

ВЫЧИСЛИТЕЛЬНЫЙ УЗЕЛ SHARXBASE  
РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ  
ШБМА.466535.002РЭ.ПО

ООО «Шаркс ДЦ»

Москва

2019

## Содержание

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ТЕРМИНОВ	6
1 ОПИСАНИЕ АРХИТЕКТУРЫ	7
1.1 Введение	7
1.2 Технические характеристики	7
1.2.1 Описание	7
1.2.1.1 Описание структуры комплекса	7
1.2.1.2 Общая схема архитектуры ПАК	8
1.2.1.3 Схема типового блока	8
1.2.1.4 Схема типового узла	9
1.2.1.5 Описание системы управления виртуализацией на основе открытого кода	10
1.2.1.6 Описание виртуального сетевого коммутатора	11
1.2.1.7 Описание подсистемы мониторинга	11
1.2.1.8 Описание распределенного хранилища данных.	11
1.2.1.9 Максимальные конфигурации ВМ	12
1.2.1.10 Максимальные конфигурации серверного узла	13
1.2.1.11 В Максимальные конфигурации сети	14
1.2.1.12 Максимальные конфигурации кластера	14
1.2.1.13 Поддерживаемые ОС и апплаинсы для ВМ	15
2 УСТАНОВКА И НАСТРОЙКА	17
2.1 Рекомендации по настройке сети	17
2.1 Первичная настройка и подготовка узла	18
2.1.1 Настройка системы управления IPMI узла	18
2.2 Описание входа в систему	19
2.3 Описание функций управления физическими узлами	21
2.3.1 Управление статусом узла: подключение, отключение, вывод в автономный режим и перенос	25
2.3.2 Управление атрибутами узла и политиками управления.	27
2.4 Описание функций управления виртуальными машинами	28
2.4.1 Описание функций управления экземплярами виртуальных машин	28
2.4.1.1 Отображение списка виртуальных машин	28

2.4.1.2	Создание виртуальной машины из шаблона	29
2.4.1.3	Изменение статуса виртуальной машины	30
2.4.1.4	Изменение выделенных ресурсов ОЗУ и ЦПУ	34
2.4.1.5	Работа с хранилищами виртуальных машин	38
2.4.1.6	Создание и удаление снимка VM	41
2.4.2	Описание работы с образами виртуальных машин	41
2.4.2.1	Загрузка iso образа	43
2.4.2.2	Создание образа datablock	44
2.4.2.3	Клонирование образа	45
2.4.2.4	Удаление образа	46
2.4.2.5	Смена владельца или группы образа	47
2.4.2.6	Изменение статуса образа	48
2.4.3	Описание работы с шаблонами виртуальных машин	48
2.4.3.1	Обновление шаблона виртуальной машины	48
2.4.3.2	Создание виртуальной машины из шаблона	49
2.4.3.3	Клонирование шаблона виртуальной машины	50
2.4.3.4	Смена владельца шаблона	50
2.4.3.5	Смена группы шаблона	51
2.4.3.6	Выдача доступа группе владельца	51
2.4.3.7	Отмена доступа группе владельца	51
2.4.3.8	Удаление шаблона	51
2.4.4	Создание шаблона VM Windows	51
2.4.5	Создание шаблона VM Linux	66
2.4.6	Группировка объектов подсистемы виртуализации	75
2.4.6.1	Иерархия меток	76
2.4.6.2	Постоянные и временные метки	76
2.4.6.3	Установка и снятие метки с объекта	76
2.4.6.4	Фильтрация объектов, с помощью меток	77
2.4.6.5	Пример структуры меток подсистемы управления виртуализацией	77
2.5	Описание функций работы с виртуальными сетями	78
2.5.1	Отображение списка виртуальных сетей	78
2.5.2	Добавление виртуальной сети	79
2.5.1	Добавление виртуальной сети на основе существующей	82
2.5.2	Удаление виртуальной сети	84

2.5.1	Изменение владельца и группы виртуальной сети.	84
2.5.2	Отображение информации о виртуальной сети	85
2.5.3	Изменить параметры виртуальной сети	87
2.5.1	Изменить или добавить диапазон IP	88
2.5.2	Резервация IP	90
2.5.3	Карта сети	91
2.6	Описание функций работы с правами доступа	91
2.6.1	Описание работы с пользователями и их правами доступа	91
2.6.1.1	Создание, удаление, изменение параметров пользователя	92
2.6.2	Описание работы с группами доступа	94
2.6.3	Описание прав доступа к объектам	95
2.6.3.1	Правила ACL	97
2.7	Описание функций работы с виртуальными маршрутизаторами	100
2.7.1	Создание шаблона виртуального маршрутизатора	100
2.7.2	Создание виртуального маршрутизатора	102
2.7.3	Настройка виртуального маршрутизатора	103
2.8	Описание функций работы с МЗИ	103
2.8.1	Управление учётными записями субъектов доступа	103
2.8.2	Создание новой УЗ для работы с МЗИ	105
2.8.3	Просмотр и изменение УЗ	109
2.8.4	Блокировка УЗ	109
2.8.5	Удаление УЗ	112
2.8.6	Управление сессиями пользователей	114
2.8.7	Регистрация и мониторинг событий	115
2.8.8	Администрирование параметров управления доступом	117
2.9	Описание подсистемы обеспечения катастрофоустойчивости	120
2.9.1	Функции и работа с подсистемой	121
2.9.2	Логика функционирования подсистемы:	122
2.10	Мониторинг из внешних систем	124
2.10.1	SharxBase SNMP traps	124
2.10.2	Интерфейс управления и мониторинга IPMI	126

Настоящее руководство по эксплуатации ШБМА.466535.002РЭ.ПО (далее – РЭ) описывает принципы работы и правила эксплуатации «ПАК» и предназначено для администраторов данного комплекса.

В документе описана архитектура «ПАК», принципы его работы, принцип работы всех компонент, информации о настройке и обслуживании.

Перед началом обслуживания «ПАК», необходимо ознакомиться с данным документом.

## Перечень сокращений и терминов

Сокращение	Расшифровка
БД	База данных
БЛОК	Минимальная конфигурация ПАК
ВМ	Виртуальная машина
МЗИ	Модуль защиты информации
УЗ	Учетная запись субъекта доступа
УЗЕЛ	Минимальная единица вычислительных ресурсов, сервер.
ПАК	Программно-аппаратный комплекс
ЦОД	Центр обработки данных
SSD	Запоминающее устройство, основанное на принципе твердотельной технологии хранения данных
VNC	Протокол удалённого доступа. к рабочему столу виртуальной машины

# 1 Описание архитектуры

## 1.1 Введение

В данном разделе приводится описание архитектуры ПАК. ПАК предназначен для создания высокопроизводительной вычислительной инфраструктуры центров обработки данных (далее – ЦОД).

## 1.2 Технические характеристики

### 1.2.1 Описание

ПАК представляет собой комплекс программных и аппаратных компонент. За базовую единицу вычислений принимается узел. Узел представляет собой сервер x86\_64 архитектуры стандартного форм-фактора с установленными в него твердотельными накопителями (далее SSD) или накопителями на жестких магнитных дисках (далее HDD), высокопроизводительными процессорами и сетевой картой 10 Гбит/с, 25, 40, 50 или 100 Гбит/с, также в конфигурации может присутствовать модуль безопасности «Соболь». На встроенные SSD в рамках каждого узла, устанавливается программное обеспечение, предоставляющее вычислительные мощности конечным потребителям. В случае использования серверов высокой плотности, 4 узла агрегируют в блок.

ПАК построен на современных принципах построения вычислительной инфраструктуры:

- горизонтальное масштабирование;
- высокая производительность;
- высокая доступность и надежность;
- отсутствие единых точек отказа;
- простота в эксплуатации и обслуживании.

#### 1.2.1.1 Описание структуры комплекса

Комплекс состоит из следующих компонент:

1. Серверный узел.
2. Серверная операционная система на основе Linux.
3. Подсистема управления виртуализацией на основе открытого исходного кода.

4. Гипервизор на основе открытого исходного кода.
5. Виртуальный сетевой коммутатор на основе открытого исходного кода.
6. Распределенное хранилище данных.
7. Сеть передачи данных.
8. Подсистема мониторинга и оповещения на основе открытого исходного кода.

### 1.2.1.2 Общая схема архитектуры ПАК

Общая схема архитектуры приведена на рисунке (см. Рисунок 1).



Рисунок 1 Общая схема архитектуры решения

Для обеспечения функционирования, минимальная конфигурация должна включать в себя не менее трех узлов. Максимальное количество узлов в кластере равно 32, или 8 блоков.

### 1.2.1.3 Схема типового блока

Схема типового блока приведена на рисунке (см. Рисунок 2).





Рисунок 2 Схема типового блока (4 узла)

- Типовые узлы агрегированы в одно устройство – блок.
- Накопители, входящие в состав каждого из узлов, объединяются в единое распределенное хранилище данных.
- Добавление новых узлов/блоков увеличивает вычислительную мощность и ресурсы хранения всего кластера.
- Подсистема управления может функционировать на любом узле кластера.

#### 1.2.1.4 Схема типового узла

Схема типового узла приведена на рисунке (см. Рисунок 3).



Рисунок 3 Схема типового узла

Каждый узел предоставляет:

- устройства хранения данных;
- вычислительные ресурсы;
- доступ к сети ЛВС.

### 1.2.1.5 Описание системы управления виртуализацией на основе открытого кода

Система управления виртуализацией ПАК, построена на основе открытого исходного кода. Она интегрирует в себя управление всеми ресурсами виртуальной среды, такими как вычислительные ресурсы, ресурсы хранения, сетевые ресурсы, мониторинг и модуль безопасности.

Система управления предоставляет собой, запущенные на узлах экземпляры системы и СУБД, которая содержит всю информацию об узлах, виртуальных машинах, сетях и другую информацию. При помощи алгоритма raft, производят выбор лидера и ему присваивается плавающий IP адрес, с помощью которого производится управление всей системой, через единую консоль управления. Лидер периодически отправляет heartbeat сообщения остальным узлам кластера, для подтверждения своего статуса. В случае, если лидер вышел из строя и heartbeat сообщения не отправляются, узлы инициируют процесс выбора нового лидера. Лидер

оперирует со всеми ресурсами кластера на запись, а также реплицирует все изменения БД на остальные узлы кластера.

#### 1.2.1.6 Описание виртуального сетевого коммутатора

Виртуальный сетевой коммутатор, установленный на каждом узле, представляет собой программное обеспечение управляющее сетевым трафиком между аппаратным интерфейсом узла и сетевыми интерфейсами виртуальных машин, централизованное управление виртуальными коммутаторами производится системой управления виртуализацией.

#### 1.2.1.7 Описание подсистемы мониторинга

Подсистема мониторинга представляет собой распределенную систему мониторинга, установленную на каждом из узлов кластера и предоставляющую данные о состоянии «ПАК» системе управления виртуализацией, которая отображает эти данные пользователям «ПАК».

#### 1.2.1.8 Описание распределенного хранилища данных.

Распределенное хранилище данных (РХД) объединяет локальные SSD диски каждого узла в кластере, в единый пул, предоставляющий ресурсы хранения вычислительным узлам и виртуальным машинам. Программное обеспечение распределённого хранилища данных, устанавливается на каждом узле в кластере и предоставляет хранилище операционной системе узла в виде блочного устройства.

Для исключения единой точки отказа хранилище использует коэффициент отказоустойчивости (уровень репликации). Коэффициент описывает количество синхронных копий данных, в кластере, он коррелирует с количеством узлов в кластере, которые могут выйти из строя без потери данных и падения производительности. При минимальной конфигурации из трех узлов, коэффициент отказоустойчивости равен 2, выход из строя 1 узла, не приводит к отсутствию доступа и потере целостности данных. При конфигурации, состоящей из 4 и более узлов, коэффициенте отказоустойчивости равен 3, выход из строя 2 узлов, не приводит к отсутствию доступа и потере целостности данных.

Хранилище защищает данные от потери и гарантирует их целостность с помощью 64-битной контрольной суммы и ведении версионности, для каждого контролируемого сектора. В отличие от других технологий хранения данных, таких как RAID или ZFS, хранилище не полагается на дублирование данных на устройства, поэтому каждый диск, добавленный пул, добавляет емкость и производительность кластеру, причем не только для новых данных, но и

для существующих. При наличии достаточных копий данных, диски могут быть добавлены или удалены без потери производительности и доступа к ним.

Каждый узел отвечает за данные, хранящиеся на его локальных дисках. Узлы взаимодействуют друг с другом для предоставления доступа клиентам. Подсистема предоставляет общий пул хранения, объединяющий все доступные емкости. Подсистема хранения состоит из двух частей - сервера хранения и клиента хранилища, которые установлены на каждом физическом узле. Каждый узел выступает в обеих ролях. Для клиентов хранилища, тома предоставляются в виде блочных устройств в /dev/\* и дальнейшая работа с ними производится как с обычными дисковыми устройствами. Данные по томам могут считываться и записываться всеми клиентами одновременно, согласованность чтения и записи гарантируется с помощью протокола синхронной репликации.

### 1.2.1.9 Максимальные конфигурации ВМ

Максимумы виртуальной машины представляют ограничения, применимые к вычислениям, памяти, виртуальным адаптерам и устройствам хранения, виртуальным сетевым устройствам, виртуальным периферийным портам и графическим видеоустройствам.

Таблица 1 Список подсетей

Параметр	Максимум
<b>Вычислительные ресурсы</b>	
vCPU	384
<b>Память</b>	
ОЗУ ВМ	4ТВ
<b>Виртуальные адаптеры и устройства хранения данных</b>	
Размер виртуального диска	неограниченно*
IDE контроллеры для одной ВМ	28**
IDE устройства для одной ВМ	28**
IDE CDROM для одной ВМ	28**
Виртуальные SATA адаптеры для одной ВМ	28**
Виртуальные SATA устройства для одного виртуального SATA адаптера	28**
<b>Виртуальные сетевые устройства</b>	
Виртуальные сетевые адаптеры для одной ВМ	28**
<b>Виртуальные периферийные порты</b>	

USB хост контроллеры для одной VM	28**
USB устройства, подключенные к VM	28**
Параллельные порты для одной VM	28**
Серийные порты для одной VM	28**

\* хранилище данных на ПАК SharXbase не ограничивает размер виртуального диска для VM, можно задать любой размер, будет создан тонкий диск, который будет расти и занимать место только пропорционально своего реального объема, умноженного на фактор репликации; ограничение по объему будет наступать только при заполнении самого хранилища при достижении 90%

\*\* ограничение KVM на использование 32 PCI устройства, из них 4 обязательных (host bridge, usb and isa bridge, graphics cards, memory balloon device) и 28 подключаемых.

#### 1.2.1.10 Максимальные конфигурации серверного узла

Максимумы узла будут зависеть от выбранной модели серверной платформы и обычно подбираются в зависимости от задач заказчика, тем не менее платформа имеет рассчитанную и проверенную мощность для вычислительных ресурсов, памяти, хранилища, сетевых максимумов, кластера и пула ресурсов.

Таблица 2 Максимумы узла

Параметр	Максимум
<b>Вычислительные ресурсы</b>	
Логические CPU	768
<b>Виртуальные машины</b>	
VM на узел	250*
vCPU на узел	4096
vCPU на 1 ядро	32
<b>Память</b>	
ОЗУ на хост	12TB
SWAP файлы	1 на VM
<b>Хранилище данных</b>	
Виртуальные диски на хост	1000

\* при ограничении ресурсов на ВМ и использовании не более одного аттачмента на ВМ возможно масштабирование до 1000 ВМ на узел

### 1.2.1.11 В Максимальные конфигурации сети

Максимумы сети представляют собой достижимые максимальные пределы конфигурации в сетевых средах.

Таблица 3 Максимумы узла

Параметр	Максимум
<b>Физические сетевые карты</b>	
igbn 1 GB Ethernet ports (Intel)	16
ixgbe 10 GB Ethernet ports (Intel)	16
nmlx4_en 40 GB Ethernet Ports (Mellanox)	4
nmlx5_core 25 GB Ethernet Ports (Mellanox)	4
nmlx5_core 100 GB Ethernet Ports(Mellanox)	4
i40en 10 GB Ethernet Ports (Intel)	8
i40en 40 GB Ethernet Ports (Intel)	4
<b>SR-IOV</b>	
SR-IOV количество виртуальных функций на хост	1024
SR-IOV количество физических 10G сетевых карт на хост	8

### 1.2.1.12 Максимальные конфигурации кластера

Максимумы кластера представляют собой достижимые максимальные пределы конфигурации в пределах одного кластера SharXbase, состоящего из нескольких блоков.

Таблица 4 Максимумы узла

Параметр	Максимум
Количество хостов/узлов в кластере	64
Количество блоков	8
Хранилище	

Количество объектов в хранилище (моментальные снимки, тома)	30000
Количество VM на кластер	8000
Размер диска в хранилище	4ТВ (если объем больше, такой диск нужно разбить на партиции)
Объем хранилища	не ограничен

### 1.2.1.13 Поддерживаемые ОС и апплайны для VM

В таблице перечислены поддерживаемые операционные системы для виртуальных машин, в случае отсутствия ос, необходимо отправить запрос в техническую поддержку, для уточнения возможности ее установки и проведения тестирования, для добавления в данный список.

Таблица 5 – Список поддерживаемых операционных систем

Наименование
Microsoft Windows Server 2003 R2, 2008, 2008 r2, 2012R2, 2016
Microsoft Windows Vista, 7, 8, 8.1, 10
Red Hat Enterprise Linux 6, 7
CentOS 6, 7
Fedora (28 – 30)
SUSE Linux Enterprise server (11 – 13)
Oracle Linux (7.0 – 7.5)
Alt Server 8.2
Astra Linux Special Edition (1.2 – 1.6)
Astra Linux Common Edition (1.11 – 2.12)
Ubuntu Server (18.04.2, 19.04)
Ubuntu (14.04, 16.04, 18.04, 18.10, 19.04)
Debian 7.0 – 10.0
Alpine Linux 3.6
Alpine Linux 3.7
Alpine Linux 3.8

Amazon Linux 2
Devuan 1-2
FreeBSD 11-12

Таблица 6 – Список поддерживаемых виртуальных аплайнсов

Наименование
Zabbix Appliance
Vrouter Alpine



## 2 Установка и настройка

### 2.1 Рекомендации по настройке сети

Таблица 7 Список стандартных логинов, паролей, адресов доступа

Описание	Адрес	Логин	Пароль
Веб-консоль управления ПАК	http://X.X.X.190/	sdcadmin	Sharx2018
SSH-консоль управления ПАК	ssh sdcadmin@X.X.X.190	sdcadmin	Sharx2018
Консоль SSH узла 01-32	ssh://X.X.X.11-44	sdcadmin	Sharx2018
Интерфейс управления узлом 01-32 (IPMI)	http://X.X.Y.11-44	root	Sharx2018
Шаблон виртуальной машины Linux	CentOS_tmpl	root	Sharx2018
Шаблон виртуальной машины Windows	Windws_tmpl	sdcadmin	Sharx2018

\* root-доступ узлам по SSH производится только сотрудниками технической поддержки производителя, в случае несогласованного доступа компания может лишиться контракта на поддержку, пользователь sdcadmin, имеет права на работу с ПАК, команды описаны далее.

В случае использования коммутаторов на базе ОС Cumulus, необходимо учесть зарезервированные VLAN для работы ОС, они отображены в таблице «Список подсетей», количество и номера этих VLAN могут быть изменены, в случае если они конфликтуют с пользовательскими VLAN. Минимальное обязательное количество равно 100, изменение размера и нумерации, необходимо учитывать при проектировании системы.

Таблица 8 Список подсетей

Описание	VLAN	Сеть	Шлюз
Подсеть управления	2	X.X.X.0/24	X.X.X.1
Подсеть продуктивная	3	X.X.Y.0/24	X.X.Y.1
Подсеть РХД	4	X.X.Z.0/24	X.X.Z.1
Зарезервированные VLAN Cumulus	3000-3999		

Таблица 9 Список TCP/UDP портов необходимых для доступа к ПАК

Описание	Порт	Протокол
Консоль веб-управления	80/443	TCP
Подсистема мониторинга	80/6443	TCP
Консоль SSH узла 01-32	22	TCP

Интерфейс управления узлом 01-32 (IPMI)	80	TCP
VNC доступ к виртуальным машинам	29876	TCP

## 2.1 Первичная настройка и подготовка узла

После монтажа оборудования, в соответствии с руководством по эксплуатации аппаратного обеспечения «ПАК», необходимо произвести проверку корректности настроек BIOS, для дальнейшей работы с «ПАК».

### 2.1.1 Настройка системы управления IPMI узла

Для входа в BIOS, необходимо включить/перезагрузить сервер. Во время загрузки сервера, нажав кнопку F2 на клавиатуре, перейти в меню настройки BIOS. Далее перейти в раздел Setup Menu → Server Management → BMC LAN Configuration. В данном разделе необходимо проверить корректность настроек IP адреса управления узла, в соответствии с таблицей IP адресов (см. Таблица 10)

Таблица 10 Параметры IPMI

Baseboard LAN configuration	
IP Source	Static
IP Address	X.X.Y.11
Subnet Mask	255.255.255.0
Gateway IP	X.X.Y.1
Dedicated Management LAN Configuration	
Remote management module	Present
IP Source	Static
IP Address	X.X.Y.11
Subnet Mask	255.255.255.0
Gateway IP	X.X.Y.1

Далее перейти в раздел User Configuration, в данном разделе задать пользователя (см Таблица 7) строка «Интерфейс управления узлом».

Таблица 11 Задаваемые параметры IPMI

Параметр	Значение
User ID	root
Privilege	Administrator
User Status	Enabled
User Password	Sharx2005

После внесенных изменений, нажмите кнопку F10, теперь доступ к консоли управления сервера, возможен через веб-интерфейс.

В случае если доступ к консоли управления узлами IPMI уже имеется, производить настройки, описанные в данном разделе не нужно.

Параметры BIOS, настроены на заводе производителя, изменение остальных параметров, не связанных с доступом к IPMI, может привести к выходу из строя или деградации производительности системы.

## 2.2 Описание входа в систему

Для входа в систему, необходимо запустить браузер на рабочем компьютере и ввести адрес веб-консоли управления (Например: <http://10.0.128.190/>). В поле логин и пароль, ввести данные учетной записи (см Рисунок 4). Для настройки работы ПАК, по протоколу https, необходимо обратиться в службу технической поддержки и предоставить ssl сертификат, для его установки в систему.

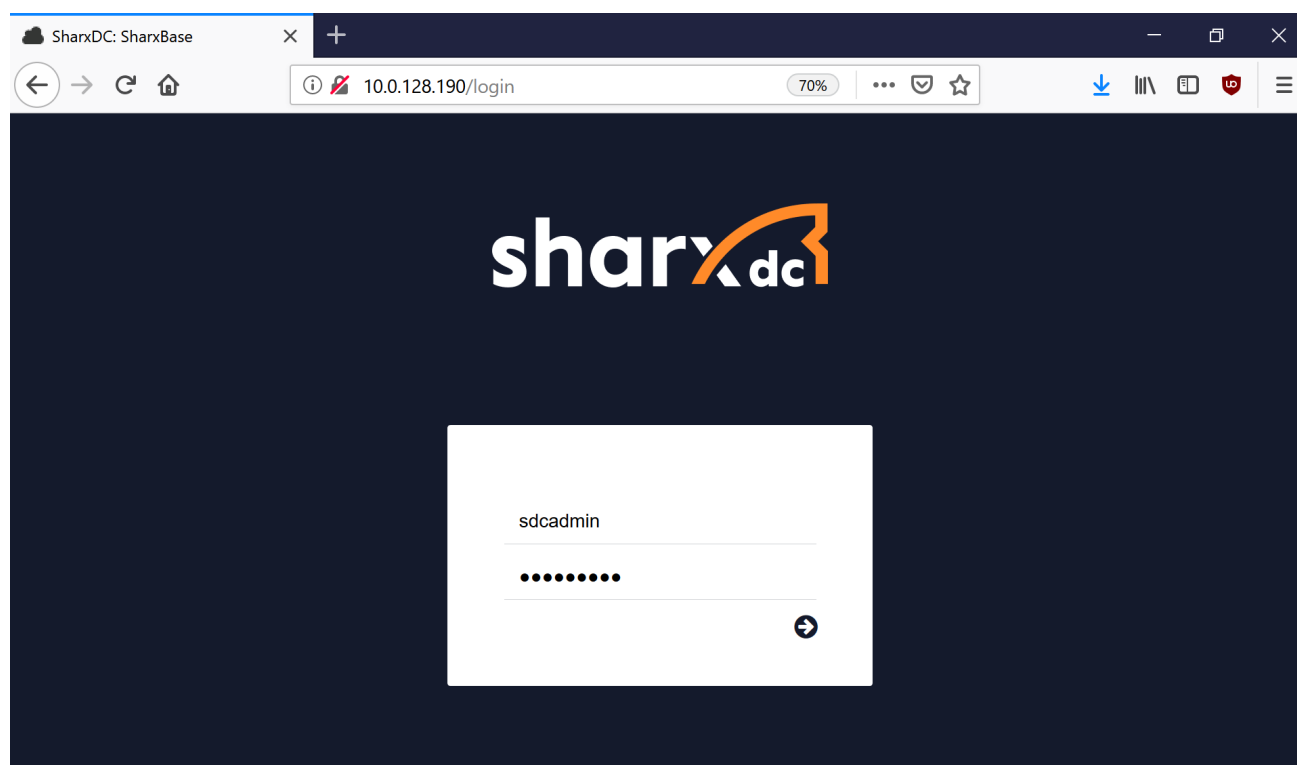


Рисунок 4 Окно входа в систему.

После успешного входа в систему, на экране появится главное окно консоли управления, с графиками нагрузки ЦПУ, ОЗУ, списком узлов и виртуальных машин (см Рисунок 5).

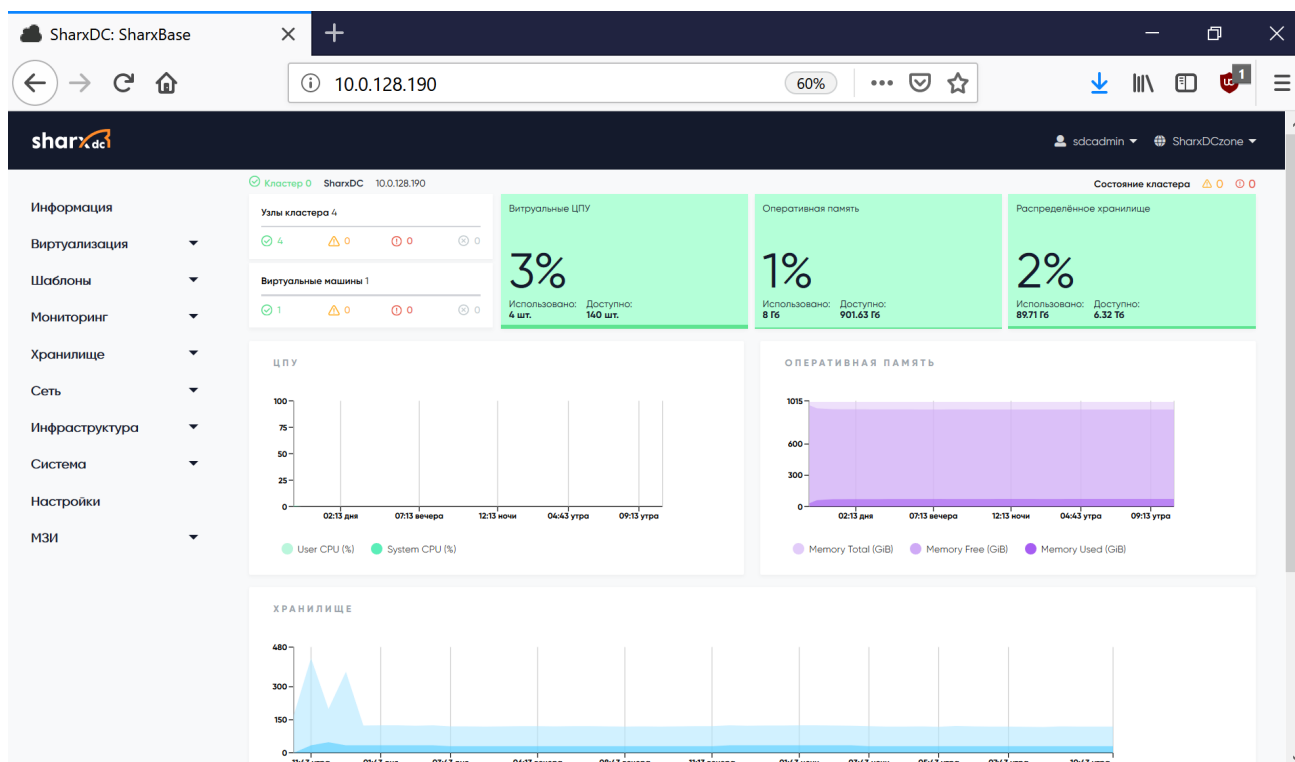


Рисунок 5 Главное окно консоли управления.

Также работу с системой можно проводить с помощью командной строки, путем подключения к системе с помощью протокола SSH. Данный функционал необходим только при работе с технической поддержкой «ПАК», все функции «ПАК» реализованы в веб-консоли управления.

Для управления системой из командной строки используются команды (см Таблица 12).

Таблица 12 Список команд управления.

Команда	Описание
sdacct	Инструмент учета и визуализации используемых ресурсов
sdcacl	Команда управления списками контроля доступа
sdcluster	Команда управления кластером
sdcdastore	Команда управления хранилищем данных
sdcdb	Команда управления базой данных системы
sdcgrouo	Команда управления группами системы
sdchost	Команда управления узлами системы
sdcmage	Команда управления образами системы
sdctemplate	Команда управления шаблонами системы
sduser	Команда управления пользователями системы
sdcvm	Команда управления виртуальными машинами
sdcvnet	Команда управления виртуальной сетью

Команда	Описание
sdcsecgroup	Команда управления группами безопасности
sdcvrouter	Команда управления виртуальным роутером

Ниже будут описаны все функции по управлению системой.

## 2.3 Описание функций управления физическими узлами

Информацию о подключенных узлах и их статусах можно получить на вкладке «Инфраструктура» → «Узлы», веб-консоли управления «ПАК». При входе в данный раздел отображается список узлов их наименование, название кластера, количество запущенных ВМ, объем выделенного ЦПУ, объем выделенного ОЗУ и статус узла.

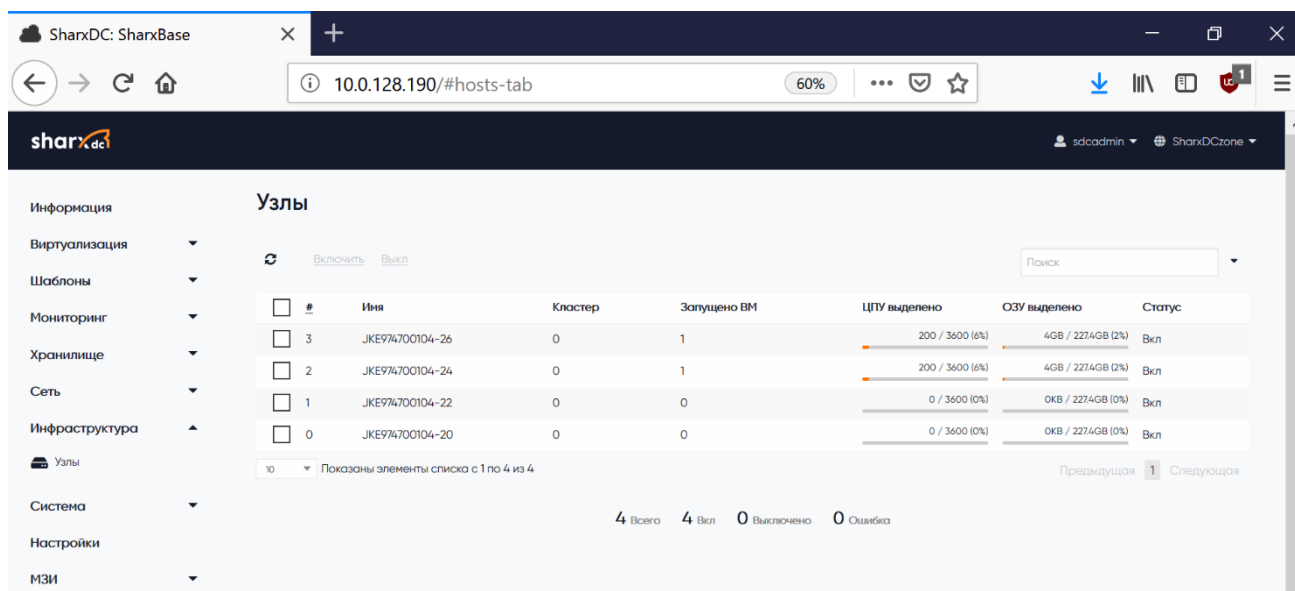


Рисунок 6 Список узлов

Для отображения информации о конкретном узле, нужно зайти в раздел описания данного узла, наведя курсор мыши на его название и нажав левую кнопку мыши. В данном разделе находится пять вкладок, информация, графики, серверы, незарегистрированные ВМ, зомби (см. Рисунок 7).

Информация об узле содержит:

- общую информацию об узле, включая его имя и драйверы, с которыми он взаимодействует;
- информация о используемых ЦПУ и оперативной памяти;
- информацию о мониторинге, включая устройства PCI;

– информацию о виртуальных машинах, запущенные на узле. Wild - это виртуальные машины, запущенные на узле, но не запущенные при помощи системы виртуализации, они могут быть в нее импортированы.

