.-~~~~-.
.- ~ ~-(      )_ _
/              )~ -..
|   БРЕСТ - сервис VNF      ',
\           v0.1-15          ',
'~,.....,~,~
```

```
2/3 Конфигурация / Configuration
в процессе... / step is in progress
```

Статус в приветствии обновляется только при подключении к маршрутизатору (если маршрутизатор находится в процессе конфигурации, необходимо выйти и подключиться позднее). При успешном запуске выводится сообщение:

```
Все сетевые функции готовы к использованию.
All Virtual Network Functions are ready to serve
```

При запуске виртуального маршрутизатора инициализация сервисов может занимать до 1 минуты.

6.3.1.3. Журнал работы VNF (система логирования) и обработка ошибок

Основной журнал процесса конфигурации VNF `/var/log/one-appliance/ONE_configure.log`.

ВНИМАНИЕ! Журнал `/var/log/one-appliance/ONE_configure.log` не ведется во время работы маршрутизатора, в него попадают сообщения только в процессе конфигурации или реконфигурации сервиса.

Для параметров VNF добавлены базовые проверки на соответствие типам и на корректность указанных значений, приведенные в таблице 12:

Таблица 12

Параметр	Корректное значение
<code>VROUTER_KEEPAIVED_PASSWOR</code>	[буквы, цифры, спецсимволы, длина не более 8 символов]
<code>VROUTER_KEEPAIVED_PASSWORD</code>	[буквы, цифры, спецсимволы, длина не более 8 символов]
<code>ONEAPP_VNF_KEEPAIVED_ETHx_PASSWORD</code>	[буквы, цифры, спецсимволы, длина не более 8 символов]
<code>ONEAPP_VNF_KEEPAIVED_INTERVAL</code>	[1...255]
<code>ONEAPP_VNF_KEEPAIVED_ETHx_INTERVAL</code>	[1...255]
<code>ONEAPP_VNF_KEEPAIVED_PRIORITY</code>	[1...255]
<code>ONEAPP_VNF_KEEPAIVED_ETHx_PRIORITY</code>	[1...255]
<code>ONEAPP_VNF_DHCP4_LEASE_TIME</code>	[1...4294967295]
<code>ONEAPP_VNF_DHCP4_ETHx_MTU</code>	[68...9000]
<code>ONEAPP_VNF_DNS_MAX_CACHE_TTL</code>	[0...604800]
<code>ONEAPP_VNF_DNS_UPSTREAM_TIMEOUT</code>	[0...4294967295]
<code>ONEAPP_VNF_SDNAT4_REFRESH_RATE</code>	[1...4294967295]
<code>ONEAPP_VNF_LB_REFRESH_RATE</code>	[1...4294967295]
<code>ONEAPP_VNF_LB_FWMARK_OFFSET</code>	[1...4294967295]
<code>ONEAPP_VNF_LBx_PORT</code>	[1...65535]
<code>ONEAPP_VNF_LBx_TIMEOUT</code>	[1...2678400]

Сообщения об ошибках и предупреждениях (errors/warnings) направляются в журнал `/var/log/one-appliance/ONE_configure.log` и дополнительно отображаются в сообщении при входе на виртуальный маршрутизатор с указанием имени сервиса.

Пример вида сообщения об ошибке:

```
* * * * *
* Ошибка сервиса VNF *
*           -           *
*  APPLIANCE ERROR  *
* * * * *
```

* * * * *

```
ОШИБКА [!]: Сбой в процессе конфигурации DHCP4
ПРЕДУПРЕЖДЕНИЕ [!]: VNF DHCP4: Неправильное имя
сетевого интерфейса: ETH012345 (настройка пропущена)
ОШИБКА [!]: VNF DHCP4: Параметр ONEAPP_VNF_DHCP4_ETH0_DNS
не является IPv4 адресом: a.b.c.d
```

Обратитесь к документации и повторите попытку конфигурации сервиса!
Read documentation and try to redeploy!

6.3.2. Функции виртуальной сети

6.3.2.1. Работа с параметрами контекстуализации

Параметры контекстуализации, указанные в шаблоне VM, определяют начальную конфигурацию VM. Для настройки VNF существуют специфичные наборы параметров для каждой из функций виртуальной сети. Параметры должны быть указаны в разделе КОНТЕХТ шаблона VM.

Если параметры поддерживают указание нескольких значений, эти значения могут быть разделены пробелами (x y), запятыми (x,y) или точками с запятой (x;y).

У каждой функции VNF есть параметр контекстуализации, который определяет, на каких сетевых интерфейсах подключенная функция будет активна, а на каких нет. Если не указывать эти параметры, то подключенная функция VNF прослушивает все доступные интерфейсы (за исключением loopback-интерфейса и интерфейса управления).

При указании в параметрах сетевых интерфейсов всегда необходимо использовать имена интерфейсов вида eth, за которыми следует индекс, начинающийся с 0, т.е. eth0 для первой сетевой карты, eth4 для пятой сетевой карты. Например, чтобы включить функцию DNS VNF только на 3-м и 4-м сетевых интерфейсах, параметр контекстуализации должен выглядеть следующим образом:

```
ONEAPP_VNF_DNS_INTERFACES="eth2 eth3"
```

6.3.2.2. Высокая доступность (keepalived)

Keepalived — это служба обеспечивающая высокую доступность VNF на основе протокола VRRP и специального сервиса, отслеживающего состояние экземпляра VM виртуального маршрутизатора и его сетевых функций.. В случае инцидента (недоступности сервиса VNF) сервис перенесет все плавающие IP-адреса и сетевые функции на другой экземпляр виртуального маршрутизатора с минимальным временем простоя.

ВНИМАНИЕ! Для работы keepalived должен быть настроен хотя бы один VNF и один плавающий IP-адрес. Также должен быть указан параметр ONEAPP_VNF_KEEPAIVED_VRID,

уникальный для подсетей. В противном случае разные ВМ с одинаковым идентификатором могут безуспешно пытаться объединиться в один и тот же кластер.

Многokратная быстрая последовательная реконфигурация ВМ или виртуального маршрутизатора (например, горячее подключение нескольких сетевых адаптеров) может привести к сбою в работе кластера Keepalived. При реконфигурации всегда необходимо проверять, находится ли экземпляр в нужном состоянии после каждого изменения.

Переход между состояниями BACKUP/MASTER и инициализацию других VNF функций можно отследить в журнале сервиса выполнив команду:

```
sudo journalctl -u keepalived
```

Основные параметры контекстуализации высокой доступности представлены в таблице 13:

Таблица 13

Параметр	Значение по умолчанию	Описание
ONEAPP_VNF_KEEPAIVED_ENABLED	NO	Включение/выключение функции keepalived (YES/NO)
ONEAPP_VNF_KEEPAIVED_INTERFACES	все интерфейсы	Список управляемых интерфейсов (<[!]ethX> ...)
VROUTER_KEEPAIVED_PASSWORD		Пароль для аутентификации VRRP (максимум 8 символов)
ONEAPP_VNF_KEEPAIVED_PRIORITY	100	Числовой приоритет VRRP маршрутизатора
ONEAPP_VNF_KEEPAIVED_VRID	1	Идентификатор VRRP маршрутизатора (1-255)
ONEAPP_VNF_KEEPAIVED_INTERVAL	1	Периодичность проверки (секунды)

Расширенные параметры контекстуализации высокой доступности представлены в таблице 14:

Таблица 14

Параметр	Значение по умолчанию	Описание
ONEAPP_VNF_KEEPAIVED_ETHx_PASSWORD		Пароль VRRP маршрутизатора для сетевого интерфейса (максимум 8 символов)
ONEAPP_VNF_KEEPAIVED_ETHx_PRIORITY	100	Числовой приоритет VRRP маршрутизатора для сетевого интерфейса

Окончание таблицы 14

Параметр	Значение по умолчанию	Описание
ONEAPP_VNF_KEEPAIVED_ETHx_VRID	1	Идентификатор VRRP маршрутизатора для сетевого интерфейса(1-255)
ONEAPP_VNF_KEEPAIVED_ETHx_INTERVAL	1	Периодичность проверки для сетевого интерфейса(секунды)

6.3.2.3. ROUTER4

Сервис VNF обеспечивает функциональность маршрутизации между различными сетями и позволяет ВМ из разных виртуальных сетей взаимодействовать друг с другом. Если включить функцию маршрутизации (параметр ONEAPP_VNF_ROUTER4_ENABLED="YES"), то по умолчанию маршрутизация будет выполняться между всеми подключенными интерфейсами (кроме интерфейса управления). Для выбора определенных интерфейсов для маршрутизации необходимо указать значение параметра ONEAPP_VNF_ROUTER4_INTERFACES.

Примечание. Функция ROUTER4 обеспечивает только маршрутизацию. Например, для того чтобы предоставить ВМ частной сети доступ к общедоступным интернет-сервисам, эту функцию необходимо использовать вместе с NAT4.

Функция ROUTER4 использует стандартные возможности IP-стека Linux по маршрутизации транзитных IP-пакетов (IP forwarding).

Основные параметры контекстуализации ROUTER4 представлены в таблице 15:

Таблица 15

Параметр	Значение по умолчанию	Описание
ONEAPP_VNF_ROUTER4_ENABLED	NO	Включение/выключение функции ROUTER4 (YES, NO)
ONEAPP_VNF_ROUTER4_INTERFACES	все интерфейсы	Список управляемых интерфейсов (<![ethX> ...)

6.3.2.4. DHCP4

VNF предоставляет сервис протокола динамической настройки узла (DHCPv4), реализованный с помощью DHCP-сервера ISC Kea версии 2.2.0.

При настройке DHCPv4 всегда необходимо указывать список интерфейсов в параметре ONEAPP_VNF_DHCP4_INTERFACES. В противном случае работа службы будет распространяться на все интерфейсы (несвязанные с управлением) и все настроенные подсети.

По умолчанию, сервис предоставляет сетевую конфигурацию для DHCP-

клиентов основываясь на конфигурации интерфейсов, включенных параметром ONEAPP_VNF_DHCP4_INTERFACES. Конфигурация создается на основе заданных постоянных параметров контекста виртуальных сетей (например, ETH0_GATEWAY), а не из действующей конфигурации конкретных сетевых интерфейсов. Настройки могут быть предопределены параметрами контекстуализации DHCP VNF, с указанием сетевого интерфейса или псевдонима, например:

```

CONTEXT=[
ONEAPP_VNF_DHCP4_ETHx="<CIDR>:<start IP>-<end IP>",
ONEAPP_VNF_DHCP4_ETHx_DNS="<IP> ...",
ONEAPP_VNF_DHCP4_ETHx_GATEWAY="<IP> ...",
ONEAPP_VNF_DHCP4_ETHx_MTU="<number>",
ONEAPP_VNF_DHCP4_ETHx_ALIASy="<CIDR>:<start IP>-<end IP>",
ONEAPP_VNF_DHCP4_ETHx_ALIASy_DNS="<IP> ...",
ONEAPP_VNF_DHCP4_ETHx_ALIASy_GATEWAY="<IP> ...",
ONEAPP_VNF_DHCP4_ETHx_ALIASy_MTU="<number>",
...
]

```

Параметры контекстуализации для псевдонимов сетевых интерфейсов применяются только в том случае, если подсеть псевдонима уникальна (т.е. ни один другой интерфейс не использует ту же подсеть). В противном случае конкретная конфигурация псевдонима сетевого адаптера игнорируется. Контекстуализация основных (без псевдонимов) интерфейсов всегда имеет приоритет над псевдонимами сетевых интерфейсов для одной и той же подсети.

Пример

В ВМ настроены интерфейс и его псевдонимом — eth0: 192.168.0.1/255.255.0.0 и eth0 alias 0: 192.168.1.100/255.255.0.0, и следующая контекстуализация DHCP4 VNF:

```

CONTEXT=[
ONEAPP_VNF_DHCP4_ETH0_DNS="8.8.8.8",
ONEAPP_VNF_DHCP4_ETH0_ALIAS0_DNS="4.4.4.4",
ONEAPP_VNF_DHCP4_ETH0_ALIAS0="192.168.0.0/16:192.168.100.100-192.168.200.250",
...
]

```

В этом примере интерфейс eth0 и его псевдоним используют одну подсеть, но имеются два разных параметра, переопределяющих настройки сервера имен и пула IP-адресов (по-умолчанию и конкретно заданные). Таким образом, когда VNF пытается создать конфигурацию DHCP4, он встречает конфликт пулов ад-

ресов и параметров (DNS, GATEWAY, и MTU). Именно по этому переменные сетевого интерфейса (ONEAPP_VNF_DHCP4_ETH0) всегда главнее в таких сценариях (ONEAPP_VNF_DHCP4_ETH0_ALIAS0 и ONEAPP_VNF_DHCP4_ETH0_ALIAS0_DNS будут проигнорированы).

Конечная сгенерированная конфигурации из этого примера:

```
...
"subnet4": [
{
"subnet": "192.168.0.0/16",
"pools": [ { "pool": "192.168.0.2-192.168.255.254" } ],
"option-data": [
{ "name": "domain-name-servers", "data": "8.8.8.8" },
{ "name": "routers", "data": "192.168.0.1" }
],
"reservations": [
{ "flex-id": "'DO-NOT-LEASE-192.168.101.1'", "ip-address": "192.168.0.1" },
{ "flex-id": "'DO-NOT-LEASE-192.168.101.100'", "ip-address": "192.168.1.100" }
],
"reservation-mode": "all"
},
```

Для более тонкой настройки конфигурации подсетей можно напрямую передать параметры DHCP-сервера с помощью параметра ONEAPP_VNF_DHCP4_SUB. Значением параметра должна являться корректная JSON-конфигурация для ISC Kea (раздел subnet4 section), закодированная в Base64. Так же может быть указано больше переменных конфигурации, и они должны оканчиваться на числовые индексы (например, ONEAPP_VNF_DHCP4_SUBNET0). Определения подсетей такими контекстными параметрами всегда имеет приоритет над другими интерфейс-специфичными параметрами (например, заданный параметр ONEAPP_VNF_DHCP4_SUBNET отключает любую контекстуализацию, основанную на конфигурации интерфейса).

Так же возможна живая переконфигурация и адаптирование к контексту по мере внесения изменений. Возможным последствием может являться то, что некоторые прежде назначенные переменные могут оставаться активными даже после их удаления! Для примера, проблема может возникнуть, если переменные вида ONEAPP_VNF_DHCP4_SUBNET были заданы, но теперь вы желаете использовать переменные интерфейсов (вида ONEAPP_VNF_DHCP4_ETHx), удаляете первую переменную, но она все еще продолжает существовать в рамках контекста. Обходным решением является назначение переменным пустого контекста, вместо их удаления (для примера, ONEAPP_VNF_DHCP4_SUBNET0="").

Примечание. Не рекомендуется удалять ранее использованные параметры контекстуализации, вместо этого необходимо задать пустую строку в качестве значения. Далее можно безопасно их удалить после повторной контекстуализации или перезагрузки виртуального маршрутизатора.

Трансляция MAC-адреса в IPv4

В ПК СВ существует прямая корреляция между MAC и IPv4 адресами, выделенными сетевым интерфейсам виртуальных машин. MAC-адреса сетевых интерфейсов формируются из:

- 2-байтового префикса (по умолчанию 02:00). Он может быть назначен переменной `MAC_PREFIX` в `oned.conf`;
- шестнадцатеричного представления назначенного IPv4-адреса (например, 01:02:03:04 для адреса 1.2.3.4).

К службе DHCP сервера дополнительно подключен модуль (hook) для реализации функции назначения IPv4 адреса на основе MAC-адреса виртуальной машины. Это позволяет VM получать с помощью DHCP такой же адрес, какой она бы получила при обычном использовании виртуальных сетей (параметры которых передаются через статичный контекст VM). Это позволяет подключать к виртуальной сети VM, не использующие настройку через контекстуализацию (т.е. без установленного пакета `one-context`).

Примечание. Функция трансляции MAC-адреса в IPv4 работает полностью автономно, без обращения к серверу управления. Функция включена по умолчанию и может быть отключена переменной `ONEAPP_VNF_DHCP4_MAC2IP_ENABLED`.

Трансляция может быть настроена на работу только в определенных подсетях с помощью параметра `ONEAPP_VNF_DHCP4_MAC2IP_SUBNETS`, который принимает в качестве значения список диапазонов в формате CIDR. Для оставшихся сетей, не определенных в этом параметре, применяются обычные правила выделения адресов DHCP-сервером. Отсутствующий или пустой параметр включает работу трансляции MAC в IPv4 во всех подсетях.

ВНИМАНИЕ! При включенной трансляции MAC-адреса в IPv4 запросы с MAC-адресов, которые не могут быть преобразованы в подходящий IP-адрес, игнорируются.

При настройке DHCP для VM, не находящихся под управлением ПК СВ, необходимо задать значение параметра `ONEAPP_VNF_DHCP4_MAC2IP_SUBNETS` или полностью отключить функцию трансляции MAC-адреса в IPv4 (`ONEAPP_VNF_DHCP4_MAC2IP_ENABLED="NO"`). В противном случае может возникнуть проблема неработоспособности DHCP.

Основные параметры контекстуализации DHCP4 представлены в таблице 16:

Таблица 16

Параметр	Значение по умолчанию	Описание
ONEAPP_VNF_DHCP4_ENABLED	NO	Включение/выключение функции DHCP4 (YES/NO)
ONEAPP_VNF_DHCP4_INTERFACES	all ifaces	Список управляемых интерфейсов (<[!]ethX> ...). Может быть указан в следующих форматах: - ethX – имя сетевого интерфейса (например, eth0); - ethX/IP – имя сетевого интерфейса с IP-адресом для точного определения адреса прослушивания и создания подсети в случае, если интерфейсу назначено более одного IP-адреса (например, eth0/192.168.1.1).
ONEAPP_VNF_DHCP4_AUTHORITATIVE	YES	Определяет, является ли DHCP-сервер авторитативным (YES/NO)
ONEAPP_VNF_DHCP4_LEASE_TIME	3600	Время аренды IP-адреса (секунды)
ONEAPP_VNF_DHCP4_DNS		DNS-сервер по умолчанию (IP-адрес)
ONEAPP_VNF_DHCP4_GATEWAY		Шлюз по умолчанию (IP-адрес)
ONEAPP_VNF_DHCP4_MAC2IP_ENABLED	YES	Включение/отключение трансляции MAC-адреса в IPv4 (YES/NO)

Расширенные параметры контекстуализации DHCP4 представлены в таблице 17:

ВНИМАНИЕ! Параметры ONEAPP_VNF_DHCP4_ETHx_DNS/GATEWAY/MTU применяются только при наличии хотя бы одного диапазона, указанного в параметре ONEAPP_VNF_DHCP4_ETHx. Аналогично, параметры ONEAPP_VNF_DHCP4_ETHx_ALIASy_DNS/GATEWAY/MTU активны при указании хотя бы одного диапазона в ONEAPP_VNF_DHCP4_ETHx_ALIASy.

Таблица 17

Параметр	Описание
ONEAPP_VNF_DHCP4_ETHx	Диапазон IP-адресов подсети/пула VM (<CIDR>:<start IP>-<end IP>)
ONEAPP_VNF_DHCP4_ETHx_DNS	Пул интерфейсов DNS (<IP> ...)
ONEAPP_VNF_DHCP4_ETHx_GATEWAY	Пул сетевых шлюзов (<IP> ...)
ONEAPP_VNF_DHCP4_ETHx_MTU	Максимальный передаваемый модуль данных (MTU) (число)
ONEAPP_VNF_DHCP4_ETHx_ALIASy	Диапазон IP-адресов псевдонимов сетевых интерфейсов (<CIDR>:<start IP>-<end IP>)

Окончание таблицы 17

Параметр	Описание
ONEAPP_VNF_DHCP4_ETHx_ALIASy_DNS	Пул интерфейсов DNS для псевдонимов сетевых интерфейсов (<IP> ...)
ONEAPP_VNF_DHCP4_ETHx_ALIASy_GATEWAY	Пул сетевых шлюзов для псевдонимов сетевых интерфейсов (<IP> ...)
ONEAPP_VNF_DHCP4_ETHx_ALIASy_MTU	Максимальный передаваемый модуль данных (MTU) для псевдонимов сетевых интерфейсов (число)
ONEAPP_VNF_DHCP4_MAC2IP_SUBNETS	Список подсетей для трансляции MAC-адреса в IPv4 (<network>/<prefix> ...)

6.3.2.5. DNS

Сервис VNF предоставляет службу DNS, которая может делегировать запросы вышестоящим серверам (на основе параметров контекста сети) или напрямую разрешать DNS-запросы самостоятельно.

По умолчанию VNF использует корневые серверы DNS (из `dns-root-data` от Astra Linux) для самостоятельного разрешения запросов. DNS также может перенаправлять запросы (в случае использования `ONEAPP_VNF_DNS_USE_ROOTSERVERS="NO"`) на другие настроенные DNS-серверы, указанные в `ONEAPP_VNF_DNS_NAMESERVERS` или автоматически настроенные из параметров виртуальных сетей.

В режиме перенаправления запросов автоматическая настройка параметров обычно нежелательна, поэтому следует явно указать вышестоящие DNS-сервера, например:

```
CONTEXT=[
ONEAPP_VNF_DNS_NAMESERVERS="8.8.8.8, 8.8.4.4",
...
]
```

Сервис может быть ограничен только для обслуживания определенных сетевых интерфейсах через `ONEAPP_VNF_DNS_INTERFACES`. Помимо описанного выше синтаксиса для перечисления интерфейсов, для которых необходимо включить или выключить функцию (`ethX`, `!ethX`), в случае DNS также можно задать дополнительный IP-адрес для прослушивания и порт для конкретного интерфейса (`ethX/IP[@port]`), например:

```
CONTEXT=[
ONEAPP_VNF_DNS_INTERFACES="eth0, eth1/10.0.0.1, eth2/192.168.0.1@53",
...
]
```

Функция DNS может быть отключена для протокола TCP (через `ONEAPP_VNF_DNS_TCP_DISABLED="YES"`) или UDP (через `ONEAPP_VNF_DNS_UDP_DISABLED="YES"`).

Примечание. Не рекомендуется отключать протокол UDP, поскольку многие общедоступные серверы DNS используют только протокол UDP.

Для полного контроля над DNS VNF можно использовать возможность указания полного конфигурационного файла для DNS-сервера Unbound (ONEAPP_VNF_DNS_CONFIG). Значением должна быть строка в кодировке Base64 с корректным содержимым unbound.conf.

Основные параметры контекстуализации DNS представлены в таблице 18:

Таблица 18

Параметр	Значение по умолчанию	Описание
ONEAPP_VNF_DNS_ENABLED	NO	Включение/выключение функции DNS (YES/NO)
ONEAPP_VNF_DNS_INTERFACES	все интерфейсы	Список интерфейсов для прослушивания
ONEAPP_VNF_DNS_MAX_CACHE_TTL	3600	Максимальное время кэширования (секунды)
ONEAPP_VNF_DNS_USE_ROOTSERVERS	YES	Использование корневых DNS-серверов напрямую (YES/NO)
ONEAPP_VNF_DNS_NAMESERVERS		Список вышестоящих серверов имен для пересылки запросов (<IP>[@<PORT>] ...)
ONEAPP_VNF_DNS_UPSTREAM_TIMEOUT	1128	Время ожидания исходящего соединения к серверу имен (миллисекунды)

Расширенные параметры контекстуализации DNS представлены в таблице 19:

Таблица 19

Параметр	Значение по умолчанию	Описание
ONEAPP_VNF_DNS_CONFIG		Конфигурация Unbound сервера (в кодировке Base64)
ONEAPP_VNF_DNS_ALLOWED_NETWORKS		Список клиентских сетей, из которых разрешено делать запросы (<network>/<prefix> ...)
ONEAPP_VNF_DNS_TCP_DISABLED	NO	Включение/отключение TCP (YES/NO)
ONEAPP_VNF_DNS_UDP_DISABLED	NO	Включение/отключение UDP (YES/NO)

6.3.2.6. NAT4

Сервис VNF предоставляет функцию транслирования IPv4 адресов (Network Address Translation, маскардинг) для подключенных сетевых интерфейсов через указанные выходные интерфейсы.

ВНИМАНИЕ! Выходной интерфейс всегда должен быть указан в параметре ONEAPP_VNF_NAT4_INTERFACES_OUT.

Без указания выходного интерфейса функция NAT4 не сможет быть запущена.

Основные параметры контекстуализации NAT4 представлены в таблице 20:

Т а б л и ц а 20

Параметр	Значение по умолчанию	Описание
ONEAPP_VNF_NAT4_ENABLED	NO	Включение/выключение функции NAT (YES/NO)
ONEAPP_VNF_NAT4_INTERFACES_OUT		Обязательный параметр: выходной интерфейс для NAT (<[!]ethX> ...)

6.3.2.7. SDNAT4

П р и м е ч а н и е. Для работы функции SDNAT4 необходимо настроить ПК СВ для использования службы сервера OneGate.

Функция SDNAT4 схожа с функцией NAT4, поскольку реализована при помощи двустороннего NAT: SNAT (исходящий NAT) и DNAT (целевой NAT).

SDNAT4 сопоставляет виртуальные сети, позволяя прозрачно передавать трафик (для какого-либо целевого IP-адреса, например публичного) из одной сети на устройство в другой сети без необходимости прямого подключения устройства к первой сети (то есть, без раскрытия адреса конечного устройства в первой сети). Механизм реализуется с помощью сопоставления указанных двух IP-адресов из разных сетей. Такое сопоставление обслуживается виртуальным маршрутизатором, к которому должны быть подключены все связанные сети. Внешний IP-адрес для сопоставления должен быть присоединен к VM в качестве внешнего псевдонима сетевого интерфейса.

Интерфейсы на виртуальном маршрутизаторе, между которыми может быть установлено сопоставление, всегда должны быть указаны в параметре контекстуализации ONEAPP_VNF_SDNAT4_INTERFACES, в противном случае никакие правила применяться не будут (параметр отличается от подобных параметров в других функциях VNF, где пустой список по умолчанию означает все интерфейсы).

Как только список интерфейсов передается в VNF, служба, развернутая внутри виртуального маршрутизатора, начинает отслеживать изменения в распределении IP-адресов через OneGate. На основе агрегированных данных создается список пар для SNAT/DNAT, где конечная часть — это IP-адрес внешнего псевдонима сетевого интерфейса, а исходная часть - реальный IP-адрес, назначенный VM, к которой происходит подключение.

ВНИМАНИЕ! Обязательно должен быть установлен параметр шаблона

EXTERNAL=YES, в противном случае псевдоним будет настроен как внутренний и в виртуальной машине появится дополнительный IP-адрес. Использование внешних псевдонимов также может быть реализовано для всех IP-адресов виртуальной сети, если параметр EXTERNAL=YES задан непосредственно в шаблоне вашей виртуальной сети.

Такой псевдоним может быть присоединен к ВМ (например, с идентификатором 10) командой:

```
onevm nic-attach 10 --file external-nic-alias.tpl
```

Основные параметры контекстуализации SDNAT4 представлены в таблице 21:

Таблица 21

Параметр	Значение по умолчанию	Описание
ONEAPP_VNF_SDNAT4_ENABLED	NO	Включение/выключение функции SDNAT4 (YES/NO)
ONEAPP_VNF_SDNAT4_INTERFACES		Обязательный параметр: список интерфейсов для работы функции SDNAT4 (<![ethX> ...)
ONEAPP_VNF_SDNAT4_REFRESH_RATE	30	Интервал обновления правил сопоставления (секунды)

6.3.2.8. LB (LoadBalancer)

Примечание. Для работы функции LB (LoadBalancer) необходимо настроить ПК СВ для использования службы сервера OneGate.

Функция предоставляет службу балансировщика нагрузки, которая для заданных входящих подключений будет перенаправлять трафик и балансировать нагрузку на пул статических и/или динамических реальных серверов.

Функция LoadBalancer основана на Linux Virtual Server (LVS/IPVS) и использует вспомогательные средства пакета `ipvsadm`, входящего в состав репозитория Astra Linux.

Основные параметры контекстуализации LB представлены в таблице 22:

Примечание. Основные параметры влияют на все настроенные балансировщики нагрузки.

Таблица 22

Параметр	Значение по умолчанию	Описание
ONEAPP_VNF_LB_ENABLED	NO	Включение/выключение функции балансировщика нагрузки (YES/NO)

Окончание таблицы 22

Параметр	Значение по умолчанию	Описание
ONEAPP_VNF_LB_ONEGATE_ENABLED	NO	Включение/выключение динамических реальных серверов с помощью OneGate (YES/NO)
ONEAPP_VNF_LB_REFRESH_RATE	30	Частота обновления пула реальных серверов (секунды)
ONEAPP_VNF_LB_FWMARK_OFFSET	10000	Начальное значение маркировки (firewall mark) для LVS/IPVS
ONEAPP_VNF_LB_CONFIG		Индивидуальные конфигурации балансировщиков нагрузки (JSON в кодировке BASE64, разделенные запятыми). При использовании этого параметра игнорируются параметры контекстуализации балансировщика нагрузки и статических реальных серверов. Динамические параметры реального сервера по-прежнему будут применяться

Параметры балансировщика нагрузки

В таблице 23 перечислены параметры, определяющие балансировщик нагрузки, если не был настроен параметр ONEAPP_VNF_LB_CONFIG.

Таблица 23

Параметр	Значение по умолчанию	Описание
ONEAPP_VNF_LB[0-9]_IP		Обязательный параметр: IP-адрес балансировщика нагрузки Примечание. Если указан только IP-адрес (не указаны ни порт, ни протокол), то весь трафик по этому IP-адресу с балансировкой нагрузки будет перенаправляться на реальные серверы в соотношении 1:1
ONEAPP_VNF_LB[0-9]_PORT		IP-порт для балансировки соединения (опционально)
ONEAPP_VNF_LB[0-9]_PROTOCOL		IP-протокол для балансировки соединения (опционально TCP, UDP или BOTH)

Окончание таблицы 23

Параметр	Значение по умолчанию	Описание
ONEAPP_VNF_LB[0-9]_METHOD	NAT	Метод LVS/IPVS (NAT или DR (Direct Routing – прямая маршрутизация) Примечание. Для работы метода прямой маршрутизации потребуются дополнительные действия на реальных серверах, которые описаны в разделе (указать после перевода)
ONEAPP_VNF_LB[0-9]_TIMEOUT	10	Допустимый тайм-аут любого реального сервера для этого LB (секунды)

Метод LVS/IPVS NAT

Балансировщик нагрузки по умолчанию будет использовать метод NAT, при котором VNF будет направлять трафик между VM и реальными серверами через себя в обоих направлениях.

Для этого метода потребуется два настроенных сетевых интерфейса в VNF и две виртуальные сети — одна общедоступная, из которой будет иницироваться трафик, и частная, где будут расположены реальные серверы:

NAT method:

```
.-----
| Client |
\-----\
eth0: client IP
|
|

(public vnet)

src: client IP <---> dest: LB IP

|
|
eth0: LB IP
.-----
DNAT >> | VNF/Vrouter | >> SNAT
\-----\
```

```

eth1: Priv IP
|
|

(private vnet)

src: client IP <---> dest: RS IP

|
|
eth0: RS IP
.-----
| Real Server |
\-----`

```

Метод LVS/IPVS DR (Direct Routing — прямая маршрутизация)

Альтернативой методу NAT является использование метода прямой маршрутизации. Например, какой-то конкретный балансировщик нагрузки (в данном случае LB0) можно переключить на метод прямой маршрутизации, установив контекстному параметру ONEAPP_VNF_LB0_METHOD (параметру lb-method в конфигурационном JSON) значение DR.

При использовании DR VNF будет видеть только входящий трафик, но исходящий трафик с любого реального сервера будет возвращаться непосредственно на VM. Для настройки DR метода потребуется только один сетевой интерфейс и только одна виртуальная сеть:

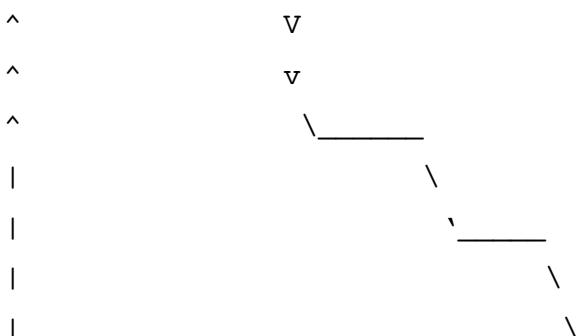
```

DR method:

.-----
| Client |
\-----`

eth0: client IP

```




```

|
|           src: client IP --> dest: LB IP
|
|
|           |
|
|           eth0: LB IP
|
|-----|
| src: LB IP --> dest: client IP           | VNF/Vrouter |
|-----|
|
|           |
|
|           src: client IP --> dest: LB IP (!!!)
|
|
|           /
|           /
|           /
|           /
|           /
^           /
^           v
^           V

lo: LB IP (!!!)
eth0: RS IP
|-----|
| Real Server |
|-----|

```

На приведенной выше схеме реальный сервер отвечает на любые запросы ARP для IP с балансировкой нагрузки, из-за этого возникает конфликт IP-адресов в одной подсети — IP балансировщика нагрузки настроен как на реальном сервере, так и на VNF.

Для предотвращения этого необходимы следующие дополнительные настройки:

- каждому реальному серверу балансировщика нагрузки, использующего DR, также должен быть назначен IP-адрес с балансировкой нагрузки — для этого можно использовать либо loopback-интерфейс, либо какой-либо интерфейс-заглушку (modprobe dummy):

```
$ ip addr add <LB_IP> dev lo
```

- на каждом реальном сервере также необходимо настроить обход проблемы ARP flux, чтобы избежать нежелательных ответов ARP:

```
# e.g. in /etc/sysctl.conf
net.ipv4.ip_nonlocal_bind=1
net.ipv4.conf.eth0.arp_ignore = 1
net.ipv4.conf.eth0.arp_announce = 2
```

Примечание. Аналогичный результат может быть достигнут и с помощью команды `arptables` – если использование `sysctl` нежелательно.

Параметры контекстуализации статического реального сервера

В таблице 24 перечислены параметры, определяющие статический реальный сервер, если не был настроен параметр `ONEAPP_VNF_LB_CONFIG`.

Таблица 24

Параметр	Значение по умолчанию	Описание
<code>ONEAPP_VNF_LB[0-9]_SERVER[0-9]_HOST</code>		Обязательный параметр: реальный адрес сервера (IP-адрес или доменное имя)
<code>ONEAPP_VNF_LB[0-9]_SERVER[0-9]_PORT</code>		Порт реального сервера (необходимо указывать если определен параметр <code>ONEAPP_VNF_LB[0-9]_PORT</code>)
<code>ONEAPP_VNF_LB[0-9]_SERVER[0-9]_WEIGHT</code>	используется из <code>ipvs</code>	Вес реального сервера
<code>ONEAPP_VNF_LB[0-9]_SERVER[0-9]_ULIMIT</code>	используется из <code>ipvs</code>	Верхний предел количества подключений к реальному серверу
<code>ONEAPP_VNF_LB[0-9]_SERVER[0-9]_LLIMIT</code>	используется из <code>ipvs</code>	Нижний предел количества подключений к реальному серверу

Использование динамических реальных серверов

Если для ПК СВ сконфигурирован сервис OneGate, то есть возможность динамически обновлять пул реальных серверов, используемый балансировщиком нагрузки.

При таком способе создаются VM, выполняющие специальную программу или скрипт, которые при начальной загрузке или при возникновении необходимости дадут команду VNF присоединить эту VM к пулу реальных серверов, используя переменные OneGate.

В таблице 25 перечислены переменные OneGate.

Таблица 25

Переменная	Описание
<code>ONEGATE_LB[0-9]_IP</code>	Обязательная переменная: IP-адрес с балансировкой нагрузки, определенный в VNF

Окончание таблицы 25

Переменная	Описание
ONEGATE_LB[0-9]_PORT	IP-порт с балансировкой нагрузки, определенный в VNF (требуется указывать, если используется для балансировщика нагрузки)
ONEGATE_LB[0-9]_PROTOCOL	IP-протокол с балансировкой нагрузки, определенный в VNF (требуется указывать, если используется для балансировщика нагрузки)
ONEGATE_LB[0-9]_SERVER_HOST	Обязательный параметр: реальный адрес сервера (IP-адрес или доменное имя)
ONEGATE_LB[0-9]_SERVER_PORT	Порт реального сервера (требуется указывать, если порт определен для балансировщика нагрузки)
ONEGATE_LB[0-9]_SERVER_WEIGHT	Вес реального сервера
ONEGATE_LB[0-9]_SERVER_ULIMIT	Верхний предел количества подключений к реальному серверу
ONEGATE_LB[0-9]_SERVER_LLIMIT	Нижний предел количества подключений к реальному серверу

Примечание. Можно определить несколько балансировщиков нагрузки на каждой VM, для этого необходимо верно определить переменные с распределением их по IP-порту или IP-протоколу.

Индекс [0-9] не обязательно должно совпадать с индексом VNF, но он должно соответствовать набору параметров балансировщика нагрузки (IP, порт и протокол) или просто IP-адресу с балансировкой нагрузки, если для балансировщика не определены ни порт, ни протокол.

Пример настроек VM с переменными OneGate:

```
onegate vm update --data ONEGATE_LB0_IP=192.168.150.100
onegate vm update --data ONEGATE_LB0_PROTOCOL=TCP
onegate vm update --data ONEGATE_LB0_PORT=80
onegate vm update --data ONEGATE_LB0_SERVER_HOST=192.168.101.1
onegate vm update --data ONEGATE_LB0_SERVER_PORT=8080
```

Примечание. В приведенном выше примере использован один индекс (0), чтобы определить этот единственный динамический реальный сервер и связать его с нужным балансировщиком нагрузки.

6.3.3. VNF как виртуальный маршрутизатор

6.3.3.1. Подготовка VNF

В этом примере будет создан виртуальный маршрутизатор в ПК СВ Брест и развернут сервис VNF в режиме высокой доступности с запущенной службой Keepalive.

1) Перейти в раздел «Сеть — Вирт. сети» и создать три виртуальные сети, параметры которых указаны в таблице 27:

Т а б л и ц а 26

Имя виртуальной сети	Подсеть	Диапазон	Шлюз	DNS
public	192.168.150.0/24	192.168.150.100 - 192.168.150.199	192.168.150.1	
vnet_a	192.168.101.0/24	192.168.101.100 - 192.168.101.199	192.168.101.111	192.168.101.111
vnet_b	192.168.102.0/24	192.168.102.100 - 192.168.102.199	192.168.102.111	192.168.102.111

2) Обратиться к разделу по созданию VNF (см 6.3.1):

- на шаге создания маршрутизатора при выборе Пользовательских атрибутов установить следующие значения (см. рис. 79):


Имя виртуальной машины 	Количество экземпляров VM	<input type="checkbox"/> Создать и поставить на паузу
<input type="text" value="vr--%i"/>	<input type="text" value="2"/>	
Пользовательские атрибуты		
DHCP4 - Включить / Enable		
ДА <input checked="" type="radio"/> НЕТ <input type="radio"/>		
DHCP4 - Список прослушиваемых интерфейсов / Listening Interfaces		
<input type="text" value="!eth0"/>		
DNS - Включить сервер / Enable DNS Server		
ДА <input checked="" type="radio"/> НЕТ <input type="radio"/>		
DNS - Список прослушиваемых интерфейсов / Listening Interfaces		
<input type="text" value="!eth0"/>		
NAT - Включить / Enable		
ДА <input checked="" type="radio"/> НЕТ <input type="radio"/>		
NAT - Список исходящих интерфейсов / Outgoing Interfaces		
<input type="text" value="eth0"/>		
SDNAT - Включить / Enable		
ДА <input type="radio"/> НЕТ <input checked="" type="radio"/>		
SDNAT - Список интерфейсов для сопоставления адресов / Mapped Interfaces		
<input type="text"/>		
*** DHCP4 - Время аренды адреса (сек) / Lease Time [sec]		
<input type="text" value="3600"/>		
*** DNS - Установка времени кэширования (сек) / Maximum Caching Time [sec]		
<input type="text" value="3600"/>		
*** DNS - Использовать корневые серверы / Use Rootservers		
ДА <input checked="" type="radio"/> НЕТ <input type="radio"/>		
LoadBalancer - Включить балансировщик / Enable LoadBalancer		
ДА <input type="radio"/> НЕТ <input checked="" type="radio"/>		
LoadBalancer - Время обновления (сек) / Refresh rate [sec]		
<input type="text" value="30"/>		
LoadBalancer - JSON-конфигурация балансировщика нагрузки / Comma separated JSON configs		
<input type="text"/>		

Рис. 79

- задать имя нового VNF;

- в области «Сеть» нажать кнопку [+Сетевой интерфейс] и добавить сетевой интерфейс public(см. рис. 80):

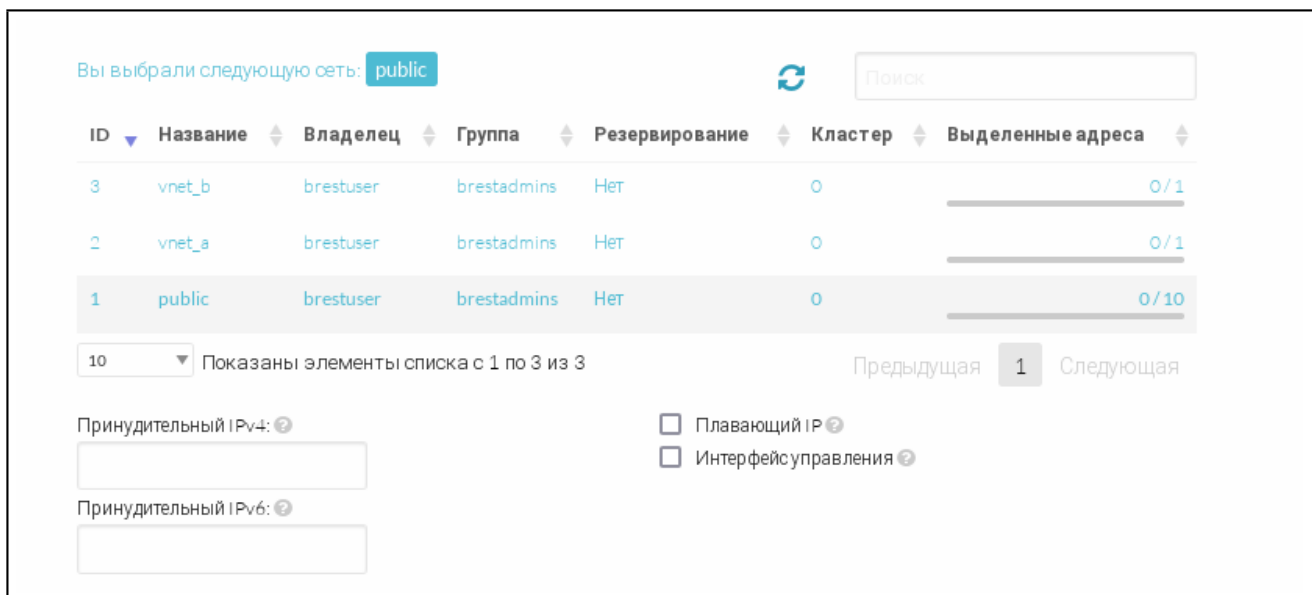


Рис. 80

- нажать кнопку [Создать экземпляр].

3) Дождаться запуска VM.

6.3.3.2. Добавление второго и третьего сетевого интерфейса

1) В веб-интерфейсе ПК СВ перейти в раздел «Экземпляры VM – Вирт. маршрутизаторы» и выбрать созданный виртуальный маршрутизатор.

2) На вкладке Сведения нажать кнопку Добавить сетевой интерфейс (см. рис. 81):

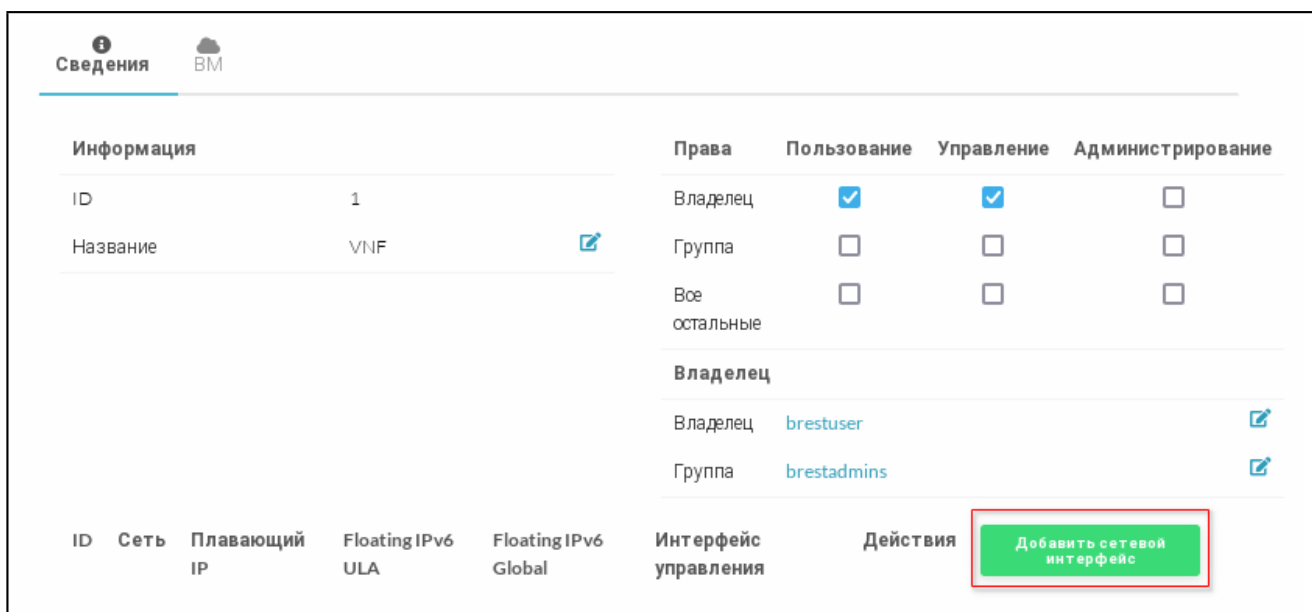


Рис. 81

3) В открывшемся окне выбрать сетевой интерфейс vnet_a, заполнить поле «Принудительный IPv4» (192.168.101.111) и установить флаг «Плавающий IP» (см. рис. 82):

Принудительный IPv4:

Принудительный IPv6:

Плавающий IP

Интерфейс управления

Рис. 82

4) Нажать кнопку [Присоединить].

5) После завершения повторной контекстуализации ВМ добавить еще один сетевой интерфейс `vnet_b`, заполнить поле «Принудительный IPv4» (192.168.102.111) и установить флаг «Плавающий IP» (см. рис. 83):

Принудительный IPv4:

Принудительный IPv6:

Плавающий IP

Интерфейс управления

Рис. 83

6.3.3.3. Проверка конфигурации

Проверить назначение плавающих IP-адресов (VIPs). Для этого необходимо воспользоваться `/etc/keepalived/ha-check-status.sh`. Например:

```
localhost:~# /etc/keepalived/ha-check-status.sh
KEEPALIVED: RUNNING
VRRP-INSTANCE(ETH0): MASTER
VRRP-INSTANCE(ETH1): MASTER
VRRP-INSTANCE(ETH2): MASTER
SYNC-GROUP(vrouter): MASTER
```

```
localhost:~# ip a | grep -e 192.168.101.111 -e 192.168.102.111
inet 192.168.101.111/32 scope global eth1
inet 192.168.102.111/32 scope global eth2
localhost:~#
```

На приведенном выше примере ВМ маршрутизатора является главной (среди экземпляров виртуального маршрутизатора, которые образуют группу высокой доступности) и имеет два плавающих IP-адреса, настроенных на сетевых интерфейсах. Ниже представлен другой пример:

```
localhost:~# /etc/keepalived/ha-check-status.sh
KEEPALIVED: RUNNING
VRRP-INSTANCE(ETH0): BACKUP
```

```
VRRP-INSTANCE(ETH1): BACKUP
VRRP-INSTANCE(ETH2): BACKUP
SYNC-GROUP(vrouter): BACKUP
```

```
localhost:~# ip a | grep -e 192.168.101.111 -e 192.168.102.111
localhost:~#
```

Этот экземпляр VM работает в режиме ожидания («резервирования») и ожидает, когда главная VM отключится, чтобы взять на себя управление. Как можно увидеть, этой VM не назначены плавающие IP-адреса.

6.3.3.4. Проверка работы виртуального маршрутизатора

Для проверки работы виртуального маршрутизатора необходимо создать две тестовые VM, подключенные к сетевым интерфейсам из разных сетей:

- VM1 на сетевом интерфейсе vnet_a;
- VM2 на сетевом интерфейсе vnet_b.

После создания тестовых VM необходимо войти на них через веб-интерфейс ПК СВ, запустить DHCP-клиенты и проверить, что они получили ожидаемые настройки. Обе тестовых VM должны иметь возможность взаимодействовать друг с другом (это можно проверить выполнив ping-запрос с VM1 на VM2) и должны иметь возможность разрешать DNS и получать доступ к интернет-ресурсам.

6.3.3.5. Подключение интерфейса управления

Подключенный к виртуальному маршрутизатору интерфейс можно настроить как интерфейс управления. Он будет использоваться только для подключения к настроенным виртуальным маршрутизаторам и на нем не будут запускаться службы VNF и маршрутизации.

Для настройки интерфейса управления необходимо:

- 1) Создать виртуальную сеть управления vnet_mgt (ПК СВ и виртуальный маршрутизатор должны быть доступны в этой сети) см. 27:

Таблица 27

Имя виртуальной сети	Подсеть	Диапазон	Шлюз	DNS
vnet_mgt	192.168.103.0/24	192.168.103.100 - 192.168.103.199	192.168.103.111	192.168.103.111

- 2) В веб-интерфейсе ПК СВ перейти в раздел «Экземпляры VM — Вирт. маршрутизаторы» и выбрать виртуальный маршрутизатор, для которого будет настроен интерфейс управления.

- 3) На вкладке «Сведения» нажать кнопку [Добавить сетевой интерфейс].
- 4) В открывшемся окне выбрать сетевой интерфейс vnet_mgt. Установить флаг «Интерфейс управления» и нажать кнопку [Присоединить] (см. рис. 84):

Принудительный IPv4:

Принудительный IPv6:

Плавающий IP Интерфейс управления

Группы безопасности

Пожалуйста выберите не менее одной группы безопасности из списка

ID	Название	Владелец	Группа
0	default	oneadmin	brestdadmins

10 Показаны элементы списка с 1 по 1 из 1

Предыдущая 1 Следующая

Присоединить

Рис. 84

- 5) Все экземпляры виртуального маршрутизатора будут перенастроены и один из них будет (повторно) выбран в качестве главного.

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 28.

Таблица 28

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 28

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 29).

Таблица 29

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 30).

Таблица 30

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 31).

Таблица 31

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.

ВНИМАНИЕ! Если при создании ВМ указать только один сервер виртуализа-

ции для развертывания, в шаблон VM будет добавлена опция `SCHED_REQUIREMENTS` с идентификатором указанного сервера. Планировщик, в таком случае, будет использовать для планирования только указанный сервер (например, при выполнении команды `onevm resched ID_VM`).

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

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.10015-01 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.10015-01 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 войти в ОС СН от имени локального администратора компьютера и 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».

П р и м е ч а н и е. Алгоритм Raft описан в документе РДЦП.10001-02 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. 85).

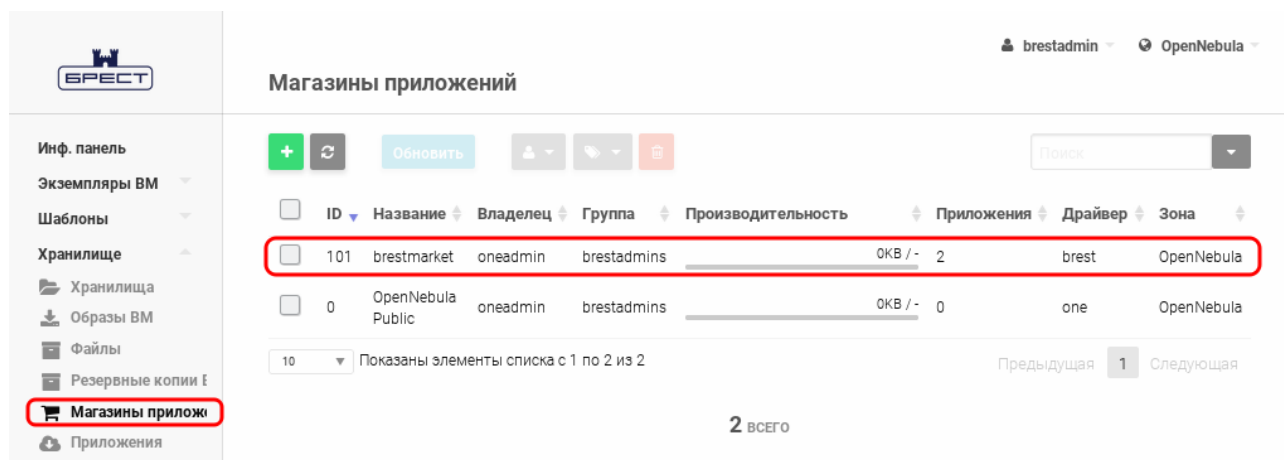


Рис. 85

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 кнопку **[+]**;
- 2) на открывшейся странице «Создать приложение в магазине приложений» (см. рис. 86) выполнить следующие действия:
 - в поле «Название» задать наименование приложения,
 - выбрать образ для создания приложения,
 - выбрать магазин приложений, в который необходимо добавить созданное приложение,
 - нажать кнопку **[Создать]**.

Создать приложение в магазине приложений

[←](#)
[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	brestdadmin	brestdadmins	default	24MB	ОС	ГОТОВО	0

10 Показаны элементы списка с 1 по 1 из 1 Предыдущая 1 Следующая

Выберите магазин приложений для создания приложения

Вы выбрали следующий Магазин приложений: **brestdmarket**

ID	Название	Владелец	Группа	Производительность	Приложения	Драйвер	Зона
101	brestdmarket	oneadmin	brestdadmins	ОКВ / -	0	brestd	OpenNebula
0	OpenNebula Public	oneadmin	brestdadmins	ОКВ / -	0	one	OpenNebula

10 Показаны элементы списка с 1 по 2 из 2 Предыдущая 1 Следующая

Рис. 86

Созданное приложение будет отображено в веб-интерфейсе ПК СВ на странице «Приложения» (см. рис. 87).

Приложения

[+](#)
[↻](#)
[☁](#)
[↓](#)
[⋮](#)
[👤](#)
[🗑](#)

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

10 Показаны элементы списка с 1 по 1 из 1 Предыдущая 1 Следующая

1 ВСЕГО

Рис. 87

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-vtomarket <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-vtomarket 1 101 "test app"
```

Созданное приложение будет отображено в веб-интерфейсе ПК СВ на странице «Приложения» (см. рис. 88).

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

10 Показаны элементы списка с 1 по 1 из 1

1 ВСЕГО

Рис. 88

10. УПРАВЛЕНИЕ СЕРВИСАМИ

10.1. Общие сведения о сервисах в ПК СВ

ПК СВ позволяет управлять сервисом, реализованным в виде многозвенного (multi-tier) приложения. Каждое звено (tier) такого сервиса представляет собой приложение, функционирующее на отдельной ВМ.

Упрощенная схема возможного многозвенного приложения представлена на рис. 89.

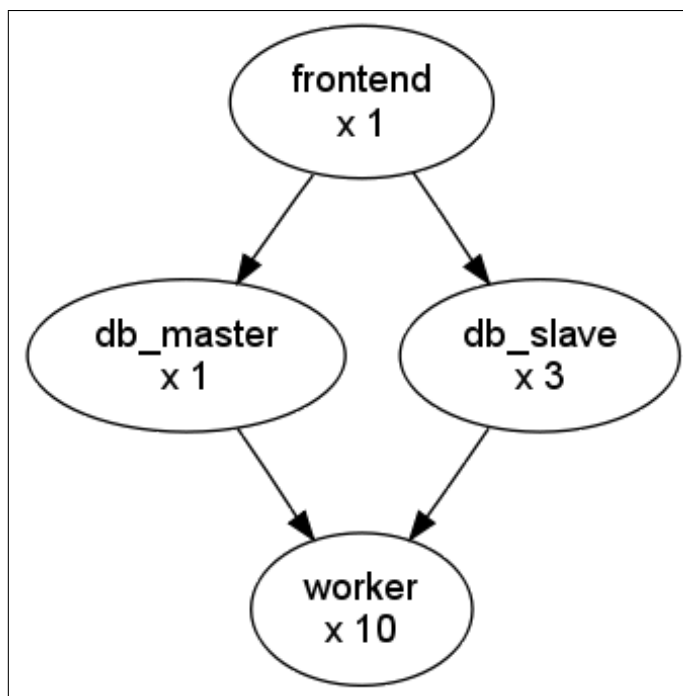


Рис. 89

Сервис, представленный на рис. 89, состоит из следующих компонентов:

- на ВМ с ролью `frontend` функционирует приложение, реализующее интерфейс взаимодействия с пользователем;
- на ВМ с ролью `db_master` функционирует приложение, реализующее мастер-сервер базы данных;
- на ВМ с ролью `db_slave` функционирует приложение, реализующее реплику сервера базы данных;
- на ВМ с ролью `worker` функционирует приложение-обработчик данных.

Обмен служебными данными между виртуальными машинами, логически объединенными в сервис, обеспечивает служба сервера OneGate (см. 10.2).

Автоматическая перенастройка сервиса в соответствии с заданными правилами (политикой эластичности) обеспечивается службой OneFlow (см. 10.3). Под перенастройкой сервиса подразумевается автоматическое изменение количества виртуальных машин с заданной ролью.

Как и в случае с VM, чтобы развернуть сервис предварительно необходимо подготовить шаблон этого сервиса (см. 10.4). Сервис может быть развернут из шаблона столько раз, сколько необходимо. В отношении каждого шаблона сервиса устанавливаются полномочия пользователей на чтение и использование. При необходимости эти полномочия могут быть изменены.

10.2. Служба сервера OneGate

10.2.1. Общие сведения о службе сервера OneGate

Служба сервера OneGate обеспечивает обмен служебной информацией между службой сервера управления и программным обеспечением, функционирующем на виртуальной машине. Это позволяет администраторам и пользователям получать диагностическую информацию, выявлять ошибки функционирования программного обеспечения. Это позволяет обеспечить автоматическую перенастройку сервиса в соответствии с заданными правилами (политикой эластичности) — см. Служба OneFlow.

Служба сервера OneGate обеспечивает соединение с VM по протоколу HTTP. Для каждого экземпляра VM формируется индивидуальный токен. Приложения, функционирующие на VM, используют этот токен для взаимодействия с API службы сервера OneGate.

Примечание. Для обеспечения взаимодействия с API службы сервера OneGate в операционной системе VM необходимо установить пакет `one-context`.

В ПК СВ служба сервера OneGate реализована в виде инструмента командной строки `opennebula-gate`, который устанавливается автоматически при установке и инициализации службы сервера управления.

Также можно развернуть службу сервера OneGate на отдельном сервере, для этого необходимо установить пакет `opennebula-gate`, который размещен в репозитории ПК СВ.

10.2.2. Настройка службы сервера OneGate

Значения параметров службы сервера OneGate представлены в конфигурационном файле `/etc/one/onegate-server.conf`, который имеет формат YAML и по умолчанию размещен на компьютере, функционирующем в качестве сервера управления. Для настройки службы сервера OneGate используются параметры, приведенные в таблице 32.