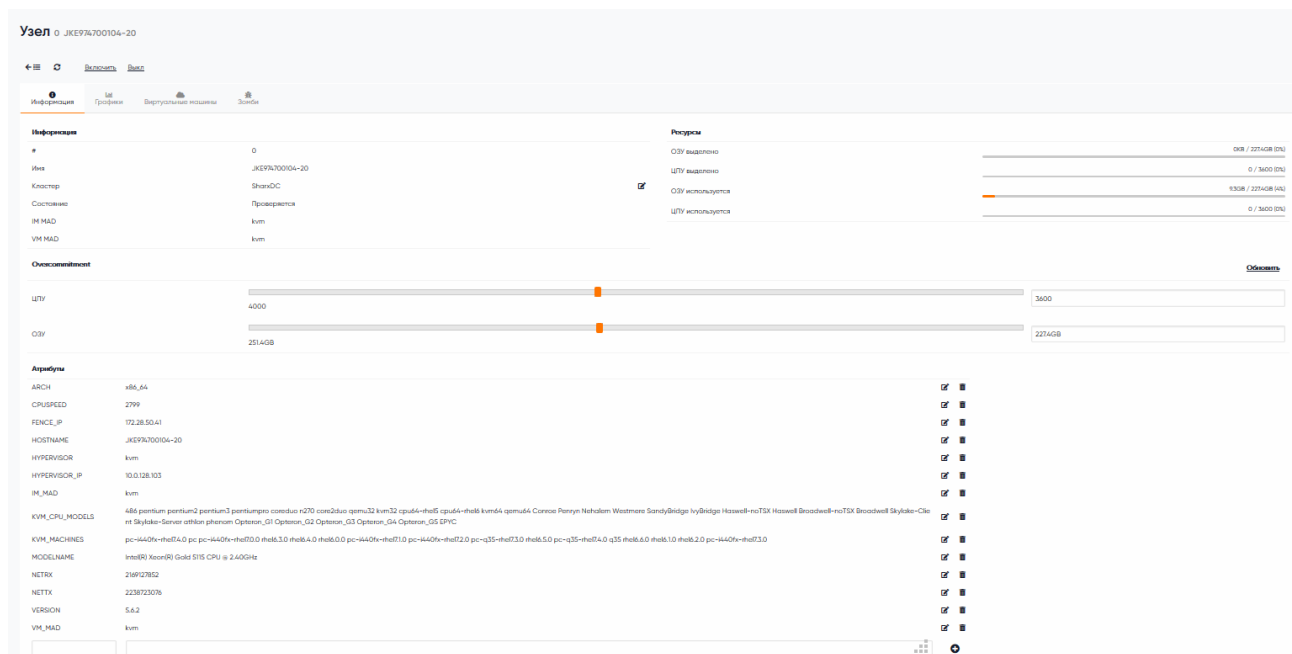


Рисунок 7 Окно отображения параметров узла

Для отображения служебной информации об узле с помощью командной строки, необходимо использовать команду `sdchost show`:

```
$ sdchost show JKE974700104-20
HOST 0 INFORMATION
ID : 0
NAME : JKE974700104-20
CLUSTER : SharxDC
STATE : MONITORED
IM_MAD : kvm
VM_MAD : kvm
LAST MONITORING TIME : 01/24 11:25:33

HOST SHARES

RUNNING VMS : 0

MEMORY
TOTAL : 251.4G
TOTAL +/- RESERVED : 227.4G
USED (REAL) : 9.3G
```

```

USED (ALLOCATED)      : 0K
CPU
TOTAL                 : 4000
TOTAL +/- RESERVED   : 3600
USED (REAL)          : 0
USED (ALLOCATED)     : 0

MONITORING INFORMATION
ARCH="x86_64"
CPUSPEED="2799"
FENCE_IP="172.28.50.41"
HOSTNAME="JKE974700104-20"
HYPERVISOR="kvm"
HYPERVISOR_IP="10.0.128.103"
IM_MAD="kvm"
KVM_CPU_MODELS="486 pentium pentium2 pentium3 pentiumpro coreduo n270 core2duo q
emu32 kvm32 cpu64-rhel5 cpu64-rhel6 kvm64 qemu64 Conroe Penryn Nehalem Westmere
SandyBridge IvyBridge Haswell-noTSX Haswell Broadwell-noTSX Broadwell Skylake-Cl
ient Skylake-Server athlon phenom Opteron_G1 Opteron_G2 Opteron_G3 Opteron_G4 Op
teron_G5 EPYC"
KVM_MACHINES="pc-i440fx-rhel7.4.0 pc pc-i440fx-rhel7.0.0 rhel6.3.0 rhel6.4.0 rhe
16.0.0 pc-i440fx-rhel7.1.0 pc-i440fx-rhel7.2.0 pc-q35-rhel7.3.0 rhel6.5.0 pc-q35
-rhel7.4.0 q35 rhel6.6.0 rhel6.1.0 rhel6.2.0 pc-i440fx-rhel7.3.0"
MODELNAME="Intel(R) Xeon(R) Gold 5115 CPU @ 2.40GHz"
NETRX="2165326240"
NETTX="2234220667"
RESERVED_CPU="400"
RESERVED_MEM="25165824"
VERSION="5.6.2"
VM_MAD="kvm"

WILD VIRTUAL MACHINES

NAME                                     IMPORT_ID  CPU      MEM
ORY

VIRTUAL MACHINES

ID USER      GROUP      NAME          STAT  UCPU  UMEM  HOST      TIME

```

Для отображения информации обо всех узлах необходимо воспользоваться командой `sdchost list`:

```
$ sdchost list
```

ID	NAME	CLUSTER	TVM	ALLOCATED_CPU	ALLOCATED_MEM	STAT
0	JKE974700104-20	SharxDC	0	0 / 3600 (0%)	0K / 227.4G (0%)	on
1	JKE974700104-22	SharxDC	0	0 / 3600 (0%)	0K / 227.4G (0%)	on
2	JKE974700104-24	SharxDC	1	200 / 3600 (5%)	4G / 227.4G (1%)	on
3	JKE974700104-26	SharxDC	1	200 / 3600 (5%)	4G / 227.4G (1%)	on

Выводимая информация также может быть отображена в формате XML при использовании ключа -x.

Узлы содержат дополнительную информацию для мониторинга. Есть возможность использовать эти переменные для создания собственных выражений учета ранжирования (RANK) и требований к размещению виртуальных машин (REQUIREMENTS) для планирования исполнения виртуальных машин. Можно также вручную добавить любой атрибут и использовать его также для RANK и REQUIREMENTS. Переменные, содержащие дополнительную информацию для мониторинга (см. Таблица 13).

Таблица 13 Список переменных для мониторинга

Переменная	Описание
HYPERVISOR	Имя гипервизора узла (полезно для выбора узлов с определенной технологией)
ARCH	Архитектура центрального процессора, например, x86_64.
MODEL_NAME	Название модели хост-процессора, например, Intel (R) Core (TM) i7-2620M CPU @ 2.70GHz.
CPUSPEED	Скорость CPU в МГц.
HOSTNAME	Имя узла
VERSION	Версия сенсоров мониторинга. Используется для контроля локальных изменений и процесса обновления
MAX_CPU	Число CPU, умноженное на 100. Например, машина с 16 ядрами будет иметь значение 1600. Значение RESERVED_CPU будет вычитаться из информации, сообщаемой системой мониторинга. Это значение отображается как TOTAL CPU полученное командой sdchost show (секция HOST SHARE).
MAX_MEM	Максимальная память, которую можно использовать для виртуальных машин. Рекомендуется вычитать память, используемую гипервизором, задавая ее с помощью RESERVED_MEM. Это значение вычитаются из указанного объема памяти. Значение отображается как TOTAL MEM полученное командой sdchost show (секция HOST SHARE).
MAX_DISK	Общий объем дискового пространства в мегабайтах в DATASTORE LOCATION.
USED_CPU	Процент используемого ЦП, умноженного на количество ядер. Это значение отображается как USED_CPU (REAL) полученное командой sdchost show (секция HOST SHARE).



Переменная	Описание
USED_MEM	Используемая память, в килобайтах. Это значение отображается в виде USED_MEM (REAL) полученное командой <code>sdchost show</code> (секция HOST SHARE).
USED_DISK	Используемое дисковое пространство в мегабайтах в DATASTORE LOCATION.
FREE_CPU	Процент неиспользуемой мощности процессора, умноженное на количество ядер. Например, если 50% CPU не используется в 4-ядерном компьютере, значение будет 200.
FREE_MEM	Доступная память для виртуальных машин в данный момент, в килобайтах.
FREE_DISK	Свободное дисковое пространство в мегабайтах в DATASTORE LOCATION
CPU_USAGE	Общее количество CPU выделенное для виртуальных машин, работающих на хосте, как это предусмотрено в параметре CPU в каждом шаблоне виртуальной машины. Это значение отображается как USED CPU (ALLOCATED) полученное командой <code>sdchost show</code> (секция HOST SHARE).
MEM_USAGE	Общее количество оперативной памяти, выделенное для виртуальных машин, работающих на хост - компьютере в соответствии со значением параметра MEMORY в каждом шаблоне виртуальной машины. Это значение отображается как USED MEM (ALLOCATED) полученное командой <code>sdchost show</code> (секция HOST SHARE).
DISK_USAGE	Общее количество дискового пространства, выделенное под образы дисков виртуальных машин, запущенных на хосте вычисленное с учетом атрибута SIZE каждого образа и с учетом характеристик хранилища данных.
NETRX	Получено из сети, байт.
NETTX	Передано в сеть, байт.
WILD	Список имен виртуальных машин, разделенных запятыми, запущенных на хосте, которые не были запущены системой управления виртуализацией и в настоящее время ею не контролируются.
ZOMBIES	Список имен виртуальных машин, разделенных запятыми, запущенных на хосте, которые были запущены системой управления виртуализацией, но в настоящее время ею не контролируются.

### 2.3.1 Управление статусом узла: подключение, отключение, вывод в автономный режим и перенос

Узел может находиться в разных системных состояниях, его можно настроить на разные режимы работы: включено (on), отключено (dsbl) и автономно (off). Различное рабочее состояние для каждого режима описано в таблице (см. Таблица 14):

Таблица 14 Список состояний узла

Статус	Состояние узла
Вкл(on)	Узел полностью работоспособен
Обновление (update)	Мониторинг узла
Выкл (dsbl)	Отключено, например, для выполнения операций технического обслуживания
Автономный (off)	Узел полностью отключен
Ошибка (error)	Ошибка при мониторинге узла, используйте <code>sdchost show</code> для описания ошибки.
Повтор (retry)	Контроль узла в состоянии ошибки

Для изменения статуса узла, необходимо выбрать узел, и перевести его в нужный режим, Включить, Выключить (см. Рисунок 8).

**Узлы**

Включить Выкл Поиск

<input type="checkbox"/>	#	Имя	Кластер	Запущено VM	ЦПУ выделено	ОЗУ выделено	Статус
<input type="checkbox"/>	3	ЖКЕ974700104-26	0	1	200 / 3600 (6%)	4GB / 227.4GB (2%)	Вкл
<input type="checkbox"/>	2	ЖКЕ974700104-24	0	1	200 / 3600 (6%)	4GB / 227.4GB (2%)	Вкл
<input type="checkbox"/>	1	ЖКЕ974700104-22	0	0	0 / 3600 (0%)	0KB / 227.4GB (0%)	Вкл
<input checked="" type="checkbox"/>	0	ЖКЕ974700104-20	0	0	0 / 3600 (0%)	0KB / 227.4GB (0%)	Вкл

10 Показаны элементы списка с 1 по 4 из 4 Предыдущая 1 Следующая

4 Всего 4 Вкл 0 Выключено 0 Ошибка

Рисунок 8 Окно изменения статуса узлов

Инструмент `sdchost` содержит три команды для соответственно выключения, перевода в автономный режим и подключения узла: `disable`, `offline` и `enable`

Примеры их выполнения:

```
$ sdchost disable 0
$ sdchost offline 0
$ sdchost enable 0
```

Где, 0 – ID узла, которое было получено при вводе команды

```
$ sdchost show JKE974700104-20
```

Также для работы с узлами применяют команду `flush`. Данная команда помечает исполняющиеся на узле виртуальные машины как подлежащие переносу, т.е. планируемые к переносу на другой узел, способный обеспечить необходимые ресурсы. Одновременно узел помечается как выключенный, чтобы новые виртуальные машины не могли быть распределены на него. Это команда используется если есть необходимость освободить узел от исполняющихся на нем виртуальных машин.

### 2.3.2 Управление атрибутами узла и политиками управления.


Атрибуты узла устанавливаются при помощи мониторинга, который время от времени активизируются на узле с целью сбора информации. Администратор может создавать собственные атрибуты либо при создании атрибутов на узле, либо при помощи команды `sdchost update`. Для маркировки узла атрибутом «production», необходимо зайти в раздел описания узла, в нижней части окна, нажать на кнопку . Внести название атрибута и его значение (см. Рисунок 9).



Рисунок 9 Окно ввода атрибута

Например, маркировка узла атрибутом «production» с добавлением собственного атрибута `TYPE`, необходимо ввести команду `sdchost update ID`, где `ID`, порядковый номер узла. После чего добавить в конец конфигурационного файла `TYPE="production"`.

```
$ sdchost update 0
.....
TYPE="production"
```

Этот атрибут может быть использован впоследствии для целей планирования исполнения виртуальной машины путем добавления нужной секции в шаблон виртуальной машины:

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

Этот атрибут запрещает запуск виртуальной машины на узлах, у которых атрибут `TYPE=production`.

Эта функция может быть полезна, если необходимо выделить набор узлов или отметить некоторые особенности разных узлов. Эти значения затем могут быть использованы для планирования исполнения виртуальных машин в качестве требования к месту размещения.

## **2.4 Описание функций управления виртуальными машинами**

В данном разделе описаны основные функции, связанные с работой экземпляров виртуальных машин, шаблонов виртуальных машин и образами дисков виртуальных машин.

### **2.4.1 Описание функций управления экземплярами виртуальных машин**

#### **2.4.1.1 Отображение списка виртуальных машин**

Информацию о созданных экземплярах виртуальных машин и их статусах можно получить на разделе «Виртуализация» → «Виртуальные машины». При переходе на данную вкладку, отображается список виртуальных машин их параметры:

- Уникальный идентификатор виртуальной машины;
- Наименование виртуальной машины;
- Статус виртуальной машины;
- Имя узла, на котором запущен экземпляр виртуальной машины;
- IP адрес виртуальной машины;
- Ярлык для запуска VNC сессии к виртуальной машине.

По умолчанию на странице отображается список из 10 экземпляров виртуальных машин, остальные виртуальные машины отображены на следующих страницах данного раздела. Для изменения количество одновременно отображаемых на странице виртуальных машин необходимо в нижнем левом углу изменить данный параметр, возможны следующие значения 10, 25, 50, 100. Для перехода на следующую страницу, в нижнем правом углу, необходимо выбрать страницу, на которую необходимо перейти (см. Рисунок 10).

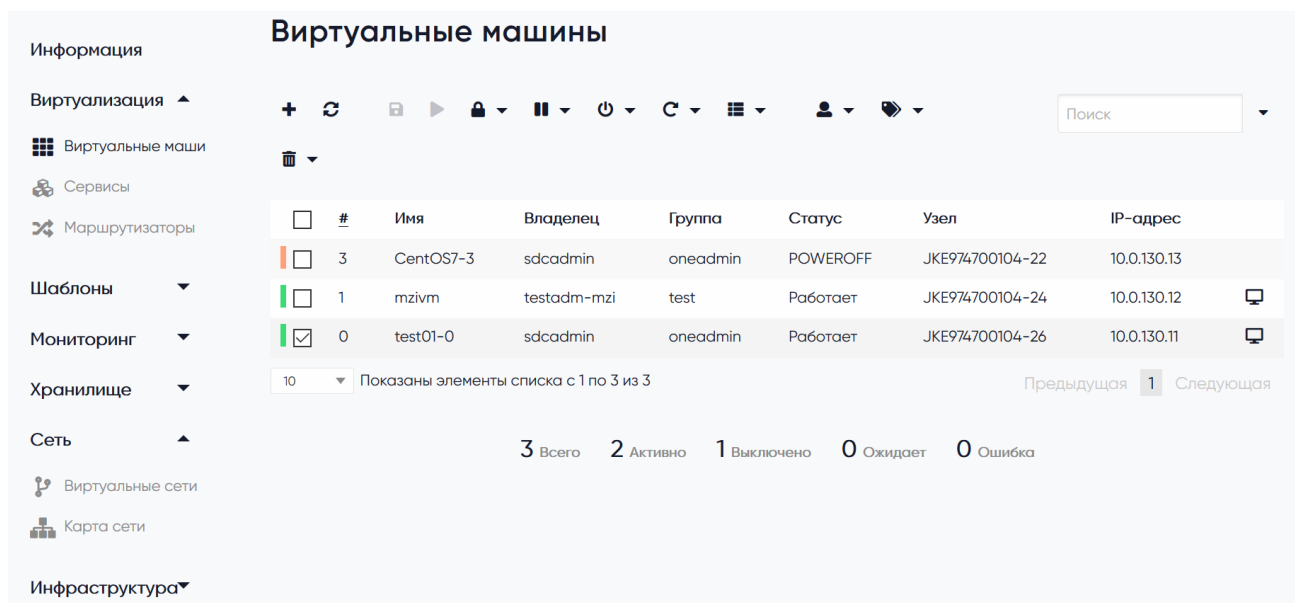



Рисунок 10 Список виртуальных машин

Для отображения списка виртуальных машин необходимо использовать команду `sdccvm list`.

```
# sdccvm list
ID USER      GROUP      NAME          STAT UCPU    UMEM HOST          TIME
  0 sdccadmin oneadmin  test01-0      runn  0.0    4G JKE9747001  1d 01h48
  1 testadm- test    mzivm         runn  0.0    4G JKE9747001  1d 01h45
  3 sdccadmin oneadmin  CentOS7-3     poff  0.0    0K JKE9747001  0d 00h24
```

### 2.4.1.2 Создание виртуальной машины из шаблона

Для создания виртуальной машины из шаблона, необходимо зайти в раздел «Виртуализация» → «Серверы», далее нажать кнопку , выбрать нужный шаблон. В появившемся окне задать параметры создаваемой ВМ (см. Рисунок 11):

- Имя ВМ;
- Количество экземпляров;
- Параметр «Создать и не включать»;
- ОЗУ;
- Размер системного диска;
- Количество ЦПУ;
- Количество вЦПУ;
- Сетевой интерфейс.

После выбора всех необходимых параметров, нажать кнопку «Создать».

Укажите параметры виртуальной машины

← Очистить все поля Создать

Вы выбрали следующий шаблон: CentOS7

#	Имя	Владелец	Группа	Время регистрации
1	CentOS7	sdccadmin	oneadmin	24/01/2019 13:03:14
0	test01	sdccadmin	oneadmin	23/01/2019 12:05:50

Показаны элементы списка с 1 по 2 из 2

Инициализировать как постоянную

Имя VM:  Количество экземпляров:   Создать и не включать

**CentOS7**

**Ресурсы**

ОЗУ:  Гб

ЦПУ:  Виртуальные ЦПУ:

**Диски**

ДИСК 0: CentOS7ays  Гб

- Сеть
- Instantiate as different User / Group
- Развернуть VM на определенном узле
- Развернуть VM на определенном хранилище
- Schedule Actions for VM
- Associate VM to a VM Group

Рисунок 11 Окно ввода параметров создаваемой VM

Для создания виртуальной машины из шаблона, с помощью командой строки, необходимо получить ID или название шаблона из которого планируется разворачивать VM и после этого инициировать процесс создания VM.

```
[root@Bqb364590047-24 ~]# sdctemplate list
ID USER          GROUP          NAME          REGTIME
  0 sdccadmin      oneadmin      test01        01/23 12:05:50
  1 sdccadmin      oneadmin      CentOS7       01/24 13:03:14
[root@Bqb364590047-24 ~]# sdctemplate instantiate 0 --name CentosFromTpl
VM ID: 1
```

### 2.4.1.3 Изменение статуса виртуальной машины

Экземпляр виртуальной машины может находиться в нескольких системных состояниях (см. Таблица 15).

Таблица 15 Список системных состояний VM

Статус	Описание
Ожидание (Pending)	По умолчанию, после создания, VM находится в состоянии «Ожидание», ожидая выделения ресурсов для нее. VM останется в этом состоянии, пока либо система либо пользователь не развернет.
Hold	Владелец задал параметры VM и задал параметр «Создать и не включать». VM не зарезервировала ресурсы, может быть переведена в статус «Ожидание» для дальнейшего запуска.
Клонирование (Cloning)	VM ожидает окончания клонирования образа или образов дисков.
Prolog	Система изменяет или устанавливает ссылки на образы дисков, для запуска на узле.
Старт (Boot)	Система ожидает от гипервизора запуска VM.
Работает (Running)	VM находится в состоянии «Работает», это включает в себя загрузку, работу и выключение самой VM внутри гипервизора.
Migrate	VM мигрирует с одного узла на другой. Это может быть live или стандартная миграция с выключением VM.
Hotplug	Идет процесс подключения или отключения виртуального диска или сетевой карты.
Snapshot	Выполняется процесс снапшотирования VM
Save	Система сохраняет файлы VM после миграции, остановки или приостановки.
Epilog	На этом этапе система очищает ресурсы узла после приостановки или выключения VM, параллельно сохраняя данные дисков на хранилище.
Shutdown	Система отправляет команду выключения с помощью ACPI сигнала виртуальной машине, ожидая выполнения этой команды, для завершения процесса выключения. Если после таймаута VM не выполнит данную команду, система посчитает что VM игнорирует ACPI сигнал и изменит системное состояние VM в running.
Stopped	Виртуальная машина приостановлена. Данные VM были сохранены на хранилище.
Suspended	Виртуальная машина приостановлена, для дальнейшего запуска на этом хосте. Нет необходимости определять хоста для запуска VM.
PowerOff	Виртуальная машина в состоянии выключена, после отправки сигнала shutdown
Undeployed	VM выключена, может быть запущена позже.
Failed	VM в состоянии ошибка.
Unknown	Система не может получать данные о VM, VM в неизвестном состоянии.
Cleanup-resubmit	VM в ожидании очистки узла, после команды восстановления статуса VM.
Done	VM в состоянии done, после команды terminate (удалить).

Изменение состояния экземпляра виртуальной машины производится на вкладке «Виртуализация» → «Виртуальные машины».

Таблица 16 Список команд управления VM

Команда	Описание
VNC	Запустить VNC консоль VM.
Сохранить как шаблон	Команда сохраняет VM как шаблон.
Включить (Resume)	Включение виртуальной машины из состояний stopped, suspended, undeployed и poweroff.
Приостановить работу VM (Suspend)	Состояние виртуальной машины сохранено на конкретном узле, после отправки команду включить, она будет запущена на этом узле, в сохранённом состоянии.
Остановить (Stop)	Состояние виртуальной машины сохранено, но VM отвязана от узла.
Отключить питание (Shutdown) poweroff	Корректное выключение экземпляра виртуальной машины, путем отправления ACPI сигнала виртуальной машине. В случае если VM не выполнила данную команду по таймауту, VM перейдет в состояние «Работает».
Отключить питание (немедленно) Power off (hard).	VM будет выключена немедленно, данную функцию нужно использовать при отсутствии поддержки ACPI виртуальной машиной.
Отменить размещение (Undeploy).	Система отправляет VM ACPI сигнал на выключение и очистку ресурсов хоста от данной VM.
Отменить размещение (немедленно) (Undeploy hard)	Система выключает VM немедленно и производит очистку ресурсов хоста от данной VM.
Перезагрузить (Reboot)	Система отправляет команду перезагрузки с помощью ACPI сигнала.
Перезагрузить (немедленно) (Reboot hard)	Система перезагружает VM немедленно.
Разместить на узле (Deploy)	Запустить VM на конкретном узле.
Перенести VM (Migrate)	Система перенесет VM на другой хоста, путем остановки VM на старом узле и включением ее на целевом узле.
Перенести VM (live) (Migrate hard)	Система перенесет VM на выбранный узел, без прекращения работы виртуальной машины.
Запретить размещение (hold)	Система переведет машину в состояние «hold», и без команды «Разместить на узле», не запустит ее.
Разрешить размещение (release)	Разрешить размещение VM.
Перепланировать (Reschedule)	Отметить VM для перемещения на более подходящий по наличию ресурсов узел. VM будет перемещена после следующего цикла мониторинга.



Команда	Описание
Отменить пересоздание (Un-Reschedule)	Отменить пересоздание ВМ, на более подходящий по параметрам узел.
Восстановить (Recover)	<p>Если виртуальная машина зависла в неизвестном состоянии или загрузка ВМ не производится, можно перевести ВМ в нужное состояние.</p> <ul style="list-style-type: none"> <li>– success - Перевести ВМ в состояние «success»;</li> <li>– failure – Перевести ВМ в состояние «failed»;</li> <li>– retry – Повторить перевод ВМ в текущее состояние;</li> <li>– delete – удалить ВМ и перевести ее в состояние «Hold»;</li> <li>– delete-recreate – удалить ВМ и перевести ее в состояние «Pending».</li> </ul>
Сменить владельца (Change owner)	Сменить владельца ВМ.
Сменить группу (Change group)	Сменить группу владельца ВМ.
Удалить (terminate)	Корректное удаление экземпляра виртуальной машины, путем отправления ACPI сигнала виртуальной машине. В случае если ВМ не выполнила данную команду по таймауту, ВМ перейдет в состояние «Работает». После выключения ВМ, все данные ВМ удалены.
Удалить немедленно (terminate hard)	ВМ будет выключена немедленно, после этого, все данные ВМ будут удалены.

Управления ВМ возможно производить из раздела «Виртуализация» → «Виртуальные машины» (см. Рисунок 10), или из вкладки выделенной виртуальной машины (см. Рисунок 12). Все команды управления описаны в списке команд управления ВМ (см. Таблица 16).

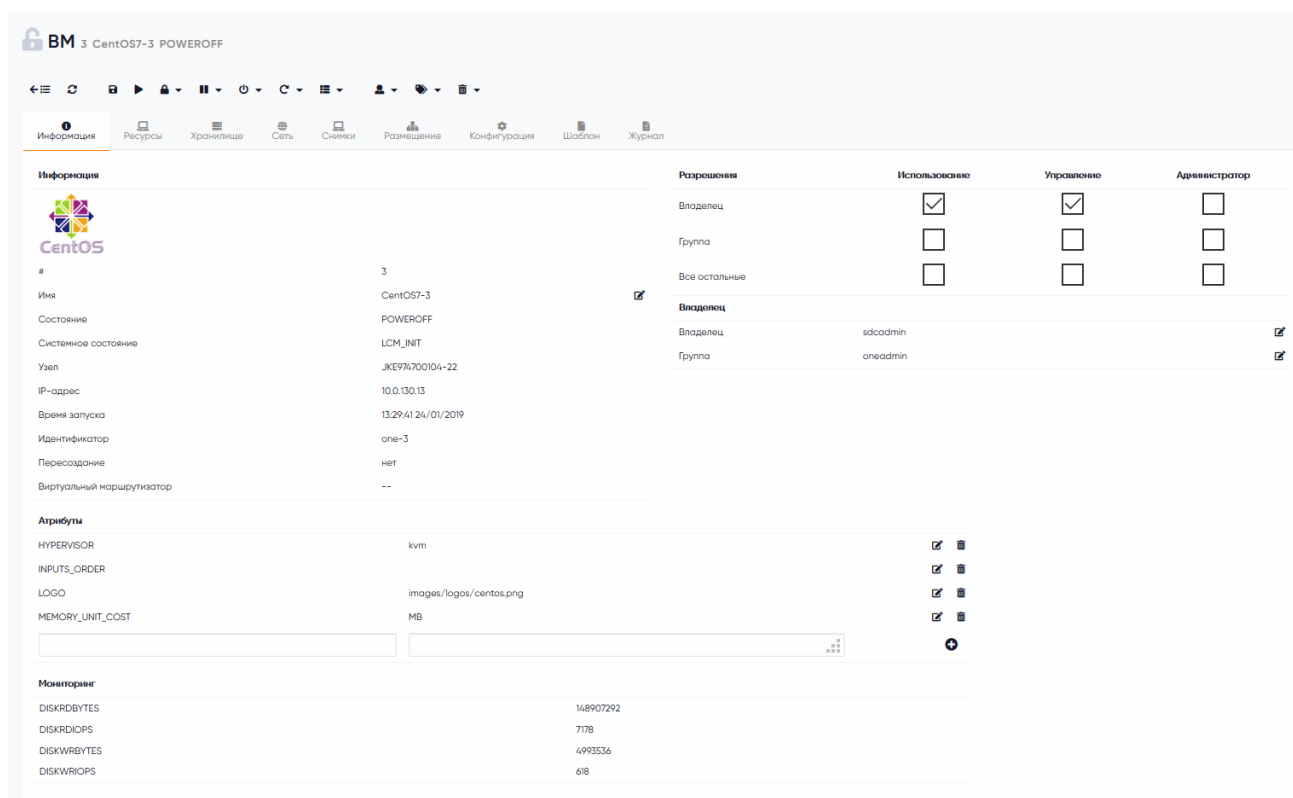


Рисунок 12 Вкладка параметров виртуальной машины

Для изменения статуса виртуальной машины с помощью командой строки, необходимо получить ID или название ВМ. Команда «`sdcvm list`» покажет список ВМ, далее необходимо ввести команду `sdcvm command vmid`, где `command` это команда из списка (см. Таблица 16)

```
# sdcvm list
  ID USER      GROUP    NAME           STAT UCPU    UMEM HOST           TIME
  0  sdccadmin  oneadmin test01-0       runn  0.8     4G  JKE9747001  1d 02h03
  1  testadm-  test     mzivm          runn  0.0     4G  JKE9747001  1d 02h00
  3  sdccadmin  oneadmin CentOS7-3      runn  1.6     2G  JKE9747001  0d 00h40
sdcvm poweroff 3
```

#### 2.4.1.4 Изменение выделенных ресурсов ОЗУ и ЦПУ

Для изменения выделенных ресурсов, необходимо выключить ВМ, перейти на вкладку «Ресурсы», в данной вкладке нажать кнопку «Изменить». В появившемся окне, можно изменить объем выделенного ОЗУ и количество ЦПУ и вЦПУ, после чего нажать кнопку «Изменить» (см. Рисунок 13). Если изменение производится администратором, при нажатии кнопки «Enforce capacity check», система проверит наличие ресурсов на узле.

×

## Изменить базовые характеристики

Enforce capacity checks ?

ОЗУ ?

2  ГБ

ЦПУ ?

1

Виртуальные ЦПУ ?

2

[Изменить](#)

Рисунок 13 Изменение объема выделенных ресурсов

Для изменения размера выделенных ресурсов ВМ, с помощью командой строки, необходимо выключить виртуальную машину изменить ее параметры после чего включить ВМ.

```
# sdcvm list
```

ID	USER	GROUP	NAME	STAT	UCPU	UMEM	HOST	TIME
0	sdcaadmin	oneadmin	test01-0	runn	0.8	4G	JKE9747001	1d 02h03
1	testadm-	test	mzivm	runn	0.0	4G	JKE9747001	1d 02h00
3	sdcaadmin	oneadmin	CentOS7-3	runn	1.6	2G	JKE9747001	0d 00h40

Далее получить информацию о конфигурации ВМ.

```
# sdcvm show 3
```

VIRTUAL MACHINE 3 INFORMATION	
ID	: 3
NAME	: CentOS7-3
USER	: sdcaadmin
GROUP	: oneadmin
STATE	: ACTIVE
LCM_STATE	: RUNNING
LOCK	: None
RESCHED	: No
HOST	: JKE974700104-22
CLUSTER ID	: 0
CLUSTER	: SharxDC

```

START TIME      : 01/24 13:29:41
END TIME        : -
DEPLOY ID       : one-3
  
```

VIRTUAL MACHINE MONITORING

```

CPU              : 0.0
MEMORY           : 2G
NETTX            : 1K
NETRX            : 0K
DISKRDBYTES      : 171752240
DISKRDIOPS       : 8054
DISKWRBYTES      : 4740608
DISKWRIOPS       : 52
  
```

PERMISSIONS

```

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

VM DISKS

ID	DATASTORE	TARGET	IMAGE	SIZE	TYPE	SAVE
0	default	sda	CentOS7sys	1.4G/20G	blloc	NO
1	-	hda	CONTEXT	1M/-	-	-

VM NICs

ID	NETWORK	BRIDGE	IP	MAC	PCI_ID
0	vlan130	ovsbr0	10.0.130.13	00:00:0a:00:82:0d	

SECURITY

NIC_ID	NETWORK	SECURITY_GROUPS
0	vlan130	0

SECURITY GROUP	TYPE	PROTOCOL	NETWORK	RANGE	
ID	NAME		VNET	START	SIZE
0	default	OUTBOUND	ALL		
0	default	INBOUND	ALL		

VIRTUAL MACHINE HISTORY

SEQ	UID	REQ	HOST	ACTION	DS	START	TIME	PROLOG
-----	-----	-----	------	--------	----	-------	------	--------

```

0 2      7424  JKE974700104 poweroff-h    0  01/24 13:29:47  0d 00h01m  0h00m03s
1 2      8960  JKE974700104 stop                0  01/24 14:09:14  0d 00h06m  0h00m00s
2 2      1072  JKE974700104 poweroff           0  01/24 14:16:18  0d 00h00m  0h00m05s
3 -      -      JKE974700104 none                0  01/24 14:23:13  0d 00h00m  0h00m00s

```

USER TEMPLATE

HYPERVISOR="kvm"

INPUTS\_ORDER=""

LOGO="images/logos/centos.png"

MEMORY\_UNIT\_COST="MB"

VIRTUAL MACHINE TEMPLATE

AUTOMATIC\_DS\_REQUIREMENTS="( \"CLUSTERS/ID\" @> 0 ) "

AUTOMATIC\_REQUIREMENTS="( CLUSTER\_ID = 0 ) & !( PUBLIC\_CLOUD = YES ) "

CONTEXT=[

```

    DISK_ID="1",
    ETH0_CONTEXT_FORCE_IPV4="",
    ETH0_DNS="8.8.8.8",
    ETH0_GATEWAY="10.0.130.1",
    ETH0_GATEWAY6="",
    ETH0_IP="10.0.130.13",
    ETH0_IP6="",
    ETH0_IP6_PREFIX_LENGTH="",
    ETH0_IP6_ULA="",
    ETH0_MAC="00:00:0a:00:82:0d",
    ETH0_MASK="255.255.255.0",
    ETH0_MTU="1500",
    ETH0_NETWORK="10.0.130.0",
    ETH0_SEARCH_DOMAIN="",
    ETH0_VLAN_ID="130",
    ETH0_VROUTER_IP="",
    ETH0_VROUTER_IP6="",
    ETH0_VROUTER_MANAGEMENT="",
    NETWORK="YES",
    PASSWORD="Sharx2018",
    SSH_PUBLIC_KEY="",
    TARGET="hda" ]

```

CPU="1"

GRAPHICS=[

```

    LISTEN="0.0.0.0",

```

```

PORT="5903",
TYPE="VNC" ]
INPUT=[
  BUS="usb",
  TYPE="tablet" ]
MEMORY="2048"
OS=[
  ARCH="x86_64",
  BOOT="" ]
TEMPLATE_ID="1"
VCPU="2"
VMID="3"

```

Выключить VM и внести изменения в ее конфигурацию.