Таблица 32

Параметр	Описание
Сетевые настройки	
<code>:one_xmlrpc</code>	Адрес для подключения к API службы управления ПК СВ по протоколу XML-RPC (по умолчанию <code>http://localhost:2633/RPC2</code>)

Продолжение таблицы 32

Параметр	Описание
:host	Сетевое имя или IP-адрес, который необходимо прослушивать (ожидать запрос на соединение с VM). По умолчанию используется IP-адрес: 127.0.0.1
:port	Порт, который необходимо прослушивать (ожидать запрос на соединение с VM). По умолчанию используется порт 5030
:ssl_server	Адрес для доступа к службе SSL-прокси (значение устанавливается только при использовании соответствующей службы)
Аутентификация	
:auth	Метод аутентификации, используемый при организации соединения с VM. Всегда имеет значение onegate (аутентификация на основе индивидуального токена VM)
:core_auth	Метод аутентификации, используемый при подключении к службе сервера управления ПК СВ. Может принимать следующие значения: cipher – при аутентификации с симметричным ключом (установлено по умолчанию); x509 – при аутентификации на основе цифровых сертификатов X.509
Настройка подключения к службе OneFlow	
:oneflow_server	Адрес для подключения к службе OneFlow (по умолчанию http://localhost:2474)
Управление доступом	
:permissions	Перечень функций API, вызов которых можно запретить/разрешить. По умолчанию разрешены вызовы всех функций API
:restricted_attrs	Перечень параметров, значения которых запрещено менять при корректировке пользовательского шаблона экземпляра VM. По умолчанию запрещено менять значения следующих параметров: - SCHED_REQUIREMENTS; - SERVICE_ID; - ROLE_NAME
:restricted_actions	Перечень действий с VM, которые запрещено выполнять. По умолчанию разрешены все действия
:vnet_template_attributes	Перечень параметров, значения которых будут использованы при создании виртуальной сети из шаблона. По умолчанию будут использованы значения следующих параметров: - NETWORK_ADDRESS; - NETWORK_MASK; - GATEWAY; - GATEWAY6; - DNS; - GUEST_MTU

Окончание таблицы 32

Параметр	Описание
Протоколирование	
DEBUG_LEVEL	Уровень протоколирования, возможные значения: «0» — регистрировать сообщения об ошибках; «1» — регистрировать предупреждения; «2» — регистрировать информационные сообщения; «3» — регистрировать общие отладочные сообщения (установлено по умолчанию)

По умолчанию служба сервера OneGate настроена на прослушивание локального адреса (localhost). Для обеспечения доступа ВМ к службе сервера OneGate необходимо в качестве значения параметра :host указать адрес сервера, на котором развернута эта служба, и к которому имеется сетевой доступ у ВМ. Кроме того, для параметра :host можно указать значение 0.0.0.0 (для прослушивания всех IP-адресов, присвоенных серверу).

После внесения изменений в конфигурационный файл необходимо перезагрузить службу сервера OneGate командой:

```
sudo systemctl restart opennebula-gate
```

10.2.3. Управление службой сервера OneGate

Чтобы запустить, перезапустить или остановить службу сервера OneGate, необходимо выполнить соответствующую команду:

```
sudo systemctl start opennebula-gate
sudo systemctl restart opennebula-gate
sudo systemctl stop opennebula-gate
```

Чтобы разрешить или запретить автоматический запуск службы сервера OneGate при запуске ОС СН, необходимо выполнить соответствующую команду:

```
sudo systemctl enable opennebula-gate
sudo systemctl disable opennebula-gate
```

Информация о работе службы сервера OneGate регистрируется в следующих файлах:

- /var/log/one/onegate.log;
- /var/log/one/onegate.error.

Кроме того, информация о работе службы сервера OneGate регистрируется в системном журнале. Для просмотра этой информации необходимо выполнить команду:

```
sudo journalctl -u opennebula-gate.service
```

10.2.4. Настройка ПК СВ для использования службы сервера OneGate

При настройке доступа ВМ к службе сервера OneGate используется параметр ONEGATE_ENDPOINT, значение которого содержит сетевое имя (IP-адрес) и порт для доступа

к службе сервера OneGate. Для настройки доступа к службе сервера OneGate необходимо на компьютере, функционирующем в качестве сервера управления, в конфигурационном файле `/etc/one/one.d/base.conf` раскомментировать и изменить значение параметра `ONEGATE_ENDPOINT`.

Пример

```
ONEGATE_ENDPOINT = "http://192.168.0.5:5030"
```

После внесения изменений необходимо перезапустить службу управления ПК СВ:

```
sudo systemctl restart opennebula
```

10.2.5. Настройка шаблона VM для использования службы сервера OneGate

10.2.5.1. Настройка шаблона VM в интерфейсе командной строки

В шаблоне VM в блоке параметров `CONTEXT` для параметра `TOKEN` необходимо установить значение `YES`.

Пример

```
CPU = "0.5"  
MEMORY = "1024"  
DISK = [  
    IMAGE_ID = "0" ]  
NIC = [  
    NETWORK_ID = "0" ]  
CONTEXT = [  
    TOKEN = "YES" ]
```

Для изменения параметров шаблона необходимо использовать команду:

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

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

10.2.5.2. Настройка шаблона VM в веб-интерфейсе ПК СВ

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

- 1) в меню слева выбрать пункт меню «Шаблоны — VM» и на открывшейся странице «Шаблоны VM» выбрать необходимый шаблон;
- 2) на открывшейся странице «Шаблон VM» нажать кнопку **[Обновить]**;
- 3) на открывшейся странице «Изменить шаблон VM» во вкладке «Контекст» (см. рис. 90):
 - а) в секции «Конфигурация» установить флаг «Добавить токен OneGate»;

б) нажать кнопку **[Обновить]**.

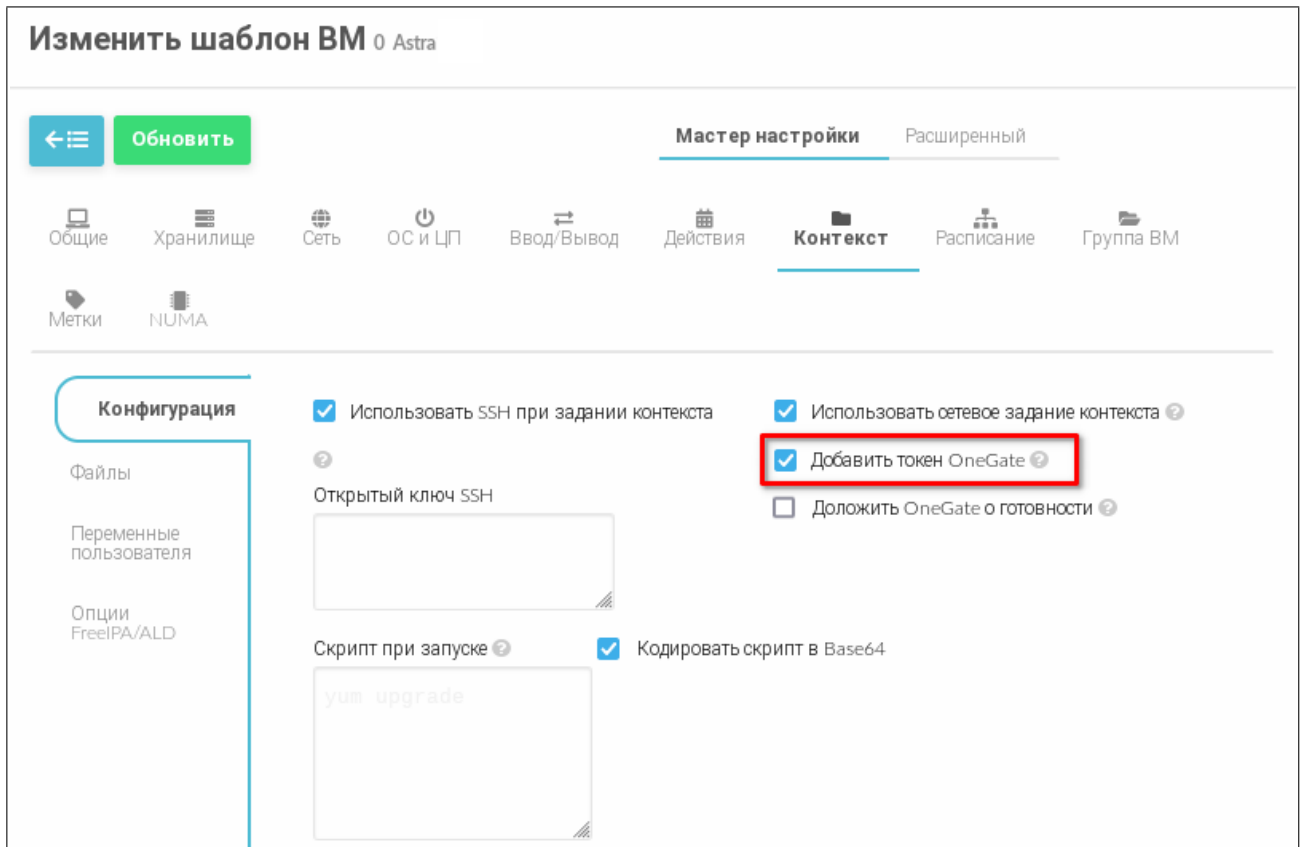


Рис. 90

10.2.6. Настройка ВМ для доступа к службе сервера OneGate

Для обеспечения взаимодействия с API службы сервера OneGate в операционной системе ВМ необходимо установить пакет `one-context`.

При развертывании экземпляра ВМ в секции CONTEXT шаблона этой ВМ будет автоматически добавлен параметр `ONEGATE_ENDPOINT`.

Кроме того, на виртуальном CD-ROM с наименованием CONTEXT, подключенном к этой ВМ, будет автоматически размещен файл `token.txt`, содержащий токен. Файл `token.txt` доступен только в ОС виртуальной машины.

Дополнительных настроек не требуется.

10.2.7. Использование клиента OneGate в ОС виртуальной машины

10.2.7.1. Особенности использования клиента OneGate

Клиент OneGate реализован в виде инструмента командной строки `onegate`, который автоматически устанавливается при установке пакета `one-context`.

Для того чтобы получить подробное описание использования инструмента командной строки `onegate`, необходимо выполнить команду:

```
onegate -h
```


10.2.7.2. Получение служебной информации о ВМ

Чтобы получить служебную информацию о ВМ, в ОС этой ВМ необходимо выполнить команду:

```
onagate vm show
```

Пример вывода после выполнения команды:

```
VM 8
NAME      : master_0_(service_1)
STATE     : RUNNING
IP        : 192.168.122.23
```

Чтобы получить служебную информацию о другой ВМ, необходимо в качестве дополнительного аргумента команды указать идентификатор ВМ.

Доступна служебная информация только тех ВМ, которые логически объединены в один сервис или подключены к одному виртуальному маршрутизатору.

10.2.7.3. Получение служебной информации сервиса

Чтобы получить служебную информацию сервиса, в состав которого входит ВМ, в ОС этой ВМ необходимо выполнить команду:

```
onagate service show
```

Пример вывода после выполнения команды:

```
SERVICE 1
NAME      : PANACEA service
STATE     : RUNNING

ROLE master
VM 8
NAME      : master_0_(service_1)
```

```
ROLE slave
```

```
VM 9
NAME      : slave_0_(service_1)
```

Чтобы получить служебную информацию о всех ВМ, логически объединенных в сервис, необходимо в качестве дополнительного аргумента команды указать `--extended`:

```
onagate service show --extended
```

Пример вывода после выполнения команды:

```
SERVICE 1
NAME      : PANACEA service
STATE     : RUNNING
```

```
ROLE master
```

```
VM 8
NAME      : master_0_(service_1)
STATE     : RUNNING
IP        : 192.168.122.23
```

```
ROLE slave
```

```
VM 9
NAME      : slave_0_(service_1)
STATE     : RUNNING
```

10.2.7.4. Получение служебной информации о виртуальном маршрутизаторе

Чтобы получить служебную информацию о виртуальном маршрутизаторе, к которому подключена ВМ, в ОС этой ВМ необходимо выполнить команду:

```
onagate vrouter show
```

Пример вывода после выполнения команды:

```
VROUTER 0
NAME      : vr
VMS       : 1
```

10.2.7.5. Получение служебной информации о виртуальной сети

Чтобы получить служебную информацию о виртуальной сети в ОС ВМ необходимо выполнить команду:

```
onagate vnet show <идентификатор_сети>
```

Доступна служебная информация только о виртуальных сетях, подключенных к тому виртуальному маршрутизатору, к которому имеется доступ ВМ.

Пример

Получение служебной информации о виртуальной сети с идентификатором 0:

```
onagate vnet show 0
```

Пример вывода после выполнения команды:

```
VNET
ID : 0
```

10.2.7.6. Изменение пользовательского шаблона экземпляра ВМ

С помощью клиента OneGate можно изменить значения параметров, размещенных в пользовательском шаблоне любой ВМ сервиса.

Пример

1) изменить значение параметра ACTIVE для ВМ с идентификатором 9:

```
onagate vm update 9 --data ACTIVE=YES
```

2) просмотреть служебную информацию о ВМ. Для этого можно воспользоваться командой:

```
onagate vm show 9 --json
```

Пример вывода после выполнения команды:

```
{
  "VM": {
    "NAME": "slave_0_(service_1)",
    "ID": "9",
    "STATE": "3",
    "LCM_STATE": "3",
    "USER_TEMPLATE": {
      "ACTIVE": "YES",
      "FROM_APP": "4fc76a938fb81d3517000003",
      "FROM_APP_NAME": "ttylinux - kvm",
      "LOGO": "images/logos/linux.png",
      "ROLE_NAME": "slave",
      "SERVICE_ID": "1"
    },
    "TEMPLATE": {
      "NIC": [ ]
    }
  }
}
```

10.2.7.7. Удаление параметра из пользовательского шаблона экземпляра ВМ

С помощью клиента OneGate можно удалить параметр, размещенный в пользовательском шаблоне любой ВМ сервиса.

Пример

1) удалить параметр ACTIVE для ВМ с идентификатором 9:

```
onagate vm update 9 --erase ACTIVE
```

2) просмотреть служебную информацию о ВМ. Для этого можно воспользоваться командой:

```
onagate vm show 9 --json
```

Пример вывода после выполнения команды:

```
{
  "VM": {
    "NAME": "slave_0_(service_1)",
    "ID": "9",
    "STATE": "3",
    "LCM_STATE": "3",
    "USER_TEMPLATE": {
      "FROM_APP": "4fc76a938fb81d3517000003",
      "FROM_APP_NAME": "ttylinux - kvm",
      "LOGO": "images/logos/linux.png",
```

```

        "ROLE_NAME": "slave",
        "SERVICE_ID": "1"
    },
    "TEMPLATE": {
        "NIC": [ ]
    }
}
}

```

10.2.7.8. Управление состоянием ВМ

С помощью клиента OneGate можно управлять состоянием ВМ, тем самым изменять конфигурацию сервиса. Для управления состоянием ВМ доступны следующие команды:

```

onagate vm resume
onagate vm stop
onagate vm suspend
onagate vm terminate
onagate vm reboot
onagate vm poweroff
onagate vm resched
onagate vm unresched
onagate vm hold
onagate vm release

```

10.2.7.9. Управление количеством ВМ в составе сервиса

С помощью клиента OneGate можно управлять количеством ВМ в составе сервиса.

Пример

1) увеличить количество ВМ с ролью «ведомый» (slave) до 2:

```
onagate service scale --role slave --cardinality 2
```

2) просмотреть служебную информацию сервиса. Для этого можно воспользоваться командой:

```
onagate service show --extended
```

Пример вывода после выполнения команды:

```

SERVICE 1
NAME      : PANACEA service
STATE     : RUNNING

ROLE master

VM 8
NAME      : master_0_(service_1)
STATE     : RUNNING

```

```
IP      : 192.168.122.23
```

```
ROLE slave
```

```
VM 9
```

```
NAME    : slave_0_(service_1)
```

```
STATE   : RUNNING
```

```
NAME    : slave_1_(service_1)
```

```
STATE   : PENDING
```

10.2.8. Взаимодействие с API службы сервера OneGate в ОС виртуальной машины

10.2.8.1. Параметры доступа к API службы сервера OneGate

Взаимодействие со службой сервера OneGate осуществляется посредством REST API. При этом заголовок запроса должен содержать следующие данные:

- X-ONEGATE-TOKEN — токен, присвоенный VM;
- X-ONEGATE-VMID — идентификатор VM.

В ОС CH значения указанных выше параметров можно получить из переменной окружения `/var/run/one-context/one_env`. Для этого можно воспользоваться командой:

```
sudo cat /var/run/one-context/one_env
```

Пример вывода после выполнения команды:

```
export TOKENTXT="N7HAQYUss4/LHPWvPHLe2A=="
export VMID="9"
export ONEGATE_ENDPOINT="http://192.168.0.1:5030"
export CONTEXT="true"
...
```

10.2.8.2. Получение служебной информации о VM

Чтобы получить служебную информацию о VM, необходимо войти в ОС этой VM и отправить запрос вида:

```
GET <ONEGATE_ENDPOINT>/vm
```

где `<ONEGATE_ENDPOINT>` — адрес доступа к службе сервера OneGate.

Пример

Получение служебной информации о VM:

```
curl -X "GET" "192.168.0.1:5030/vm" \
      --header "X-ONEGATE-TOKEN: N7HAQYUss4/LHPWvPHLe2A==" \
      --header "X-ONEGATE-VMID: 9"
```

Пример ответа сервера после выполнения запроса:

```
{
```

```

"VM": {
  "NAME": "slave_0_(service_1)",
  "ID": "9",
  "STATE": "3",
  "LCM_STATE": "3",
  "TEMPLATE": {
    "NIC": [
      {
        "IP": "192.168.122.33",
        "MAC": "02:00:ac:10:01:64",
        "NAME": "NIC0",
        "NETWORK": "virtnetwork"
      }
    ],
    "NIC_ALIAS": []
  },
  "USER_TEMPLATE": {
    "AUTOSTARTVM": "0",
    "HOT_RESIZE": {
      "CPU_HOT_ADD_ENABLED": "NO",
      "MEMORY_HOT_ADD_ENABLED": "NO"
    },
    "HYPERVISOR": "kvm",
    "INPUTS_ORDER": "",
    "MEMORY_UNIT_COST": "MB",
    "READY": "YES",
    "SERVICEUSERVM": "1"
  }
}
}

```

Чтобы получить служебную информацию о другой VM, необходимо отправить запрос вида:

```
GET <ONEGATE_ENDPOINT>/vms/<идентификатор_VM>
```

где <ONEGATE_ENDPOINT> — адрес доступа к службе сервера OneGate.

Доступна служебная информация только тех VM, которые логически объединены в один сервис или подключены к одному виртуальному маршрутизатору.

10.2.8.3. Получение служебной информации сервиса

Чтобы получить служебную информацию сервиса, в состав которого входит VM, необходимо войти в ОС этой VM и отправить запрос вида:

```
GET <ONEGATE_ENDPOINT>/service
```

где <ONEGATE_ENDPOINT> — адрес доступа к службе сервера OneGate.

Пример

Получение служебной информации о сервисе, в состав которого входит ВМ:

```
curl -X "GET" "192.168.0.1:5030/service" \
--header "X-ONEGATE-TOKEN: N7HAQYUss4/LHPWvPHLe2A==" \
--header "X-ONEGATE-VMID: 9"
```

Пример ответа сервера после выполнения запроса:

```
{
  "SERVICE": {
    "id": ...,
    "name": ...,
    "roles": [
      {
        "name": ...,
        "cardinality": ...,
        "state": ...,
        "nodes": [
          {
            "deploy_id": ...,
            "running": true|false,
            "vm_info": {
              // служебная информация о ВМ
            }
          },
          // информация о других узлах ...
        ]
      },
      // описание других ролей ...
    ]
  }
}
```

10.2.8.4. Получение служебной информации о виртуальном маршрутизаторе

Чтобы получить служебную информацию о виртуальном маршрутизаторе, к которому подключена ВМ, необходимо войти в ОС этой ВМ и отправить запрос вида:

```
GET <ONEGATE_ENDPOINT>/vrouters
```

где <ONEGATE_ENDPOINT> — адрес доступа к службе сервера OneGate.

Пример

Получение служебной информации о виртуальном маршрутизаторе, к которому подключена ВМ:

```
curl -X "GET" "192.168.0.1:5030/vrouters" \
```

```
--header "X-ONEGATE-TOKEN: N7HAQYUss4/LHPWvPHLe2A==" \
--header "X-ONEGATE-VMID: 9"
```

Пример ответа сервера после выполнения запроса:

```
{
  "VROUTER": {
    "NAME": "vr",
    "ID": "0",
    "VMS": {
      "ID": [
        "1"
      ]
    },
    "TEMPLATE": {
      "NIC": [
        {
          "NETWORK": "vnet",
          "NETWORK_ID": "0",
          "NIC_ID": "0"
        }
      ],
      "TEMPLATE_ID": "0"
    }
  }
}
```

10.2.8.5. Получение служебной информации о виртуальной сети

Чтобы получить служебную информацию о виртуальной сети, необходимо войти в ОС этой VM и отправить запрос вида:

```
GET <ONEGATE_ENDPOINT>/vnet/<идентификатор_сети>
```

где <ONEGATE_ENDPOINT> — адрес доступа к службе сервера OneGate.

Доступна служебная информация только о виртуальных сетях, подключенных к тому виртуальному маршрутизатору, к которому имеется доступ VM.

Пример

Получение служебной информации о виртуальной сети с идентификатором 0:

```
curl -X "GET" "192.168.0.1:5030/vnet/0" \
--header "X-ONEGATE-TOKEN: N7HAQYUss4/LHPWvPHLe2A==" \
--header "X-ONEGATE-VMID: 9"
```

Пример ответа сервера после выполнения запроса:

```
{
  "VNET": {
    "ID": "0",
```



```
"NAME": "vnet",
"USED_LEASES": "1",
"VROUTERS": {
  "ID": [
    "0"
  ]
},
"PARENT_NETWORK_ID": {
},
"AR_POOL": {
  "AR": [
    {
      "AR_ID": "0",
      "IP": "192.168.122.100",
      "MAC": "02:00:c0:a8:7a:64",
      "SIZE": "10",
      "TYPE": "IP4",
      "MAC_END": "02:00:c0:a8:7a:6d",
      "IP_END": "192.168.122.109",
      "USED_LEASES": "1",
      "LEASES": {
        "LEASE": [
          {
            "IP": "192.168.122.100",
            "MAC": "02:00:c0:a8:7a:64",
            "VM": "1"
          }
        ]
      }
    }
  ]
},
"TEMPLATE": {
  "NETWORK_ADDRESS": "192.168.122.0",
  "NETWORK_MASK": "255.255.255.0",
  "GATEWAY": "192.168.122.1",
  "DNS": "1.1.1.1"
}
}
```

10.2.8.6. Изменение пользовательского шаблона экземпляра ВМ

Для изменения значения параметра, а также добавления параметра в пользовательский шаблон ВМ необходимо войти в ОС этой ВМ и отправить запрос вида:

```
PUT <ONEGATE_ENDPOINT>/vm
```

где <ONEGATE_ENDPOINT> — адрес доступа к службе сервера OneGate.

Пример

Добавление параметра APP_LOAD который имеет значение «9.7»:

```
curl -X "PUT" "192.168.0.1:5030/vm" \
--header "X-ONEGATE-TOKEN: N7HAQYUss4/LHPWvPHLe2A==" \
--header "X-ONEGATE-VMID: 9"
-d "APP_LOAD=9.7"
```

Для просмотра внесенных изменений можно на сервере управления выполнить команду:

```
onevm show 9
```

Пример вывода после выполнения команды:

```
...
USER TEMPLATE
APP_LOAD="9.7"
AUTOSTARTVM="0"
HOT_RESIZE=[
CPU_HOT_ADD_ENABLED="NO",
MEMORY_HOT_ADD_ENABLED="NO" ]
HYPERVISOR="kvm"
INPUTS_ORDER=""
MEMORY_UNIT_COST="MB"
READY="YES"
...
```

Чтобы добавить параметр в пользовательский шаблон другой ВМ или изменить значение этого параметра, необходимо отправить запрос вида:

```
PUT <ONEGATE_ENDPOINT>/vms/<идентификатор_ВМ>
```

где <ONEGATE_ENDPOINT> — адрес доступа к службе сервера OneGate.

Доступно изменение пользовательского шаблона только тех ВМ, которые логически объединены в один сервис.

10.2.8.7. Удаление параметра из пользовательского шаблона экземпляра ВМ

Чтобы удалить параметр из пользовательского шаблона ВМ, необходимо войти в ОС этой ВМ и отправить запрос вида:

```
PUT <ONEGATE_ENDPOINT>/vm?type=2
```

где <ONEGATE_ENDPOINT> — адрес доступа к службе сервера OneGate.

Пример

Удаление параметра APP_LOAD:

```
curl -X "PUT" "192.168.0.1:5030/vm?type=2" \
--header "X-ONEGATE-TOKEN: N7HAQYUss4/LHPWvPHLe2A==" \
--header "X-ONEGATE-VMID: 9"
-d "APP_LOAD"
```

Для просмотра внесенных изменений можно на сервере управления выполнить команду:

```
onevm show 9
```

Пример вывода после выполнения команды:

```
...
USER TEMPLATE
AUTOSTARTVM="0"
HOT_RESIZE=[
CPU_HOT_ADD_ENABLED="NO",
MEMORY_HOT_ADD_ENABLED="NO" ]
HYPERVISOR="kvm"
INPUTS_ORDER=""
MEMORY_UNIT_COST="MB"
READY="YES"
...
```

Чтобы удалить параметр из пользовательского шаблона другой ВМ, необходимо отправить запрос вида:

```
PUT <ONEGATE_ENDPOINT>/vms/<идентификатор_ВМ>?type=2
```

где <ONEGATE_ENDPOINT> — адрес доступа к службе сервера OneGate.

Доступно изменение пользовательского шаблона только тех ВМ, которые логически объединены в один сервис.

10.2.8.8. Управление состоянием ВМ

Для управления состоянием ВМ используется запрос вида:

```
POST <ONEGATE_ENDPOINT>/vms/<идентификатор_ВМ>/action
```

где <ONEGATE_ENDPOINT> — адрес доступа к службе сервера OneGate.

Пример

Установить состояние «готова для размещения» для ВМ с идентификатором 18:

```
curl -X "POST" "192.168.0.1:5030/vms/18/action" \
--header "X-ONEGATE-TOKEN: N7HAQYUss4/LHPWvPHLe2A==" \
--header "X-ONEGATE-VMID: 9"
-d "{\"action\" : {\"perform\" : \"resched\"}}"
```

10.2.8.9. Управление количеством ВМ в составе сервиса

Чтобы изменить количество ВМ в составе сервиса, необходимо отправить запрос вида:

```
POST <ONEGATE_ENDPOINT>/service/<идентификатор_сервиса>/scale
```

где <ONEGATE_ENDPOINT> — адрес доступа к службе сервера OneGate.

Пример

Увеличение количества ВМ с ролью «обработчик» (worker) до 10:

```
curl -X "POST" "192.168.0.1:5030/service/0/scale" \
--header "X-ONEGATE-TOKEN: N7HAQYUss4/LHPWvPHLe2A==" \
--header "X-ONEGATE-VMID: 9"
-d '{"role_name': 'worker', 'cardinality' : 10, 'force': false}"
```

10.3. Служба OneFlow

10.3.1. Общие сведения о службе OneFlow

Служба OneFlow осуществляет управление сервисом, реализованным в виде многозвенного (multi-tier) приложения. Каждое звено (tier) представляет собой приложение, функционирующее на отдельной ВМ.

Кроме того, службой OneFlow обеспечивается автоматическая перенастройка сервиса в соответствии с заданными правилами (политикой эластичности). Под перенастройкой сервиса подразумевается автоматическое изменение состояния виртуальных машин, логически объединенных в сервис (остановка, запуск, перезапуск и т.д.), а также автоматическое изменение количества виртуальных машин с заданной ролью.

В ПК СВ служба OneFlow реализована в виде инструмента командной строки `opennebula-flow`, который устанавливается автоматически при установке и инициализации службы сервера управления. Также можно развернуть службу OneFlow на отдельном сервере, для этого необходимо установить пакет `opennebula-flow`, который размещен в репозитории ПК СВ.

10.3.2. Настройка службы OneFlow

Значения параметров службы OneFlow представлены в конфигурационном файле `/etc/one/oneflow-server.conf`, который имеет формат YAML и по умолчанию размещен на компьютере, функционирующем в качестве сервера управления. Для настройки службы OneFlow используются параметры, приведенные в таблице 33.

Таблица 33

Параметр	Описание
Сетевые настройки	

Продолжение таблицы 33

Параметр	Описание
:one_xmlrpc	Адрес для подключения к API службы управления ПК СВ по протоколу XML-RPC (по умолчанию http://localhost:2633/RPC2)
:subscriber_endpoint	Адрес для подключения к службе хуков (по умолчанию tcp://localhost:2101)
:autoscaler_interval	Интервал времени (в секундах) между проверками значений параметров, указанных в политике эластичности (по умолчанию 90 секунд)
:host	Сетевое имя или IP-адрес, который необходимо прослушивать (ожидать запрос на соединение). По умолчанию используется IP-адрес: 127.0.0.1
:port	Порт, который необходимо прослушивать (ожидать запрос на соединение). По умолчанию используется порт 2474
:force_deletion	Флаг, который устанавливает режим принудительного удаления VM. По умолчанию снят, т.е. режим принудительного удаления VM выключен
Настройка функционирования службы OneFlow	
:default_cooldown	Длительность паузы (в секундах) после выполнения автоматического масштабирования сервиса (по умолчанию 300 секунд). Во время паузы службой OneFlow не выполняются никаких действий
:wait_timeout	Длительность ожидания (в секундах) отчета об изменении состояния VM (по умолчанию 10 секунд)
:concurrency	Количество потоков, выделенных для работы службы OneFlow (по умолчанию 10)
:shutdown_action	Режим выключения VM перед удалением. Может принимать следующие значения: terminate – корректное завершение работы и удаление VM (установлено по умолчанию); terminate-hard – принудительное завершение работы и удаление VM
:action_number	Количество VM с заданной ролью, которым будет одновременно направлена команда на изменение состояния (по умолчанию 1)
:action_period	Интервал времени (в секундах) через который будет повторно направлена команда на изменение состояния VM с заданной ролью (по умолчанию 60 секунд). Команда повторяется до тех пор, пока все VM с заданной ролью, не получат эту команду. Количество VM, которым будет одновременно направлена команда на изменение состояния определяется параметром :action_number

Окончание таблицы 33

Параметр	Описание
:vm_name_template	Шаблон имени VM, создаваемой службой OneFlow. При формировании шаблона допускается использовать следующие переменные: - \$SERVICE_ID (идентификатор сервиса); - \$SERVICE_NAME (наименование сервиса); - \$ROLE_NAME (наименование роли); - \$VM_NUMBER (номер VM). По умолчанию установлен следующий шаблон имени VM: \$ROLE_NAME_\$VM_NUMBER_(service_\$SERVICE_ID)
:page_size	Размер страницы данных при очистке сервиса, имеющего статус DONE (по умолчанию 10)
Аутентификация	
:core_auth	Метод аутентификации, используемый при подключении к службе сервера управления ПК СВ. Может принимать следующие значения: cipher — при аутентификации с симметричным ключом (установлено по умолчанию); x509 — при аутентификации на основе цифровых сертификатов X.509
Протоколирование	
DEBUG_LEVEL	Уровень протоколирования, возможные значения: «0» — регистрировать сообщения об ошибках; «1» — регистрировать предупреждения; «2» — регистрировать информационные сообщения (установлено по умолчанию); «3» — регистрировать общие отладочные сообщения

По умолчанию служба OneFlow настроена на прослушивание локального адреса (localhost). Если служба OneFlow развернута на сервере управления и удаленное подключение к этой службе не планируется, то дополнительных настроек не требуется.

Если планируется удаленное подключение к службе OneFlow, то необходимо в качестве значения параметра :host указать адрес сервера, на котором развернута эта служба, и к которому имеется сетевой доступ. Кроме того, для параметра :host можно указать значение 0.0.0.0 (для прослушивания всех IP-адресов, присвоенных серверу).

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

```
sudo systemctl restart opennebula-flow
```

10.3.3. Управление службой OneFlow

Чтобы запустить, перезапустить или остановить службу OneFlow, необходимо выполнить соответствующую команду:

```
sudo systemctl start opennebula-flow
```

```
sudo systemctl restart opennebula-flow
```

```
sudo systemctl stop opennebula-flow
```

Чтобы разрешить или запретить автоматический запуск службы OneFlow при запуске ОС СН, необходимо выполнить соответствующую команду:

```
sudo systemctl enable opennebula-flow
```

```
sudo systemctl disable opennebula-flow
```

Информация о работе службы OneFlow регистрируется в следующих файлах:

- /var/log/one/oneflow.log;
- /var/log/one/oneflow.error.

Кроме того, информация о работе службы OneFlow регистрируется в системном журнале. Для просмотра этой информации необходимо выполнить команду:

```
sudo journalctl -u opennebula-flow.service
```

Информация о работе определенного сервиса, управляемого службой OneFlow, регистрируется в файле с наименованием /var/log/one/oneflow/<идентификатор_сервиса>.

10.3.4. Настройка ПК СВ для использования службы OneFlow

Для взаимодействия пользователя со службой OneFlow используются веб-интерфейс ПК СВ, а также инструменты командной строки oneflow и oneflow-template.

Примечание. Если служба OneFlow развернута на сервере управления и удаленное подключение к этой службе не планируется, то дополнительных настроек не требуется.

10.3.4.1. Настройка веб-интерфейса ПК СВ

При настройке веб-интерфейса ПК СВ для доступа к службе OneFlow используется параметр :oneflow_server, значение которого содержит сетевое имя (IP-адрес) и порт для доступа к службе OneFlow. Изменение значения параметра :oneflow_server производится в конфигурационном файле /etc/one/sunstone-server.conf.

Пример

```
:oneflow_server: http://192.168.0.5:2474/
```

После внесения изменений необходимо перезапустить службу веб-интерфейса ПК СВ:

```
sudo systemctl restart opennebula-sunstone
```

10.3.4.2. Настройка инструментов командной строки

Дополнительная настройка не требуется. Однако, если планируется удаленное подключение к службе OneFlow, то при вызове инструмента командной строки необходимо предварительно указывать адрес доступа к службе (ONEFLOW_URL).

Пример

```
ONEFLOW_URL=http://192.168.0.5:2474 oneflow list
```

10.4. Управление шаблонами сервиса

10.4.1. Параметры сервиса, задаваемые в шаблоне

Для установки значений параметров шаблона сервиса используется формат JSON.

10.4.1.1. Общие параметры сервиса

В общем случае для формирования шаблона сервиса необходимо определить значения параметров, приведенных в таблице 34.

Таблица 34

Параметр	Тип данных	Обязательный	Описание
custom_attrs	объект	Нет	Пользовательские параметры (неупорядоченный набор пар «параметр: значение»)
deployment	строка	Нет	Стратегия развертывания. Возможные значения: - none — все группы VM с заданной ролью разворачиваются одновременно (установлено по умолчанию); - straight — группа VM с заданной ролью разворачиваются только после запуска VM из вышестоящей группы с заданной ролью
name	строка	Нет	Наименование сервиса
networks	объект	Нет	Параметры виртуальной сети (неупорядоченный набор пар «параметр: значение»)
ready_status_gate	логический	Нет	Ожидать полного запуска VM (см. примечание ниже)
roles	массив ролей	Да	Упорядоченная последовательность значений параметров группы VM с заданной ролью (см. таблицу 35)
shutdown_action	строка	Нет	Режим выключения VM перед удалением. Может принимать следующие значения: terminate — корректное завершение работы и удаление VM (установлено по умолчанию); terminate-hard — принудительное завершение работы и удаление VM. Если значение параметра не установлено, используется значение, установленное в конфигурационном файле /etc/one/oneflow-server.conf службы OneFlow (см. 10.3)

Примечание. VM находится в состоянии полного запуска VM, если одновременно выполняются следующие условия:

- служба сервера правления ПК СВ для экземпляра VM установила следующие значения параметров:
 - STATE>=3;
 - LCM_STATE==3;

- в пользовательском шаблоне экземпляра ВМ установлено следующее значение параметра `READY=YES`.

Для изменения значений параметров в пользовательском шаблоне экземпляра ВМ используется служба сервера OneGate (см. 10.2).

10.4.1.2. Параметры группы ВМ с заданной ролью

Для группы ВМ с заданной ролью необходимо определить значения параметров, приведенных в таблице 35.

Таблица 35

Параметр	Тип данных	Обязательный	Описание
<code>name</code>	строка	Да	Наименование группы ВМ с заданной ролью
<code>cardinality</code>	число	Нет	Количество ВМ в группе (по умолчанию — одна)
<code>vm_template</code>	число	Да	Идентификатор шаблона для развертывания ВМ с заданной ролью
<code>shutdown_action</code>	строка	Нет	Режим выключения ВМ перед удалением. Может принимать следующие значения: <code>terminate</code> — корректное завершение работы и удаление ВМ (установлено по умолчанию); <code>terminate-hard</code> — принудительное завершение работы и удаление ВМ. Если значение параметра не установлено, используется значение, установленное в общих параметрах сервиса
<code>min_vms</code>	число	Нет (Да, если установлена политика эластичности)	Минимальное количество ВМ в группе. Параметр используется при автоматическом масштабировании сервиса в соответствии с заданными правилами (политикой эластичности)
<code>max_vms</code>	число	Нет (Да, если установлена политика эластичности)	Максимальное количество ВМ в группе. Параметр используется при автоматическом масштабировании сервиса в соответствии с заданными правилами (политикой эластичности)
<code>cooldown</code>	число	Нет	Длительность паузы (в секундах) после выполнения автоматического масштабирования сервиса. Если значение параметра не установлено, используется значение, установленное в конфигурационном файле <code>/etc/one/oneflow-server.conf</code> службы OneFlow (см. 10.3)

Окончание таблицы 35

Параметр	Тип данных	Обязательный	Описание
elasticity_policies	массив политик	Нет	Упорядоченная последовательность значений параметров политики эластичности (см. таблицу 36)
scheduled_policies	массив политик	Нет	Упорядоченная последовательность значений параметров политики планирования (см. таблицу 37)

10.4.1.3. Параметры политики эластичности

Для автоматической перенастройки сервиса в соответствии с заданными правилами (политикой эластичности) необходимо определить значения параметров, приведенных в таблице 36.

Таблица 36

Параметр	Тип данных	Обязательный	Описание
type	строка	Да	Тип автоматического масштабирования. Может принимать следующие значения: - CHANGE — добавление/удаление заданного количества развернутых ВМ; - CARDINALITY — установка заданного размера группы (количества развернутых ВМ); - PERCENTAGE_CHANGE — добавление/удаление количества развернутых ВМ, заданного в процентном соотношении от текущего размера группы
adjust	число	Да	Шаг положительной/отрицательной корректировки или размер группы ВМ (в зависимости от типа автоматического масштабирования). В случае необходимости уменьшить количество развернутых ВМ, перед числом следует указать знак «-»
min_adjust_step	число	Нет	Необязательный параметр для автоматической настройки PERCENTAGE_CHANGE. Минимальный шаг положительной/отрицательной корректировки — наименьшее количество ВМ, на которое будет изменен размер группы
expression	строка	Да	Условие (логическое выражение) при котором необходимо применить политику эластичности
period_number	число	Нет	Количество периодов времени, на протяжении которых выполняется условие, указанное в параметре expression. Только по прошествии этого времени будет применена политика эластичности
period	число	Нет	Длительность периода (в секундах) — используется совместно с параметром period_number

Окончание таблицы 36

Параметр	Тип данных	Обязательный	Описание
cooldown	число	Нет	Длительность паузы (в секундах) после выполнения автоматического масштабирования сервиса. Если значение параметра не установлено, используется значение, установленное в параметров группы VM с заданной ролью (см. таблицу 35)

10.4.1.4. Параметры политики планирования

Для автоматического масштабирования сервиса в соответствии с расписанием (политикой планирования) необходимо определить значения параметров, приведенных в таблице 37.