```

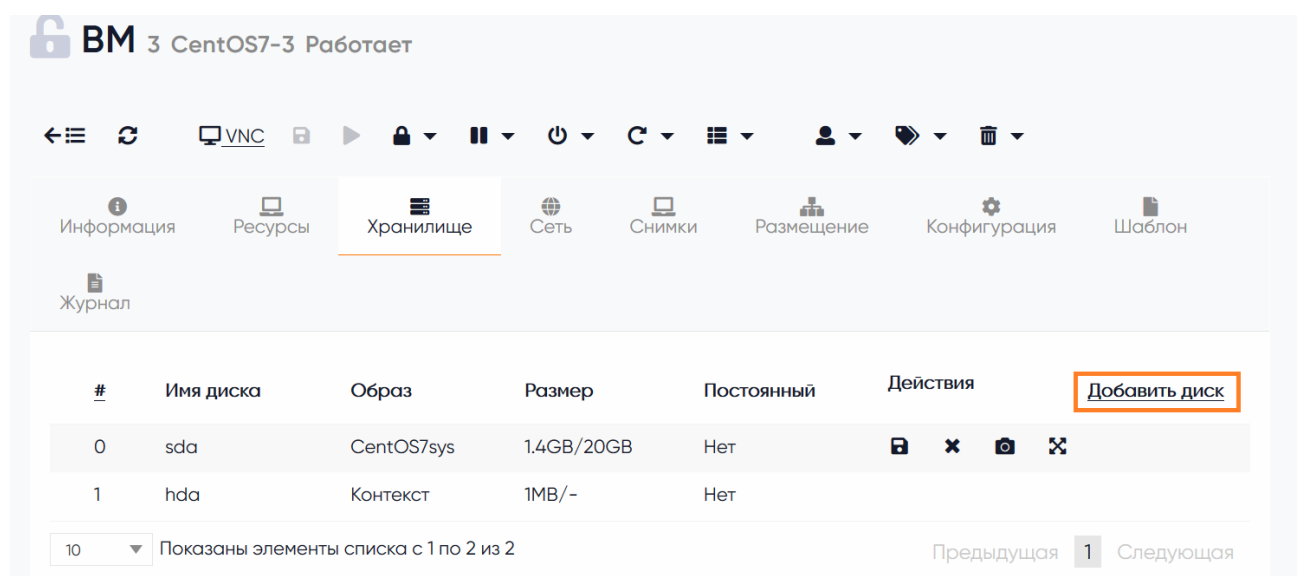
# sdcvm poweroff 3
# sdcvm resize 3 --memory 2G --vcpu 2
# sdcvm resume 3

```

### 2.4.1.5 Работа с хранилищами виртуальных машин

Все работы по управлению хранилищем VM, производится во вкладке «Хранилища». В данной вкладке возможно производить все действия, связанные с управлением дисками VM.

Для добавления виртуального образа, необходимо выключить виртуальную машину и нажать кнопку «Добавить диск» (см. Рисунок 14).







#	Имя диска	Образ	Размер	Постоянный	Действия
0	sda	CentOS7sys	1.4GB/20GB	Нет	   
1	hda	Контекст	1MB/-	Нет	

Рисунок 14 Вкладка хранилища VM

В появившемся окне со списком виртуальных дисков и образов, необходимо выбрать нужный образ и нажать кнопку «Подключить». После чего, данный диск будет подключен к виртуальной машине, и данную ВМ можно включать (см. Рисунок 15).

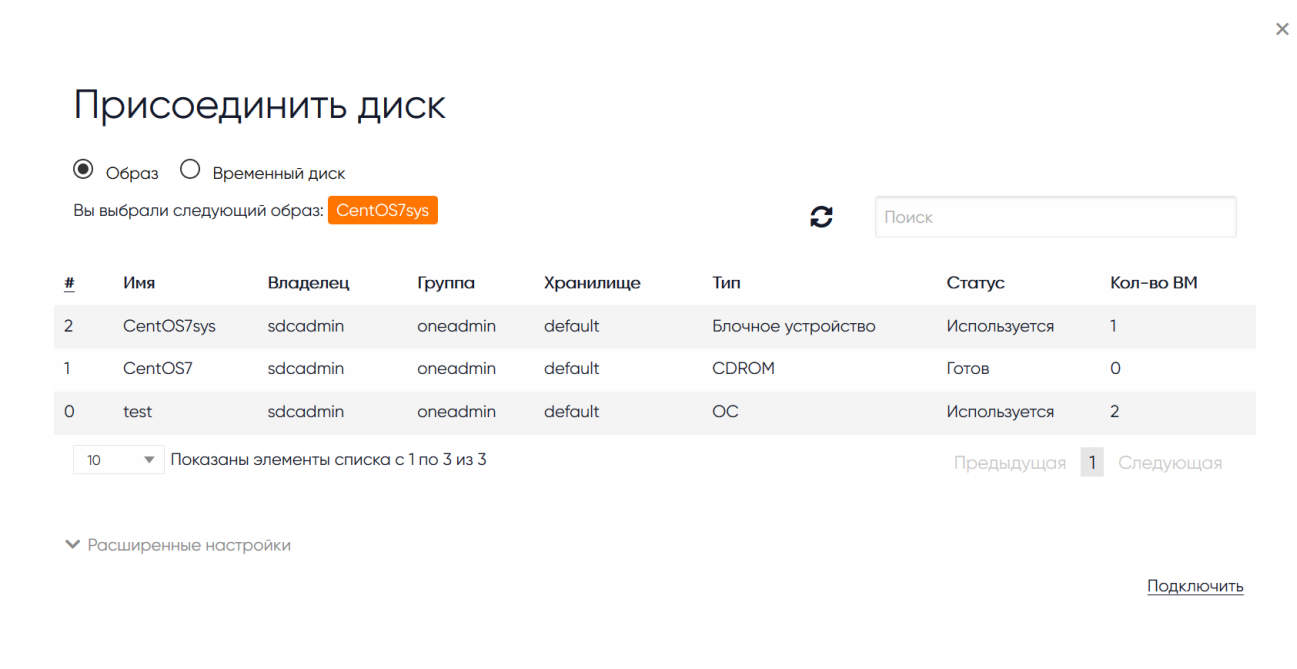
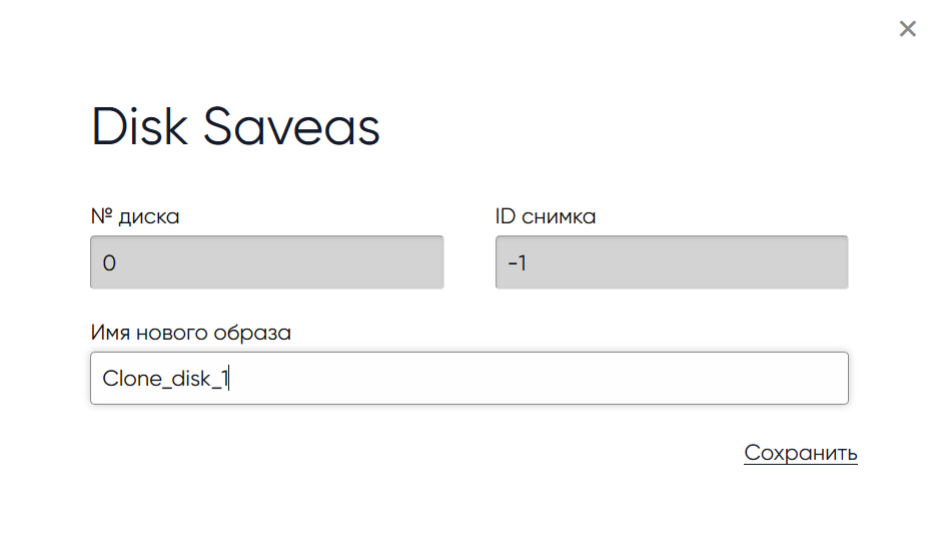


Рисунок 15 Выбор подключаемого диска

Для отключения данного диска или других дисков, подключенных к виртуальной машине, необходимо нажать кнопку «Отключить» (см. Рисунок 14) и подтвердить удаление, нажатием кнопки «ОК». Подключение и отключение дисков к ВМ, производится, когда ВМ находится в системном состоянии, выключена.

Для клонирования виртуального диска ВМ, необходимо нажать кнопку «Сохранить» (см. Рисунок 14), в появившемся окне ввести название будущего образа, который после нажатия кнопки «Сохранить» (см. Рисунок 16) созданный образ, появится в разделе «Хранилища» → «Образы ВМ».



×

## Disk Saveas

№ диска

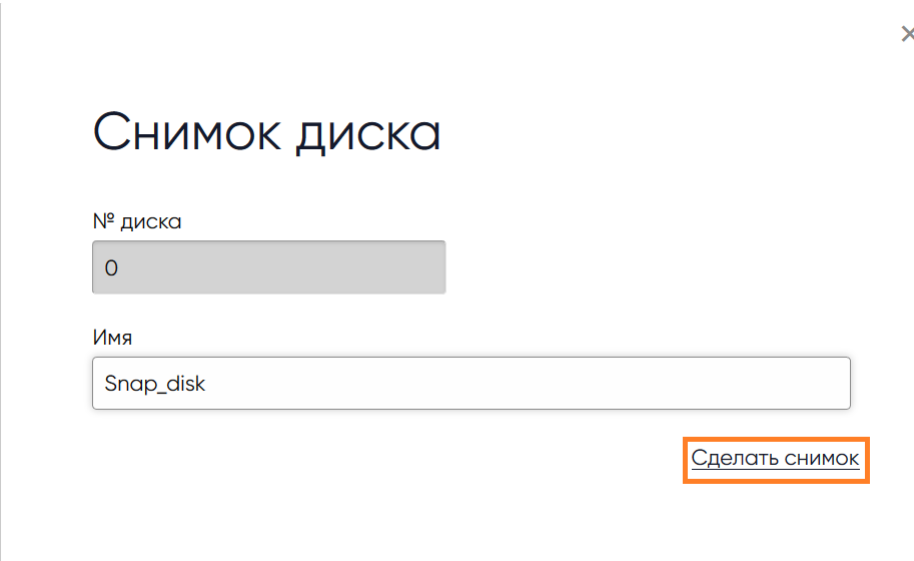
ID снимка

Имя нового образа

[Сохранить](#)

Рисунок 16 Окно ввода названия создаваемого образа

Для создания снимка виртуального диска VM, необходимо нажать кнопку «Снимок», в появившемся окне ввести название снимка и кнопку «Сделать снимок» (см. Рисунок 17).



×

## Снимок диска

№ диска

Имя

[Сделать снимок](#)

Рисунок 17 Окно создания снимка диска

После создания снимка диска, в списке виртуальных дисков, рядом с идентификатором диска, появится выпадающее меню, в котором отобразятся все снимки виртуальной машины. В данном меню, возможно создать клон данного снимка, с помощью кнопки «Сохранить», удалить выбранный снимок с помощью кнопки «Удалить» и переключиться на выбранный снимок нажав кнопку «Прервать» (см. Рисунок 18).



#	Имя диска	Образ	Размер	Постоянный	Действия	Добавить диск
0	sda	CentOS7sys	1.4GB/20GB	Нет		
<div style="display: flex; justify-content: space-around; border: 1px solid orange; padding: 2px;"> <span> Сохранить</span> <span> Восстановить</span> <span> Удалить</span> </div>						
<input type="checkbox"/>	0	15:13:33 24/01/2019	-/20GB	Snap_disk		
<input checked="" type="checkbox"/>	1	15:14:43 24/01/2019	-/20GB	Snap_disk_2		

Рисунок 18 Список снимков виртуального диска

### 2.4.1.6 Создание и удаление снимка ВМ

Для создания с снимка ВМ, необходимо перейти во вкладку «Снимки» и нажать кнопку «Создать снимок». После создания с снимка ВМ, возможно переключить ВМ на его работу, нажав кнопку «Прервать», а также удалить данный снимок, нажав кнопку «Удалить» (см. Рисунок 19).

**ВМ 3 CentOS7-3** Работает

← ≡ ↻ VNC 🔒 ▶ ⏸ ⏹ ⏪ ⏩ ⏴ ⏵ 👤 🗑

Информация Ресурсы Хранилище Сеть **Снимки** Размещение Конфигурация Шаблон Журнал

#	Имя	Временная метка	Действия	Сделать снимок
0	Снимок ВМ №1	12:13:56 25/01/2019	Восстановить  Удалить	
1	Снимок ВМ №2	12:15:18 25/01/2019	Восстановить  Удалить	
2	Снимок ВМ №3	12:15:40 25/01/2019	Восстановить  Удалить	

Рисунок 19 Список снимков ВМ

### 2.4.2 Описание работы с образами виртуальных машин

Распределенное хранилище данных позволяет администраторам системы настраивать образы, которые могут выступать системными дисками виртуальных машин или виртуальными дисками с данными для виртуальных машин. Эти образы могут использоваться одновременно несколькими виртуальными машинами, а также совместно с другими пользователями.

Образы разделены на 6 типов, изменить тип образа, можно с помощью команды `sdcimage chtype`.

Первые три типа образов, диска предназначены для виртуальных машин:

OS: Образ загрузочного диска, операционной системы.

CDROM: Образ диска, доступный только для чтения.

DATABLOCK: Образ с данными, стандартный образ диска, для виртуальной машины.

Остальные типы образов, это файловые образы:

KERNEL: Файл используемый как ядро виртуальной машины (VM attribute OS/KERNEL\_DS)

RAMDISK: Файл используемый как диск ОЗУ виртуальной машины (VM attribute OS/INITRD\_DS)

CONTEXT: Файл контекстуализации, который используется для настройки виртуальной машины (VM attribute CONTEXT/FILES\_DS)

Жизненный цикл образов описан в таблице (см. Таблица 17).

Таблица 17 Жизненный цикл образов

Статус	Описание
LOCKED	Файл образа, копируется или создается
LOCKED_USED	Файл образа копируется или создается в хранилище данных, а виртуальные машины ждут завершения операции
LOCKED_USED_PERS	Файл образа копируется или создается в хранилище данных, а виртуальные машины ждут завершения операции. Для дисков с параметром «Постоянный»
READY	Образ готов к использованию
USED	Не постоянный образ используется, как минимум одной виртуальной машиной, может использоваться другими виртуальными машинами
USED_PERS	Образ используется постоянной виртуальной машиной, новые виртуальные машины не имеют доступ к данному образу
DISABLED	Образ отключен владельцем, новые виртуальные машины не имеют доступа к данному образу
ERROR	Состояние ошибки. Подробную информацию об ошибке смотрите <code>sdcmage show</code> .
DELETE	Образ удаляется из хранилища
CLONE	Образ клонируется

Постоянный диск (статический), это диск который может использоваться только одной виртуальной машиной, в случае необходимости использования данных на этом диске, его тип необходимо изменить параметр, "постоянный (нет)", постоянный диск при создании, отображается в интерфейсе управления.

Временный диск, это диск который может использоваться несколькими виртуальными машинами, например, все диски шаблонов являются не постоянными, и при создании новой виртуальной машины, данный диск клонируется, все новые данные записываются на новый клонируемый диск, а старые хранятся на шаблонном диске, в случае клонирования уже нового диска, его данные будут полностью скопированы.

Управление образами производится через веб-интерфейс или с помощью команды `sdcimage`. По умолчанию, вкладка управления образами отображается только в административной консоли. Для подробного описания команды `sdcimage`, необходимо воспользоваться `man`.

#### 2.4.2.1 Загрузка iso образа

Для загрузки и управления образа iso виртуальной машины, необходимо зайти в раздел Хранилища → Образы ВМ. Нажать на кнопку «+», после чего необходимо указать:

1. Имя образа;
2. Описание;
3. Тип диска «CD\_ROM только для чтения»;
4. Хранилище «default»
5. Расположение образа «Загрузить», в появившемся окне, выбрать файл iso образа.

Далее нажать кнопку «Создать» (см. Рисунок 20). После того, как образ будет загружен в кластер, статус данного образа изменится в «Готов», после чего, его можно будет использовать в ВМ.

**Создание образа**

← Очистить все поля Создать Мастер настройки Расширенная настройка

Имя:

Описание:

Тип:

Хранилище:

Постоянный образ:

**Расположение образа**

Путь к файлу  Загрузить  Пустой образ диска

No file selected.

▼ Расширенные настройки

Рисунок 20 Окно ввода параметров iso образа

Для создания образа в командной консоли необходимо ввести следующие команды

```
$ sdcimage create -name Gparted_live --datastore default --path /home/user/GParted.iso --description "ISO image of GParted live cd"
```

#### 2.4.2.2 Создание образа datablock

Для создания образа пустого диска, необходимо зайти в раздел Хранилища → Образы ВМ. Нажать на кнопку «+», после чего необходимо указать:

1. Имя образа;
2. Описание;
3. Тип диска «Generic storage datablock»;
4. Хранилище «default»
5. Расположение образа «Пустой образ», размер указывают в мегабайтах.

Далее нажать кнопку «Создать». Статус данного образа изменится в «Готов», и его можно будет использовать в ВМ.

### Создание образа

← Очистить все поля Создать

Мастер настройки Расширенная настройка

Имя:

Описание:

Тип:

Хранилище:

Постоянный образ:

**Расположение образа**

Путь к файлу
  Загрузить
  Пустой образ диска

Размер:  ГБ

Расширенные настройки

Рисунок 21 Окно ввода параметров datablock образа

Для создания образа в командной консоли необходимо ввести следующие команды:

```
$ sdcimage create --datastore default --name New_VM_disk --path /var/lib/one/datastores/0/linuxvm/disk.0 --description " Empty VM disk"
```

### 2.4.2.3 Клонирование образа

Для клонирования образа VM, необходимо его выбрать и нажать кнопку «Клонировать»

### Образы дисков VM

#	Имя	Владелец	Группа	Хранилище	Тип	Статус	Кол-во VM	
<input checked="" type="checkbox"/>	3	New VM disk	sdccadmin	oneadmin	default	Блочное устройство	Заблокирован	0
<input type="checkbox"/>	2	CentOS7sys	sdccadmin	oneadmin	default	Блочное устройство	Используется	1
<input type="checkbox"/>	1	CentOS7	sdccadmin	oneadmin	default	CDROM	Готов	0
<input type="checkbox"/>	0	test	sdccadmin	oneadmin	default	OC	Используется	2

Показаны элементы списка с 1 по 4 из 4

4 Всего 38.9 GB Общий объем

Рисунок 22 Выбор образа VM для клонирования

В следующем окне необходимо задать имя клонированного образа и нажать кнопку «Клонировать»

## Клонировать образ

Имя

Расширенные настройки


Клонировать

Рисунок 23 Окно именованя нового клона

Для клонирования образа с помощью командной строки, необходимо ввести следующую команду

```
$ sdcimage clone 0 LinuxVM LinuxVMClone
```

## 2.4.2.4 Удаление образа

Для удаления образа ВМ, необходимо выделить один или несколько образов и нажать кнопку удалить «»

Образы дисков ВМ

Клонировать

<input type="checkbox"/>	#	Имя	Владелец	Группа	Хранилище	Тип	Статус	Кол-во ВМ
<input checked="" type="checkbox"/>	3	New VM disk	sdccadmin	oneadmin	default	Блочное устройство	Заблокирован	0
<input type="checkbox"/>	2	CentOS7sys	sdccadmin	oneadmin	default	Блочное устройство	Используется	1
<input type="checkbox"/>	1	CentOS7	sdccadmin	oneadmin	default	CDROM	Готов	0
<input type="checkbox"/>	0	test	sdccadmin	oneadmin	default	ОС	Используется	2

Показаны элементы списка с 1 по 4 из 4


4 Всего 38.9 GB Общий объем

Рисунок 24 Окно выбора образа для удаления

Для удаления образа с помощью командной строки, необходимо ввести следующую команду:

```
$ sdcimage create --datastore default --name LinuxVM --path /home/cloud/images/ubuntu-desktop/disk.0 --description "LinuxVM for guide"
```

## 2.4.2.5 Смена владельца или группы образа

Для смены владельца или группы образа, необходимо выделить один или несколько образов и нажать кнопку «». В выпадающем меню выбрать «Сменить владельца» или «Сменить группу», в появившемся окне выбрать нового владельца или группу образа, после чего нажать «ОК».

×

### Сменить владельца

Выберите нового владельца

Пожалуйста выберите плъзователя из списка




#	Имя	Группа	Драйвер авторизации	Статус	Виртуальные машины	ОЗУ	ЦПУ
4	testadm-mzi	test	sharx-scm	active	1 / -	4GB / -	2 / -
3	mzi01	users	sharx-scm	active	0 / -	0KB / -	0 / -
2	sdccadmin	oneadmin	core	core	2 / -	6GB / -	3 / -
1	serveradmin	oneadmin	server_cipher	server_cipher	0 / -	0KB / -	0 / -
0	oneadmin	oneadmin	core	core	-	-	-

10 Показаны элементы списка с 1 по 5 из 5

Предыдущая 1 Следующая

**OK**

Рисунок 25 Окно выбора владельца образа

×

### Сменить группу

Выберите новую группу

Вы выбрали следующую Группу: **users**




#	Имя	Пользователи	Виртуальные машины	ОЗУ	ЦПУ
100	test	1	1 / -	4GB / -	2 / -
1	users	1	0 / -	0KB / -	0 / -
0	oneadmin	3	-	-	-

10 Показаны элементы списка с 1 по 3 из 3

Предыдущая 1 Следующая

**OK**

Рисунок 26 Окно выбора группы образа

## 2.4.2.6 Изменение статуса образа

Также для удобства работы с образами в главное меню «Образы ВМ» выведены следующие функции:

- Включить - функция изменяет статус образа в состояние «Готов»;
- Отключить - функция изменяет статус образа в состояние «Выключен»;
- Сделать постоянным - функция изменяет свойство диска «Постоянный»;
- Сделать не постоянным - функция изменяет свойство диска «Не постоянный».

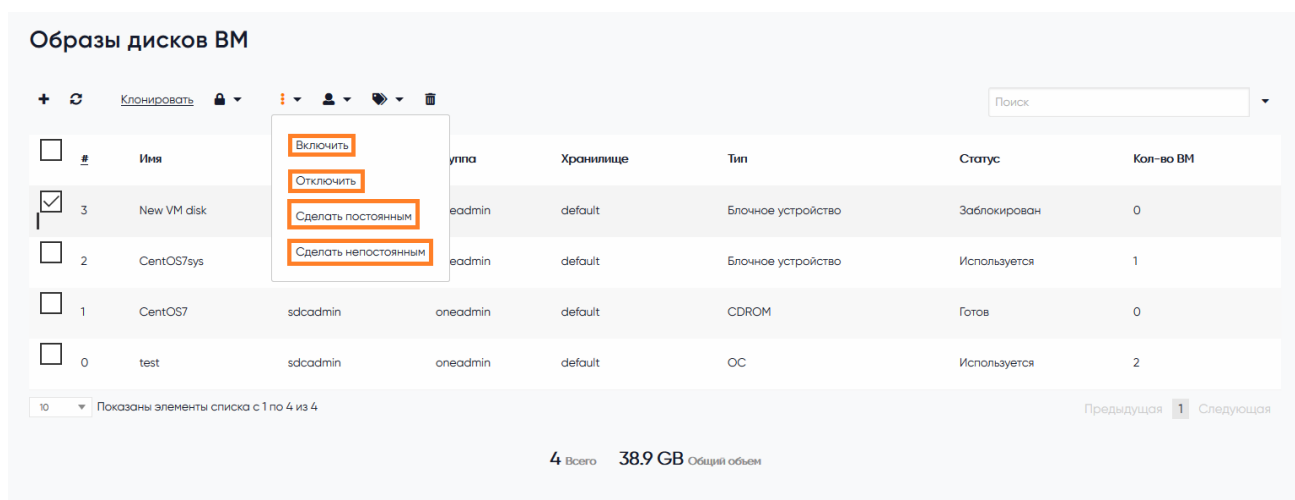


Рисунок 27 Окно выбора образа и изменения статуса

## 2.4.3 Описание работы с шаблонами виртуальных машин

Шаблоны ВМ предназначены для быстрого создания ВМ, с установленным и настроенным ПО, а также заданными характеристиками ВМ. Все действия, связанные с шаблонами ВМ, производятся в разделе «Шаблоны» → «Виртуальные машины».

### 2.4.3.1 Обновление шаблона виртуальной машины

Для обновления параметров шаблона виртуальной машины, необходимо зайти в раздел «Шаблоны» → «Виртуальные машины». Выбрать шаблон, в котором необходимо изменить параметры, нажать кнопку «Обновить», далее внести изменения в данный шаблон, например, изменить описание шаблона, после чего нажать кнопку «Обновить» (см. Рисунок 28).



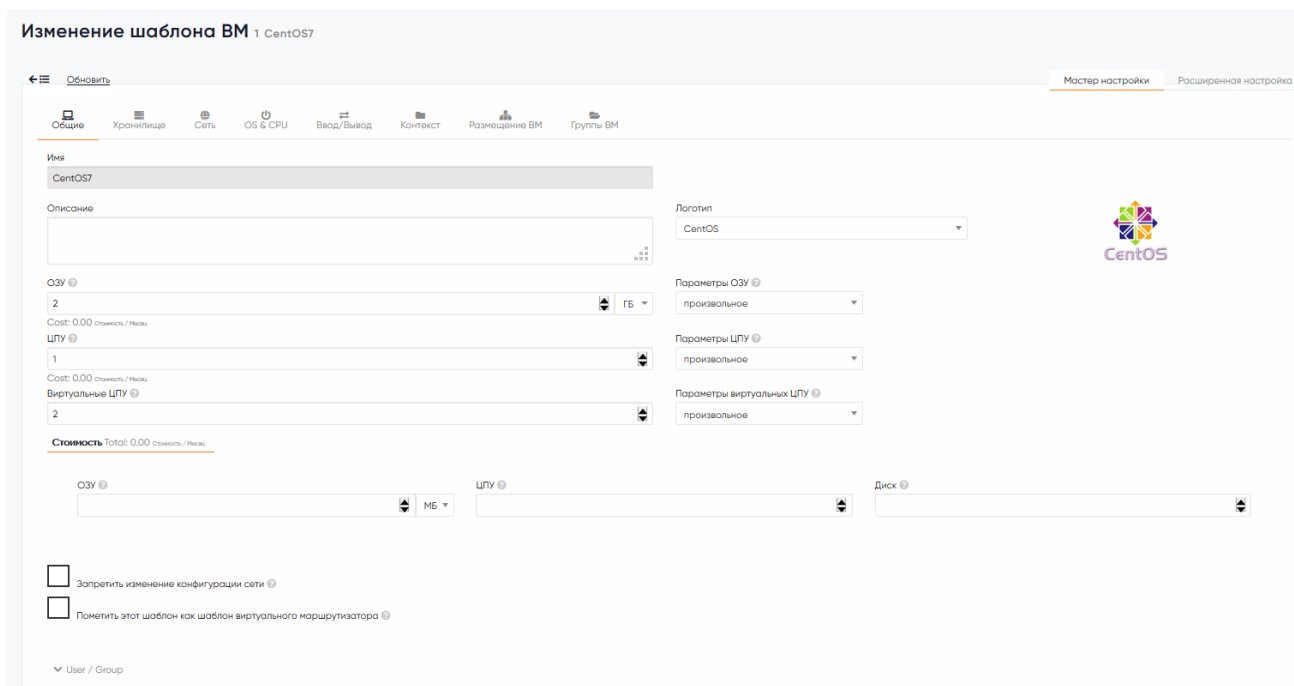


Рисунок 28 Окно изменения шаблона

### 2.4.3.2 Создание виртуальной машины из шаблона

Для создания виртуальной машины из шаблона, необходимо зайти в раздел «Шаблоны» → «Виртуальные машины», выбрать нужный шаблон, далее нажать кнопку «Развернуть». После этого необходимо задать параметры создаваемой VM:

- Имя VM;
- Количество экземпляров;
- Параметр «Создать и не включать»;
- ОЗУ;
- Размер системного диска;
- Количество ЦПУ;
- Количество вЦПУ;
- Сетевой интерфейс.

После выбора всех необходимых параметров, нажать кнопку «Создать» (см. Рисунок 29).

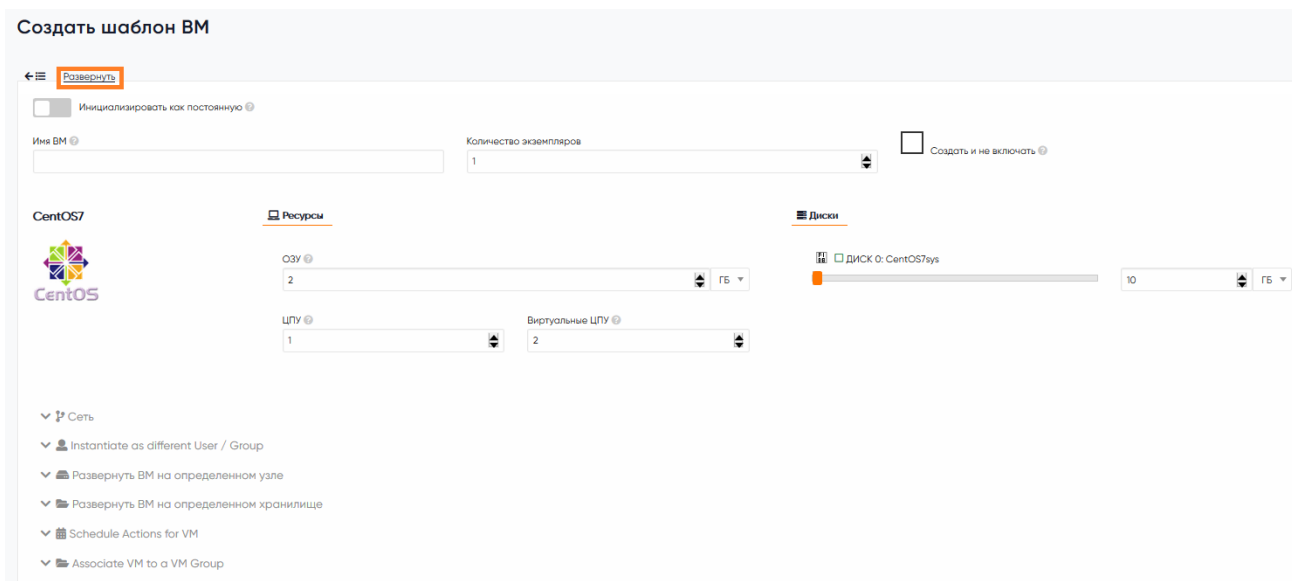


Рисунок 29 Окно создания ВМ

### 2.4.3.3 Клонирование шаблона виртуальной машины

Для клонирования шаблона ВМ, необходимо нажать кнопку «Клонировать», в появившемся окне, ввести название клона шаблона ВМ, и кнопку «Клонировать» (см. Рисунок 30).

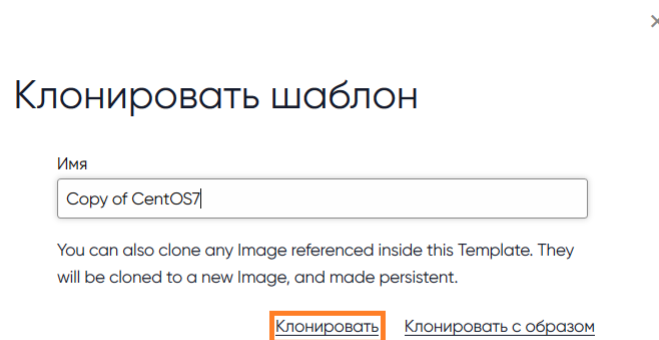


Рисунок 30 Окно клонирования шаблона ВМ

### 2.4.3.4 Смена владельца шаблона

Для смены владельца необходимо нажать кнопку «Сменить владельца», в появившемся окне, выбрать целевого владельца шаблона.

#### 2.4.3.5 Смена группы шаблона

Для смены группы необходимо нажать кнопку «Сменить группу», в появившемся окне, выбрать целевую группу шаблона.

#### 2.4.3.6 Выдача доступа группе владельца

Для выдачи доступа к шаблону VM, группе к которой подключен данный шаблон, необходимо нажать кнопку «Дать доступ».

#### 2.4.3.7 Отмена доступа группе владельца

Для отмены доступа к шаблону VM, группе к которой подключен данный шаблон, необходимо нажать кнопку «Отменить доступ».

#### 2.4.3.8 Удаление шаблона

Для удаления шаблона, необходимо нажать кнопку «Удалить», после этого необходимо подтвердить удаление.

### 2.4.4 Создание шаблона VM Windows

Создание шаблона виртуальной машины, состоит из 4 этапов:

1. Подготовка образов.
2. Создание первичного, пустого шаблона.
3. Запуск VM, установка ОС, настройка ОС.
4. Создание шаблона на основе настроенной VM.

Ниже подробно описаны все этапы.

#### 1. Подготовка образов (images)

Необходимо загрузить два образа в раздел «Хранилища» → «Образы VM». Нажать кнопку «+», после этого ввести название образа, тип «CD-ROM только для чтения», описание и место хранения.

Далее нажать кнопку «Выбрать файл» и в появившемся окне выбрать из списка нужный образ, после чего нажать кнопку «Открыть». Заполнив все параметры, необходимо нажать кнопку «Создать».

После загрузки образов ОС и драйверов, необходимо создать образ диска, на который будет установлена ОС и задать параметры, указанные ниже, после чего нажать кнопку «Создать».

### 1.1. Образ инсталляционного диска ОС

- Тип: CD-ROM.
- Расположение образа: загрузить со своего компьютера через интерфейс управления.
- Целевое устройство: HD.
- Драйвер монтирования образа: RAW.

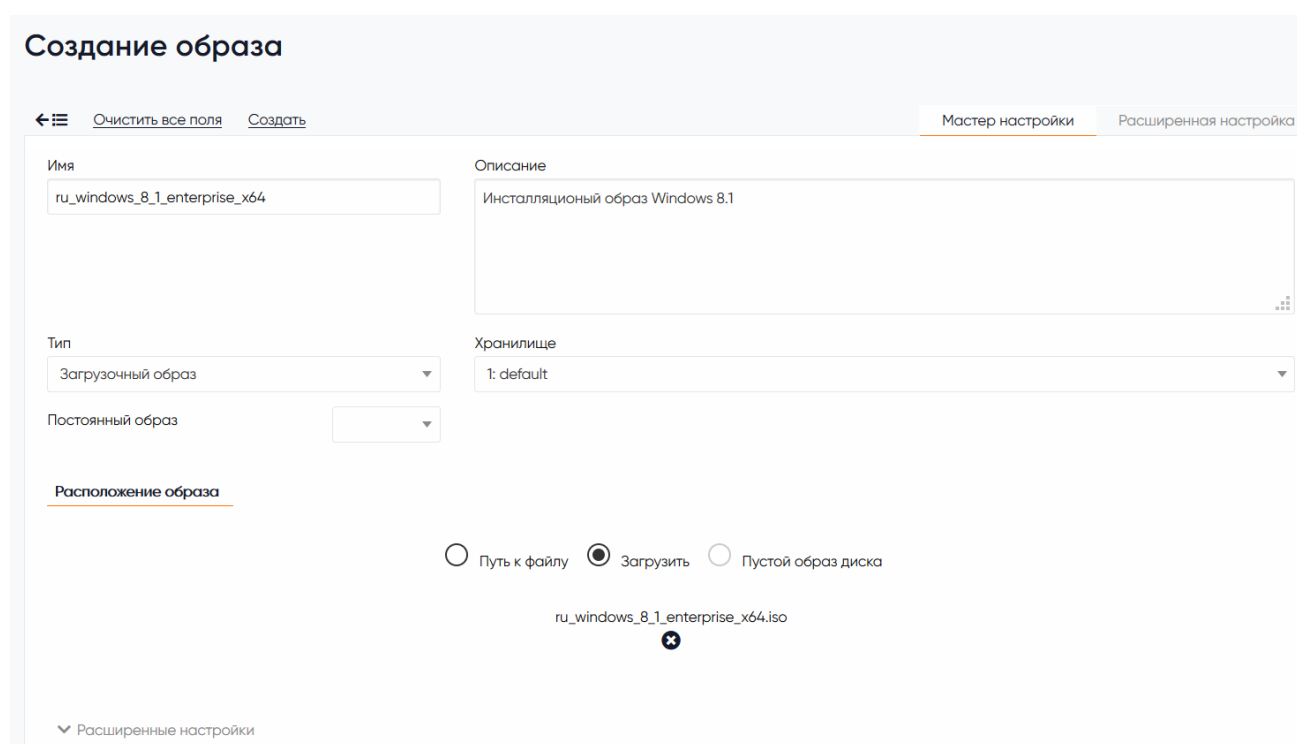


Рисунок 31 Добавление инсталляционного диска Windows

### 1.2. Образ SharxBaseTools

Образ загружен автоматически, при необходимости его можно запросить у производителя открыв заявку по почте "support@sharxdc.ru":

- Тип: CD-ROM
- Расположение образа: загрузить со своего компьютера через интерфейс управления
- Целевое устройство: HD
- Драйвер монтирования образа: RAW

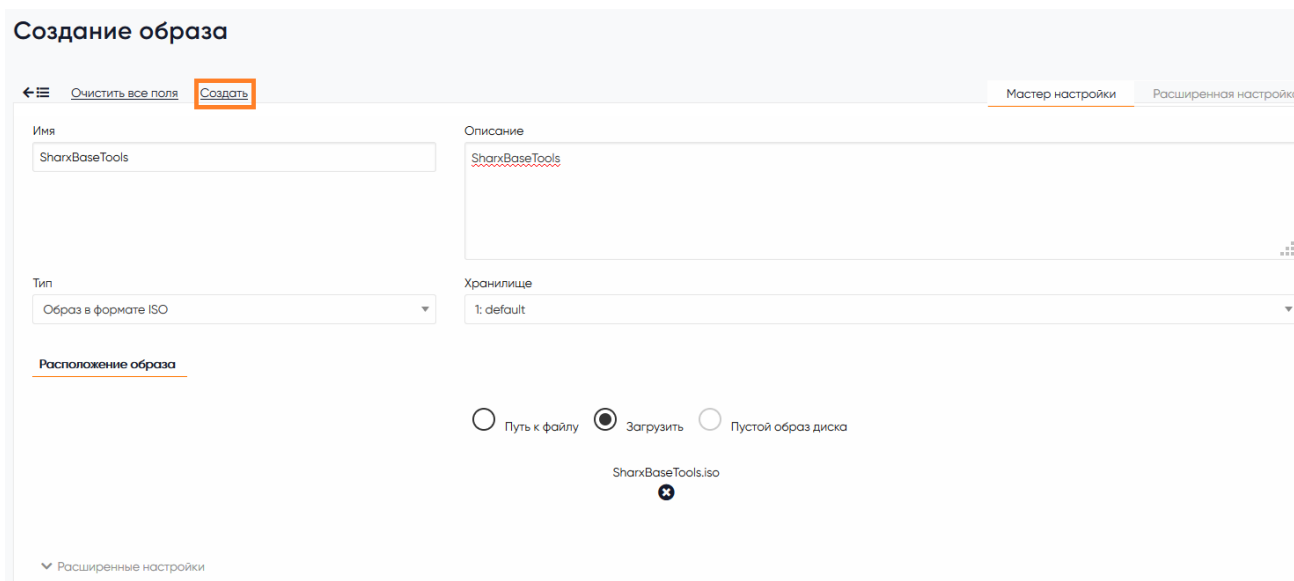


Рисунок 32 Добавление инсталляционного диска SharxBaseTools

### 1.3. Образ чистого диска для установки

- Тип: Блочное устройство (Datablock)
- Расположение образа: Пустой образ диска
- Образ постоянный: да
- Размер в МБ: 50000, размер минимального диска для ОС Windows необходимо уточнить в документации
- Целевое устройство: SD
- Драйвер монтирования образа: RAW

Создание образа

← Очистить все поля Создать

Мастер настройки Расширенная настройка

Имя: Win8.1

Описание: Образ чистого диска для создания VM Windows

Тип: Блочное устройство

Хранилище: 1: default

Постоянный образ

Расположение образа

Путь к файлу  Загрузить  Пустой образ диска

Размер: 500 ГБ

Расширенные настройки

Рисунок 33 Добавление пустого образа диска для чистой установки

## 2. Создание первичного, пустого шаблона

Далее необходимо создать шаблон VM, для этого необходимо перейти в раздел «Шаблоны» → «Виртуальные машины», нажать кнопку «+», во вкладке «Общие» внести необходимые параметры будущей VM, эти данные возможно изменить после создания шаблона

### 2.1. Общие

- ОЗУ: 4ГБ
- ЦПУ: 1
- ВЦПУ: 2
- Логотип: Windows

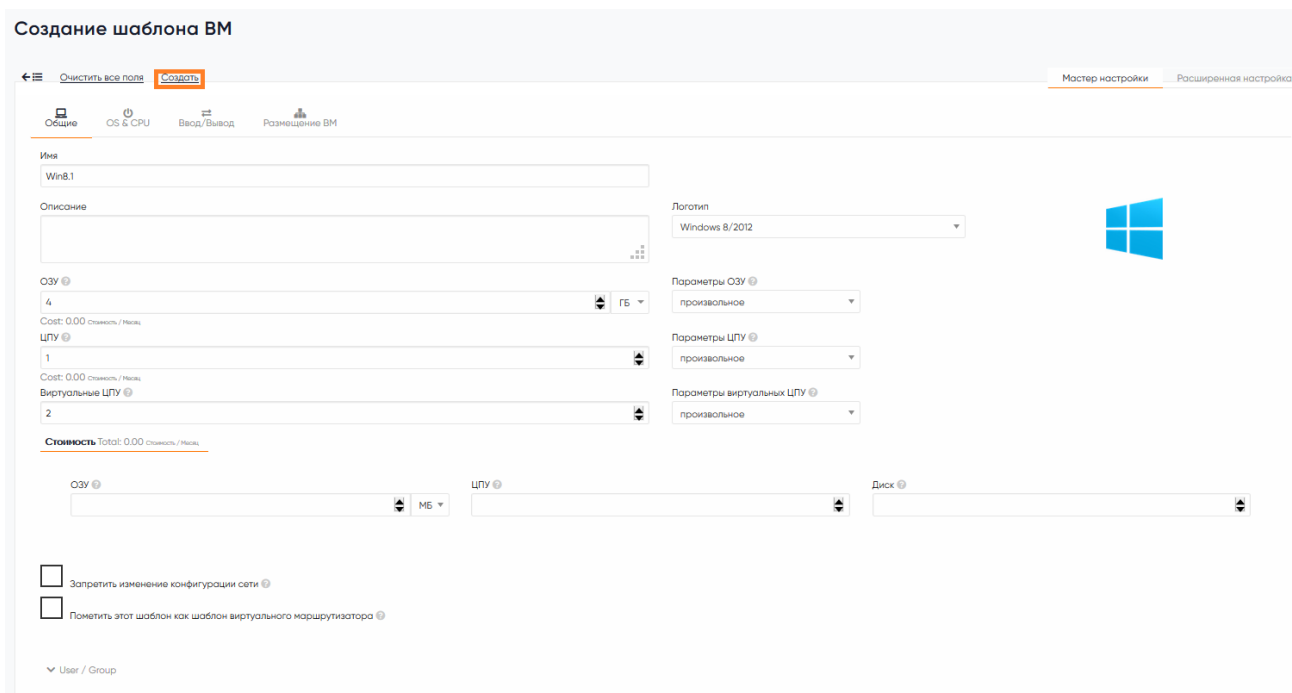


Рисунок 34 Добавление шаблона VM - Общие

## 2.2. Хранилище

Далее во вкладке «Хранилища», необходимо добавить три диска, загруженные ранее:

- Образ установочного диска ОС;
- Образ драйверов для ОС;
- Образ пустого диска для ОС.

Добавить 3 диска с образами добавленными ранее.

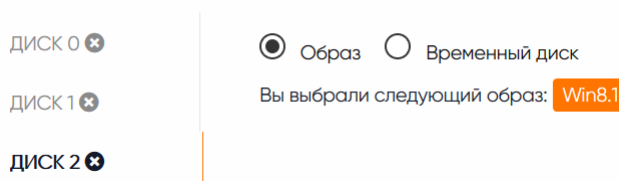


Рисунок 35 Добавление шаблона VM - Хранилище

Для выбранных образов нужно зайти в расширенные настройки ниже списка всех доступных образов и добавить следующие параметры:

- Для инсталляционного образа:
  - Шина (Bus): Parallel ATA (IDE)

^ Расширенные настройки

Образ

Идентификатор образа <input type="text"/>	Имя образа <input type="text" value="WindowsISO"/>
Идентификатор владельца образа <input type="text"/>	Имя владельца образа <input type="text" value="sdcadmin"/>
Префикс устройства <sup>?</sup> <input type="text" value="sdc"/>	Драйвер для подключения образа <input type="text"/>
Шина <input type="text" value="Parallel ATA (IDE)"/>	Только чтение <input type="text"/>
Контроллер шины данных <input type="text"/>	Тип инициализации диска <input type="text"/>
Кэш <input type="text"/>	Политика ввода/вывода <input type="text"/>
Сбросить <input type="text"/>	Size on instantiate <sup>?</sup> <input type="text" value=""/> ГБ

Рисунок 36 Параметры инсталляционного диска

- Для пустого диска:
- Шина (Bus): SCSI



^ Расширенные настройки

Образ

Идентификатор образа <input type="text"/>	Имя образа <input type="text" value="Win8.1"/>
Идентификатор владельца образа <input type="text"/>	Имя владельца образа <input type="text" value="sdcadmin"/>
Префикс устройства ? <input type="text" value="sdc"/>	Драйвер для подключения образа <input type="text"/>
Шина <input type="text" value="SCSI"/>	Только чтение <input type="text"/>
Контроллер шины данных <input type="text"/>	Тип инициализации диска <input type="text"/>
Кэш <input type="text"/>	Политика ввода/вывода <input type="text"/>
Сбросить <input type="text"/>	Size on instantiate ? <input type="text"/> <input type="text" value="ГБ"/>

Рисунок 37 Параметры пустого диска

- Для образа SharxBaseTools:
  - Шина (Bus): Parallel ATA (IDE)

^ Расширенные настройки

Образ

Идентификатор образа <input type="text"/>	Имя образа <input type="text" value="SharxBaseTools"/>
Идентификатор владельца образа <input type="text"/>	Имя владельца образа <input type="text" value="sdcadmin"/>
Префикс устройства ? <input type="text" value="sdc"/>	Драйвер для подключения образа <input type="text"/>
Шина <input type="text" value="Parallel ATA (IDE)"/>	Только чтение <input type="text"/>
Контроллер шины данных <input type="text"/>	Тип инициализации диска <input type="text"/>
Кэш <input type="text"/>	Политика ввода/вывода <input type="text"/>
Сбросить <input type="text"/>	Size on instantiate ? <input type="text" value=""/>

Рисунок 38 Параметры диска SharxBaseTools

### 2.3. Сеть

На вкладке «Сети», указать VLAN для сетевого интерфейса и, если в этом есть необходимость, добавить дополнительный сетевой интерфейс.

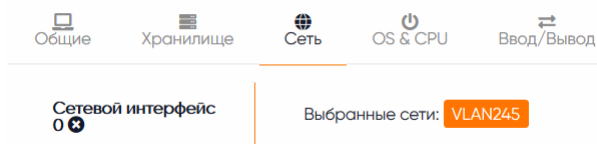


Рисунок 39 Добавление шаблона VM - Сеть

### 2.4. OS & CPU

Архитектура ЦПУ: x86\_64

Порядок загрузки: указать первым инсталляционный диск

- ACPI = «Да»;
- APIC = «Да»;
- Местное время = «Да»;
- QEMU Guest Agent = «Да».

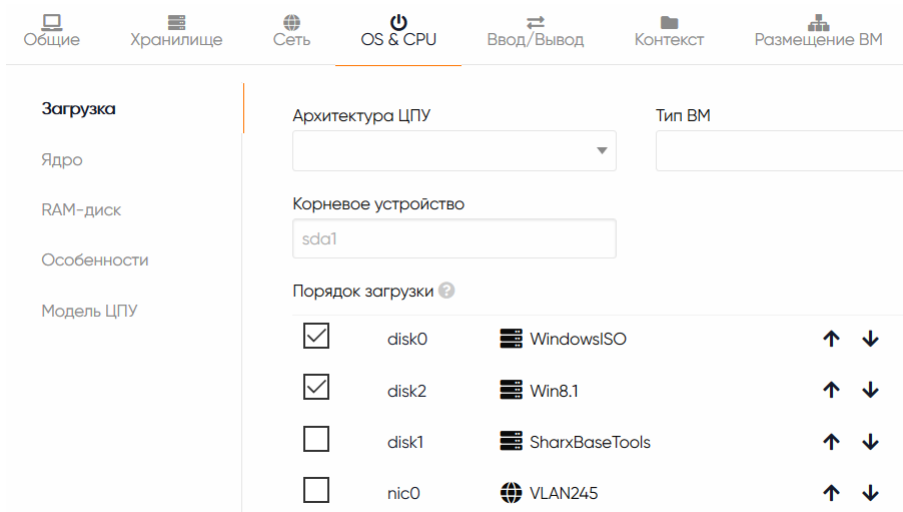


Рисунок 40 Добавление шаблона VM - Параметры загрузки

## 2.5. Ввод/вывод. Устройства ввода

Тип: Планшетный ПК.

Шина: USB.

Нажать кнопку «Добавить».

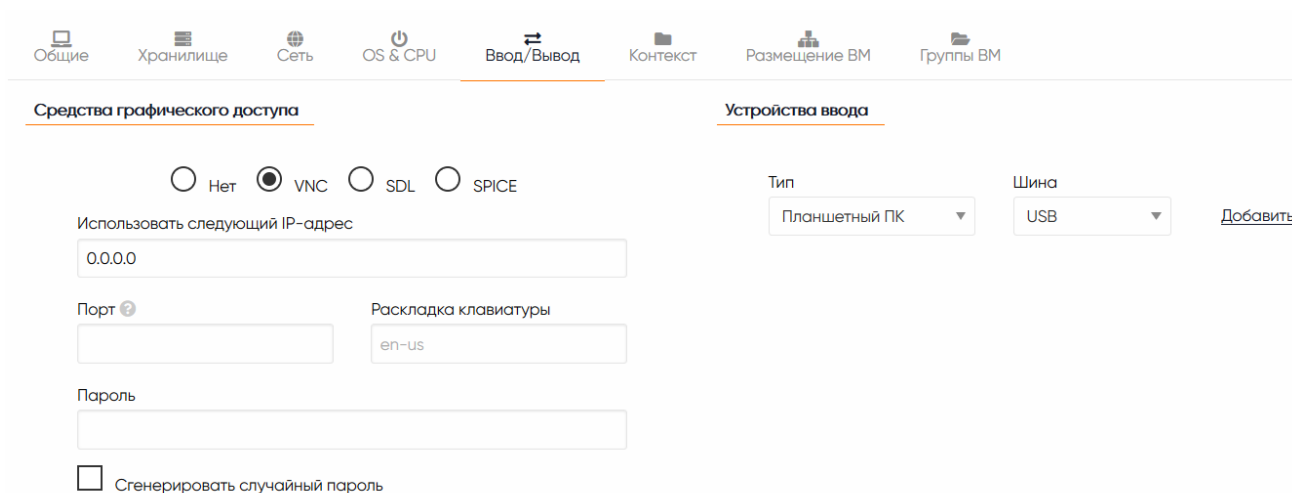


Рисунок 41 Добавление шаблона VM - Параметры загрузки

## 2.6. Завершение

Для автоматизации настройки разворачиваемых виртуальных машин, предусмотрена возможность отправки параметров виртуальной машины, таких как название VM, имя пользователя и пароль, настройка сетевых параметров.

Возможно задание статических параметров и динамических, с возможностью ввода при разворачивании VM. Для задания имени VM, на вкладке «Контекст», в подразделе «Пользовательские переменные», указать следующие ключи:

- SET\_HOSTNAME = \$name, где \$name переменная, присваивающая название VM, в соответствии с названием виртуальной машины в системе. В имени виртуальной машины, должно состоять из латинских букв «a-z», «A-Z», цифр «0-9» и символа «-».

Для автоматического создания пользователя и пароля, с административными правами, в случае если необходимо задавать имя и пароль, после каждого создания VM, необходимо на вкладке «Контекст», в подразделе «Пользовательский ввод», указать следующие ключи:

- USERNAME, тип «Текст», любое описание;
- PASSWORD, тип «Пароль», любое описание.

При задании пароля, необходимо учесть что данный пароль, должен состоять минимум из 8 символов, состоящих из заглавных и прописных латинских букв, цифр и спецсимволов (!, \$, #, %, @, ^, &). После задания параметров контекста, первый этап закончен и необходимо завершить его нажатием кнопки «Создать».

### 3. Запуск VM

Следующим этапом является запуск VM, на основе созданного шаблона. Необходимо указать имя VM, и ее параметры после чего необходимо запустить VNC консоль.

#### 3.1. Запуск VM

Запустить новую VM из шаблона используя кнопку Развернуть

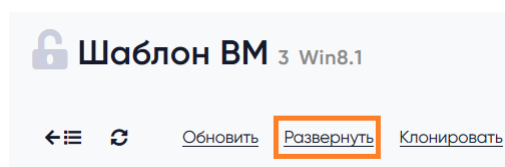


Рисунок 42 Управление запуском VM из шаблона

Для VM должны быть заполнены все поля.

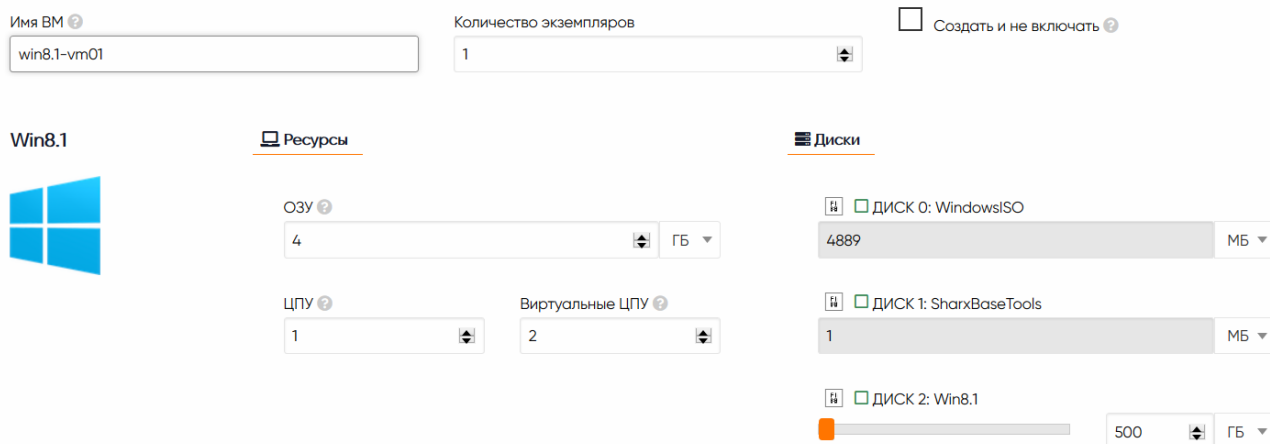


Рисунок 43 Управление запуском VM из шаблона, согласование параметров

В разделе Виртуальные машины состояние виртуальной машины последовательно будет изменяться PENDING/BOOT/START/RUNNING

После запуска VM, необходимо запустить VNC консоль, в появившемся окне, отобразится консоль выбранной VM и начнется установка OS Windows.

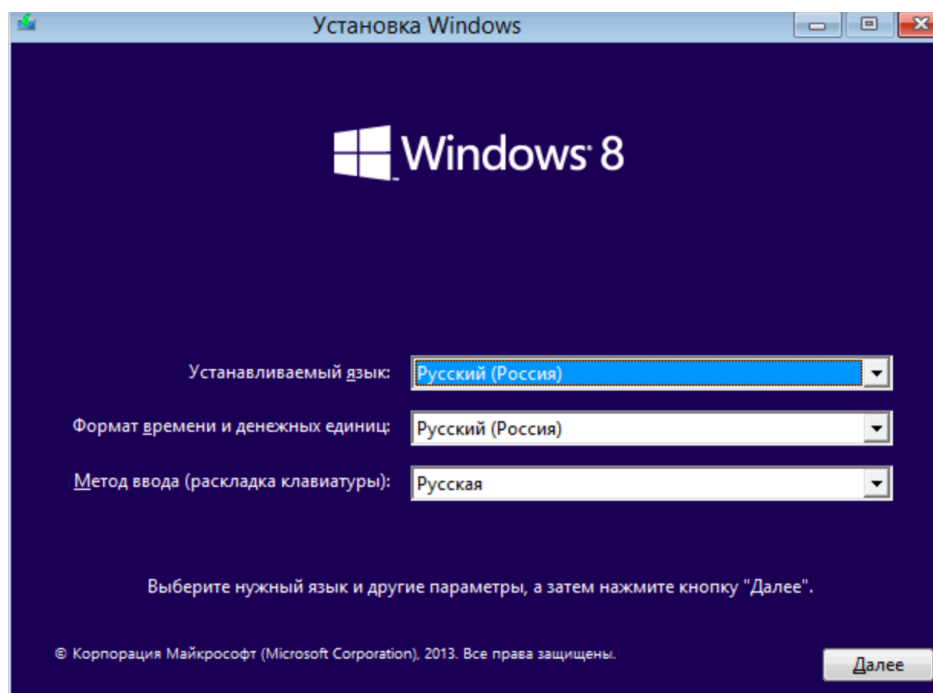
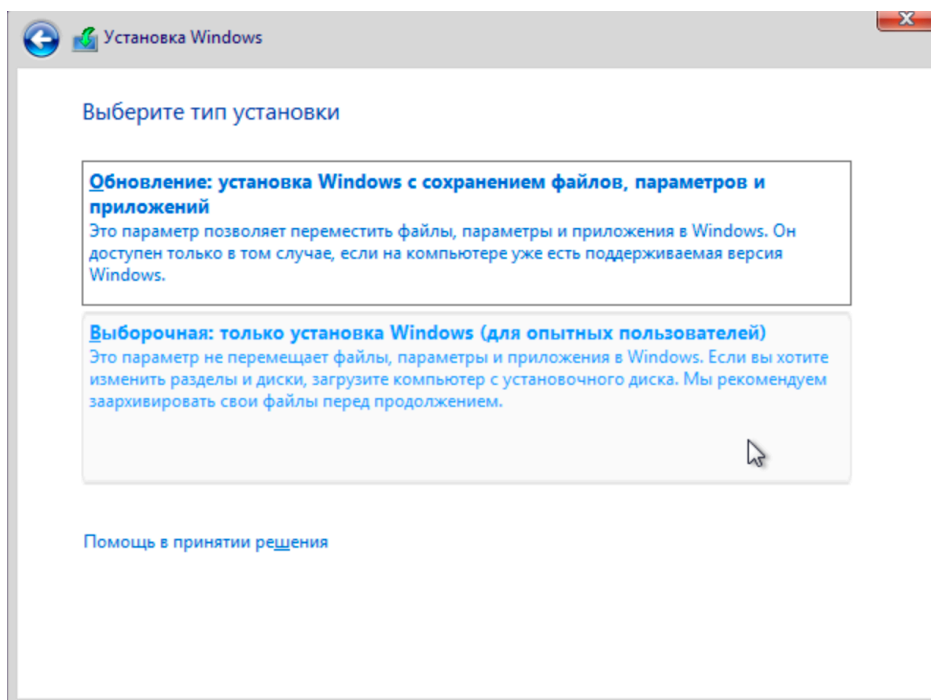


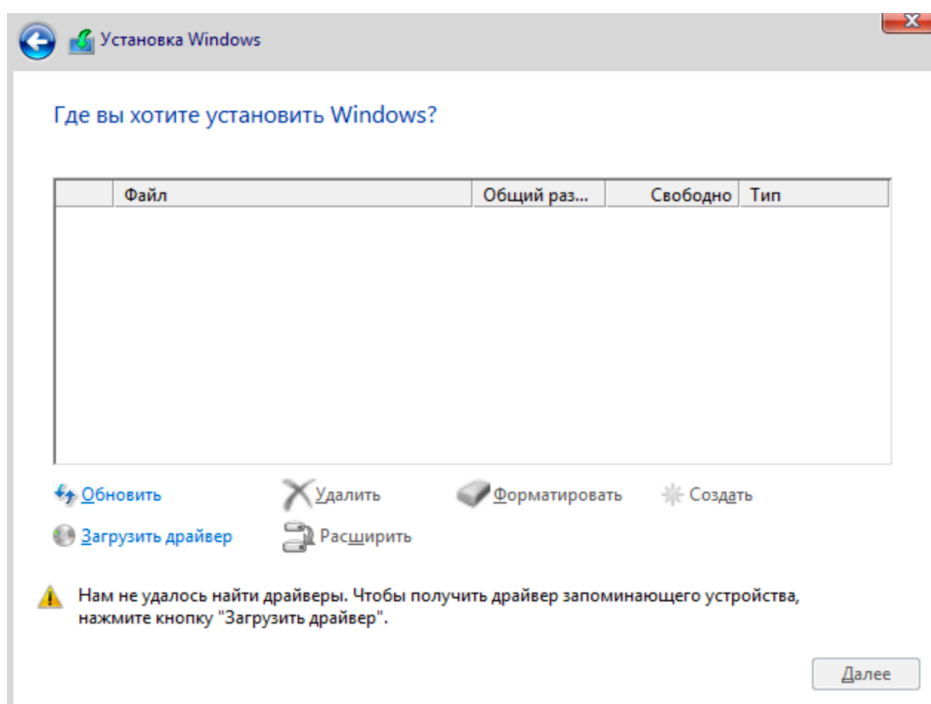
Рисунок 44 Запуск VM - удачный старт инсталлятора

### 3.2. Установка ОС

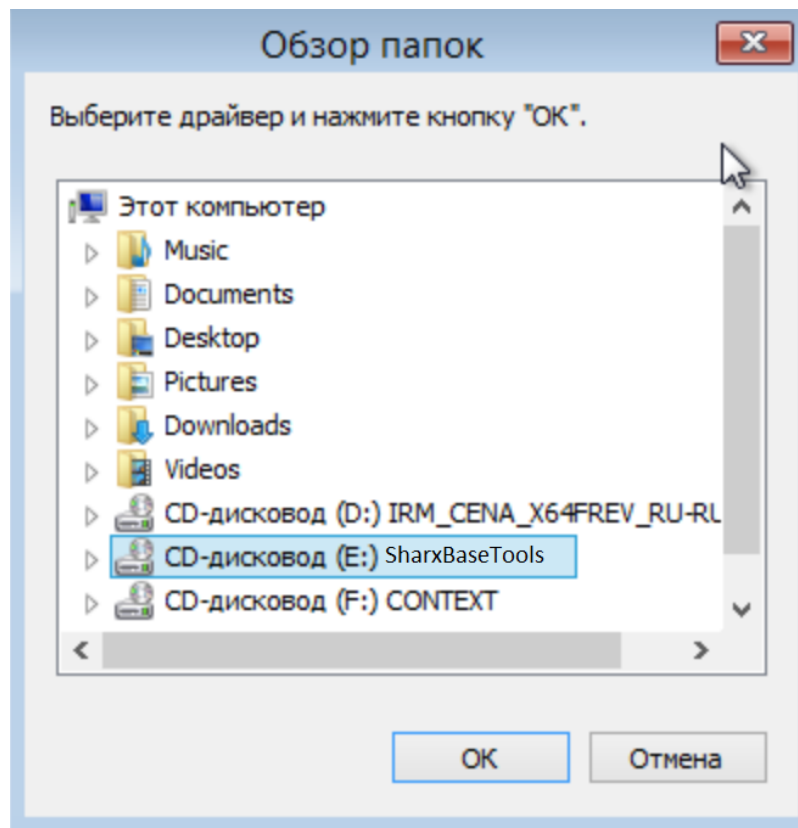
При установке ОС необходимо выбрать тип: Выборочная:



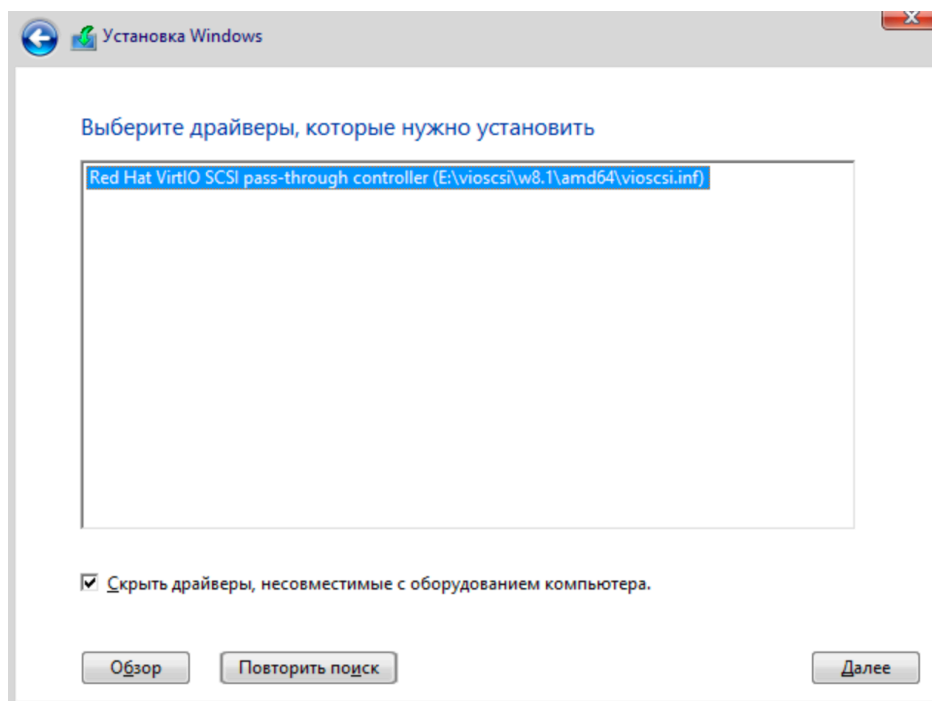
Выбрать опцию «Загрузить драйвер»:



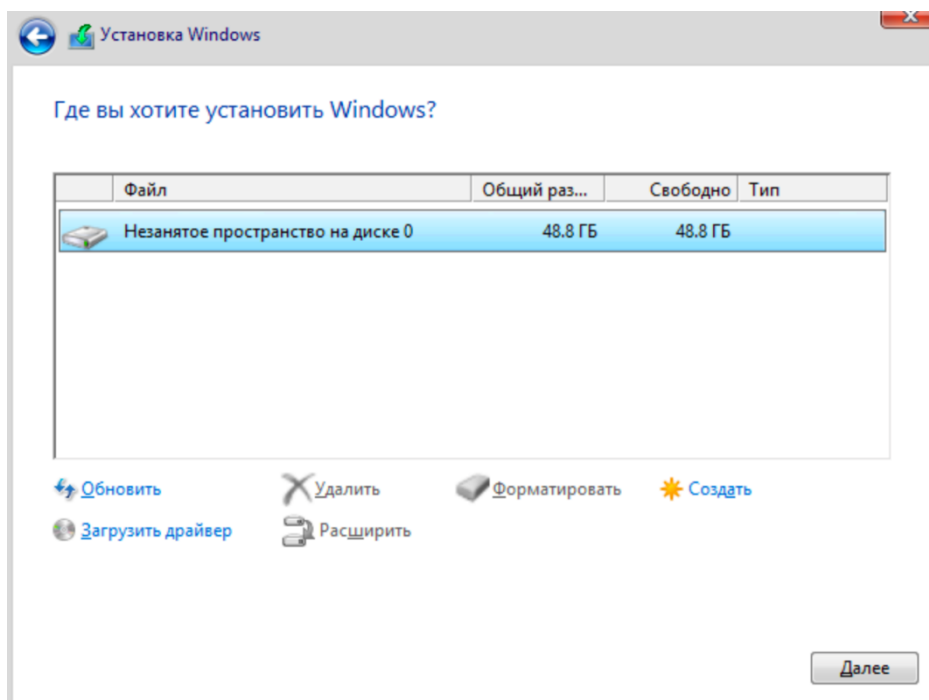
Найти в CD-ROM подключенный образ SharxBaseTools:



В образе SharxBaseTools выбрать папку с SCSI драйверами для своей версии Windows, например: `vioscsi/w8.1/amd64` и установить:



После установки драйверов появится доступное для установки пространство:



Далее производится стандартная установка ОС Windows, после чего необходимо произвести дополнительные настройки перед подготовкой конечного Шаблона.

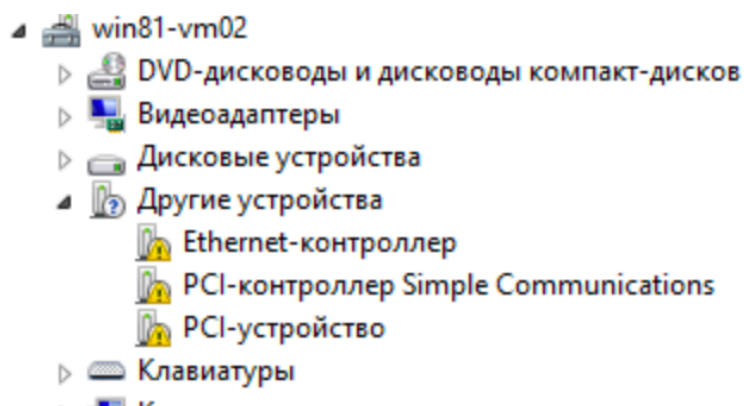
### 3.3. Установка драйверов

#### 3.3.1. Qemu-agent

После установки ОС, необходимо установить qemu-guest-agent, хранящийся на диске SharxBaseTools, в папке guest-agent, в зависимости от типа ОС, необходимо установить qemu-ga-x64.msi или qemu-ga-x32.msi пакет.

#### 3.3.2. Network adapter, Serial Driver, Baloon Driver

Далее перейти в Диспетчер устройств и обновить драйвера для всех неопознанных устройств:



В качестве места расположения драйверов указываем CD-ROM с SharxBaseTools.

### 3.4. Контекстуализация



Для корректной автонастройки сети необходимо установить пакет контекстуализации. Файл context-\*.msi находится на диске SharxBaseTools в папке guest-agent.

#### 4. Создание шаблона на основе настроенной VM

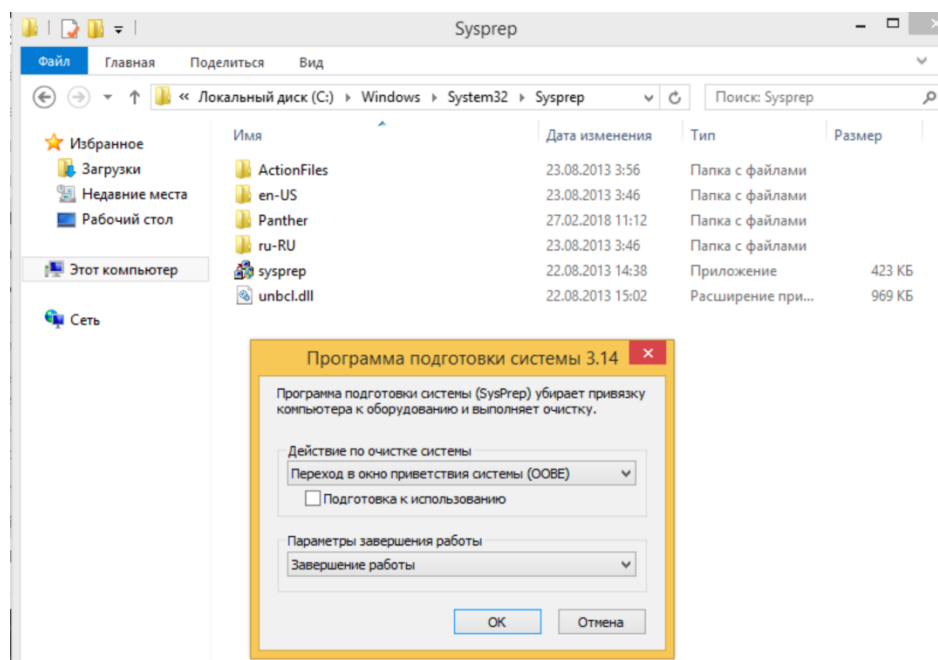
##### 4.1. Sysprep

Для исключения личных параметров (пользователи, сети, история операций и т.д.) из шаблона используется программа sysprep.

Программа Sysprep может удалить все сведения, относящиеся к операционной системе, из установленного образа Windows, включая идентификатор безопасности компьютера (SID). Затем установку Windows можно записать в образ и установить по всей организации.

Запустить sysprep по адресу:

C://Windows/System32/Sysprep/sysprep.exe



После подготовки VM и ее выключении приложением sysprep, данную виртуальную машину необходимо сохранить как конечный шаблон.

##### 4.2. Создание шаблона и удаление временных файлов

Для этого необходимо нажать кнопку «Сохранить как шаблон», на вкладке параметров VM, указав название шаблона и установив активным параметр «Статичности VM». Затем удалить старый созданный на первом этапе шаблон и виртуальную машину.

На этом подготовка шаблона VM закончена.

## 2.4.5 Создание шаблона VM Linux

Создание шаблона виртуальной машины, состоит из 4 этапов:

1. Подготовка образов.
2. Создание первичного, пустого шаблона.
3. Запуск VM, установка ОС, настройка ОС.
4. Создание шаблона на основе настроенной VM.

В данной инструкции описывается создание шаблона ОС CentOS, с точки зрения установки ОС на базе ядра Linux, инструкция будет отличаться только командами установки агентов qemu-kvm и файлов концептуализации, которые будут описаны.

### 1. Подготовка образов (images)

Необходимо загрузить два образа в раздел «Хранилища» → «Образы VM». Нажать кнопку «+», после этого ввести название образа, тип «CD-ROM только для чтения», описание и место хранения.

Далее нажать кнопку «Выбрать файл» и в появившемся окне выбрать из списка нужный образ, после чего нажать кнопку «Открыть». Заполнив все параметры, необходимо нажать кнопку «Создать».

После загрузки образов ОС и драйверов, необходимо создать образ диска, на который будет установлена ОС и задать параметры, указанные ниже, после чего нажать кнопку «Создать».

#### 1.1. Образ инсталляционного диска ОС

- Тип: CD-ROM
- Расположение образа: загрузить со своего компьютера через интерфейс управления
- Целевое устройство: HD
- Драйвер монтирования образа: RAW

## Создание образа

← ☰ Очистить все поля Создать

Имя CentOS 7	Описание
Тип Образ в формате ISO	Хранилище 1: default

Расположение образа

Путь к файлу
  Загрузить
  Пустой образ диска

CentOS7.iso

### 1.2. Образ SharxBaseTools

Образ загружен автоматически, при необходимости его можно запросить у производителя открыв заявку по почте "support@sharxdc.ru":

- Тип: CD-ROM
- Расположение образа: загрузить со своего компьютера через интерфейс управления
- Целевое устройство: HD
- Драйвер монтирования образа: RAW

### 1.3. Образ чистого диска для установки

- Тип: Блочное устройство (Datablock)
- Расположение образа: Пустой образ диска
- Образ постоянный: да
- Размер в МБ: 8000, размер минимального диска для ОС Linux необходимо уточнить в документации на ОС.
- Целевое устройство: SD
- Драйвер монтирования образа: RAW

### Создание образа

← Очистить все поля Создать

Имя: CentOS

Описание:

Тип: Блочное устройство

Хранилище: 1: default

Постоянный образ:

Расположение образа

Путь к файлу
  Загрузить
  Пустой образ диска

Размер: 8000 МБ

## 2. Создание первичного, пустого шаблона

Далее необходимо создать шаблон VM, для этого необходимо перейти в раздел «Шаблоны» → «Виртуальные Машины», нажать кнопку «+», во вкладке «Общие» внести необходимые параметры будущей VM, эти данные возможно изменить после создания шаблона

### 2.1. Общие

- ОЗУ: 1 ГБ
- ЦПУ: 1
- ВЦПУ: 1
- Логотип: CentOS

### Создать шаблон VM

← Очистить все поля Создать МАСТЕР НАСТРОЙКИ РАСШИРЕННАЯ НАСТРОЙКА

ОБЩИЕ
  ХРАНИЛИЩА
  СЕТИ
  ПАРАМЕТРЫ ЗАГРУЗКИ
  ВВОД/ВЫВОД
  КОНТЕКСТ
  ПЛАНИРОВАНИЕ
  VM GROUP

Наименование: CentOS7

Описание: CentOS7 linux

ОЗУ @: 1 ГБ

ЦПУ @: 1

Кол-во ВЦПУ @: 1

Гипервизор:  KVM

Логотип: CentOS

Изменение параметров ОЗУ @: любое значение

Изменение параметров ЦПУ @: любое значение

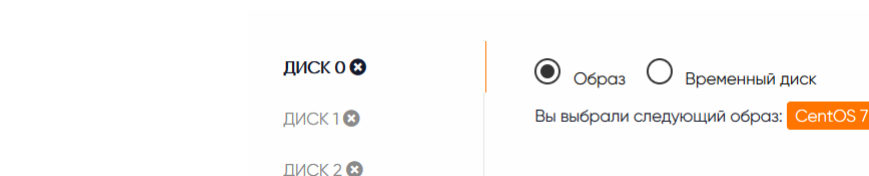
Изменение параметров vЦПУ @: любое значение

### 2.2. Хранилище

Далее во вкладке «Хранилища», необходимо добавить три диска, загруженные ранее:

- Образ установочного диска ОС;
- Образ драйверов для ОС;
- Образ пустого диска для ОС.

Добавить 3 диска с образами добавленными ранее:



Для выбранных образов нужно зайти в расширенные настройки ниже списка всех доступных образов и добавить следующие параметры:

- Для инсталляционного образа:
  - Шина (Bus): Parallel ATA (IDE)

^ Расширенные настройки

Образ

Идентификатор образа <input type="text"/>	Имя образа <input type="text" value="CentOS 7"/>
Идентификатор владельца образа <input type="text"/>	Имя владельца образа <input type="text" value="sdcadmin"/>
Префикс устройства <sup>?</sup> <input type="text" value="sdc"/>	Драйвер для подключения образа <input type="text"/>
Шина <input type="text" value="Parallel ATA (IDE)"/>	Только чтение <input type="text"/>
Контроллер шины данных <input type="text"/>	Тип инициализации диска <input type="text"/>
Кэш <input type="text"/>	Политика ввода/вывода <input type="text"/>
Сбросить <input type="text"/>	Size on instantiate <sup>?</sup> <input type="text"/> ГБ

- Для пустого диска:
  - Шина (Bus): SCSI

^ Расширенные настройки

Образ

Идентификатор образа

Имя образа

Идентификатор владельца образа

Имя владельца образа

Префикс устройства ?

Драйвер для подключения образа

Шина

Только чтение

Контроллер шины данных

Тип инициализации диска

Кэш

Политика ввода/вывода

Сбросить

Size on instantiate ?

 ГБ

- Для образа SharxBaseTools
  - Шина (Bus): Parallel ATA (IDE)

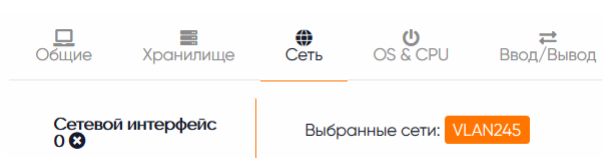
Расширенные настройки

**Образ**

Идентификатор образа <input type="text"/>	Имя образа <input type="text" value="SharxBaseTools"/>
Идентификатор владельца образа <input type="text"/>	Имя владельца образа <input type="text" value="sdcadmin"/>
Префикс устройства ? <input type="text" value="sdc"/>	Драйвер для подключения образа <input type="text"/>
Шина <input type="text" value="Parallel ATA (IDE)"/>	Только чтение <input type="text"/>
Контроллер шины данных <input type="text"/>	Тип инициализации диска <input type="text"/>
Кэш <input type="text"/>	Политика ввода/вывода <input type="text"/>
Сбросить <input type="text"/>	Size on instantiate ? <input type="text" value="ГБ"/>

### 2.3. Сеть

На вкладке «Сети», указать VLAN для сетевого интерфейса и, если в этом есть необходимость, добавить дополнительный сетевой интерфейс.



### 2.4. OS & CPU. Параметры загрузки

Архитектура ЦПУ: x86\_64

Порядок загрузки: указать первым инсталляционный диск

- ACPI = «Да»;
- APIC = «Да»;
- Местное время = «Да»;
- QEMU Guest Agent = «Да».

Общие Хранилище Сеть OS & CPU Ввод/Вывод Контекст Размещение VM

**Загрузка**

Ядро

RAM-диск

Особенности

Модель ЦПУ

Архитектура ЦПУ: x86\_64

Тип VM: [ ]

Корневое устройство: sda1

Порядок загрузки

<input checked="" type="checkbox"/>	disk0	CentOS 7	↑ ↓
<input checked="" type="checkbox"/>	disk2	CentOS	↑ ↓
<input type="checkbox"/>	disk1	SharxBASETools	↑ ↓
<input type="checkbox"/>	nic0	VLAN245	↑ ↓

## 2.5. Ввод/вывод. Устройства ввода

Тип: Планшетный ПК

Шина: USB

Нажать кнопку "Добавить"

### Устройства ввода

Тип: Планшетный ПК

Шина: USB

[Добавить](#)

## 2.6. Завершение

Для автоматизации настройки разворачиваемых виртуальных машин, предусмотрена возможность отправки параметров виртуальной машины, таких как название VM, имя пользователя и пароль, настройка сетевых параметров.

Возможно задание статических параметров и динамических, с возможностью ввода при разворачивании VM. Для задания имени VM, на вкладке «Контекст», в подразделе «Пользовательские переменные», указать следующие ключи:

- SET\_HOSTNAME = \$name, где \$name переменная, присваивающая название VM, в соответствии с названием виртуальной машины в системе. В имени виртуальной машины, должно состоять из латинских букв «a-z», «A-Z», цифр «0-9» и символа «-».

Для автоматического создания пользователя и пароля, с административными правами, в случае если необходимо задавать имя и пароль, после каждого создания VM, необходимо на вкладке «Контекст», в подразделе «Пользовательский ввод», указать следующие ключи:

- USERNAME, тип «Текст», любое описание;
- PASSWORD, тип «Пароль», любое описание.



- SSH\_PUBLIC\_KEY, строка для установки публичного ключ пользователя, в случае в контекстуализации указан пользователь, именно ему будут присвоены данные ключи, в случае отсутствия пользователя, данный ключ будет выдан пользователю root.

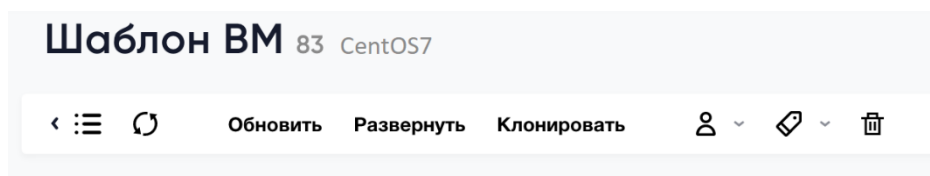
После задания параметров контекста, первый этап закончен и необходимо завершить его нажатием кнопки «Создать».

### 3. Запуск VM

Следующим этапом является запуск VM, на основе созданного шаблона. Необходимо указать имя VM, и ее параметры после чего необходимо запустить VNC консоль.

#### 3.1. Запуск VM

Запустить новую VM из шаблона используя кнопку Развернуть



Для VM должны быть заполнены все поля.

### Создать шаблон VM

← ☰ Развернуть

Инициализировать как постоянную

Имя VM       Количество экземпляров        Создать и не включать

CentOS\_7

**Ресурсы**

ОЗУ  ГБ

ЦПУ       Виртуальные ЦПУ

**Диски**

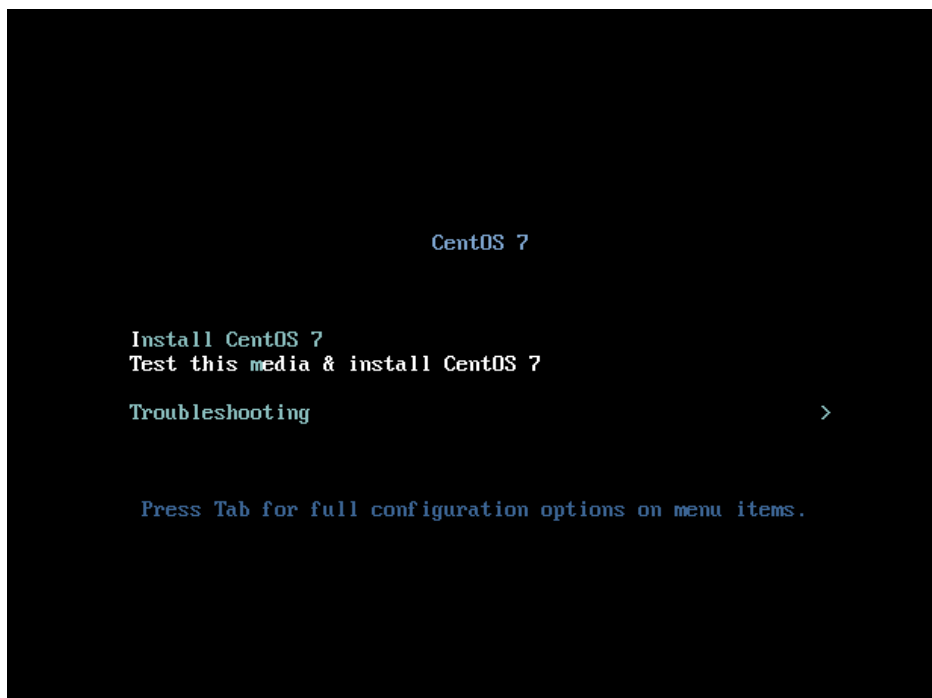
ДИСК 0: CentOS 7  МБ

ДИСК 1: SharxBaseTools  МБ

ДИСК 2: CentOS  МБ

В разделе Виртуальные машины состояние виртуальной машины последовательно будет изменяться PENDING/BOOT/START/RUNNING

После запуска VM, необходимо запустить VNC консоль, в появившемся окне, отобразится консоль выбранной VM и начнется установка OS CentOS.



Далее производится стандартная установка ОС CentOS, после чего необходимо произвести дополнительные настройки перед подготовкой конечного Шаблона.

### 3.2. Установка пакетов

#### 3.2.1. Qemu-agent

После установки ОС, необходимо установить qemu-guest-agent, хранящийся на диске SharxBaseTools, в папке guest-agent, в зависимости от типа ОС, необходимо установить необходимый пакет.

Необходимо подключить cdrom к ОС Linux