Таблица 37

Параметр	Тип данных	Обязательный	Описание
type	строка	Да	Тип автоматического масштабирования. Может принимать следующие значения: - CHANGE — добавление/удаление заданного количества развернутых VM; - CARDINALITY — установка заданного размера группы (количества развернутых VM); - PERCENTAGE_CHANGE — добавление/удаление количества развернутых VM, заданного в процентном соотношении от текущего размера группы
adjust	число	Да	Шаг положительной/отрицательной корректировки или размер группы VM (в зависимости от типа автоматического масштабирования). В случае необходимости уменьшить количество развернутых VM, перед числом следует указать знак «-»
min_adjust_step	число	Нет	Необязательный параметр для автоматической настройки PERCENTAGE_CHANGE. Минимальный шаг положительной/отрицательной корректировки — наименьшее количество VM, на которое будет изменен размер группы
recurrence	строка	Нет	Расписание начала автоматического масштабирования (в формате команды cron)
start_time	строка	Нет	Точное время начала автоматического масштабирования
period	число	Нет	Точное время начала автоматического масштабирования

Окончание таблицы 37

Параметр	Тип данных	Обязательный	Описание
cooldown	число	Нет	Длительность паузы (в секундах) после выполнения автоматического масштабирования сервиса. Если значение параметра не установлено, используется значение, установленное в параметров группы VM с заданной ролью (см. таблицу 35)

10.4.2. Управление шаблонами сервиса в интерфейсе командной строки**10.4.2.1. Создание шаблона**

Для создания шаблона сервиса необходимо использовать команду:

```
oneflow-template create <файл_json>
```

где <файл_json> — файл в формате JSON, в котором указаны значения параметров шаблона сервиса.

Пример

Файл `my_service.json` с параметрами шаблона сервиса:

```
{
  "name": "my_service",
  "deployment": "straight",
  "ready_status_gate": true,
  "roles": [
    {
      "name": "frontend",
      "vm_template": 0
    },
    {
      "name": "db_master",
      "parents": [
        "frontend"
      ],
      "vm_template": 1
    },
    {
      "name": "db_slave",
      "parents": [
        "frontend"
      ],
      "cardinality": 3,
      "vm_template": 2
    }
  ]
}
```

```

    "name": "worker",
    "parents": [
      "db_master",
      "db_slave"
    ],
    "cardinality": 10,
    "vm_template": 3
  }
]
}

```

Создание шаблона:

```
oneflow-template create my_service.json
```

Пример вывода после успешного выполнения команды:

```
ID: 0
```

10.4.2.2. Отображение доступных шаблонов и просмотр информации о шаблоне

Для отображения шаблонов, доступных пользователю, необходимо использовать команду:

```
oneflow-template list
```

Пример вывода после выполнения команды:

ID	USER	GROUP	NAME	REGTIME
0	oneadmin	brestadm	my_service	05/22 13:38:5

Для просмотра полной информации о шаблоне необходимо использовать команду:

```
oneflow-template show <идентификатор_шаблона>
```

Пример вывода после выполнения команды `oneflow-template show 0`:

```

SERVICE TEMPLATE 0 INFORMATION
ID : 0
NAME : my_service
USER : oneadmin
GROUP : brestadmins
REGISTRATION TIME : 05/22 13:38:59

```

PERMISSIONS

OWNER : um-

GROUP : ---

OTHER : ---

TEMPLATE CONTENTS

```

{
  "name": "my_service",
  "deployment": "straight",

```

```
"ready_status_gate": true,
"roles": [
  {
    "name": "frontend",
    "vm_template": 0,
    "cardinality": 1
  },
  {
    "name": "db_master",
    "parents": [
      "frontend"
    ],
    "vm_template": 1,
    "cardinality": 1
  },
  {
    "name": "db_slave",
    "parents": [
      "frontend"
    ],
    "cardinality": 3,
    "vm_template": 2
  },
  {
    "name": "worker",
    "parents": [
      "db_master",
      "db_slave"
    ],
    "cardinality": 10,
    "vm_template": 3
  }
],
"description": "",
"registration_time": 1684751939
}
```

10.4.2.3. Изменение параметров шаблона

Для изменения параметров шаблона необходимо использовать команду:

```
onetemplate update <идентификатор_шаблона>
```

После ввода команды откроется текстовый редактор для редактирования шаблона сервиса.

10.4.2.4. Клонирование шаблона

Клонировать существующий шаблон возможно с помощью команды:

```
onemplate clone <идентификатор_шаблона> <наименование_нового_шаблона>
```

При использовании аргумента `--recursive` будут клонированы все шаблоны ВМ, перечисленные в шаблоне сервиса. При этом в новом шаблоне будут указаны клонированные шаблоны ВМ.

10.4.2.5. Удаление шаблона

Для удаления шаблона необходимо выполнить команду:

```
onflow-template delete <идентификатор_шаблона>
```

Также можно указать необходимость удаления шаблонов ВМ, перечисленных в шаблоне сервиса. Для этого в качестве аргументов команды необходимо указать следующие параметры:

- «`--delete-vm-templates`» — для удаления всех шаблонов ВМ, перечисленных в шаблоне сервиса;
- «`--delete-images`» — для удаления всех шаблонов ВМ, перечисленных в шаблоне сервиса, а также удаления всех образов дисков, указанных в шаблонах этих ВМ.

10.4.3. Управление шаблонами сервиса в веб-интерфейсе ПК СВ

10.4.3.1. Создание шаблона

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

- 1) в меню слева выбрать пункт меню «Шаблоны — Сервисы»;
- 2) на открывшейся странице «Шаблоны Сервисов» нажать кнопку **[+]** и в открывшемся меню выбрать пункт «Создать»;
- 3) на открывшейся странице «Создать шаблон службы» задать значения параметров шаблона одним из способов:
 - во вкладке «Мастер настройки» установить необходимые значения параметров, заполнив поля формы. В том числе настроить роли виртуальных машин (см. рис. 91);

Создать шаблон службы



[←](#) [Сброс](#) [Создать](#) **Мастер настройки** [Расширенный](#)

Название

Описание

- ▼ Конфигурация сети
- ▼ Конфигурация значений пользовательских атрибутов
- ▼ Запланированные действия службы
- ▼ Расширенные параметры сервиса

Роли [+](#)

 frontend  db_master

Имя роли	Количество VM
<input type="text" value="db_master"/>	<input type="text" value="1"/>

Рис. 91

- во вкладке «Расширенный» указать непосредственно значения параметров в формате JSON (см. рис. 92);

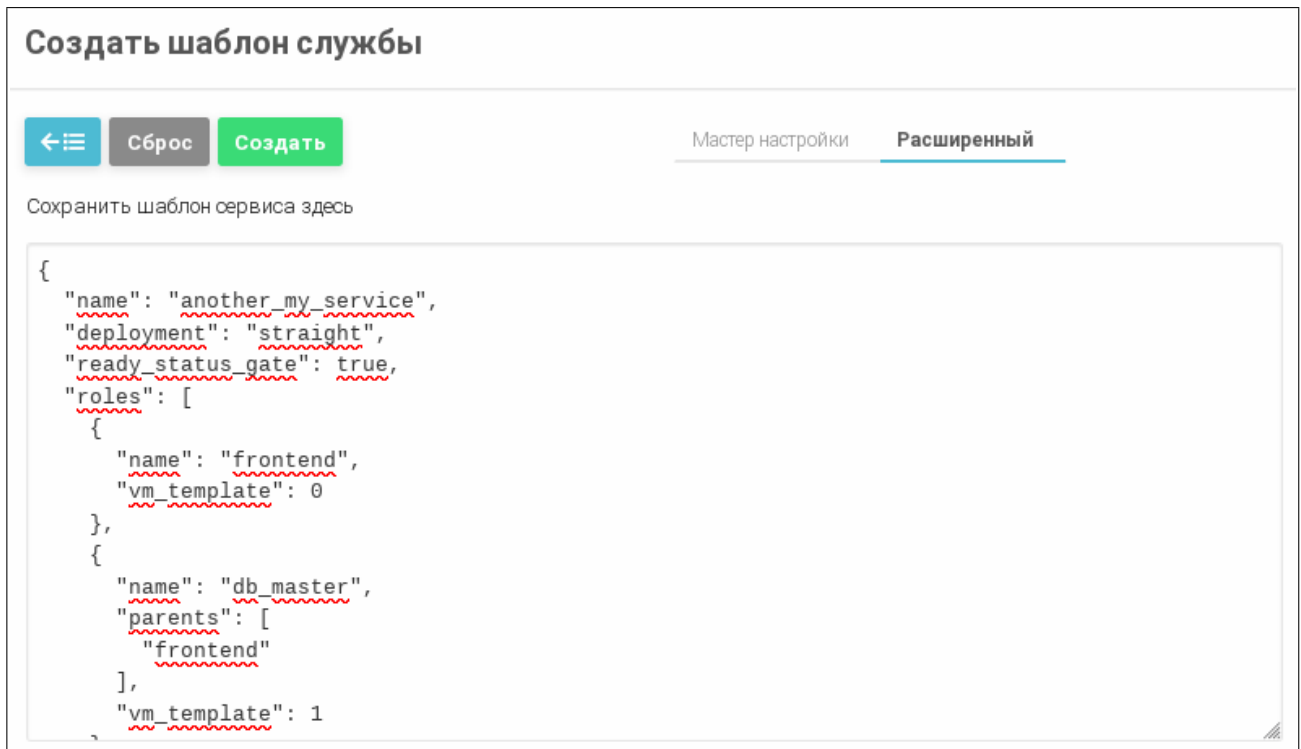


Рис. 92

4) на странице «Создать шаблон службы» нажать кнопку **[Создать]**. После этого на открывшейся странице «Шаблоны Сервисов» отобразится созданный шаблон (см. рис. 93).

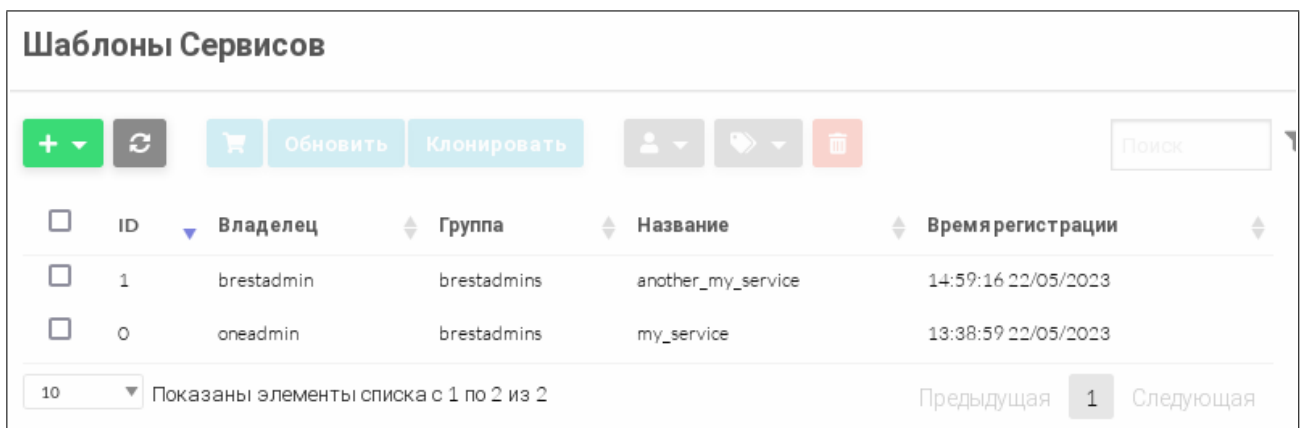


Рис. 93

10.4.3.2. Отображение доступных шаблонов и просмотр информации о шаблоне

Для отображения шаблонов, доступных пользователю, в веб-интерфейсе ПК СВ необходимо в меню слева выбрать пункт меню «Шаблоны — Сервисы». На открывшейся странице «Шаблоны Сервисов» будет отображена таблица шаблонов (см. рис. 93).

Для просмотра информации о конкретном шаблоне необходимо на странице «Шаблоны Сервисов» выбрать необходимый шаблон. После этого откроется страница шаблона (вкладка «Сведения») — см. рис. 94.

Шаблон Сервиса 0 my_service

← ≡ + ↻ 🛒 Обновить Клонировать 👤 📄 🗑️

📄 **Сведения** 🛠️ Роли 📄 Шаблон

Информация	Права	Пользование	Управление	Администрирование	
ID	0	Владелец	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Название	my_service ✎	Группа	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Время регистрации	13:38:59 22/05/2023	Все остальные	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Описание		Владелец			
Стратегия	straight	Владелец	oneadmin		✎
Действие при выкл.	-	Группа	brestdadmins		✎
Ready Status Gate	да				
Automatic Deletion	нет				

Рис. 94

10.4.3.3. Изменение параметров шаблона

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

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

10.4.3.4. Клонирование шаблона

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

- 1) в меню слева выбрать пункт меню «Шаблоны — Сервисы»;
- 2) на открывшейся странице «Шаблоны Сервисов» выбрать необходимый шаблон;
- 3) на открывшейся странице «Шаблон Сервиса» нажать кнопку **[Клонировать]**;
- 4) на открывшейся странице «Клонировать шаблон сервиса» (см. рис. 95):
 - если необходимо клонировать все шаблоны ВМ, перечисленные в шаблоне сервиса, установить флаг «Clone VM templates associated»;
 - нажать кнопку **[Клонировать]**.

Клонировать шаблон сервиса

2 my_service

Название

Copy of my_service

Clone VM templates associated

Клонировать

Рис. 95

10.4.3.5. Удаление шаблона

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

- 1) в меню слева выбрать пункт меню «Шаблоны — Сервисы»;
- 2) на открывшейся странице «Шаблоны Сервисов» отметить необходимые шаблоны и нажать на кнопку **[Удалить]** (см. рис. 96);

Шаблоны Сервисов

+ Обновить Клонировать

<input type="checkbox"/>	ID	Владелец	Группа	Название	Время регистрации
<input checked="" type="checkbox"/>	1	brestadmin	brestadmins	another_my_service	14:59:16 22/05/2023
<input type="checkbox"/>	0	oneadmin	brestadmins	my_service	13:38:59 22/05/2023

Показаны элементы списка с 1 по 2 из 2

Предыдущая 1 Следующая

Рис. 96

- 3) в открывшемся окне «Подтвердить» нажать одну из кнопок (см. рис. 97):
 - **[Удалить]** — для удаления только шаблона сервиса;
 - **[Delete VM Templates]** — для удаления шаблона сервиса и всех шаблонов VM, перечисленных в шаблоне сервиса;
 - **[Delete Images and VM Templates]** — для удаления шаблона сервиса и всех шаблонов VM, перечисленных в шаблоне сервиса, а также удаления всех образов дисков, указанных в шаблонах этих VM.

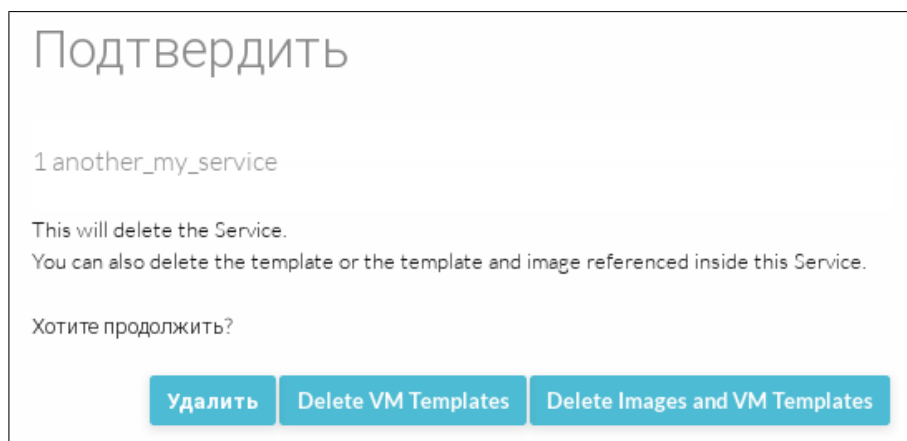


Рис. 97

10.4.4. Настройка автоматического удаления сервиса

Экземпляры ВМ из состава сервиса могут быть удалены в соответствии с заданными правилами (политикой эластичности). В какой-то момент может оказаться, что в ПК СВ не запущено ни одной ВМ из состава сервиса, но сервис будет продолжать функционировать и потреблять вычислительные ресурсы ПК СВ. Чтобы избежать этого, можно настроить автоматическое удаление сервиса.

10.4.4.1. В интерфейсе командной строки

Чтобы настроить автоматическое удаление сервиса, необходимо в шаблон сервиса добавить следующий параметр:

```
"automatic_deletion": true
```

Порядок изменения параметров шаблона в интерфейсе командной строки представлен в 10.4.2.3.

10.4.4.2. В веб-интерфейсе ПК СВ

Чтобы настроить автоматическое удаление сервиса, в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

- 1) в меню слева выбрать пункт меню «Шаблоны — Сервисы»;
- 2) на открывшейся странице «Шаблоны Сервисов» выбрать необходимый шаблон;
- 3) на открывшейся странице «Шаблон Сервиса» нажать кнопку **[Обновить]**;
- 4) на открывшейся странице «Изменить шаблон службы» во вкладке «Мастер настройки» в секции «Расширенные параметры сервиса» установить флаг «Automatic deletion of service when all VMs terminated»(см. рис. 98);

Изменить шаблон службы 0 my_service

[←](#) [Обновить](#) Мастер настройки [Расширенный](#)

Название
my_service

Описание

▼ Конфигурация сети
▼ Конфигурация значений пользовательских атрибутов
▼ Запланированные действия службы
▲ Расширенные параметры сервиса

Стратегия ⓘ Действие при выкл.

Ждать пока VM сообщат, что они готовы через OneGate, чтобы считать их работающими
 Automatic deletion of service when all VMs terminated

Рис. 98

5) на странице «Изменить шаблон службы» нажать кнопку **[Обновить]**.

10.5. Управление экземплярами сервиса

10.5.1. Жизненный цикл экземпляра сервиса

Жизненный цикл экземпляра сервиса включает состояния, отображенные на рис. 99.

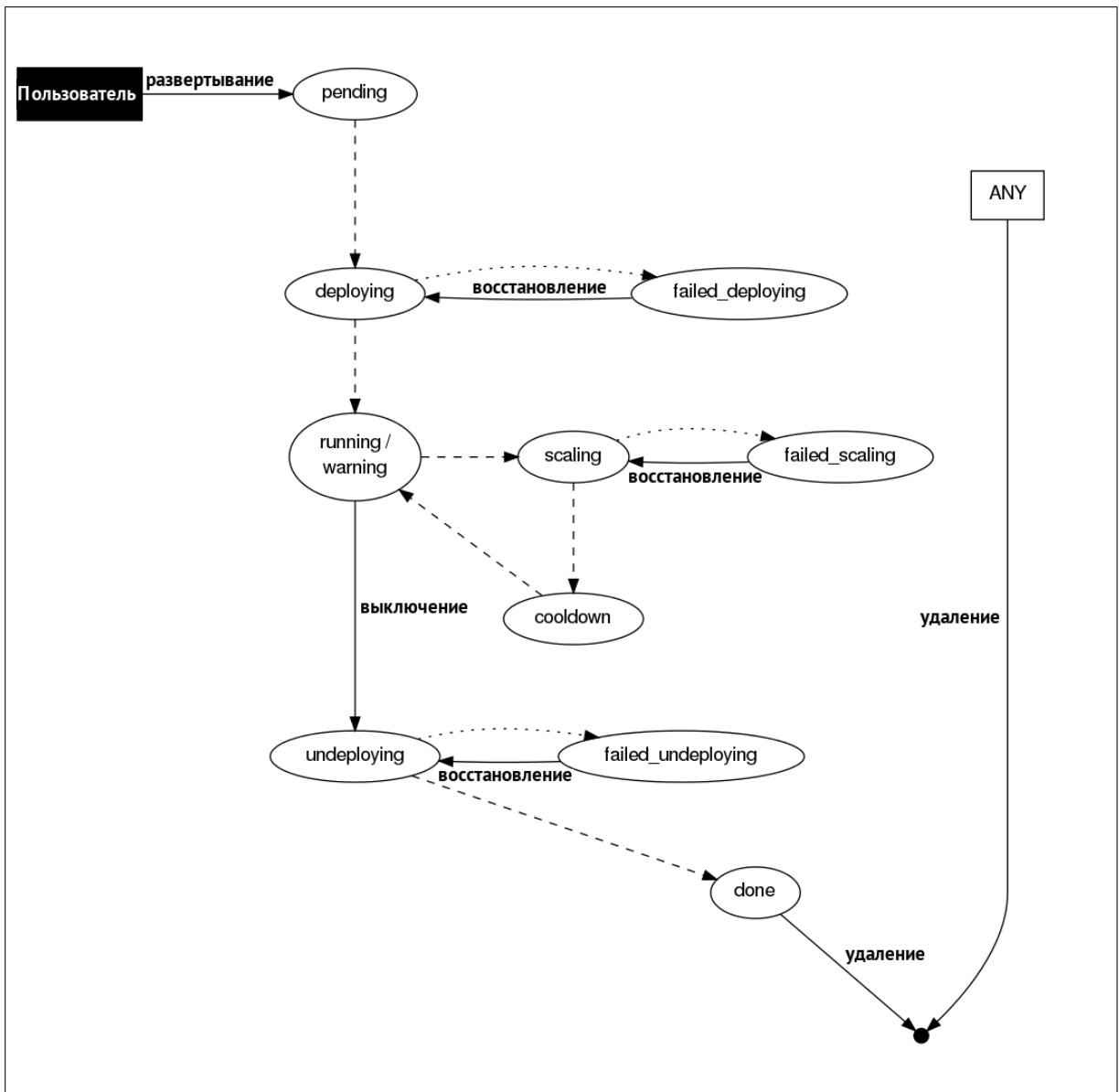


Рис. 99

Краткие описания состояний сервиса приведены в таблице 38.

Таблица 38

Состояние сервиса	Описание
PENDING	Исходное состояние сервиса. Сервис находится в этом состоянии, пока служба OneFlow не начнет процесс развертывания этого сервиса
DEPLOYING	Начался процесс развертывания каких-либо групп VM с заданной ролью
RUNNING	Все группы VM с заданной ролью из состава сервиса успешно развернуты
WARNING	Обнаружена ошибка при развертывании VM
SCALING	Начался процесс автоматического масштабирования группы VM с заданной ролью
COOLDOWN	Пауза между итерациями автоматического масштабирования группы VM с заданной ролью

Окончание таблицы 38

Состояние сервиса	Описание
UNDEPLOYING	Начался процесс отмены развертывания каких-либо групп ВМ с заданной ролью
FAILED_DEPLOYING	Обнаружена ошибка при развертывании сервиса
FAILED_UNDEPLOYING	Обнаружена ошибка во время отмены развертывания сервиса
FAILED_SCALING	Обнаружена ошибка во время автоматического масштабирования сервиса

При этом каждая группа ВМ с заданной ролью может быть в одном из состояний, описание которых приведено в таблице 39.

Таблица 39

Состояние группы	Описание
PENDING	Ожидание начала процесса развертывания
DEPLOYING	Начался процесс развертывания ВМ. Группа ВМ с заданной ролью находится в этом состоянии, пока статус всех ВМ из состава группы не примет значение RUNNING
RUNNING	Статус всех ВМ из состава группы имеет значение RUNNING
WARNING	Обнаружена ошибка при развертывании ВМ
SCALING	Начался процесс автоматического масштабирования. Группа ВМ с заданной ролью находится в этом состоянии, пока необходимое количество ВМ не будет развернуто или выключено
COOLDOWN	Пауза между итерациями автоматического масштабирования группы
UNDEPLOYING	Начался процесс выключения каких-либо ВМ. Группа ВМ с заданной ролью находится в этом состоянии, пока статус всех ВМ из состава группы не примет значение DONE
FAILED_DEPLOYING	Обнаружена ошибка при развертывании ВМ из состава группы
FAILED_UNDEPLOYING	Обнаружена ошибка во время отмены развертывания ВМ из состава группы
FAILED_SCALING	Обнаружена ошибка во время автоматического масштабирования ВМ из состава группы

10.5.2. Управление экземплярами сервиса в интерфейсе командной строки

10.5.2.1. Развертывание экземпляра сервиса

Для развертывания сервиса из шаблона можно воспользоваться командой:

```
onflow-template instantiate <идентификатор_шаблона>
```

10.5.2.2. Отображение развернутых сервисов

Для отображения развернутых сервисов необходимо использовать команду `onflow list`.

Пример вывода после выполнения команды:

ID	USER	GROUP	NAME	STARTTIME	STATE
1	oneadmin	oneadmin	my_service	10/28 17:42:46	PENDING

Кроме того, можно использовать команду `oneflow top` для непрерывного отображения развернутых сервисов.

Для просмотра полной информации о сервисе необходимо использовать команду:
`oneflow show <идентификатор_сервиса>`

10.5.2.3. Управление состоянием сервиса

Для управления состоянием сервиса используются команды, описание которых приведено в таблице 40.

Таблица 40

Команда	Описание
<code>oneflow delete</code>	Выключение сервиса. Эта команда запускает процесс корректного выключения всех развернутых экземпляров ВМ. Если в настройках сервиса указан тип развертывания <code>straight</code> , то процесс выключения групп ВМ с заданной ролью производится в обратном порядке
<code>oneflow recover</code>	Восстановление после сбоя. Используется для автоматического возобновления функционирования в штатном режиме (см. 10.5.4)
<code>oneflow recover --delete</code>	Принудительное удаление экземпляра сервиса. Используется, если в процессе удаления ВМ произошла ошибка
<code>oneflow purge-done</code>	Удаление всех сервисов, состояние которых имеет значение <code>DONE</code>

10.5.2.4. Добавление и удаление групп ВМ в экземпляре сервиса

ВНИМАНИЕ! Добавить или удалить группу ВМ с заданной ролью в экземпляре сервиса можно только в том случае, если состояние этого сервиса имеет значение `RUNNING`.

Чтобы добавить группу ВМ с заданной ролью, необходимо выполнить команду:
`oneflow add-role <идентификатор_сервиса> <файл_json>`

где:

- `<идентификатор_сервиса>` — идентификатор экземпляра сервиса;
- `<файл_json>` — файл в формате JSON, в котором указаны значения параметров шаблона сервиса.

Пример

Файл `role.json` с параметрами группы ВМ:

```
{
  "name": "MASTER",
  "cardinality": 1,
```



```

"vm_template": 0,
"min_vms": 1,
"max_vms": 2,
"elasticity_policies": [],
"scheduled_policies": []
}

```

Добавление группы ВМ в экземпляр сервиса с идентификатором 0:

```
oneflow add-role 0 role.json
```

После получения команды на добавление группы ВМ с заданной ролью в сервис, состояние этого сервиса примет значение DEPLOYING. Сервис находится в этом состоянии, пока статус необходимого количества ВМ из состава группы не примет значение RUNNING.

Чтобы удалить группу ВМ с заданной ролью, необходимо выполнить команду:

```
oneflow remove-role <идентификатор_сервиса> <наименование_группы>
```

После получения команды на удаление группы ВМ с заданной ролью из сервиса, состояние этого сервиса примет значение UNDEPLOYING. Сервис находится в этом состоянии до тех пор, пока все ВМ из состава группы не будут удалены. После этого состояние сервиса примет значение RUNNING.

10.5.2.5. Управление группой ВМ из состава экземпляра сервиса

Для управления состоянием всех ВМ из состава группы ВМ с заданной ролью используется следующая команда:

```
oneflow action <наименование_сервиса> <наименование_группы_ВМ> <действие>
```

В отношении группы ВМ с заданной ролью допускается выполнять следующие действия:

- terminate;
- terminate-hard;
- undeploy;
- undeploy-hard;
- hold;
- release;
- stop;
- suspend;
- resume;
- reboot;
- reboot-hard;
- poweroff;
- poweroff-hard;
- snapshot-create;

- snapshot-revert;
- snapshot-delete;
- disk-snapshot-create;
- disk-snapshot-revert;
- disk-snapshot-delete.

Кроме того, возможно указать, что заданное в команде действие применялось не одновременно ко всем VM из состава группы, а поочередно в отношении одной или нескольких VM. Для этого используются следующие аргументы команды:

- «-n» или «--number» — количество VM с заданной ролью, которым будет одновременно направлена команда на изменение состояния за одну итерацию;
- «-p» или «--period» — пауза (в секундах) между итерациями.

Если аргументы «--number» и «--period» не указаны, то используются соответственно значения параметров «:action_number» и «:action_period», заданные в конфигурационном файле `/etc/one/oneflow-server.conf` службы OneFlow (см. 10.3.2).

Пример

Направить всем VM из состава группы с ролью `my-role` сервиса `my-service` команду на перезагрузку. При этом за одну итерацию команда на перезагрузку будет направлена только двум VM из состава группы. Пауза между итерациями составляет 300 секунд:

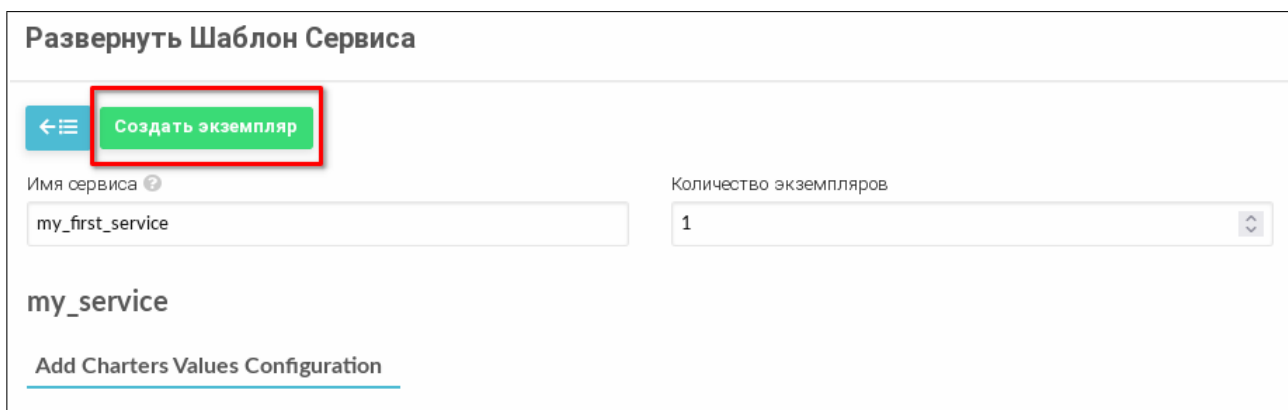
```
oneflow action my-service my-role reboot --period 300 --number 2
```

10.5.3. Управление экземплярами сервиса в веб-интерфейсе ПК СВ

10.5.3.1. Развертывание экземпляра сервиса

Для того чтобы развернуть сервис из шаблона, в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

- 1) в меню слева выбрать пункт меню «Шаблоны — Сервисы»;
- 2) на открывшейся странице «Шаблоны Сервисов» выбрать необходимый шаблон;
- 3) на открывшейся странице «Шаблон Сервиса» нажать кнопку **[+]** и в открывшемся меню выбрать пункт «Создать экземпляр»;
- 4) на открывшейся странице «Развернуть Шаблон Сервиса» (см. рис. 100):
 - а) в поле «Имя сервиса» задать наименование сервиса;
 - б) указать количество экземпляров сервиса;
 - в) нажать кнопку **[Создать экземпляр]**.



Развернуть Шаблон Сервиса

[←](#) **Создать экземпляр**

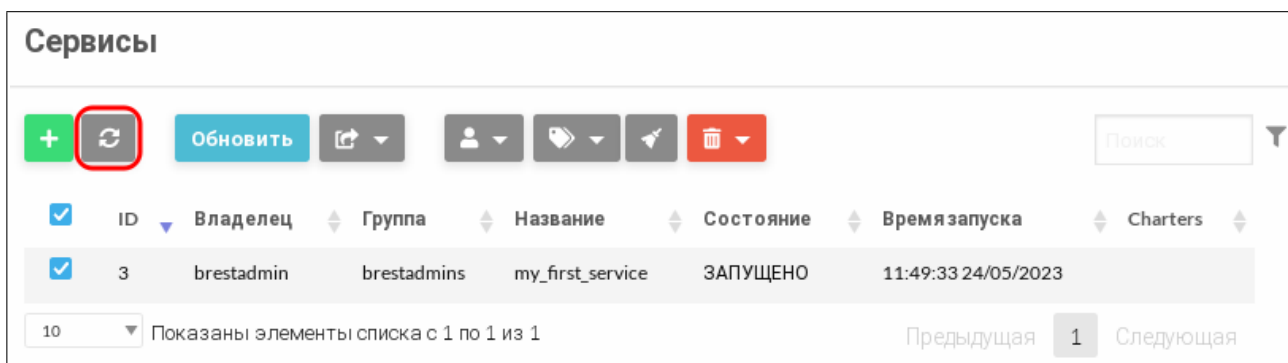
Имя сервиса Количество экземпляров

my_service

[Add Charters Values Configuration](#)

Рис. 100

5) в меню слева выбрать пункт меню «Экземпляры ВМ – Сервисы» и дождаться пока в поле «Состояние» для созданного на предыдущем шаге сервиса значение РАЗВОРАЧИВАЕТСЯ не изменится на ЗАПУЩЕНО. Для обновления информации на странице можно воспользоваться кнопкой **[Обновить]**. (см. рис. 101).



Сервисы

[+](#) [↻](#) **Обновить** [↗](#) [👤](#) [📁](#) [📧](#) [🗑️](#)

<input checked="" type="checkbox"/>	ID	Владелец	Группа	Название	Состояние	Времязапуска	Charters
<input checked="" type="checkbox"/>	3	brestadmin	brestadmins	my_first_service	ЗАПУЩЕНО	11:49:33 24/05/2023	

10 Показаны элементы списка с 1 по 1 из 1 Предыдущая 1 Следующая

Рис. 101

10.5.3.2. Отображение развернутых сервисов

Для отображения развернутых сервисов в веб-интерфейсе ПК СВ необходимо в меню слева выбрать пункт меню «Экземпляры ВМ – Сервисы». На открывшейся странице «Сервисы» будет отображена таблица экземпляров сервисов (см. рис. 101).

Для просмотра полной информации о сервисе необходимо на странице «Сервисы» выбрать необходимый сервис. После этого откроется страница сервиса (вкладка «Сведения») — см. рис. 102.

Сервис 3 my_first_service ЗАПУЩЕНО

← ☰ ↻ Обновить ↗ 👤 📁 🔍 🗑️

Сведения ⚙️ Журнал 📅 Действия 📅

Информация	Права	Пользование	Управление	Администрирование	
ID	3	Владелец	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Название	my_first_service ↗	Группа	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Время запуска	11:49:33 24/05/2023	Все остальные	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Стратегия	straight	Владелец			
Действие при выкл.	-	Владелец	brestdadmin	↗	
Состояние	ЗАПУЩЕНО	Группа	brestdadmins	↗	
Ready Status Gate	нет				
Automatic Deletion	нет				

Рис. 102

10.5.3.3. Управление состоянием сервиса

Для управления состоянием сервиса используются следующие кнопки веб-интерфейса:

- **[Удалить]** (см. рис. 103) — инициирует команду `onflow delete` (выключение сервиса). Эта команда запускает процесс корректного выключения всех запущенных экземпляров VM. Если в настройках сервиса указан тип развертывания `straight`, то процесс выключения групп VM с заданной ролью производится в обратном порядке;

Сервис 3 my_first_service ЗАПУЩЕНО

← ☰ ↻ Обновить ↗ 👤 📁 🔍 🗑️

Сведения ⚙️ Журнал 📅 Действия 📅

Удалить

Рис. 103

- **[Восстановить]** (см. рис. 104) — инициирует команду `onflow recover` (восстановление после сбоя). Используется для автоматического возобновления функционирования в штатном режиме (см. 10.5.4);

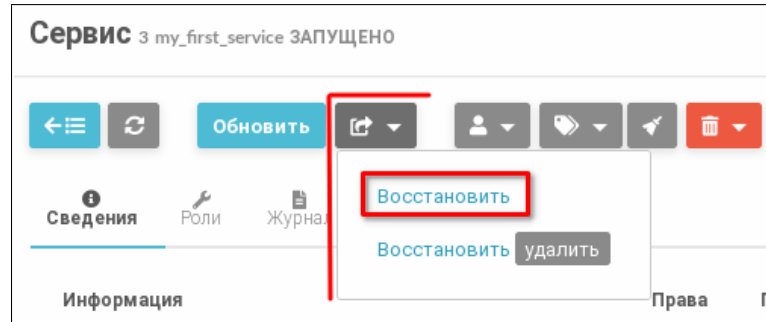


Рис. 104

- **[Восстановить - удалить]** (см. рис. 105) — инициирует команду `onflow recover --delete` (принудительное удаление экземпляра сервиса). Используется, если в процессе удаления VM произошла ошибка;

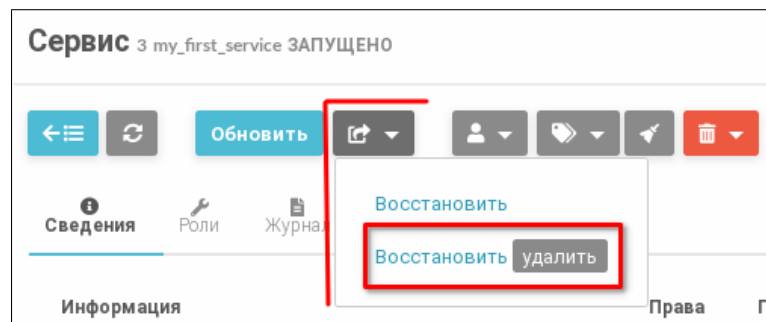


Рис. 105

- **[Очистить]** (см. рис. 106) — инициирует команду `onflow purge-done`. Используется для удаления всех сервисов, состояние которых имеет значение DONE.

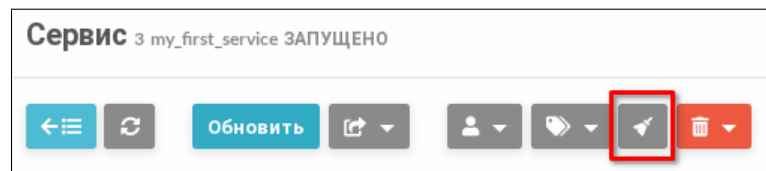


Рис. 106

10.5.3.4. Управление группой VM из состава экземпляра сервиса

Для управления состоянием всех VM из состава группы VM с заданной ролью в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

- 1) в меню слева выбрать пункт меню «Экземпляры VM — Сервисы»;
- 2) на открывшейся странице «Сервисы» выбрать необходимый сервис;
- 3) на открывшейся странице «Сервис» во вкладке «Роли» выбрать группу VM, состояние которой необходимо изменить. После этого станут доступны кнопки для управления состоянием группы VM (см. рис. 107).