```
mount mount /dev/sr0 /mnt/
cd /mnt/guest-agent/
```

#### **CentOS/RHEL 6**

```
yum install -y qemu-guest-agent
```

#### **CentOS/RHEL 7**

```
yum install -y qemu-guest-agent
```

#### **OpenSUSE**

```
zypper install -y qemu-guest-agent
```

#### **Debian/Ubuntu**

```
apt-get install -y qemu-guest-agent
```

#### 3.2.2. Контекстуализация

Для корректной автонастройки сети необходимо установить пакет контекстуализации. Файл context находится на диске SharxBaseTools в папке guest-agent.

```
mount mount /dev/sr0 /mnt/  
cd /mnt/guest-agent/
```

### CentOS/RHEL 6

```
yum install -y epel-release  
yum install -y context-[0-9]*el6*rpm
```

### CentOS/RHEL 7

```
yum install -y epel-release  
yum install -y context-[0-9]*el7*rpm
```

### OpenSUSE

```
zypper --no-gpg-check install -y context-[0-9]*suse*rpm
```

### Debian/Ubuntu

```
apt-get purge -y cloud-init  
dpkg -i context_*deb || apt-get install -fy
```

После установки пакетов контекстуализации и агентов сети, необходимо перейти к созданию конечного шаблона.

#### 4. Создание шаблона на основе настроенной VM

Виртуальную машину, необходимо выключить и нажать кнопку «Сохранить как шаблон», на вкладке параметров VM, указав название шаблона и установив активным параметр «Сделать новый образ постоянным», удалить старый созданный на первом этапе шаблон и виртуальную машину.

На этом подготовка шаблона VM CentOS закончена.

#### 2.4.6 Группировка объектов подсистемы виртуализации

Метки используются для удобства группировки объектов, в подсистеме управления виртуализацией, таких как:

- Виртуальные машины;
- Шаблоны;
- Образы VM;
- Виртуальные сети;
- Пользователи;
- Группы.









Метки необходимы для удобства фильтрации списков объектов, отображаются в левой части экрана, в каждом из разделов подсистемы управления виртуализации, при нажатии на любую из меток, в списке отобразятся объекты, на которые установлена данная метка.

Метки распространяются внутри одной группы, для установки меток на объекты подсистемы управления виртуализацией необходимо иметь права управление, на данный объект. Администратор платформы, видит все метки установленные пользователями всех групп.

### 2.4.6.1 Иерархия меток

При создании меток, возможно создавать иерархию, путем добавления к названию метки, символа "/". Например, возможно создать иерархию меток "Клиент01/Linux", "Клиент01/Windows". При установки дочерней метки, например "Клиент01/Windows", родительская метка "Клиент01" автоматически не устанавливается, но это возможно сделать, в дальнейшем.


#### Редактировать метки

- v  Клиент01
  -    Linux
  -    Windows
- v  Клиент02
  -    Linux
  -    Windows

### 2.4.6.2 Постоянные и временные метки





Все создаваемые метки, являются временными и существуют, до тех пор, пока метка, установлена хотя бы на одном объекте, если необходимо чтобы метка не удалялась, ее необходимо заблокировать, путем нажатия на кнопку "замок". Для разблокировки необходимо аналогично нажать на кнопку замок, после чего состояние метки перейдет обратно в "разблокировано".

### 2.4.6.3 Установка и снятие метки с объекта






Для установки метки на объект или группу объектов, необходимо выделить их и нажать кнопку метки "", после этого в выпадающем меню, выбрать существующую метку либо

ввести название новой метки. После чего нажать кнопку "Enter". Метка появится в левой части экрана и при нажатии на нее, отобразятся объекты на которые установлена данная метка.

#### Редактировать метки

- Клиент01
  -   Linux
  -   Windows
- Клиент02
  -   Linux
  -   Windows

#### Редактировать метки

- Клиент01
  -   Linux
  -   Windows
- Клиент02
  -   Linux
  -   Windows
- НоваяМетка
  -   НоваяМетка

#### 2.4.6.4 Фильтрация объектов, с помощью меток

Для фильтрации объектов любого из разделов подсистемы управления виртуализацией, необходимо перейти в данный раздел, нажать на название метки и в правом окне появится отфильтрованный список объектов, для отмены фильтра по имени метки, нажмите на данную метку повторно.

#### 2.4.6.5 Пример структуры меток подсистемы управления виртуализацией

- Наименование компании
  - Наименование типа ОС (Windows/Linux)
  - Наименование проекта, продукта
- Наименование отдела эксплуатирующего ВМ
  - Наименование проекта, продукта
  - Наименование компании

Более сложная структура может привести к неудобству использования меток.

## 2.5 Описание функций работы с виртуальными сетями

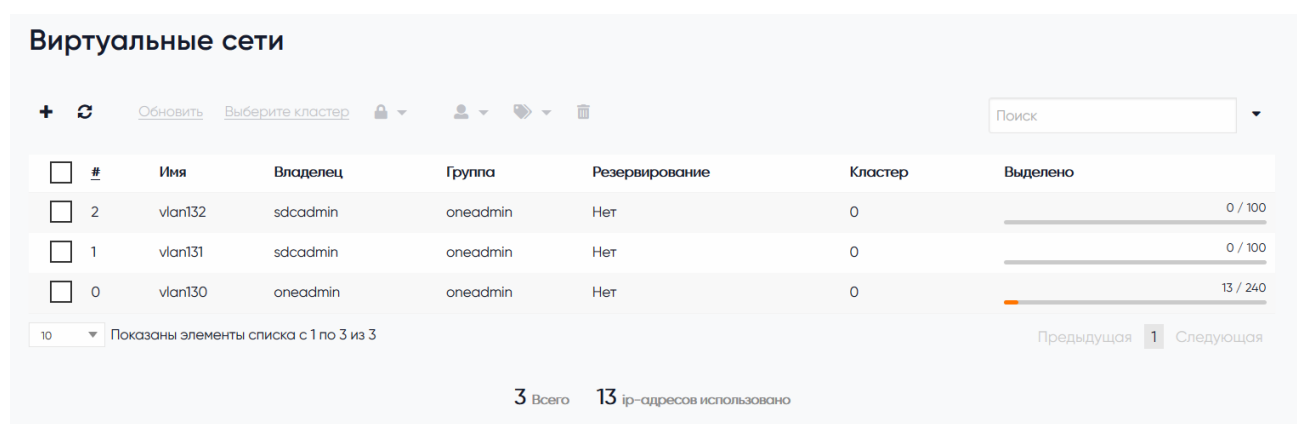
Каждый узел подключен двумя сетевыми интерфейсами к портам коммутатора, эти порты включены в режиме trunk, настройка нужных VLAN ID для VM производится путем настройки виртуальных сетей. Каждой виртуальной сети может быть присвоен владелец и группа.

### 2.5.1 Отображение списка виртуальных сетей

Для отображения списка виртуальных сетей, необходимо перейти в раздел «Сети» → «Виртуальные сети». При переходе в данный раздел, отображается список виртуальных сетей и их параметры:

- Уникальный идентификатор виртуальной сети;
- Владелец виртуальной сети;
- Группа виртуальной сети;
- Наименование виртуальной сети;
- Количество выделенных IP.

По умолчанию на странице отображается список из 10 виртуальных сетей, остальные сети отображены на следующих страницах данного раздела. Для изменения количество одновременно отображаемых на странице виртуальных сетей, необходимо в нижнем левом углу изменить данный параметр, возможны следующие значения 10, 25, 50, 100. Для перехода на следующую страницу, в нижнем правом углу, необходимо выбрать страницу, на которую необходимо перейти (см. Рисунок 45).



<input type="checkbox"/>	#	Имя	Владелец	Группа	Резервирование	Кластер	Выделено
<input type="checkbox"/>	2	vlan132	sdccadmin	oneadmin	Нет	0	0 / 100
<input type="checkbox"/>	1	vlan131	sdccadmin	oneadmin	Нет	0	0 / 100
<input type="checkbox"/>	0	vlan130	oneadmin	oneadmin	Нет	0	13 / 240

10 Показаны элементы списка с 1 по 3 из 3

3 Всего 13 ip-адресов использовано

Предыдущая 1 Следующая

Рисунок 45 Список виртуальных сетей

Для отображения списка виртуальных сетей с помощью командной строки, необходимо ввести следующие команды.

```
# sdcvnet list
```

ID	USER	GROUP	NAME	CLUSTERS	BRIDGE	LEASES
0	oneadmin	oneadmin	vlan130	0	ovsbr0	13
1	sdccadmin	oneadmin	vlan131	0	ovsbr0	0
2	sdccadmin	oneadmin	vlan132	0	ovsbr0	0

## 2.5.2 Добавление виртуальной сети

Для добавления сети, необходимо получить номер VLAN тега, который будет использоваться при настройке сети. После получения номера VLAN, зайти в раздел «Сети» → «Виртуальные сети». В данном разделе нажать кнопку «+», ввести данные (см. Рисунок 46, Рисунок 47, Рисунок 48, Рисунок 49):

- Вкладка «Общие»;
  - Наименование сети;
  - Описание;
- Вкладка «Конфигурация»;
  - Имя интерфейса сетевого моста;
  - VLAN ID, номер тега VLAN.
- Вкладка «Адреса»;
  - Первый IP адрес, первый ip адрес в диапазоне адресов;
  - Размер, количество выдаваемых адресов;
- Вкладка «Контекст»;
  - Адрес сети;
  - Маска сети;
  - Шлюз;
  - DNS;
  - MTU сетевых интерфейсов VM.

← Очистить все поля Создать Мастер настройки Расширенная настройка

Общие **Конфигурация** Адреса Безопасность QoS Контекст

Имя: VLAN245      Кластер: 0: SharxDC

Описание: Production VLAN

Рисунок 46 Создание виртуальной сети. Вкладка «Общие»

### Создать Виртуальную сеть

← Очистить все поля Создать Мастер настройки Расширенная настройка

Общие **Конфигурация** Адреса QoS Контекст

Интерфейс сет. моста: ovsbr245

Тип сети: Open vSwitch

Изоляция трафика средствами OVS. Группы безопасности не применимы

Фильтрация MAC спуфинга  
 Фильтрация IP спуфинга

VLAN ID: Ручное определение номера VLAN: 245

Физическое устройство:

Рисунок 47 Создание виртуальной сети. Вкладка «Конфигурация»

### Создать Виртуальную сеть

← Очистить все поля Создать Мастер настройки Расширенная настройка

Общие Конфигурация **Адреса** QoS Контекст

AR **+**

IPv4    IPv4/6    IPv6    Ethernet

First IPv4 address: 10.2.45.150      Первый MAC-адрес:

Размер: S1

▼ Расширенные настройки

Рисунок 48 Создание виртуальной сети. Вкладка «Адреса»



## Создать Виртуальную сеть

← Очистить все поля Создать

Мастер настройки Расширенная настройка

Общие Конфигурация Адреса QoS **Контекст**

Адрес сети: 10.2.45.0      Маска сети: 255.255.255.0

Адрес шлюза: 10.2.45.1      Шлюз IPv6:

Адрес DNS сервера: 10.2.45.1      MTU сетевых интерфейсов VM: 1500

**Пользовательские атрибуты**

Ключ	Значение
<input type="text"/>	<input type="text"/>

Рисунок 49 Создание виртуальной сети. Вкладка «Контекст»

Введя все данные, необходимо нажать кнопку «Создать». После создания сети, можно подключать данную сеть к виртуальной машине и после перезагрузки VM, настройки сети будут автоматически прописаны внутри VM.

Для создания виртуальной сети с помощью командной строки, необходимо создать файл конфигурации `vlan245.xml`.

```

NAME      = "VLAN245"
VN_MAD    = "ovswitch"
BRIDGE    = "ovsbr245"
VLAN_ID   = "245"

AR=[
  TYPE = "IP4",
  IP   = "10.2.45.150",
  SIZE = "51"
]

DNS       = "10.2.45.1"
GATEWAY   = "10.2.45.1"

DESCRIPTION = "Production VLAN"

```

И ввести следующую команду:

```
# sdcvnet create vlan245.xml
```

ID: 4

### 2.5.1 Добавление виртуальной сети на основе существующей

«ПАК» предоставляет пользователям упрощенную функцию «самообслуживания», с помощью которой пользователь может создать дочернюю виртуальную сеть, для группы ВМ. Виртуальные машины, сетевая карта которых будет подключена к дочерней сети, будет получать ip из зарезервированного диапазона, с параметрами родительской виртуальной сети, такими как маска сети, шлюз, подсеть, DNS сервер. Для создания резервирования виртуальной сети, необходимо перейти в раздел «Сети» → «Виртуальные сети», наведя курсор мыши на родительскую виртуальную сеть и нажав левую кнопку мыши. В данном разделе, нажать кнопку «Зарезервированы», в появившемся окне ввести количество резервируемых ip адресов и название создаваемой дочерней виртуальной сети (см. Рисунок 50).

Зарезервировано

Количество адресов  
30

Добавить в новую виртуальную сеть  Добавить в текущий список резерва

Имя виртуальной сети  
New\_virtual\_network

Расширенные настройки

Зарезервированы


Рисунок 50 Резервирование сети

При необходимости расширить диапазон, уже созданных созданной резервированной виртуальной сети, необходимо нажать кнопку «Добавить в ранее созданную», в появившемся окне ввести количество резервируемых ip адресов и выделить существующую резервируемую сеть (Рисунок 51).

## Зарезервировано

Количество адресов  
30

Добавить в новую виртуальную сеть  Добавить в текущий список резерва

Выбранные сети: New\_virtual\_network 

#	Имя	Владелец	Группа	Резервирование	Кластер	Выделено
5	New_virtual_network	sdcadmin	oneadmin	Да	0	0 / 30

50 Показаны элементы списка с 1 по 1 из 1 Предыдущая **1** Следующая

Расширенные настройки

Зарезервированы

Рисунок 51 Добавление диапазона в существующую сеть

Для удаления виртуальной сети с помощью командной строки, необходимо ввести следующую команду указанием id сети (`sdcvnet reserve NetworkID -n NewNetworkName -s N`), где `NetworkID` номер родительской виртуальной сети, `NewNetworkName` имя создаваемой дочерней сети, `N` – количество выделяемых ip адресов.