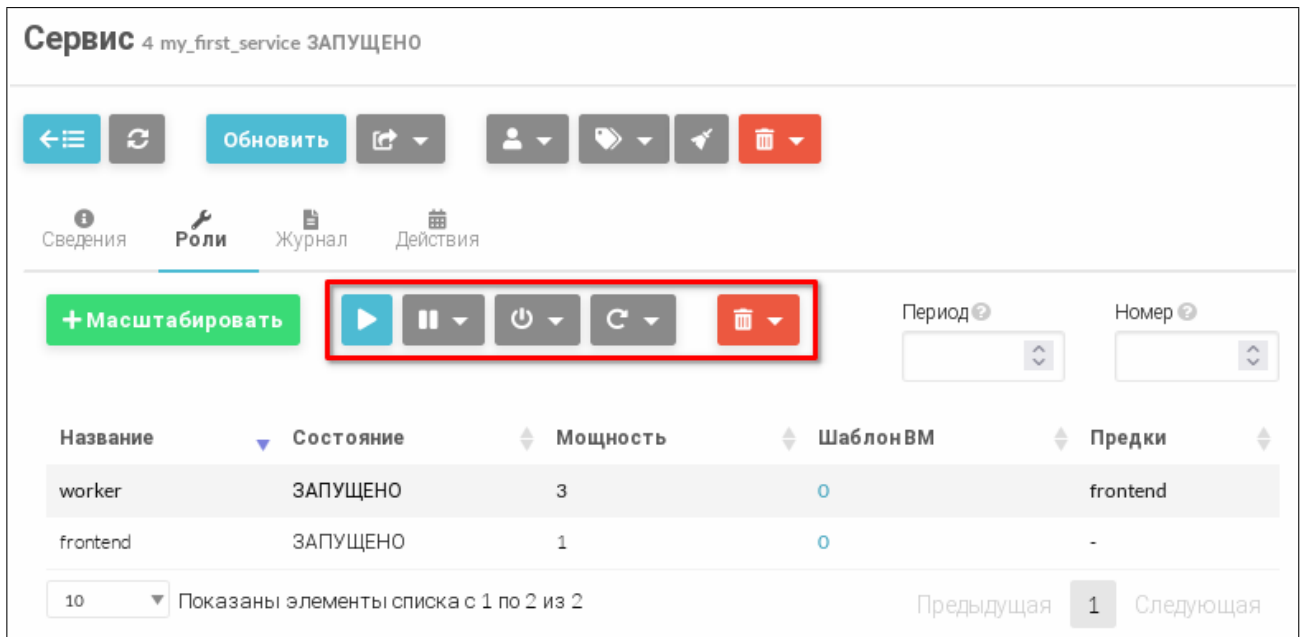


Рис. 107

Также можно указать, что заданное в команде действие применялось не одновременно ко всем VM из состава группы, а поочередно в отношении одной или нескольких VM. Для этого используются следующие поля для ввода:

- «Номер» — количество VM с заданной ролью, которым будет одновременно направлена команда на изменение состояния за одну итерацию;
- «Период» — пауза (в секундах) между итерациями.

Если значения параметров «Номер» и «Период» не указаны, то используются соответственно значения параметров «:action_number» и «:action_period», заданные в конфигурационном файле `/etc/one/oneflow-server.conf` службы OneFlow (см. 10.3.2).

Для управления состоянием конкретной VM из состава группы VM с заданной ролью в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

- 1) в меню слева выбрать пункт меню «Экземпляры VM — Сервисы»;
- 2) на открывшейся странице «Сервисы» выбрать необходимый сервис;
- 3) на открывшейся странице «Сервис» во вкладке «Роли» выбрать группу VM, состояние которой необходимо изменить, и пролистать страницу вниз;
- 4) на странице «Сервис» во вкладке «Роли» в секции VM выбрать необходимую VM (допускается выбрать несколько VM). После этого станут доступны кнопки для управления состоянием группы VM (см. рис. 108).

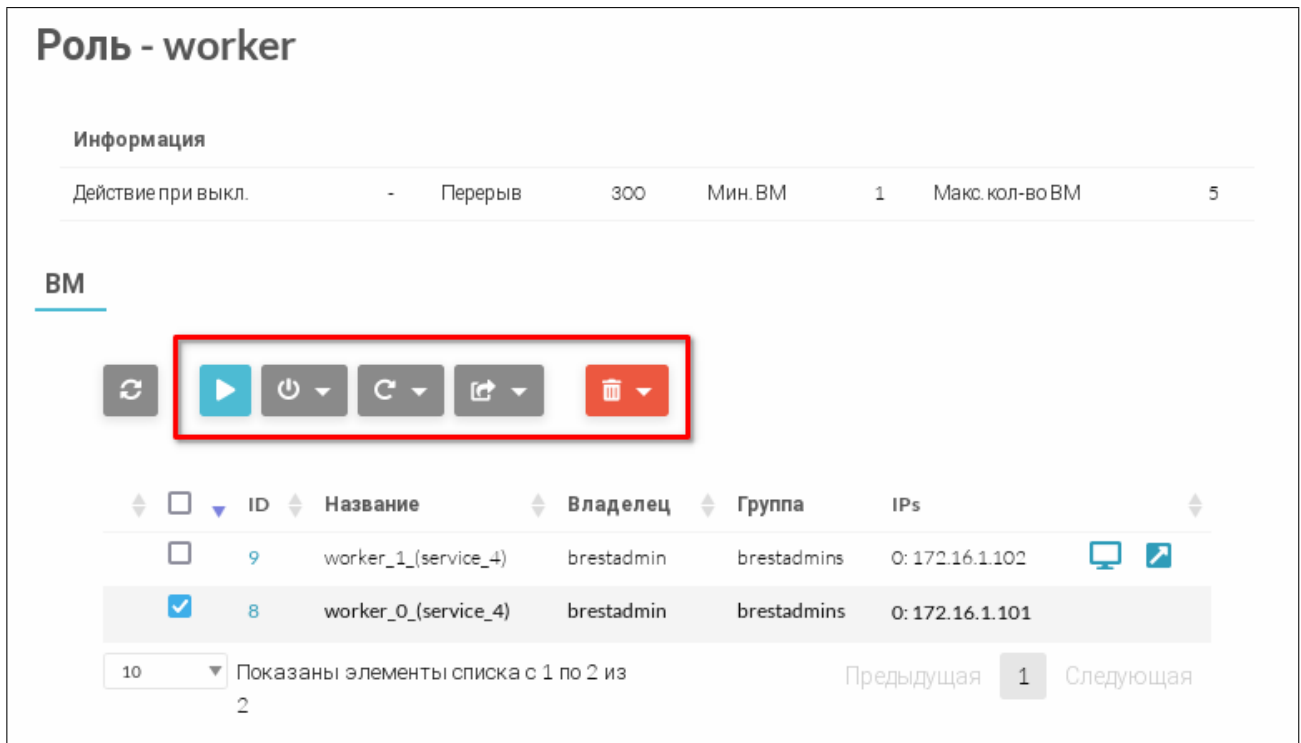


Рис. 108

10.5.4. Особенности восстановления после сбоя

Некоторые ошибки, возникшие в процессе функционирования сервиса, могут быть устранены в автоматическом режиме с помощью команды `onflow recover`. Последовательность автоматических действий при выполнении этой команды приведена в таблице 41.

Таблица 41

Исходное состояние сервиса	Описание автоматических действий	Новое состояние сервиса
FAILED_DEPLOYING	VM, имеющие статус DONE или FAILED, уничтожаются. VM со статусом UNKNOWN развертываются	DEPLOYING
FAILED_UNDEPLOYING	Возобновляется процесс удаления сервиса	UNDEPLOYING
FAILED_SCALING	VM, имеющие статус DONE или FAILED, уничтожаются. VM со статусом UNKNOWN развертываются. Если в процессе автоматического масштабирования производилось уменьшение количества VM, то возобновляется действие по выключению заданных VM	SCALING
COOLDOWN	Пропуск паузы, немедленное возобновление функционирования	RUNNING

10.6. Автоматическое масштабирование сервиса

10.6.1. Особенности масштабирования сервиса

Количество развернутых VM в группе с заданной ролью может быть изменено в ручном режиме, в автоматическом режиме в соответствии с заданными правилами или по

расписанию.

После начала процесса масштабирования группа ВМ с заданной ролью и сервис будут переведены в состояние `SCALING`. Для достижения указанного размера группы ВМ с заданной ролью, в этой группе будут разворачиваться или уничтожаться ВМ. При этом для этой группы ВМ должны быть установлены значения максимального и минимального количества ВМ в группе (см. 10.4).

После завершения процесса масштабирования группа ВМ с заданной ролью и сервис будут переведены в состояние `COOLDOWN` (пауза). Продолжительность паузы определяется в шаблоне сервиса (см. 10.4). Затем группа ВМ с заданной ролью и сервис будут переведены в состояние `RUNNING`.

10.6.2. Изменение размера группы ВМ в ручном режиме

10.6.2.1. В интерфейсе командной строки

Для изменения количества развернутых ВМ в группе с заданной ролью можно воспользоваться командой:

```
onflow scale <идентификатор_сервиса> <наименование_роли> \  
  <необходимое_количество_ВМ>
```

Если необходимо установить такое количество развернутых ВМ, которое лежит вне диапазона максимального и минимального значений, заданных для группы ВМ, то следует использовать аргумент «`--force`».

10.6.2.2. В веб-интерфейсе ПК СВ

Для изменения количества развернутых ВМ в группе с заданной ролью в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

- 1) в меню слева выбрать пункт меню «Экземпляры ВМ — Сервисы»;
- 2) на открывшейся странице «Сервисы» выбрать необходимый сервис;
- 3) на открывшейся странице «Сервис» во вкладке «Роли» выбрать группу ВМ, размер которой необходимо изменить, и нажать на кнопку **[Масштабировать]** (см. рис. 109);

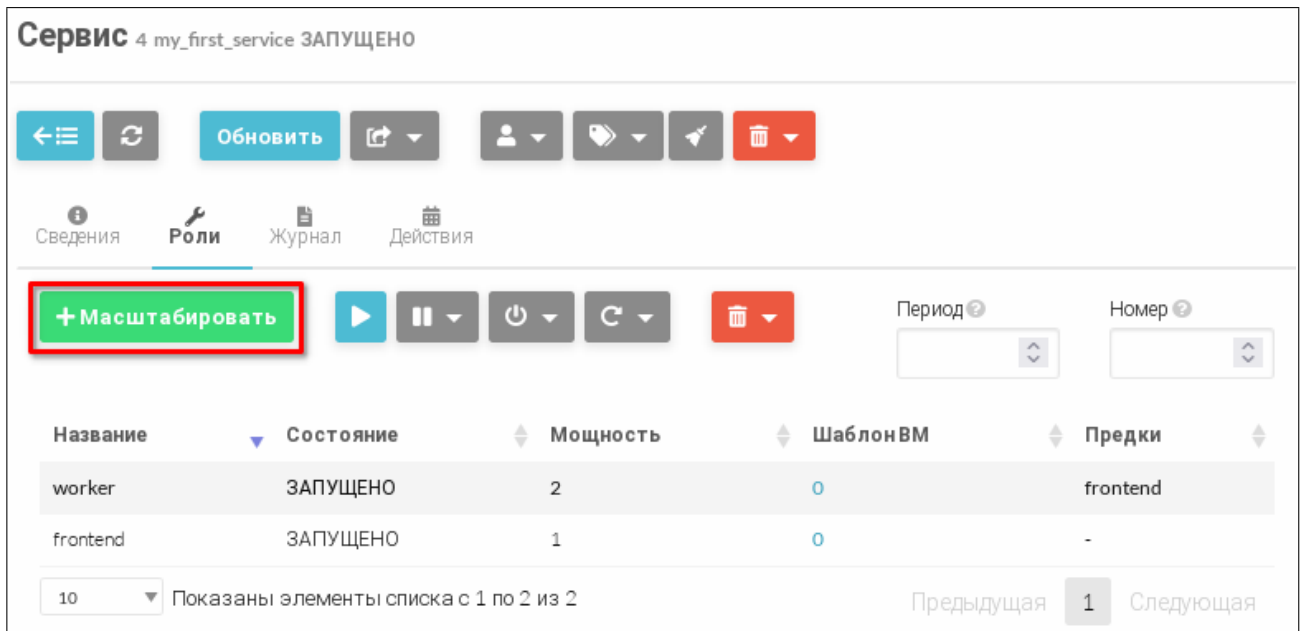


Рис. 109

4) в открывшемся окне «Масштабировать» (см. рис. 110):

- указать необходимое количество VM, которое должно быть развернуто в группе с заданной ролью;
- если необходимо установить такое количество развернутых VM, которое лежит вне диапазона максимального и минимального значений, заданных для группы VM, то следует установить флаг «Принудительно»;
- нажать кнопку **[Масштабировать]**.

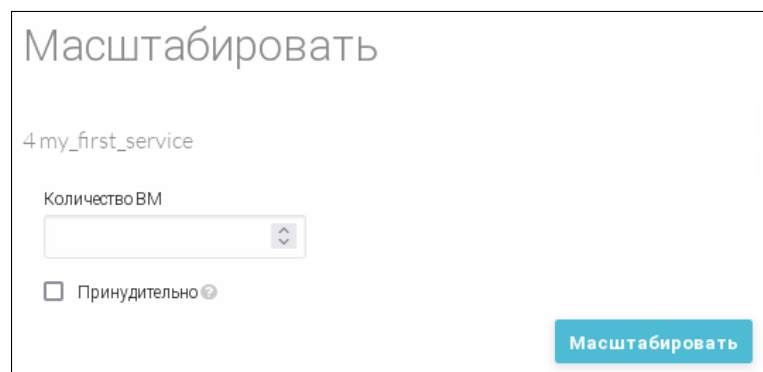


Рис. 110

10.6.3. Настройка автоматического масштабирования

10.6.3.1. Общие настройки автоматического масштабирования

Значения параметров автоматического изменения размера группы VM с заданной ролью определяются в шаблоне сервиса (см. 10.4). Как для политики эластичности, так и для политики планирования процесс автоматического масштабирования определяется параметрами, приведенными в таблице 42.

Таблица 42

Параметр	Тип данных	Обязательный	Описание
type	строка	Да	Тип автоматического масштабирования. Может принимать следующие значения: - CHANGE — добавление/удаление заданного количества развернутых ВМ; - CARDINALITY — установка заданного размера группы (количества развернутых ВМ); - PERCENTAGE_CHANGE — добавление/удаление количества развернутых ВМ, заданного в процентном соотношении от текущего размера группы
adjust	число	Да	Шаг положительной/отрицательной корректировки или размер группы ВМ (в зависимости от типа автоматического масштабирования). В случае необходимости уменьшить количество развернутых ВМ, перед числом следует указать знак «-»
min_adjust_step	число	Нет	Необязательный параметр для автоматической настройки PERCENTAGE_CHANGE. Минимальный шаг положительной/отрицательной корректировки — наименьшее количество ВМ, на которое будет изменен размер группы

10.6.3.2. Настройка политики эластичности

Политика эластичности — это правило, в соответствии с которым производится запуск автоматического масштабирования группы ВМ с заданной ролью. Массив политик эластичности размещается в шаблоне сервиса (см. 10.4). Процесс автоматического масштабирования группы ВМ в соответствии с заданным правилом начинается при достижении определенного условия, заданного в параметре `expression`. Условие применения политики эластичности представляет собой логическое выражение, в котором указаны наименования параметров, числа и символы логических операций. В качестве операндов могут выступать:

- значения параметров пользовательского шаблона экземпляра ВМ. Значения этих параметров могут быть установлены или изменены приложениями, функционирующими в ОС виртуальной машины. Для этого используется служба сервера OneGate (см. 10.2);
- значения параметров ВМ, предоставляемые драйвером виртуализации, такие как CPU, NETTX и NETRX.

Политика эластичности определяется параметрами, представленными в таблице 43.

Таблица 43

Параметр	Тип данных	Обязательный	Описание
expression	строка	Да	Условие (логическое выражение) при котором необходимо применить политику эластичности
period_number	число	Нет	Количество периодов времени, на протяжении которых выполняется условие, указанное в параметре expression. Только по прошествии этого времени будет применена политика эластичности
period	число	Нет	Длительность периода (в секундах) — используется совместно с параметром period_number

В случае выполнении условия, заданного в политике эластичности, начнется процесс автоматического масштабирования в соответствии с заданными значениями общих параметров (см. таблицу 42).

Пример

Реализация масштабирования пользовательского сервиса:

- в приложении, функционирующим в ОС виртуальной машины случае, для контроля нагрузки используется параметр с наименованием `workload`;
- с помощью службы сервера OneGate значение этого параметра записывается в пользовательский шаблон экземпляра ВМ;
- в шаблоне сервиса для группы ВМ с заданной ролью установлена следующая политика эластичности — если значение параметра `workload` больше 50 на протяжении 30 секунд (3 периода по 10 секунд), то необходимо дополнительно развернуть две ВМ:

```
"elasticity_policies" : [
{
  "expression" : "workload > 50",
  "period_number" : 3,
  "period" : 10

  "type" : "CHANGE",
  "adjust" : 2,
},
...
]
```

10.6.3.3. Настройка политики планирования

Политика планирования определяет расписание и/или периодичность повторения автоматического масштабирования группы ВМ с заданной ролью. Массив политик плани-

рования размещается в шаблоне сервиса (см. 10.4). Политика эластичности определяется параметрами, представленными в таблице 44.

Таблица 44

Параметр	Тип данных	Обязательный	Описание
recurrence	строка	Нет	Расписание начала автоматического масштабирования (в формате команды cron)
start_time	строка	Нет	Точное время начала автоматического масштабирования

При выполнении условия, заданного в политике планирования, начнется процесс автоматического масштабирования в соответствии с заданными значениями общих параметров (см. таблицу 42).

10.6.4. Просмотр установленных политик автоматического масштабирования

10.6.4.1. В интерфейсе командной строки

Значения параметров установленных политик эластичности и планирования можно просмотреть, выполнив команду:

```
onflow show <идентификатор_сервиса>
```

Пример вывода после выполнения команды:

```
SERVICE 4 INFORMATION
ID : 4
NAME : my_first_service
...
ROLE worker
...
ROLE ELASTICITY
ADJUST EXPRESSION EVALS PERIOD COOL
+ 2 WORKLOAD[--] > 50 0/3 10s -

ROLE ELASTICITY SCHEDULE
ADJUST TIME
= 3 0 9 * * mon,tue,wed,thu,fri
...
```

где:

- в информационном блоке `ROLE ELASTICITY` представлена политика эластичности для группы ВМ с наименованием `worker`;
- в информационном блоке `ROLE ELASTICITY SCHEDULE` представлена политика планирования для группы ВМ с наименованием `worker`.

10.6.4.2. В веб-интерфейсе ПК СВ

Для просмотра значений параметров установленных политик эластичности и планирования, в веб-интерфейсе ПК СВ необходимо выполнить следующие действия:

- 1) в меню слева выбрать пункт меню «Экземпляры VM — Сервисы»;
- 2) на открывшейся странице «Сервисы» выбрать необходимый сервис;
- 3) на открывшейся странице «Сервис» во вкладке «Роли» выбрать группу VM, установленные политики которой необходимо просмотреть, и пролистать страницу вниз;
- 4) на странице «Сервис» во вкладке «Роли» (см. рис. 111):
 - в секции «Стратегии масштабируемости» отображены установленные политики эластичности;
 - в секции «Запланированные стратегии» отображены установленные политики планирования.

Роль - worker

Информация

Действие при выкл.	-	Перерыв	300	Мин. VM	1	Макс. кол-во VM	5
--------------------	---	---------	-----	---------	---	-----------------	---

VM

↺ ▶ ⏻ ↻ 🔄 🗑️

ID	Название	Владелец	Группа	IPs
9	worker_1_(service_4)	brestadmin	brestadmins	0: 172.16.1.102
8	worker_0_(service_4)	brestadmin	brestadmins	0: 172.16.1.101

Показаны элементы списка с 1 по 2 из 2

← 1 →

Стратегии масштабируемости

Тип	Подстроить	Мин.	Выражение	#	Период	Перерыв
CHANGE	2	-	workload > 50	0/3	10	-

Запланированные стратегии

Тип	Подстроить	Мин.	Формат времени	Временное выражение
CARDINALITY	3	-	Повторяемость	0 9 * * mon,tue,wed,thu,fri

Рис. 111

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.10001-02 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
ACL	— Access Control List (список контроля доступа)
AR	— Address Ranges (диапазон IP-адресов)
VDC	— Virtual Data Center (виртуальный дата-центр)