```
# sdcvnet reserve 4 -n MyVNET -s 10
Reservation VNET ID: 14
```

## 2.5.2 Удаление виртуальной сети

Для удаления виртуальной сети, необходимо перейти в раздел «Сети» → «Виртуальные сети», выделить нужную виртуальную сеть и нажать кнопку «Удалить» и после этого нажать кнопку «Ок» (см. Рисунок 52).

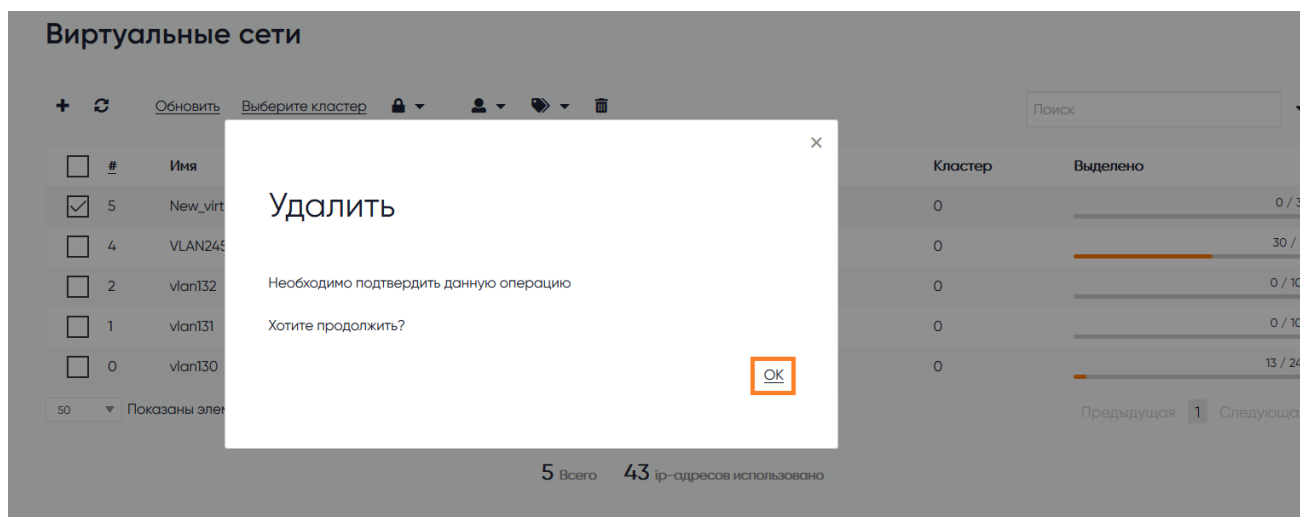



Рисунок 52 Удаление виртуальной сети

Для удаления виртуальной сети с помощью командной строки, необходимо ввести следующую команду указанием id сети.

```
# sdcvnet delete 5
```

## 2.5.1 Изменение владельца и группы виртуальной сети.

Для изменения владельца и группы виртуальной сети, необходимо перейти в раздел «Сети» → «Виртуальные сети», выделить нужную виртуальную сеть и нажать кнопку «». В

выпадающем меню выбрать кнопку «Сменить владельца», «Сменить группу», после чего в списке выбрать нужного владельца или группы и нажать кнопку «Ок» (см. Рисунок 53).

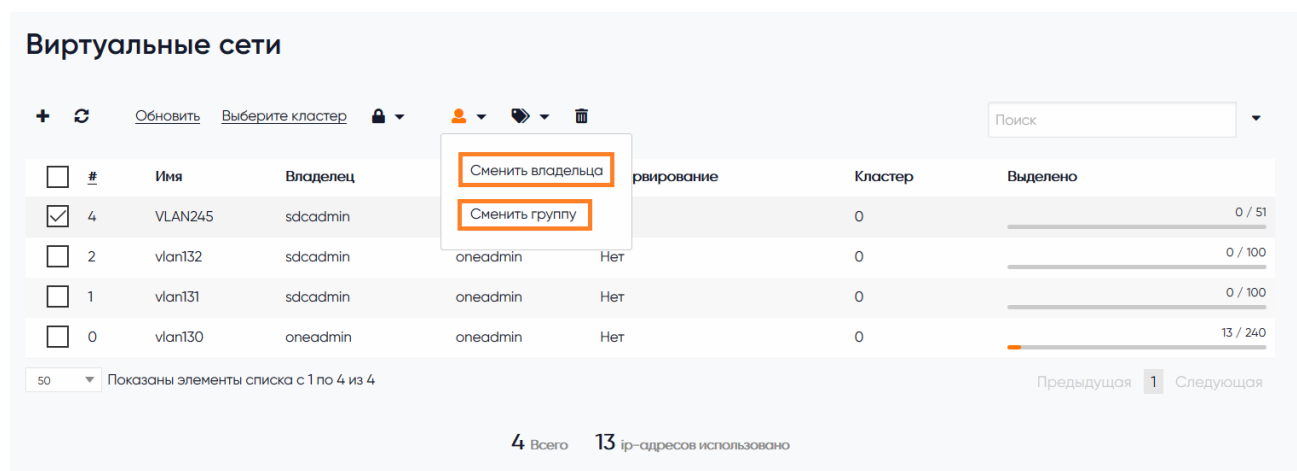


Рисунок 53 Смена владельца и группы виртуальной сети

Для смены владельца или группы виртуальной сети с помощью командной строки, необходимо ввести следующую команду «`sdcvnet chown networkid userid groupid`».

```
# sdcvnet chown 3 3 3
```

### 2.5.2 Отображение информации о виртуальной сети

Для отображения информации о текущей конфигурации виртуальной сети, нужно зайти в раздел описания данной сети, наведя курсор мыши на ее название и нажав левую кнопку мыши. В данном разделе находятся вкладки, информация, адреса, выделено (см. Рисунок 54).

Информация о виртуальной сети содержит:

- Наименование;
- VLAN ID;
- Указан владелец и группа виртуальной сети;
- Права на данную виртуальную сеть;
- QoS для трафика;
- Атрибуты.

Вкладка адреса содержат информацию о выделенных диапазонах адресов, вкладка выделено, отображает список выделенных и зарезервированных ip адресов и VM.

Виртуальная сеть 4 VLAN245

← Обновить Зарезервированы Выберите кластер

Информация Адреса Выделено Безопасность Виртуальные маршрутизаторы Кластеры

Информация	Разрешения	Использование	Управление	Администратор
# 4	Владелец	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Имя VLAN245	Группа	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN ID 245	Все остальные	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
AUTO VLAN ID Нет	<b>Владелец</b>			
OUTER VLAN ID --	Владелец sdcadmin			<input checked="" type="checkbox"/>
AUTO OUTER VLAN ID Нет	Группа oneadmin			<input checked="" type="checkbox"/>
<b>QoS для входящего трафика</b>	<b>QoS для исходящего трафика</b>			
Средняя нагрузка на сеть -- Кбайт/сек	Средняя нагрузка на сеть -- Кбайт/сек			
Пиковая нагрузка на сеть -- Кбайт/сек	Пиковая нагрузка на сеть -- Кбайт/сек			
Пиковый всплеск -- Кбайт	Пиковый всплеск -- Кбайт/сек			
<b>Атрибуты</b>				
BRIDGE ovsbr245				<input checked="" type="checkbox"/>
DESCRIPTION Production VLAN				<input checked="" type="checkbox"/>
Адрес DNS сервера 10.2.45.1				<input checked="" type="checkbox"/>
GATEWAY 10.2.45.1				<input checked="" type="checkbox"/>
GUEST_MTU 1500				<input checked="" type="checkbox"/>
NETWORK_ADDRESS 10.2.45.0				<input checked="" type="checkbox"/>
NETWORK_MASK 255.255.255.0				<input checked="" type="checkbox"/>
PHYDEV				<input checked="" type="checkbox"/>
SECURITY_GROUPS 0				<input checked="" type="checkbox"/>
VLAN_ID 245				<input checked="" type="checkbox"/>
VN_MAD ovswitch				<input checked="" type="checkbox"/>

Рисунок 54 Информация о виртуальной сети

Для отображения информации о виртуальной сети с помощью командной строки, необходимо ввести следующую команду с указанием id сети.

```
# sdcvnet show 4
VIRTUAL NETWORK 4 INFORMATION
ID           : 4
NAME        : VLAN245
USER       : sdcadmin
GROUP     : sdcadmin
CLUSTERS  : 0
BRIDGE    : ovsbr245
VN_MAD    : ovswitch
VLAN ID   : 245
USED LEASES : 3

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

```

VIRTUAL NETWORK TEMPLATE
BRIDGE="ovsbr245"
DNS="10.2.45.1"
GATEWAY="10.2.45.1"
GUEST_MTU="1500"
NETWORK_ADDRESS="10.2.45.0"
NETWORK_MASK="255.255.255.0"
PHYDEV=""
SECURITY_GROUPS="0"
VLAN_ID="245"
VN_MAD="ovswitch"

```

#### ADDRESS RANGE POOL

```
AR 0
```

```
SIZE          : 50
```

```
LEASES       : 3
```

RANGE	FIRST	LAST
MAC	00:07:0a:02:2d:64	00:07:0a:02:2d:95
IP	10.2.45.100	10.2.45.149

#### LEASES

AR	OWNER	MAC	IP	IP6
0	V:85	00:07:0a:02:2d:64	10.2.45.100	-
0	V:-1	00:07:0a:02:2d:65	10.2.45.101	-
0	V:-1	00:07:0a:02:2d:67	10.2.45.103	-

### 2.5.3 Изменить параметры виртуальной сети

Для изменения параметров ранее созданной виртуальной сети, необходимо зайти в раздел «Сети» → «Виртуальные сети», выделить нужную сеть и нажать кнопку «Обновить».

Изменить можно следующие данные.

- Вкладка «Общие» (см. Рисунок 46);
  - Описание;
- Вкладка «Конфигурация» (см. Рисунок 47);
  - VLAN ID, номер тега VLAN;
- Вкладка «Контекст» (см. Рисунок 49);

- Адрес сети;
- Маска сети;
- Шлюз;
- DNS;
- MTU сетевых интерфейсов VM.

Для изменения параметров виртуальной сети, с помощью командной строки, необходимо ввести следующие команды «sdcvnet update ID», где ID это уникальный идентификатор виртуальной сети, после чего изменить данные и сохранить их.

```
# sdcvnet update 4
BRIDGE="ovsbr245"
DNS="10.2.45.1"
GATEWAY="10.2.45.1"
GUEST_MTU="1500"
NETWORK_ADDRESS="10.2.45.0"
NETWORK_MASK="255.255.255.0"
PHYDEV=""
SECURITY_GROUPS="0"
VLAN_ID="245"
VN_MAD="ovswitch"
```

### 2.5.1 Изменить или добавить диапазон IP

Информация о выдаваемых ip адресах виртуальной сети, отображается в разделе «Информация» данной виртуальной сети, на вкладке «Адреса». На данной вкладке можно получить информацию о текущей конфигурации диапазонов, обновить эту конфигурацию и добавить новый диапазон.

Для изменения конфигурации диапазона, необходимо выделить нужный диапазон ip и нажать кнопку «Обновить» (см. Рисунок 55). Изменить возможно только диапазон ip адресов.



## Изменить диапазон ip-адресов 0

IPv4
  IPv4/6
  IPv6
  Ethernet

First IPv4 address

10.2.45.150

Первый MAC-адрес

00:00:0a:02:2d:96

Размер

50

▼ Расширенные настройки

Обновить

Рисунок 55 Редактирование диапазона адресов

Для добавления дополнительного диапазона, необходимо нажать кнопку «+» «Диапазон адресов». Внести «Первый IP адрес», «Размер», «Первый MAC» и нажать кнопку «Добавить» (см. Рисунок 56).

## Новый диапазон адресов

IPv4
  IPv4/6
  IPv6
  Ethernet

First IPv4 address

10.2.45.200

Первый MAC-адрес

Размер

32

▼ Расширенные настройки

Очистить все поля

Добавить

Рисунок 56 Новый диапазон адресов

Для изменения параметров, добавления и удаления диапазон виртуальной сети с помощью командной строки, необходимо ввести следующие команды. Изменение существующего диапазона производится следующей командой «sdcvnet updatear NetworkID AddressRangeID», изменить возможно только параметр «SIZE»

```
# sdcvnet updatear 4 0
AR=[
  AR_ID="0",
  IP="10.2.45.150",
  MAC="00:07:0a:02:2e:96",
```

```
SIZE="105",
TYPE="IP4" ]
```

Добавление диапазона производится с помощью команды «sdcvnet addar NetworkID --ip w.x.y.z --size N»

```
# sdcvnet addar 4 --ip 10.2.46.240 --size 10
```

Удаление диапазона производится с помощью команды «sdcvnet rmar NetworkID AddressRangeID»

```
# sdcvnet rmar 4 1
```

## 2.5.2 Резервация IP

Адрес можно маркировать зарезервированный, после чего: он не будет выдаваться виртуальным машинам. Для резервации IP адреса, необходимо перейти в раздел «Информацию» на вкладку «Выделено», ввести нужный IP адрес и нажать кнопку «Зарезервировать». Для удаления IP адреса из списка зарезервированных IP адресов, нажмите кнопку «▶», напротив IP (см. Рисунок 57).

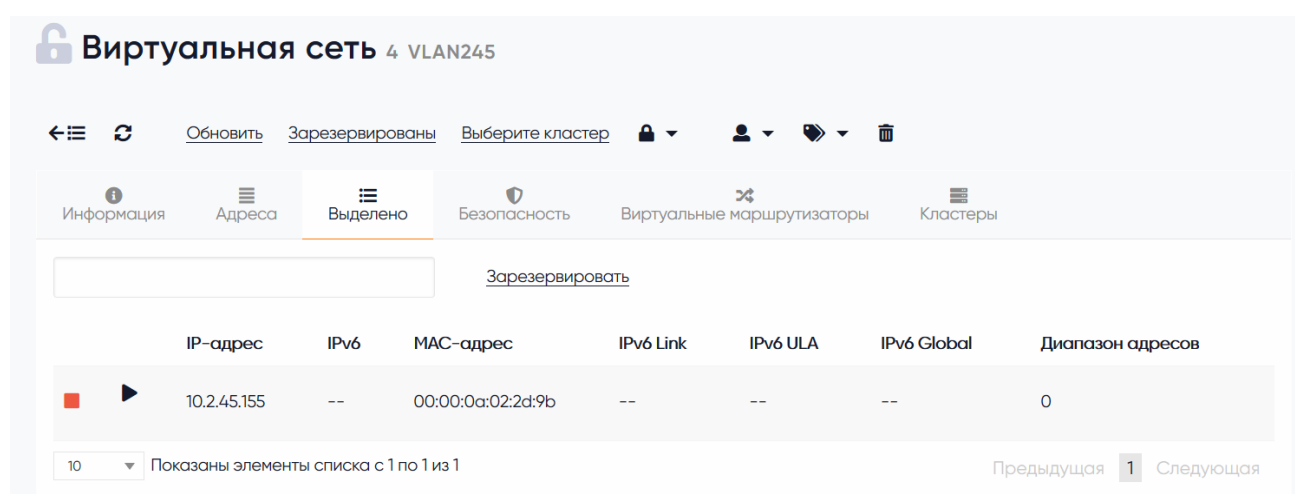


Рисунок 57 Резервирование IP

Для удержания ip с помощью командной строки, необходимо ввести следующую команду «sdcvnet hold NetworkID IP».

```
# sdcvnet hold 5 10.2.46.155
```

Для удаления из списка удержанных ip необходимо ввести следующую команду «# sdcvnet release NetworkID IP».

```
# sdcvnet release 5 10.2.46.155
```

### 2.5.3 Карта сети

В разделе «Сети» подраздел «Карта сети», отображается карта сети «ПАК», для отображения названий ВМ, необходимо нажать кнопку «Показать ВМ», для скрытия списка ВМ нажать кнопку «Скрыть ВМ», обновить страницу с помощью кнопки «↻» и сбросить параметры отображения нажав кнопку «✖» (см. Рисунок 58).

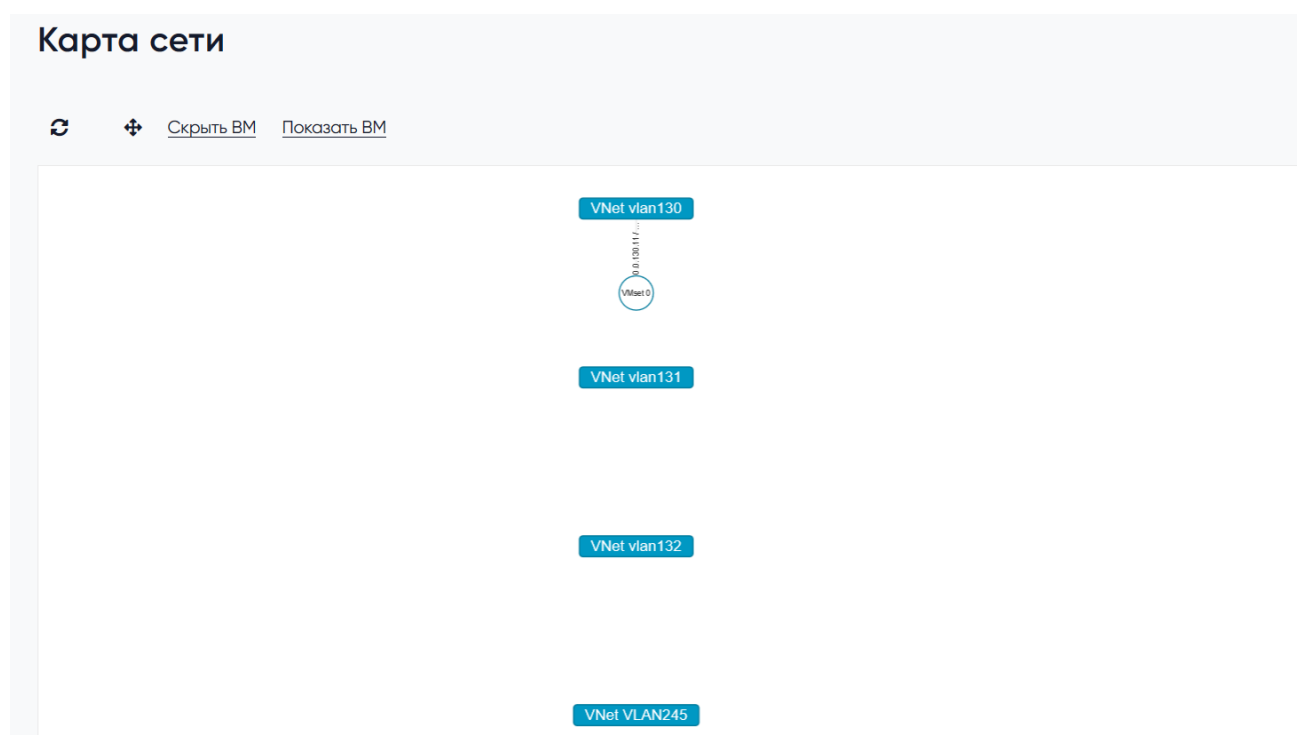


Рисунок 58 Карта сети

## 2.6 Описание функций работы с правами доступа

### 2.6.1 Описание работы с пользователями и их правами доступа

ПАК реализует полный функционал управления правами доступа пользователей. Пользователи системы разделяются на 3 типа:

- Администраторы. Пользователи с полными правами ко всем подсистемам;
- Стандартные пользователи. Пользователи, с основными правами для работы с системой;
- Сервисные пользователи. Встроенные пользователи, для подсистем и служб.

Комплекс унаследовал классическую UNIX модель прав доступа к файлам. По умолчанию, любой объект, созданный пользователем, может быть использован и управляем, только данным пользователем. Пользователь может предоставить права доступа, другим пользователям, входящим в его группу, или другим пользователем всей системы.

При создании группы, может быть задан администратор данной группы, который может создавать пользователей в данной группе, управлять ресурсами данной группы.

### 2.6.1.1 Создание, удаление, изменение параметров пользователя

При создании пользователя используется логин и пароль, также каждому пользователю присваивается уникальный ID, и группа. После установки системы, создается 2 пользователя по умолчанию `sdcadmin` и `serveradmin`, а также две группы `sdcadmin` и `users`.

Для создания пользователя необходимо зайти в раздел «Система» → «Пользователи». Далее нажать кнопку «+», ввести имя пользователя, пароль и группу, также дополнительную группу, при необходимости (см. Рисунок 59). После введения всех данных, нажать кнопку «Создать».

Создание пользователя

← Очистить все поля Создать

Имя пользователя  
sdcsuser01

Пароль  
•••••

Подтвердите пароль  
•••••

Способ аутентификации  
Стандартный

Основная группа  
1: users

Дополнительные группы

Выберите группы из списка:

#	Имя
100	test
1	users
0	oneadmin

50 Показаны элементы списка с 1 по 3 из 3

← Предыдущая 1 Следующая →

Рисунок 59 Создание пользователя

Для создания пользователя, с помощью командной строки, необходимо ввести в командной строке следующие команды:

```
$ sdcuser create sdcuser password
```

```
ID: 22
```

После создания пользователя, его параметры можно проверить и изменить в окне, свойство учетной записи. Для этого необходимо перейти в раздел «Система» → «Пользователи», выбрать нужного пользователя, и перейти в его параметры. В данной разделе, возможно сменить следующие параметры (см. Рисунок 60):

- Пароль;
- Способ аутентификации;
- Квоты;
- Группы;
- Тип интерфейса;
- Загрузить публичный ключ SSH;
- Язык интерфейса.

**Пользователь 5 sdcuser01**

← ≡ ↻ 👤 ⚙️ 🗑️

Информация | Группы | Квоты | Отчетность | Стоимость ресурсов | Аутентификация

**Информация**

#	5	
Имя	sdcuser01	
Порядок данных в таблицах	-	✎
Язык интерфейса	-	✎
Интерфейс	-	✎

**Атрибуты**

TOKEN_PASSWORD	a7b1a0a0bf1346bb8dd021ef7125ff3f1f1c6d15	✎ 🗑️
----------------	--	------

+

Рисунок 60 Параметры пользователя

Для смены группы в которую входит пользователь, нажать кнопку «Группы» и выбрать целевую группу пользователя и нажать кнопку «Применить изменения».

Для смены группы пользователя в командной строке, необходимо ввести следующую команду.

```
$ sdcuser chgrp newuser sdcadmin
```

Для вывода списка все пользователей и их групп необходимо ввести команду.

```
$ sdcuser list
```

ID	NAME	GROUP	AUTH	VMS	MEMORY	CPU
0	sdadmin	sdadmin	core	-	-	-
1	serveradmin	sdadmin	server_c	0 / -	0M / -	0.0 / -
2	newuser	sdadmin	core	0 / -	0M / -	0.0 / -

Для вывода данных, о конкретном пользователей, необходимо ввести следующую команду.

```
$ sdcuser show testuser
```

USER 2 INFORMATION

```
ID           : 22
NAME         : testuser
GROUP        : sdadmin
PASSWORD     : 07a6e833afba67a07e3697f2b42c5a89781d7ce0
AUTH_DRIVER  : core
ENABLED      : Yes
```

TOKENS

USER TEMPLATE

```
TOKEN_PASSWORD="0906b99821eba8bd2ba12b35a707c075d322b5f6"
```

RESOURCE USAGE & QUOTAS

Для изменения типа аутентификации пользователя, введите следующую команду.

```
$ sdcuser chauth newuser public
```

## 2.6.2 Описание работы с группами доступа

Группы доступа, необходимы для изоляции пользователей и ресурсов. Пользователи могут использовать только те ресурсы, владельцами которых они являются, ресурсы, входящие в группы и ресурсы открытые для всех пользователей системы.

По умолчанию создано две группы `sdadmin`, `users`. Для разграничения доступа, возможно создание дополнительных групп пользователей.

Для отображения списка текущих групп, необходимо перейти в раздел «Система» → «Группы».

Для создания группы, необходимо перейти в раздел «Система» → «Группы», нажать кнопку «+».

Далее ввести имя группы, стандартный пользовательский интерфейс, стандартный административный интерфейс, создать администратора данной группы, выдать права данной группе (см. Рисунок 61).

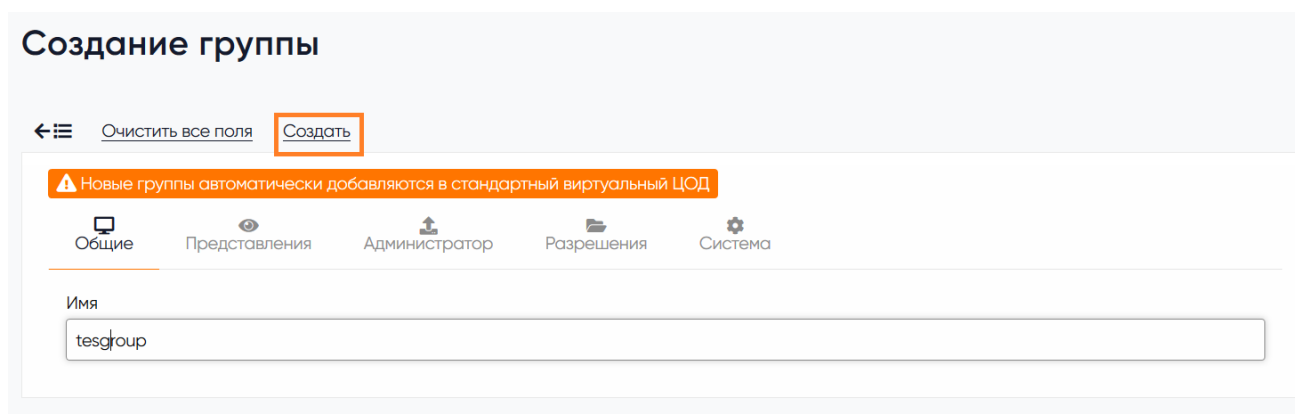


Рисунок 61 Создание группы

### 2.6.3 Описание прав доступа к объектам

Права доступа к объектам (ресурсам), выдаются субъектам, владельцу (owner), пользователям входящим в группу (group) и остальным пользователям (others). Каждому субъекту присваивается три параметра доступа использование (USE), управление (MANAGE) and администрирование (ADMIN). Права доступа применяются ко всем объектам системы кроме, пользователей, групп и узлов.

- Использование (USE) – позволяет использовать объект без его изменения. Создание VM из шаблонов, подключение образами и сетей. Данный параметр пользователь может установить, для предоставления доступа к объекту, остальным пользователям, входящим в группу пользователя или остальным пользователям системы;
- Управление (MANAGE) – Операции управления, позволяют пользователям, изменять ресурсы, останавливать VM, отключать сетевые интерфейсы. Указав параметр «Управление» пользователь предоставит права управления пользователям, входящем в его группу или остальным пользователям системы;

- Администрирование (ADMIN) – Позволяет мигрировать VM, изменять права VM, изменять права шалона, удалять и изменять группы.

Для объекта «Виртуальные машины» возможно гранулировать все действия разделив их на 3 типа прав доступа. Данные параметры, настраиваются с помощью cli.

- VM\_ADMIN\_OPERATIONS
- VM\_MANAGE\_OPERATIONS
- VM\_USE\_OPERATIONS

Список операций, которые можно распределить между 3 типами прав:

- Перенести VM (Migrate);
- Удалить (Delete);
- Сбросить состояние (Recover);
- Повтор операции (Retry);
- Развенуть (Deploy);
- Освободить ресурсы (Undeploy);
- Пересоздать и отменить пересоздание (Resched, unresched);
- Приостановить создание (Hold);
- Продолжить создание (Release);
- Приостановить (Stop);
- Остановить (Suspend);
- Старт (Resume);
- Перезагрузить (Reboot);
- Выключить (Poweroff);
- Добавить/Отключить диск(Disk-attach/detach);
- Подключить/Отключить сетевой адаптер (Nic-attach/detach);
- Создать/Удалить/Восстановить снимок диска (create, delete and revert);
- Создать/Удалить/Восстановить снимок VM (create, delete and revert);
- Удалить (Terminate);
- Изменить размер диска (Disk-resize);
- Изменить конфигурацию (Update conf);
- Переименовать (Rename);
- Изменить параметры ОЗУ, ЦПУ (Resize);
- Сохранить диск (Disk-saveas).



При работе с объектами платформы, пользователь при необходимости может произвести блокировку объекта, что не возволит например, удалить объект по ошибке. По умолчанию, платформа блокирует все операции над объектом, но при разных правах на объект, у разных пользователей, блокировка работает следующим образом.

- Использование (USE): блокирует все возможные операции;
- Управление (MANAGE): блокирует операции относящиеся к управлению ит рированию;
- Администрирование (ADMIN): блокирует операции относящиеся к администрированию.

Ресурсы которые возможно заблокировать, описаны ниже:

- Виртуальные машины;
- Сети;
- Образы дисков;
- Шаблоны;
- Виртуальные роутеры;
- Магазин приложений.

Важно отметить, что блокировки не действуют на пользователя Администратор платформы.

Управление правами доступа возможно производить как с помощью веб-интерфейса, так и с помощью командной строки cli.

### 2.6.3.1 Правила ACL

Любые операции, производимые пользователем или группой пользователей, проверяются в правилах ACL. Каждая операция, генерирует запрос к правилам ACL и система может подтвердить запрос при наличие доступа к объекту или операции либо оклонить его. Данные правила позволяют администраторам платформы, настраивать права пользователей в соответствии с их требованиями к инфраструктуре. Механизм ACL является расширенным механизмом настройки прав доступа и в обычных условиях, достаточно использовать стандартный механизм выдачи прав, на основе заранее сгенерированных ACL правил.

Правила состоят из следующих частей:

Пользователь – указывается в виде его ID;

Объект – состоит из списка объектов, перечисляемых через «+» и отделяемых «/» с указанием ID подмножества ресурсов;

Права – список прав доступа, использование, управление, администрирование, при использовании нескольких перечисляемых через «+».

Зона – по умолчанию, указывается значение 0 или \*. В первом случае это ID зоны по умолчанию или \* при использовании всех.

ID для пользователя может быть описано, как #ID пользователя, @ID группы или \* для всех.

Ресурсы перечисляемые списком:

- V : VM – Виртуальная машина;
- H : HOST – Узел;
- N : NET – Сеть;
- I : IMAGE – Образы дисков;
- U : USER – Пользователи;
- T : TEMPLATE - Шаблоны;
- G : GROUP – Группы;
- D : DATASTORE – Хранилища;
- C : CLUSTER – Кластеры;
- Z : ZONE – Зоны;
- v : VDC – Виртуальные ДЦ;
- R : VROUTER – Виртуальные роутеры;
- M : MARKETPLACE
- A : MARKETPLACEAPP

ID ресурса имеет аналогичное описание, но для описания кластера используется %ID

Пример 1:

```
#22 VM+NET+IMAGE+TEMPLATE/* CREATE #0
```

Пользователь с id 22 получил права на созданием объектов виртуальных машин, сетей, образов, шаблонов в кластере 0.

Пример 2:

```
#22 NET/#22 USE #0
```

Пользователь с id 22 получил права на использование сети с ID22, пользователь сможет создавать VM на основе шаблонов с данной сетью при добавлении к MANAGE подключать данные сети к своим vm в кластере 0.

Пример 3:

```
#22 NET/@22 USE #0
```

Пользователь с id 22 получил права на использование всех сетей принадлежащих группе ID22, пользователь сможет создавать VM на основе шаблонов с данными сетями при добавлении к MANAGE подключать данные сети к своим vm в кластере 0.

Пример 3:

```
#22 NET/%0 USE #0
```

Пользователь с id 22 получил права на использование всех сетей принадлежащих кластеру ID0, пользователь сможет создавать VM на основе шаблонов с данными сетями при добавлении к MANAGE подключать данные сети к своим vm в кластере 0.

Для создания ACL правила, можно использовать веб-интерфейс или cli. В случае если необходимо изменить правило, его нужно удалить и создать заново.

Просмотр правил в cli

```
$ sdcac1 list
ID      USER RES_VHNIUTGDCOZSvRMAP  RID OPE_UMAC  ZONE
0       @1    V--I-T---O-S----P        *   ---c      *
1       *     -----Z-----          *   u---      *
2       *     -----MA-             *   u---      *
3       @1    -H-----              *   -m--      #0
4       @1    --N----D-----          *   u---      #0
5       @100  -H-----              *   -m--      #0
6       @100  --N----D-----          *   u---      #0
7       @100  V-NI-T---O-S-R---        *   ---c      *
8       @100  V-----O-----         @100 u---      *
9       #2    ----U-----            @100 umac      *
10      #2    V-NI-T---O-S-R--P        @100 um--      *
11      #2    -----R---             *   ---c      *
12      #2    -----G-----         #100 -m--      *
```

Созание правила в cli

```
$ sdcac1 create #22 NET/@22 USE #0
ID: 524
$ sdcac1 list
524     #22    --N-----          @22    u---      #0
```

Удаление правила в cli

```
$ sdcac1 delete 524
```

## 2.7 Описание функций работы с виртуальными маршрутизаторами

Виртуальные маршрутизаторы обеспечивают маршрутизацию внутри виртуальных сетей кластера. Пользователи могут подключать виртуальные сети через веб-интерфейс и с помощью командной строки. Виртуальный маршрутизатор может быть развернута в режиме высокой доступности, путем создания нескольких экземпляров ВМ для виртуального маршрутизатора и реализации функции плавающего ip адреса.

### 2.7.1 Создание шаблона виртуального маршрутизатора

Шаблон виртуального маршрутизатора предоставляется в виде образа ВМ, который загружается в хранилище образов ВМ (см. 2.4.2). После загрузки образа виртуального маршрутизатора, необходимо перейти в раздел «Шаблоны» → «Шаблоны виртуального роутера», нажать кнопку «+». В появившемся списке необходимо заполнить следующие данные (см. Рисунок 62).

Вкладка «Общие»:

- Наименование;
- Описание;
- Гипервизор;
- Логотип
- ОЗУ
- ЦПУ
- Кол-во ВЦПУ

Вкладка «Хранилища»:

- Диск 0;

## Создание шаблона виртуального маршрутизатора

Очистить все поля **Создать** Мастер настройки Расширенная настройка

Общие Хранилище Сеть OS & CPU Ввод/Вывод Контекст Метки

Имя: vrouter-tmpl

Описание: Vrouter template

Логотип: Linux

ОЗУ: 1 GB

Параметры ОЗУ: произвольное

Cost: 0.00 Стоимость / Месяц

ЦПУ: 1

Параметры ЦПУ: произвольное

Cost: 0.00 Стоимость / Месяц

Виртуальные ЦПУ: 1

Параметры виртуальных ЦПУ: произвольное

Стоимость Total: 0.00 Стоимость / Месяц

ОЗУ: MB ЦПУ: Диск:

Запретить изменение конфигурации сети

Пометить этот шаблон как шаблон виртуального маршрутизатора

Рисунок 62 Создание шаблона виртуального маршрутизатора

Остальные параметры можно отставить по умолчанию, после ввода данных, нажать кнопку «Создать». Если все параметры заданы правильно, после нажатия кнопки «Создать», появится окно со списком, в котором будет новый шаблон маршрутизатора (см. Рисунок 63).

### Шаблоны виртуальных маршрутизаторов

+ ↻ Обновить Развернуть Клонировать

<input type="checkbox"/>	#	Имя	Владелец	Группа	Время регистрации
<input type="checkbox"/>	2	vrouter-tmpl	sdcadmin	oneadmin	25/01/2019 16:22:22

50 Показаны элементы списка с 1 по 1 из 1

1 Всего

Предыдущая 1 Следующая

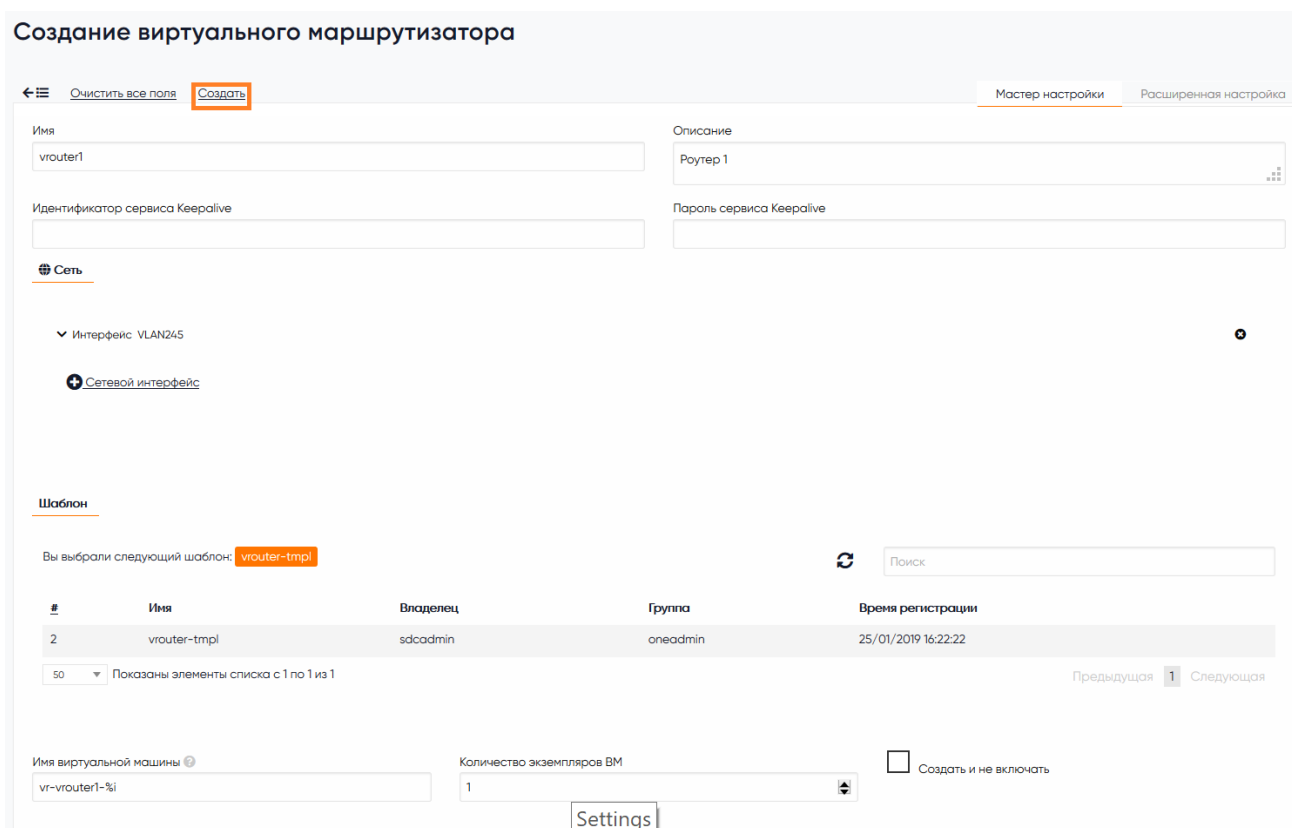
Рисунок 63 Подтверждение создания шаблона

Для создания шаблона виртуального маршрутизатора, необходимо воспользоваться командой.

## 2.7.2 Создание виртуального маршрутизатора

Для создания виртуального маршрутизатора необходимо зайти в раздел «Виртуализация» → «Маршрутизация», нажать кнопку «+», выбрать шаблон маршрутизатора, и ввести следующие параметры (см. Рисунок 64):

- Наименование;
- Описание;
- Сетевой интерфейс 1;
  - VLAN ID, номер тега VLAN;
- Сетевой интерфейс 2;
  - Force IP;
- Шаблон;
- Количество экземпляров.



**Создание виртуального маршрутизатора**

← Очистить все поля **Создать** Мастер настройки Расширенная настройка

Имя:  Описание:

Идентификатор сервиса Keeralive:  Пароль сервиса Keeralive:

**Сеть**

Интерфейс VLAN245

Сетевой интерфейс

**Шаблон**

Вы выбрали следующий шаблон: **vrouter-templ**

#	Имя	Владелец	Группа	Время регистрации
2	vrouter-templ	sdcadmin	oneadmin	25/01/2019 16:22:22

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

Имя виртуальной машины  Количество экземпляров VM:   Создать и не включать

**Settings**

Рисунок 64 Создание виртуального маршрутизатора

Для создания виртуального маршрутизатора, необходимо воспользоваться командой «sdcvrouter». Перед созданием виртуального коммутатора, необходимо подготовить файл конфигурации.

```
$ vi vrouter-01.txt
NAME = vrouter-01
NIC = [
  NETWORK="internal-net",
  IP="192.168.1.2" ]
NIC = [
  NETWORK="external-net",
  IP="192.168.1.2" ]
```

Далее создать виртуальный маршрутизатор, используя ранее созданную конфигурацию.

```
$ sdcvrouter create myvr.txt
ID: 1
```

После создания виртуального маршрутизатора необходимо подключить виртуальный маршрутизатор к шаблону.

```
$ sdcvrouter instantiate <vrouterid> <templateid>
```

### 2.7.3 Настройка виртуального маршрутизатора

Описание настройки виртуального маршрутизатора не входит в данный документ и будет описано в отдельном документе.

## 2.8 Описание функций работы с МЗИ

Модуль предназначен для расширения функциональности механизмов управления пользовательскими паролями, логинами и политиками их хранения, регистрации событий информационной безопасности, а также для управления сессиями субъектов доступа.

Модуль является программным средством защиты информации от несанкционированного доступа путем идентификации и аутентификации, а также авторизации субъектов доступа. Модуль рассчитан на применение в автоматизированных системах до класса 1Г (включительно), в государственных информационных системах до 1 класса (включительно) и информационных системах персональных данных до 1 уровня защищенности (включительно).

### 2.8.1 Управление учётными записями субъектов доступа

Для просмотра учетных записей (далее – УЗ), необходимо перейти в раздел «Система» подраздел «Пользователи» (см. Рисунок 65).

#	Наименование	Группа	Драйвер авторизации	Статус	Серверы	ОЗУ	ЦПУ
114	Test02	users	sharx-scm	active		0 / -	0KB / - 0 / -
111	Test01	users	sharx-scm	active		0 / -	0KB / - 0 / -
110	usertest20	users	sharx-scm	active		0 / -	0KB / - 0 / -
109	testuseradd	sdadmin	core	core		0 / -	0KB / - 0 / -
107	usertest157	users	sharx-scm	active		0 / -	0KB / - 0 / -
104	usertest14	users	sharx-scm	active		0 / -	0KB / - 0 / -
103	usertest13	users	sharx-scm	deleted		0 / -	0KB / - 0 / -
102	usertest12	users	sharx-scm	deleted		0 / -	0KB / - 0 / -
101	usertest11	users	sharx-scm	deleted		0 / -	0KB / - 0 / -
100	usertest9	users	sharx-scm	deleted		0 / -	0KB / - 0 / -
98	slyladmin	shoadmin	sharx-scm	active		0 / -	0KB / - 0 / -
97	usertest10	users	sharx-scm	deleted		0 / -	0KB / - 0 / -
96	sharx_user_test2	users	sharx-scm	active		0 / -	0KB / - 0 / -
94	sdadmin	sdadmin	core	core		0 / -	0KB / - 0 / -
91	sharxscm_admin_test4	users	sharx-scm	active		0 / -	0KB / - 0 / -
90	sharxscm_admin_test3	users	sharx-scm	active		0 / -	0KB / - 0 / -

Рисунок 65 Список пользователей для МЗИ

На странице отобразится список УЗ пользователей Системы в табличном виде.

Для каждой УЗ показаны следующие атрибуты:

- «Драйвер авторизации» - драйвер, который использовался при создании УЗ (МЗИ работает только для субъектов доступа с драйвером sharx-scm);
- «Статус» - статус УЗ - «активна» (active)/ «блокирована» (blocked)/ «на удалении» (deleted).

Для УЗ с драйвером, отличным от sharx-scm, в колонке «Статус» отображается имя драйвера. В столбцах «#», «Наименование», «Группа», «Серверы», «ОЗУ», «ЦПУ» отображаются данные Системы, МЗИ не влияет на процесс их генерации и отображения. Для обновления списка УЗ следует нажать кнопку обновить.

Фильтрация записей списка УЗ возможна на всех вкладках с помощью формы поиска (см. Рисунок 66):

Рисунок 66 Форма поиска



В поле поиска нужно ввести строку символов, которая является поисковой подстрокой в множестве значений реквизитов УЗ. В списке будут выводиться УЗ, указанные реквизиты которых имеют введённую поисковую подстроку. Также можно выбрать количество отображаемых на странице УЗ с помощью выпадающего списка внизу страницы:

### 2.8.2 Создание новой УЗ для работы с МЗИ

Для создания УЗ следует нажать кнопку «+». На странице отобразится форма ввода информации о субъекте доступа (Рисунок 67).

## Создать пользователя

< ☰
Очистить все поля
Создать

Имя пользователя

Пароль

Подтвердите пароль

Способ аутентификации

Стандартный
▼

Основная группа

По умолчанию
▼

Дополнительные группы

Пожалуйста, выберите одну или несколько групп из списка

↻

#	Наименование
106	Test2
105	kirillgroup
102	Test_Group
100	Test_Admins
1	users
0	admin

▼
1

Рисунок 67 Создание пользователя для МЗИ

Необходимо заполнить реквизиты новой УЗ. Для использования МЗИ нужно выбрать в качестве способа аутентификации драйвер sharx-scm (см. Рисунок 68).

Способ аутентификации

- ✓ Стандартный
- Публичный
- ssh
- x509
- ldap
- server\_cipher
- server\_x509
- sharx-scm**
- Настраиваемый

Пожалуйста, выберите одну или несколько групп из списка

Поиск

Рисунок 68 Выбор способа аутентификации

При вводе данных, противоречащих правилам, заданным в настройках, будет выведено предупреждение (Рисунок 69).

### Создать пользователя

Очистить все поля Создать

Имя пользователя  
user12345678

Пароль Подтвердите пароль  
\*\*\*\*\*

Способ аутентификации  
sharx-scm

Основная группа  
105: kirillgroup

Дополнительные группы

Пожалуйста, выберите одну или несколько групп из списка

#	Наименование
106	Test2
105	kirillgroup
102	Test_Group
100	Test_Admins
1	users
0	admin

100

Пароль должен содержать специальные символы

Рисунок 69 Вывод предупреждения об ошибке ввода

Для сохранения новой УЗ нужно нажать кнопку «Создать». Для возврата к списку УЗ нужно нажать кнопку «<» - введенные данные при этом не сохранятся. При нажатии кнопки

«Очистить все поля» будет осуществлен возврат к первоначальным значениям реквизитов (по умолчанию – пустым полям).

После сохранения будет осуществлен переход на вкладку «Пользователи», где будет отмечено, что создана новая УЗ с указанием ее ID и наименования (Рисунок 70).

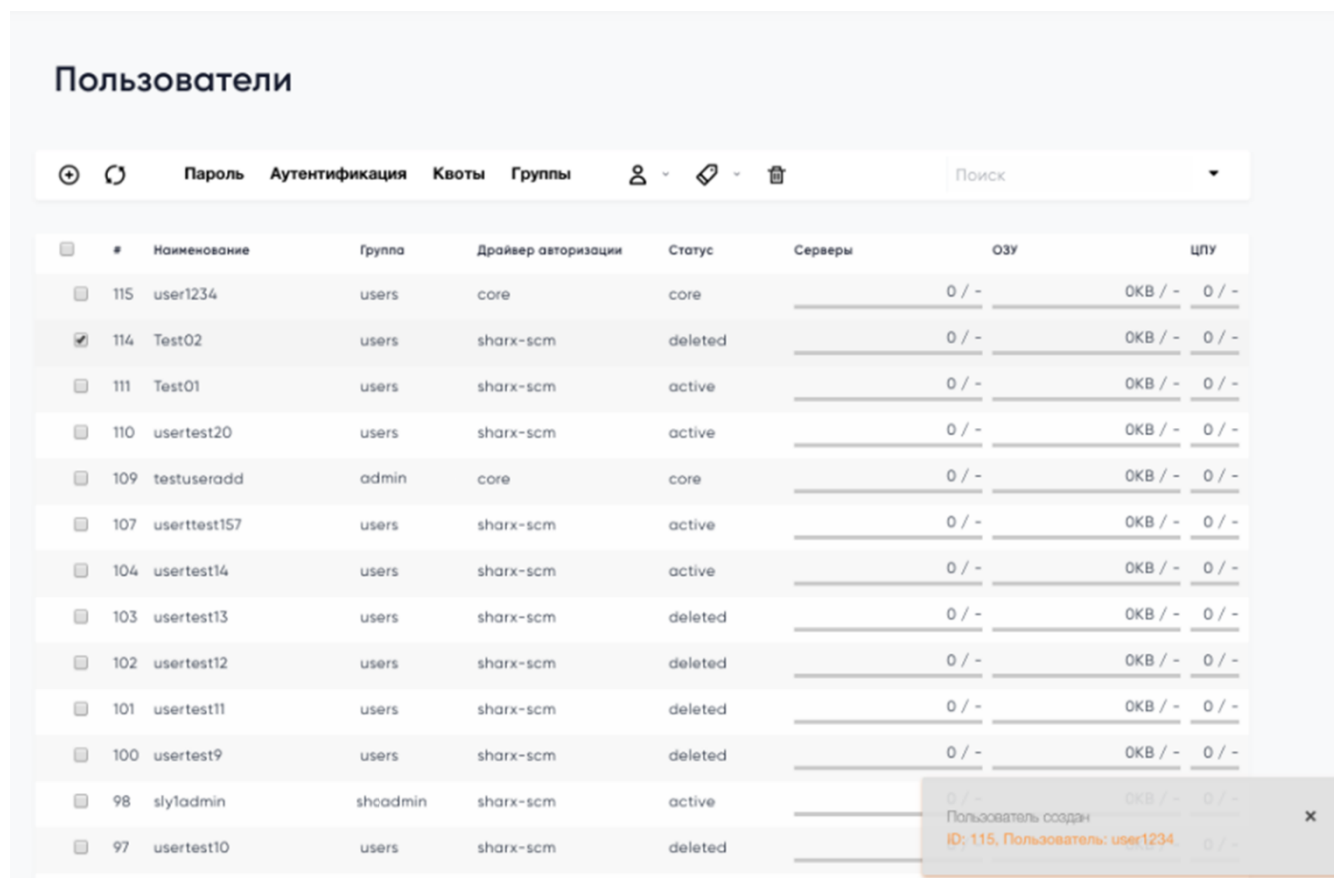


Рисунок 70 Вывод уведомления об изменениях

## 2.8.3 Просмотр и изменение УЗ

Для просмотра атрибутов или внесения изменений в УЗ субъекта доступа необходимо нажать на нужную УЗ – откроется карточка УЗ (см. Рисунок 71).

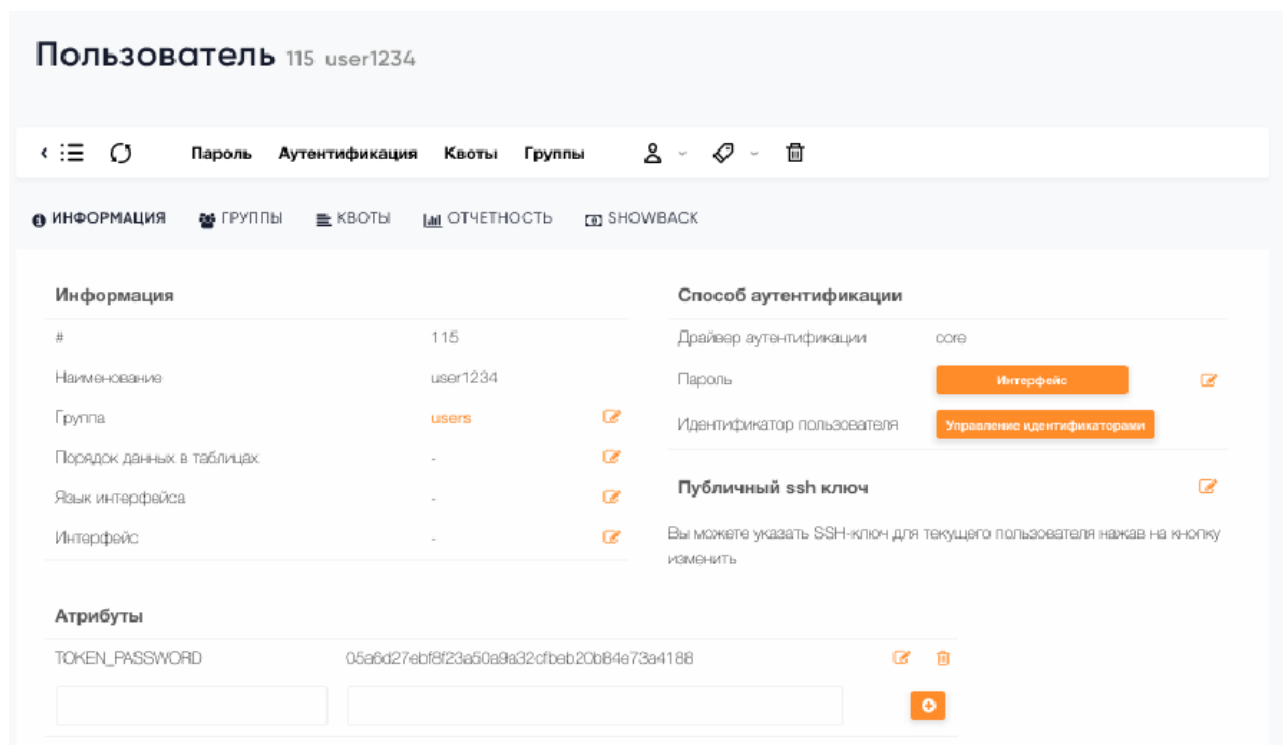


Рисунок 71 Список атрибутов УЗ

Для того чтобы действие МЗИ распространилось на УЗ, нужно в поле «Драйвер аутентификации» выбрать sharx-scm. Для изменения поля нужно нажать кнопку «Изменить». Изменения будут сохранены после ввода информации в поле, дополнительное подтверждение не требуется. Для возврата к списку УЗ нужно нажать кнопку «<<» - введенные данные при этом не сохраняются.

## 2.8.4 Блокировка УЗ

Для блокировки УЗ необходимо выбрать пункт меню «Блокировки» МЗИ (см. Рисунок 72)

Рисунок 72 Меню блокировки

Откроется соответствующая страница. Следует нажать кнопку «+» - отобразится форма блокировки, где указывается логин УЗ и причина блокировки (см. Рисунок 72).

Рисунок 72 Окно создание блокировки

Для сохранения блокировки УЗ нужно нажать кнопку «Создать». Для возврата к списку заблокированных УЗ нужно нажать кнопку «<» - введенные данные при этом не сохранятся. При нажатии кнопки «Очистить все поля» будет осуществлен возврат к первоначальным значениям реквизитов (по умолчанию – пустым полям).

На странице «Пользователи» статус УЗ поменяется на «blocked» (см. Рисунок 73)

### Пользователи

Пароль Аутентификация Квоты Группы
  
Поиск

<input type="checkbox"/>	#	Наименование	Группа	Драйвер авторизации	Статус	Серверы	ОЗУ	ЦПУ
<input type="checkbox"/>	39	newuser	users	core	unknown	_____	0 / -	ОКВ / - 0 / -
<input type="checkbox"/>	36	deluser	users	sharx-scm	deleted	_____	0 / -	ОКВ / - 0 / -
<input type="checkbox"/>	35	checkblock	users	sharx-scm	active	_____	0 / -	ОКВ / - 0 / -
<input type="checkbox"/>	34	testadm	shcadmin	core	unknown	_____	0 / -	ОКВ / - 0 / -
<input type="checkbox"/>	33	secadmin	shcadmin	core	unknown	_____	0 / -	ОКВ / - 0 / -
<input type="checkbox"/>	32	nonadmin	shcadmin	core	unknown	_____	0 / -	ОКВ / - 0 / -
<input type="checkbox"/>	31	slyadmin	shcadmin	sharx-scm	active	_____	0 / -	ОКВ / - 0 / -
<input type="checkbox"/>	30	kirilladmin	users	sharx-scm	blocked	_____	0 / -	ОКВ / - 0 / -
<input type="checkbox"/>	22	t1234	users	sharx-scm	active	_____	0 / -	ОКВ / - 0 / -

Рисунок 73 Отображение списка пользователей

Для разблокировки нужно выбрать УЗ и нажать кнопку «Удалить», затем нажать кнопку «ОК» (см. Рисунок 74).

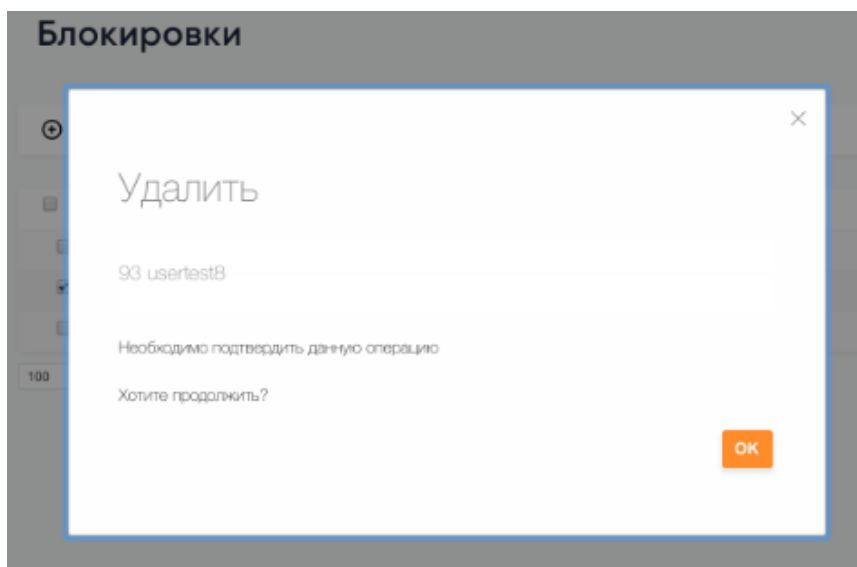


Рисунок 74 Окно удаления блокировки

## 2.8.5 Удаление УЗ

Для удаления УЗ нужно выбрать УЗ на вкладке «Пользователи» и нажать кнопку «Удалить», а затем подтвердить удаление, нажав «ОК» (см. Рисунок 75)

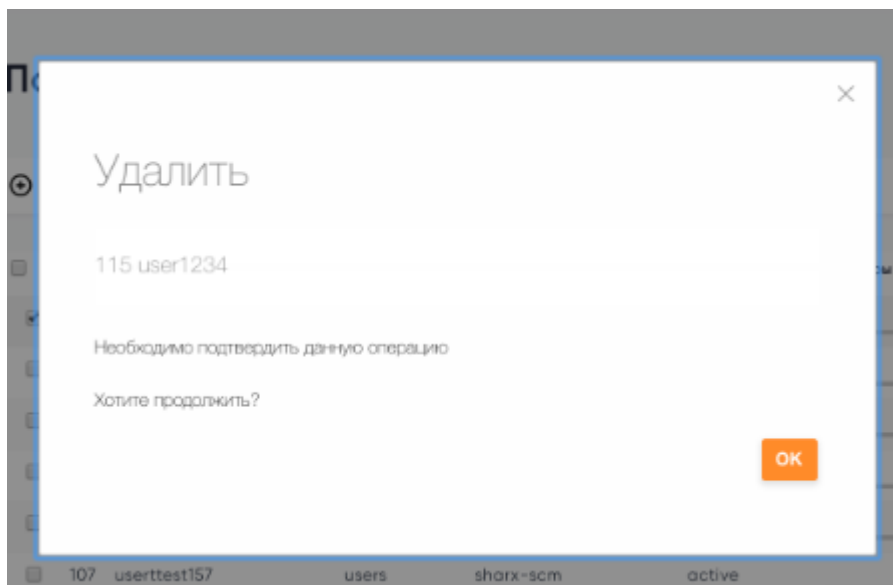


Рисунок 75 Удаление пользователя

После удаления учетной записи будет осуществлен переход на вкладку «Пользователи», где будет отмечено, что удалена УЗ с указанием ее ID и логина (см. Рисунок 76)



## Пользователи

Пароль Аутентификация Квоты Группы
👤 🔖 🗑️
Поиск

<input type="checkbox"/>	#	Наименование	Группа	Драйвер авторизации	Статус	Серверы	ОЗУ	ЦПУ
<input checked="" type="checkbox"/>	114	Test02	users	sharx-scm	deleted		0 / -	0KB / - 0 / -
<input type="checkbox"/>	111	Test01	users	sharx-scm	active		0 / -	0KB / - 0 / -
<input type="checkbox"/>	110	usertest20	users	sharx-scm	active		0 / -	0KB / - 0 / -
<input type="checkbox"/>	109	testuseradd	shcadmin	core	core		0 / -	0KB / - 0 / -
<input type="checkbox"/>	107	usertest157	users	sharx-scm	active		0 / -	0KB / - 0 / -
<input type="checkbox"/>	104	usertest14	users	sharx-scm	active		0 / -	0KB / - 0 / -
<input type="checkbox"/>	103	usertest13	users	sharx-scm	deleted		0 / -	0KB / - 0 / -
<input type="checkbox"/>	102	usertest12	users	sharx-scm	deleted		0 / -	0KB / - 0 / -
<input type="checkbox"/>	101	usertest11	users	sharx-scm	deleted		0 / -	0KB / - 0 / -
<input type="checkbox"/>	100	usertest9	users	sharx-scm	deleted		0 / -	0KB / - 0 / -
<input type="checkbox"/>	98	sly1admin	shcadmin	sharx-scm	active		0 / -	0KB / - 0 / -
<input type="checkbox"/>	97	usertest10	users	sharx-scm	deleted		0 / -	0KB / - 0 / -
<input type="checkbox"/>	96	sharx_user_test2	users	sharx-scm	active		0 / -	0KB / - 0 / -

Удален пользователь 114 Test02
 ✕

Рисунок 76 Уведомление об удалении пользователя

УЗ будет сохранена в БД с пометкой об удалении период времени, указанный в настройках. После истечения этого периода УЗ будет удалена окончательно, а логин можно будет использовать повторно. Просмотреть список удаленных УЗ можно, выбрав пункт меню «Удаленные УЗ». Откроется страница с перечнем удаленных УЗ, где будут отображены имя УЗ, дата удаления, а также дата, до которой информация об УЗ будет храниться в БД (см. Рисунок 77).

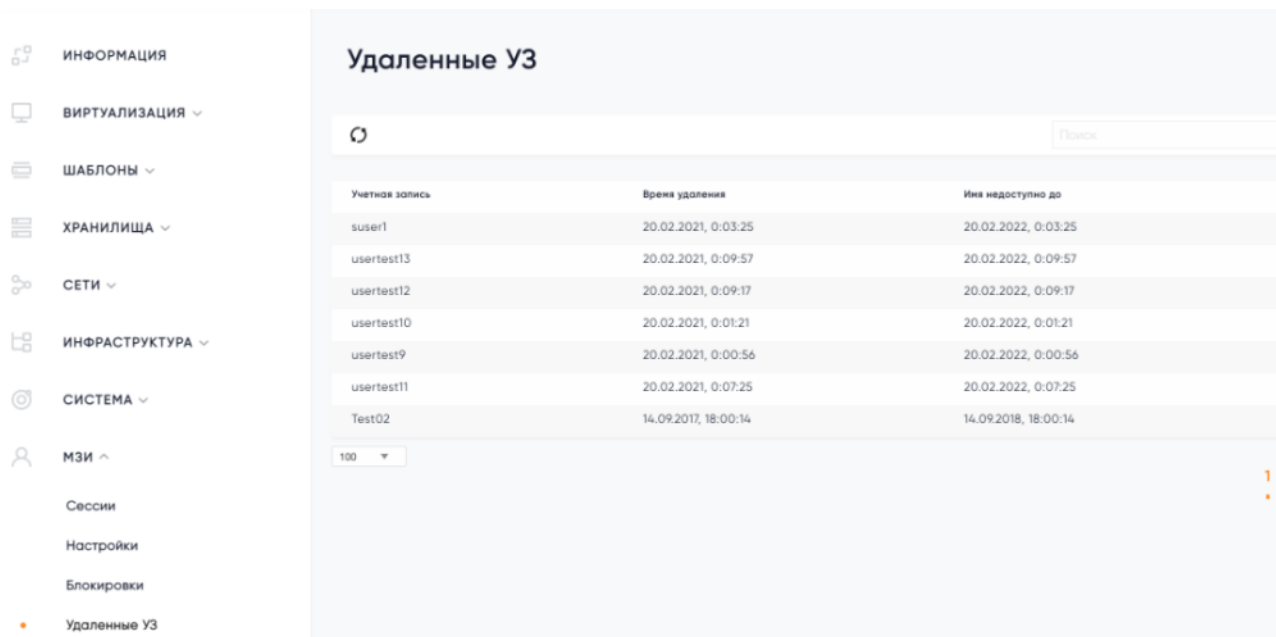


Рисунок 77 Список удаленных пользователей

## 2.8.6 Управление сессиями пользователей

Для работы с сессиями пользователей необходимо выбрать пункт меню «Сессии» (см. Рисунок 78)

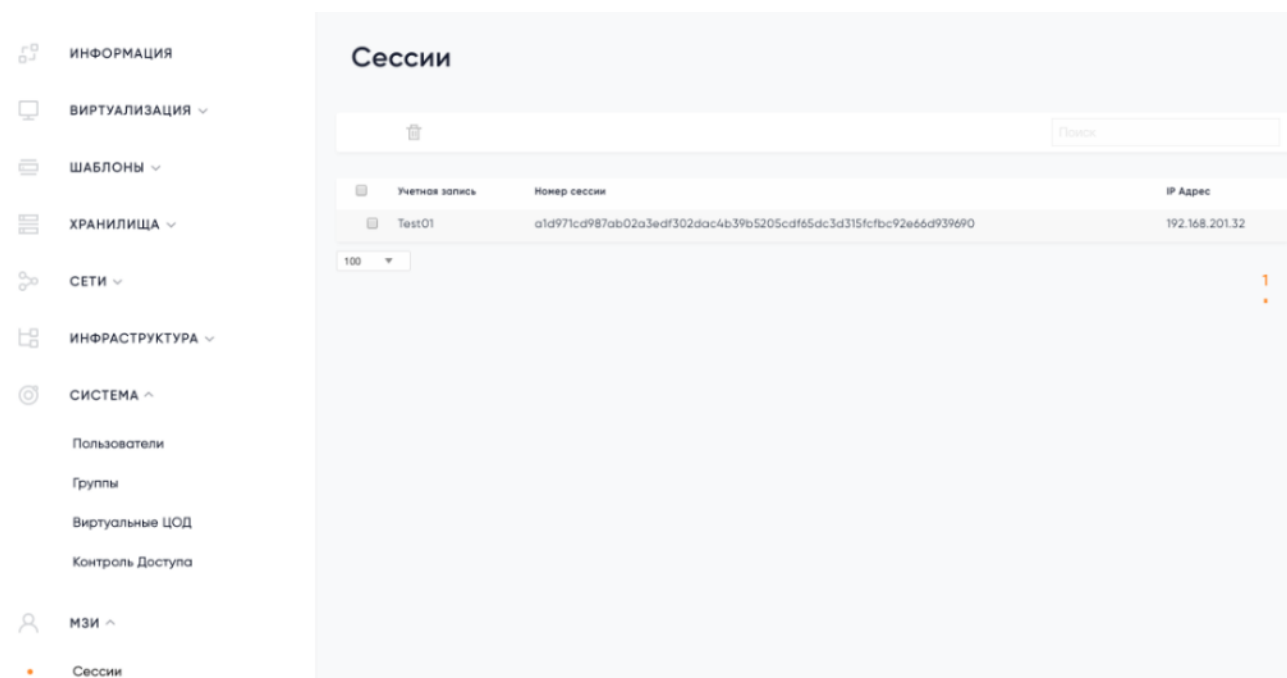


Рисунок 78 Список сессий

На странице отобразится список сессий субъектов доступа с указанием логина; номера сессии; ip-адреса узла, с которого была открыта сессия. Для того чтобы удалить сессию из списка нужно выбрать ее, и нажать кнопку «Удалить», а затем подтвердить удаление, нажав «ОК» (см. Рисунок 79).

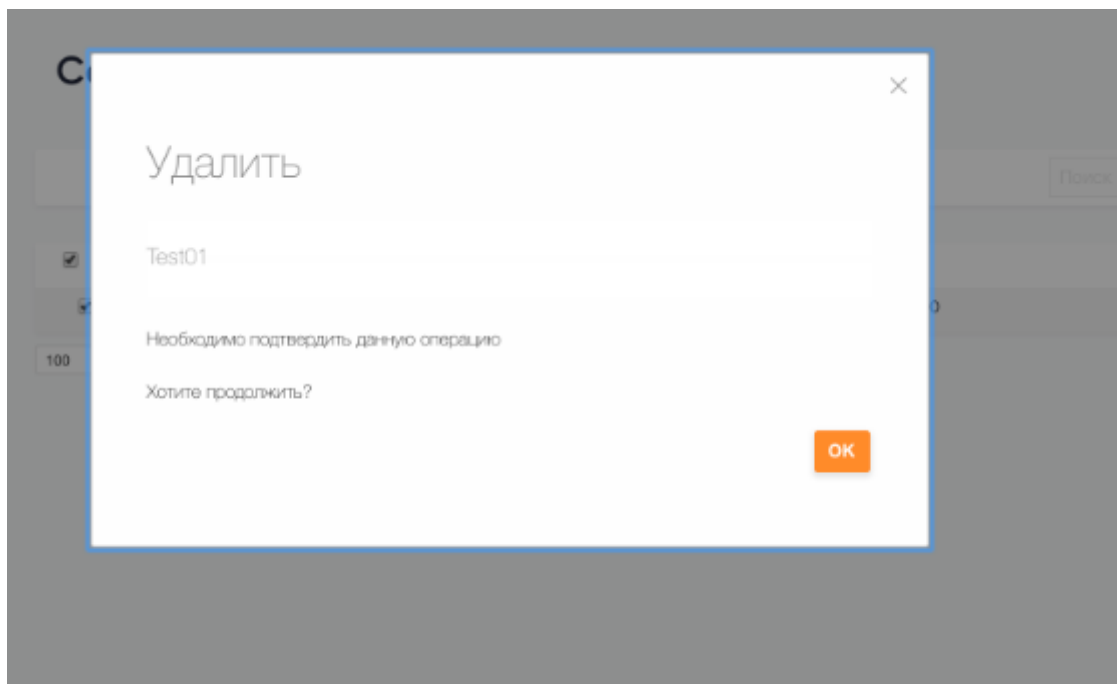


Рисунок 79 Окно удаления сессии

### 2.8.7 Регистрация и мониторинг событий

Для управления настройками журнала событий нужно перейти в пункт меню «Настройки» (см. Рисунок 80)

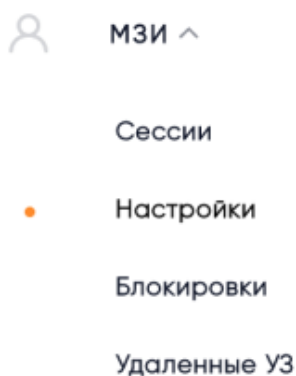


Рисунок 80 Настройка журнала событий

Настройки журнала выглядят следующим образом (см. Рисунок 81)

Журнал событий	
вход	true ▼
выход	true ▼
попытка доступа к страницам модуля	true ▼
создание пользователя	true ▼
автоблокировка пользователя	true ▼
обновление пользователя	true ▼
блокировка пользователя	true ▼
снятие блокировки с пользователя	true ▼
удаление пользователя	true ▼
обновление настроек	true ▼
добавление пользователя в группу	true ▼
удаление пользователя из группы	true ▼
изменение группы пользователя	true ▼

Рисунок 81 Список параметров журнала событий

Для каждого из событий можно проставить одно из следующих значений:

- true (логируются все случаи возникновения события);
- false (события данного типа не логируются вообще);
- success (логируются только успешные события данного типа);
- failure (логируются только неуспешные события данного типа).

Файлы, хранящие информацию о зарегистрированных событиях, хранятся в соответствующей системной директории: /var/log/one/ и совместимы с форматом хранения данных Syslog. Директория может быть изменена.

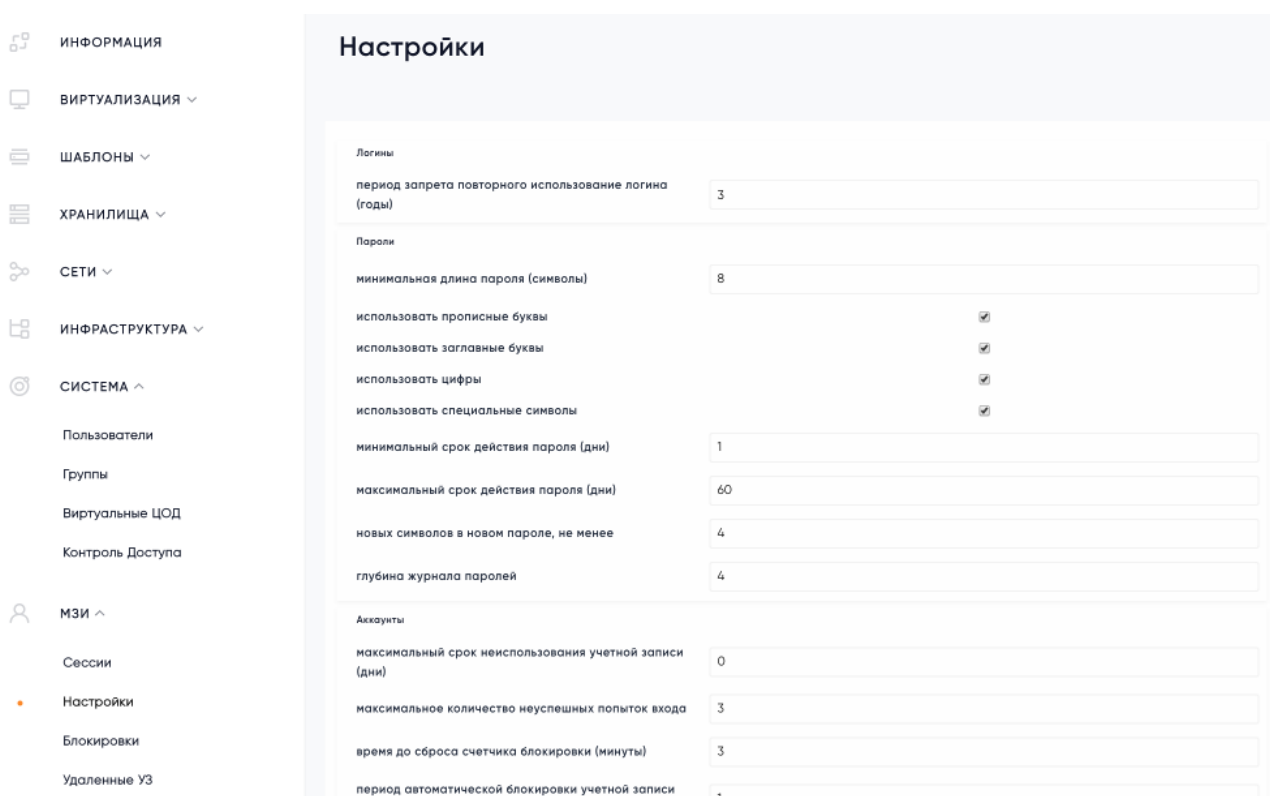
Модуль обеспечивает настройку вида хранения журнальной информации, так что можно выбрать каждый из данных видов и/или отдельные виды хранения информации:

- в системном журнале (Syslog);
- в файле.

Для сохранения настроек журнала нужно выбрать действие «Сохранить».

## 2.8.8 Администрирование параметров управления доступом

Для изменения настроек выбрать пункт меню «МЗИ/ Настройки». на странице отобразится форма «Настройки» (см. Рисунок 82).



Настройки	
<b>Логины</b>	
период запрета повторного использования логина (годы)	3
<b>Пароли</b>	
минимальная длина пароля (символы)	8
использовать прописные буквы	<input checked="" type="checkbox"/>
использовать заглавные буквы	<input checked="" type="checkbox"/>
использовать цифры	<input checked="" type="checkbox"/>
использовать специальные символы	<input checked="" type="checkbox"/>
минимальный срок действия пароля (дни)	1
максимальный срок действия пароля (дни)	60
новых символов в новом пароле, не менее	4
глубина журнала паролей	4
<b>Аккаунты</b>	
максимальный срок неиспользования учетной записи (дни)	0
максимальное количество неуспешных попыток входа	3
время до сброса счетчика блокировки (минуты)	3
период автоматической блокировки учетной записи	1

Рисунок 82 Меню настроек МЗИ

Можно установить характеристики для создаваемого логина, пароля, сессии и аккаунта, а также настроить характеристики журнала событий. Для установки параметров логина необходимо выбрать группу «Логины»

Параметр периода запрета повторного использования логина (в годах) – по умолчанию 3 года. Если установить значение «0», то УЗ будут удаляться сразу после того, как администратор подтвердит удаление УЗ. Логин, соответственно, также можно будет сразу же использовать повторно. Для редактирования параметров использования пароля УЗ нужно выбрать группу «Пароли» (см. Рисунок 83)

## Пароли

минимальная длина пароля (символы)	<input type="text" value="8"/>
использовать прописные буквы	<input checked="" type="checkbox"/>
использовать заглавные буквы	<input checked="" type="checkbox"/>
использовать цифры	<input checked="" type="checkbox"/>
использовать специальные символы	<input checked="" type="checkbox"/>
минимальный срок действия пароля (дни)	<input type="text" value="1"/>
максимальный срок действия пароля (дни)	<input type="text" value="60"/>
новых символов в новом пароле, не менее	<input type="text" value="4"/>
глубина журнала паролей	<input type="text" value="4"/>

Рисунок 83 Группа «Пароли»

Параметрами использования пароля УЗ являются:

- минимальная длина пароля (символы) – по умолчанию 8 символов;
- использование прописных букв – по умолчанию включено;
- использование заглавных букв – по умолчанию включено;
- использование специальных символов – по умолчанию включено;
- использование цифр – по умолчанию включено;
- минимальный срок действия пароля (дни) - по умолчанию 1 день;
- максимальный срок действия пароля (дни) - по умолчанию 60 дней;
- минимальное количество новых символов в новом пароле – по умолчанию не менее 4;
- глубина журнала паролей – по умолчанию 4.

Срок действия пароля - срок обновления паролей УЗ, по истечении которого пользователю будет предложено пройти процедуру обновления пароля. Если установить значение «0» для параметра «минимальный срок действия пароля (дни)», то проверка на минимальный срок действия пароля при его смене будет отключена. Значение «0» для параметра «максимальный срок действия пароля (дни)» отключает проверку на максимальный срок действия пароля при его смене.

Глубина журнала паролей – это проверка на ввод уже использовавшегося ранее пароля. При установке значения «0» для этого параметра проверка на наличие повторяющихся паролей будет отключена. Для сохранения изменений нужно выбрать действие «Сохранить». Для

редактирования параметров учетной записи необходимо выбрать группу полей «Аккаунты» (см. Рисунок 84)

Аккаунты	
максимальный срок неиспользования учетной записи (дни)	<input type="text" value="45"/>
максимальное количество неуспешных попыток входа	<input type="text" value="3"/>
время до сброса счетчика блокировки (минуты)	<input type="text" value="5"/>
период автоматической блокировки учетной записи (минуты)	<input type="text" value="60"/>

Рисунок 84 Группа «Аккаунты»

Данная группа настроек позволяет управлять следующими характеристиками:

- максимальный срок неиспользования учетной записи (в днях) – по умолчанию 45 дней;
- максимальное количество неуспешных попыток входа – количество попыток идентификации-аутентификации при входе в Систему, после которого УЗ временно блокируется, по умолчанию 3;
- время до сброса счетчика блокировки (в минутах) – по умолчанию 5 минут;
- период автоматической блокировки УЗ (в минутах) – по умолчанию 60 минут.

Значение «0» для параметра «максимальный срок неиспользования учетной записи (дни)» означает, что УЗ не будут блокироваться по истечению срока неактивности.

Значение «0» для параметра «период автоматической блокировки учетной записи (минуты)» означает, что при срабатывании счетчика блокировки на ввод неверного пароля УЗ будут блокироваться на неопределенный срок – без даты окончания периода блокировки. Для сохранения изменений нужно выбрать действие «Сохранить». Редактирование параметров сессии осуществляется с помощью группы полей «Сессии» (см. Рисунок 85)

Сессии	
максимальное число параллельных сессий	<input type="text" value="2"/>
максимальный период бездействия пользователя (минуты)	<input type="text" value="5"/>

Рисунок 85 Группа «Сессии»

Данная группа настроек позволяет управлять следующими характеристиками:

- максимальное число параллельных сессий – по умолчанию 2;
- максимальный период бездействия пользователя (в минутах) – период бездействия, после которого сессия будет закрыта, по умолчанию 5 минут.

Значение «0» для параметра «максимальное число параллельных сессий» означает, что количество параллельных сессий не ограничено.

Значение «0» для параметра «максимальный период бездействия пользователя (минуты)» означает, что сессия не будет прекращена при бездействии пользователя. Для сохранения изменений нужно выбрать действие «Сохранить».

## 2.9 Описание подсистемы обеспечения катастрофоустойчивости

Данная подсистема служит для создания копий виртуальных машин и их передачи в направлении от основного в резервный ЦОД (далее Кластер Источник – Кластер Назначения), для последующего запуска на мощностях Кластера Назначения, в случае выхода из строя Кластера Источника.

Подсистема определяет следующий перечень объектов в рамках ПАК SharxBase:

- Кластер источник – кластер физических узлов, обеспечивающий функционирование виртуальных машин. Данный кластер является инициатором репликации ВМ. Кластер источник может являться Кластером Назначения для одного или нескольких Кластеров Источников ПАК.
- Кластер назначения – данный кластер ПАК SharxBase является конечной точкой репликации/копирования снимка или снимков ВМ. Каждый кластер назначения может одновременно являться Кластером Источником.
- Группа репликации – логическая единица. Данная группа включает в себя одну или несколько виртуальных машин, для которых выполняется репликация. Для каждой группы могут быть указаны один или несколько Кластеров назначения, а также расписание, определяющее частоту репликации машин, входящих в данную группу.
- Виртуальные машины – виртуальные машины, которые могут быть добавлены в Группу репликации в рамках Кластера Источника.



## 2.9.1 Функции и работа с подсистемой

Взаимодействие пользователя с подсистемой обеспечения катастрофоустойчивости производится через веб-интерфейс, позволяющий выполнить следующие задачи:

- Настройку кластера или кластеров назначения:
  - Добавление;
  - Изменение;
  - Удаление;

Данная операция является зеркальной, так при определении кластера назначения на кластере источнике, кластер источник должен быть определен как кластер назначения на определяемом кластере.

Настройку групп репликации:

- Создание группы;
  - Определение имени группы;
  - Определение кластера назначения;
  - Настройку перечня ВМ в группе;
  - Настройку расписания репликации для группы;
  - Настройку ограничения использования ширины канала;
  - Настройку e-mail оповещения о успешности выполнения задач;
  - Изменение группы;
  - Изменение имени группы;
- Изменение кластера/кластеров назначения;
  - Изменение перечня ВМ в составе группы;
  - Изменение расписания репликации для группы;
- Удаление группы;
- Настройку сетевых интерфейсов ВМ в группах репликации:
  - Настройку ip адреса для каждого сетевого порта ВМ;
  - Настройку сети кластера назначения;
  - Настройку VLAN для каждого сетевого порта;

После добавления ВМ в группу репликации активируются поля, позволяющие выбрать VLAN и имя сети, в которых ВМ будет функционировать после восстановления на кластере назначения. Данные о VLAN и имени сети получены с кластера назначения автоматически.

- Принудительный запуск выполнения репликации для группы или групп репликации;

- Принудительный запуск процесса восстановления виртуальных машин в группе или группах репликации на кластере назначения;
- Визуальное отображения статуса выполнения репликации или восстановления для групп репликации;
- Принудительный запуск проверки доступности кластера назначения с кластера источника и наоборот;
- Визуальное отображение состояния доступности кластера назначения, для кластера источника.

## 2.9.2 Логика функционирования подсистемы:

- Осуществляется начальная настройка отношений кластеров:
  - На кластере источнике указывается кластер назначения;
  - На кластере и/или кластерах назначения указывается кластер источник;
  - Осуществляется проверка доступности кластеров в направлениях:
    - кластер источник – кластер назначения;
    - кластер назначения – кластер источник;
- Осуществляется настройка Групп репликации:
  - Определяется имя группы репликации;
  - Определяется кластер или кластеры назначения;
  - Осуществляется добавление ВМ в группу. ВМ в группе может быть от 1 до 10;
  - Осуществляется определение правил перенастройки сетевых интерфейсов для виртуальных машин в Группе репликации:
    - Осуществляется выбор виртуальной сети из списка;
    - При необходимости - определяется новый ip-адрес;
  - Осуществляется определение периодичности выполнения репликации:
    - Месяцы;
    - Недели;
    - Дни;
    - Часы;
    - Минуты, с гранулярностью в пять минут;
  - Осуществляется настройка e-mail адреса, для отправки оповещений о успешности выполнения репликации;

- Для вновь созданной группы репликации могут быть осуществлены следующие действия:
  - Настройка:
    - Изменение имени группы;
    - Изменение списка кластеров назначения;
    - Изменение состава ВМ в группе, а также правил перенастройки сетевых интерфейсов;
  - Удаление;
  - Ручная инициация запуска репликации для групп, посредством нажатия кнопки “Выполнить сейчас”;
- Для ВМ в группах Репликации, по расписанию или в ручном режиме, осуществляется репликация между кластером источником и кластером назначения. Осуществляется:
  - Выполнение единовременного снимка для всех ВМ в группе;
  - На уровне распределенного хранилища – осуществляется передача снимков ВМ;
  - На уровне Подсистемы – осуществляется сбор метаданных о ВМ и передача этой информации экземпляру Подсистемы на кластере назначения;
- На кластере источнике и кластере назначения отображается информация о статусе выполнения репликации, успешности выполнения предыдущих шагов и расписания выполнения репликации;
- На кластере назначения отображается информация о переданных в рамках репликации Группам и ВМ в них – далее Локальные копии;
- Локальные копии могут быть принудительно восстановлены, посредством нажатия кнопки “Восстановить”;
- Для переданных Групп репликации и ВМ в них могут быть осуществлены следующие действия:
  - Восстановление Группы и ВМ в ее составе;
  - Удаление Группы и ВМ в ее составе;
- На кластере назначения может быть сформирован план восстановления, в данный план могут быть включены переданные Группы репликации и копии ВМ в их составе.
- Для Групп репликации добавленных в план восстановления могут быть настроены следующие параметры:
  - Последовательность восстановления;
  - Таймаут после восстановления;

– Группа может быть удалена из плана;

## 2.10 Мониторинг из внешних систем

### 2.10.1 SharxBase SNMP traps

Для визуализации параметров различных компонентов в платформе SharXbase задействованы различные тесты оборудования, результаты которых, кроме внутреннего отображения в платформе можно переслать во внешние системы через SNMP trap.

В системе работает специальный демон, который следит за состоянием параметров и выполняет отправку сообщений при достижении пограничных значений, описанных в правилах. Демон работает только на VIP ноде и шлет сообщения от адреса VIP платформы. Информация внутри ALERT сообщения содержит данные о: ноде (имя хоста), уровне критичности (critical, major, minor) и о причине срабатывания (см. Рисунок 86 и Рисунок 87).

Description	Source	Time	Severity
.1.3.6.1.4.1.51279.1.1.0	10.1.128.101	2019-04-26 11:59:15	
.1.3.6.1.4.1.51279.1.1.0	10.1.128.101	2019-04-26 11:57:15	

---

**Source:** 10.1.128.101      **Timestamp:** 39 hours 12 minutes 56 seconds      **SNMP Version:** 2  
**Trap OID:** .1.3.6.1.4.1.51279.1.1.0      **Community:** public  
**Variable Bindings:**

---

**Name:** .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0  
**Value:** [TimeTicks] 39 hours 12 minutes 56 seconds (14117600)

---

**Name:** snmpTrapOID  
**Value:** [OID] .1.3.6.1.4.1.51279.1.1.0

---

**Name:** .1.3.6.1.4.1.51279.1.1.0.1  
**Value:** [OctetString] 1.3.6.1.4.1.51279.1.1.0[alertname=webui\_server\_inactive,instance=JKE974600024-20,service=sd-webui]

---

**Name:** .1.3.6.1.4.1.51279.1.1.0.2  
**Value:** [OctetString] major

---

**Name:** .1.3.6.1.4.1.51279.1.1.0.3  
**Value:** [OctetString] Status: major - Alert: webui\_server\_inactive Summary: Sharx cloud WebUI service is inactive JKE974600024-20 Description: Sharx cloud WebUI service is inactive

---

**Description:**

Рисунок 86 SNMP сообщение о падении веб-интерфейса платформы

Description	Source	Time	Severity
1.3.6.1.4.1.51279.1.1.0	10.1.128.101	2019-04-26 11:59:15	
1.3.6.1.4.1.51279.1.1.0	10.1.128.101	2019-04-26 11:57:15	

<b>Source:</b>	10.1.128.101	<b>Timestamp:</b>	39 hours 14 minutes 56 seconds	<b>SNMP Version:</b>	2
<b>Trap OID:</b>	.1.3.6.1.4.1.51279.1.1.0	<b>Community:</b>	public		
<b>Variable Bindings:</b>					
<b>Name:</b>	.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0				
<b>Value:</b>	[TimeTicks] 39 hours 14 minutes 56 seconds (14129600)				
<b>Name:</b>	snmpTrapOID				
<b>Value:</b>	[OID] .1.3.6.1.4.1.51279.1.1.0				
<b>Name:</b>	.1.3.6.1.4.1.51279.1.1.0.1				
<b>Value:</b>	[OctetString] 1.3.6.1.4.1.51279.1.1.0[alertname=webui_server_inactive,instance=JKE974600024-20,service=sdc-webui]				
<b>Name:</b>	.1.3.6.1.4.1.51279.1.1.0.2				
<b>Value:</b>	[OctetString] info				
<b>Name:</b>	.1.3.6.1.4.1.51279.1.1.0.3				
<b>Value:</b>	[OctetString] Status: OK				
<b>Description:</b>					

Рисунок 87 SNMP сообщение о восстановлении веб-интерфейса платформы

Таблица 18 Список алертов

service	severity	description
sdcl-cloud	critical	Sharx cloud core daemon failed
sdcl-coud	critical	Sharx cloud core daemon is inactive
sdcl-scheduler	critical	Sharx cloud scheduler daemon failed
sdcl-scheduler	critical	Sharx cloud scheduler daemon is inactive
sdcl-webui	critical	Sharx cloud WebUI service failed
sdcl-webui	critical	Sharx cloud WebUI service is inactive
sdcl-novnc	critical	Sharx novnc service failed
sdcl-novnc	critical	Sharx novnc service is inactive
sdcl-gate	major	Sharx gate service failed
sdcl-gate	major	Sharx gate service is inactive
sdcl-flow	major	Sharx flow service failed
sdcl-flow	major	Sharx flow service is inactive
sdcl-sds-server	critical	Sharx SDS server service failed
sdcl-sds-server	critical	Sharx SDS server service is inactive
sdcl-sds-server_1	critical	Sharx SDS server service failed
sdcl-sds-server_1	critical	Sharx SDS server service is inactive
sdcl-sds-server_2	critical	Sharx SDS server service failed
sdcl-sds-server_2	critical	Sharx SDS server service is inactive
sdcl-sds-block	critical	Sharx SDS block service failed
sdcl-sds-block	critical	Sharx SDS block service is inactive
sdcl-sds-mgmt	critical	Sharx SDS mgmt service failed
sdcl-sds-mgmt	critical	Sharx SDS mgmt service is inactive
sdcl-sds-beacon	critical	Sharx SDS beacon service failed
sdcl-sds-beacon	critical	Sharx SDS beacon service is inactive
sdcl-sds-cgmove	critical	Sharx SDS cgmove service failed

service	severity	description
sdcsds-cgmove	critical	Sharx SDS cgmove service is inactive
sdcsds-controller	critical	Sharx SDS controller service failed
sdcsds-controller	critical	Sharx SDS controller service is inactive
sdcsds-kdump	major	Sharx SDS kdump service failed
sdcsds-kdump	major	Sharx SDS kdump service is inactive
sdcsds-reaffirm	major	Sharx SDS reaffirm service failed
sdcsds-reaffirm	major	Sharx SDS reaffirm service is inactive
sdcsds-slice	major	Sharx SDS slice service failed
sdcsds-slice	major	Sharx SDS slice service is inactive
mysql	major	mysql service failed
mysql	major	mysql service is inactive
sdcsvirt-submodule	major	sdcsvirt-submodule service failed
sdcsvirt-submodule	major	sdcsvirt-submodule service is inactive
nginx	major	nginx service failed
nginx	major	nginx service is inactive
cassandra	major	cassandra service failed
cassandra	major	cassandra service is inactive
sdcmetric	major	sdcmetric service failed
sdcmetric	major	sdcmetric service is inactive
sdchost-metric	major	sdchost-metric service failed
sdchost-metric	major	sdchost-metric service is inactive
chronyd	major	chronyd service failed
chronyd	major	chronyd service is inactive
smartd	major	smartd service failed
smartd	major	smartd service is inactive
root filesystem	major	85% usage threshold reached
root filesystem	critical	95% usage threshold reached
var filesystem	major	85% usage threshold reached
var filesystem	critical	95% usage threshold reached
datastores/0 filesystem	major	85% usage threshold reached
datastores/0 filesystem	critical	95% usage threshold reached
datastores/1 filesystem	major	85% usage threshold reached
datastores/1 filesystem	critical	95% usage threshold reached
datastores/2 filesystem	major	85% usage threshold reached
datastores/2 filesystem	critical	95% usage threshold reached
/var/tmp/upload filesystem	major	85% usage threshold reached
/var/tmp/upload filesystem	critical	95% usage threshold reached

## 2.10.2 Интерфейс управления и мониторинга IPMI

Платформа SharXbase может работать на серверах различных производителей, одним из рекомендованных вендоров является: Intel.

Intel использует в своих платформах контроллер управления основной платой (BMC) для удаленного мониторинга и управления. Этот контроллер использует IPMI - интеллектуальный интерфейс управления платформой, предназначенный для автономного мониторинга и управления функциями, встроенными непосредственно в аппаратное и микропрограммное обеспечения серверных платформ.

Ключевые характеристики IPMI — мониторинг, восстановление функций управления, журналирование и инвентаризация, которые доступны независимо от процессора, BIOS'a и операционной системы. Функции управления платформой могут быть доступны, даже если система находится в выключенном состоянии.

Сам контроллер BMC предоставляет веб-интерфейс для мониторинга и управления платформой. Через веб-интерфейс в меню “Server Health” -> “Sensor Readings” можно получить информацию о состоянии сенсоров (см. Рисунок 88).

#### Sensor Readings

This page displays system sensor information, including readings and status. You can toggle viewing the thresholds for the sensors by pressing the Show Thresholds button below.

Refreshing readings every 60 seconds

Select a sensor type category:

Sensor Readings: 78 sensors

Name	Status	Health	Reading	Low CT	Low NC	High NC	High CT
Pwr Unit Status	All deasserted	OK	0x0000	N/A	N/A	N/A	N/A
Pwr Unit Redund	reports full redundancy has been regained	OK	0x0001	N/A	N/A	N/A	N/A
IPMI Watchdog	All deasserted	OK	0x0000	N/A	N/A	N/A	N/A
Physical Scrty	All deasserted	OK	0x0000	N/A	N/A	N/A	N/A
SMI Timeout	All deasserted	OK	0x0000	N/A	N/A	N/A	N/A
System Event Log	All deasserted	OK	0x0000	N/A	N/A	N/A	N/A
System Event	All deasserted	OK	0x0000	N/A	N/A	N/A	N/A
Button	All deasserted	OK	0x0000	N/A	N/A	N/A	N/A
BMC Watchdog	All deasserted	OK	0x0000	N/A	N/A	N/A	N/A
VR Watchdog	All deasserted	OK	0x0000	N/A	N/A	N/A	N/A
SSB Therm Trip	All deasserted	OK	0x0000	N/A	N/A	N/A	N/A
IO Mod Presence	reports the device has been inserted or is present	OK	0x0002	N/A	N/A	N/A	N/A
BMC FW Health	All deasserted	OK	0x0000	N/A	N/A	N/A	N/A
System Airflow	Normal	OK	14 CFM	N/A	N/A	N/A	N/A
BB CPU2 VR Temp	Normal	OK	24 degrees C	5 degrees C	10 degrees C	110 degrees C	115 degrees C
BB Inlet Temp	Normal	OK	23 degrees C	5 degrees C	10 degrees C	60 degrees C	65 degrees C
HSBP Temp	Normal	OK	17 degrees C	0 degrees C	5 degrees C	50 degrees C	55 degrees C
SSB Temp	Normal	OK	46 degrees C	2 degrees C	5 degrees C	98 degrees C	103 degrees C
BB BMC Temp	Normal	OK	39 degrees C	5 degrees C	10 degrees C	85 degrees C	90 degrees C
BB CPU1 VR Temp	Normal	OK	33 degrees C	5 degrees C	10 degrees C	110 degrees C	115 degrees C
BB REAR Temp	Normal	OK	37 degrees C	5 degrees C	10 degrees C	110 degrees C	115 degrees C
IO Mod Temp	Normal	OK	33 degrees C	2 degrees C	5 degrees C	75 degrees C	80 degrees C
HSBP PSOC Temp	Normal	OK	21 degrees C	0 degrees C	5 degrees C	105 degrees C	110 degrees C

Рисунок 88 Состояние сенсоров контроллера BMC

Контроллер фиксирует события, которые происходят с системой: включение, выключение, срабатывание триггеров по пограничным значениям (thresholds). Список событий доступен через веб-интерфейс в меню “Server Health” -> “Event Log” (см. Рисунок 89).

### Event Log

Below is a table of the events from the system's event log. You can choose a category from the pull-down box to filter the events, and also sort them by clicking on a column header.

Select an event log category:

**Event Log: 437 event entries**  
**Event Log is 12% full.**

Event ID	Time Stamp	Sensor Name	Sensor Type	Description
437	03/27/2019 04:38:50	Pwr Unit Redund	Power Unit	reports full redundancy has been regained - Asserted
436	03/27/2019 04:38:48	Pwr Unit Redund	Power Unit	reports the unit is still functioning with the minimum amount of resources needed for normal operation - Deasserted
435	03/27/2019 04:38:48	Pwr Unit Redund	Power Unit	reports redundancy has been lost - Deasserted
434	03/27/2019 04:38:47	PS1 Status	Power Supply	reports the power supply's input (AC/DC) has been lost - Deasserted
433	03/27/2019 04:38:45	SmaRT - CLST	OEM Reserved	transition to OK from external device. reports it has been deasserted. - Asserted
432	03/27/2019 04:38:41	PS1 Status	Power Supply	reports the power supply's input (AC/DC) has been lost - Asserted
431	03/27/2019 04:38:41	PS1 Status	Power Supply	reports a predictive failure has been detected for the power supply - Deasserted
430	03/27/2019 04:38:41	Pwr Unit Redund	Power Unit	reports the unit is still functioning with the minimum amount of resources needed for normal operation - Asserted
429	03/27/2019 04:38:41	Pwr Unit Redund	Power Unit	reports redundancy has been lost - Asserted

Рисунок 89 Event Log контроллера BMC

Рекомендуется собирать для мониторинга информацию о состоянии оборудования именно из IPMI, чтобы не зависеть от работоспособности операционной системы.

Для отправки событий мониторинга во внешние системы, нужно настроить оповещения в меню «Configuration» -> «Alerts» (см. Рисунок 90). В окне конфигурации нужно выбрать все, либо выбранные триггеры и указать IP адрес коллектора сбора оповещений. В интерфейсе доступно два IP адреса для сбора сообщений.

### Alerts

Configure which system events generate Alerts and the external network destinations they should be sent to.

**Globally Enable Platform Event Filtering:**  Enabled  Disabled

**Log Event on Filter Action:**  Enabled  Disabled

**Selected events will trigger action:**

<input type="checkbox"/> Temperature Sensor Out of Range	<input type="checkbox"/> Watchdog Timer
<input type="checkbox"/> System Restart	<input type="checkbox"/> Voltage Sensor Out of Range
<input type="checkbox"/> Fan Failure	<input type="checkbox"/> Chassis Intrusion
<input type="checkbox"/> Power Supply Failure	<input type="checkbox"/> Memory Error
<input type="checkbox"/> BIOS: Post Error Code	<input type="checkbox"/> FRB Failure
<input type="checkbox"/> Node Manager Exception	<input type="checkbox"/> Hard Drive Failure

**LAN Channel to Configure:**

**Alert Destination #1:**

SNMP Send SNMP Alerts to IP:

Email Send Email to:

**Alert Destination #2:**

SNMP Send SNMP Alerts to IP:

Email Send Email to:

Рисунок 90 Настройка оповещений в контроллере BMC

Список трапов подробно перечислен в MIB файле, который можно скачать вместе с пакетом обновления прошивки по ссылке:

<https://downloadcenter.intel.com/en/download/28697/-Intel-S2600TP-EFI>



Файл MIB содержит в текстовом формате описание всех трапов, а также может быть загружен во внешние системы мониторинга или коллекторы для распознавания событий.

Последняя версия файла на момент написания документации: ВМС-MIB.mib